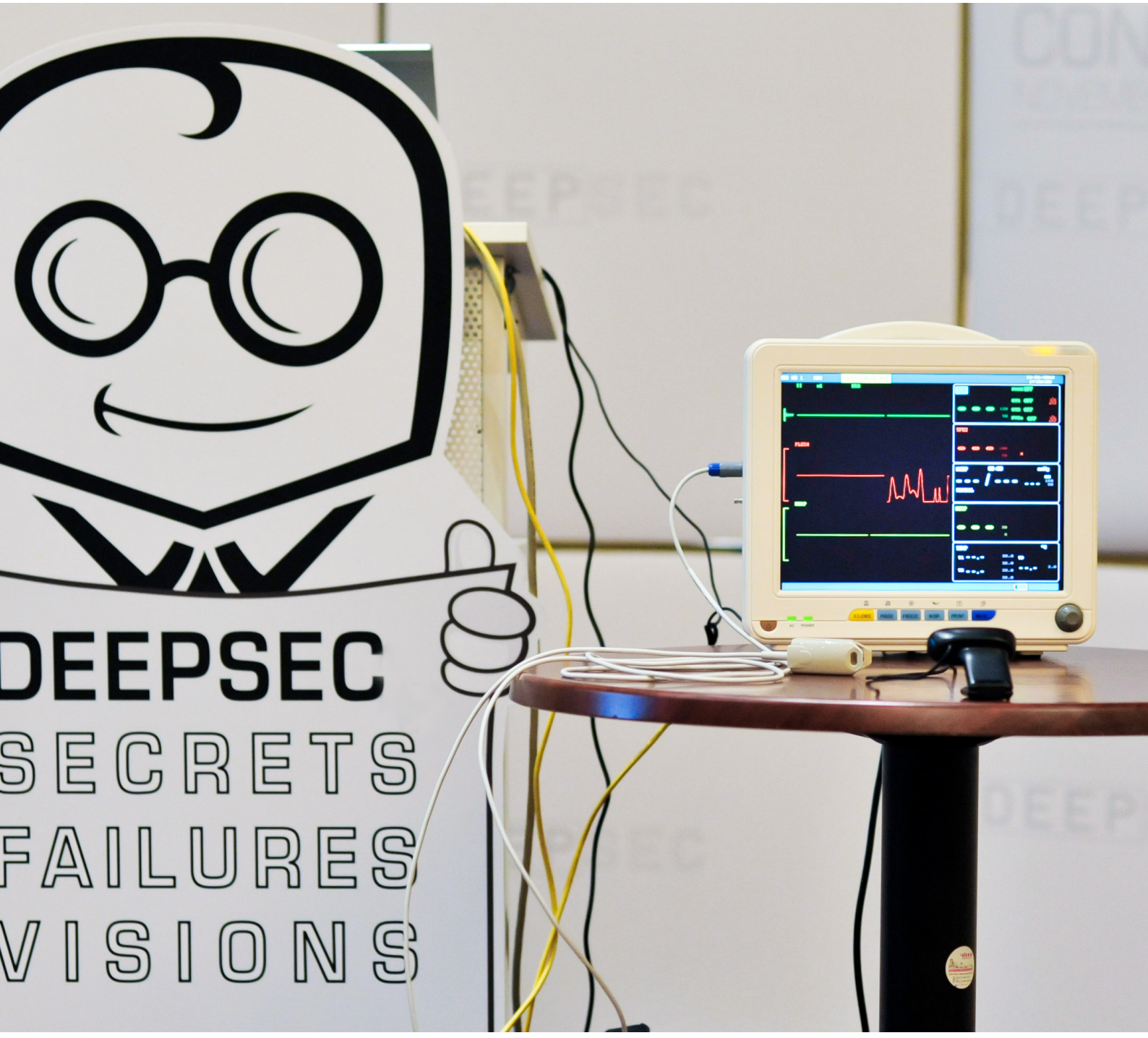
DeepSec



Press review

media coverage 2012-1015

contents

private blogs, personal experiences

press release

contents

http://www.golem.de/news/aslr-speicherrandomisierung-unter-linux-mangelhaft-1412-111010.html

ASLR

Speicher-Randomisierung unter Linux mangelhaft

Datum: 8.12.2014, 16:00

Autor: Hanno Böck

Die Randomisierung des Speicherlayouts (ASLR) gilt als wichtige Maßnahme, um die Ausnutzung von Sicherheitslücken zu erschweren. Unter Linux hat das Konzept Mängel, aber viel gravierender ist, dass vielfach ASLR überhaupt nicht eingesetzt wird.Zu den häufigsten Sicherheitslücken gehören Fehler in der Speicherverwaltung von C-Programmen, beispielsweise klassische Buffer Overflows. Moderne Betriebssysteme haben inzwischen eine Reihe von Schutzmaßnahmen implementiert, um die Ausnutzung von solchen Fehlern zu erschweren. Eine Möglichkeit ist die sogenannte Address Space Layout Randomisation (ASLR).

Eine Strategie zur Ausnutzung von Sicherheitslücken ist es häufig, das System des Opfers dazu zu bringen, an eine bestimmte Stelle im Speicher zu springen und dort Code auszuführen. Damit derartige Angriffe jedoch funktionieren, muss der Angreifer wissen, an welchen Speicheradressen sich was befindet. Hier setzt ASLR an: Durch die zufällige Verteilung von Code, Heap und Stack im Speicher werden solche Angriffe enorm erschwert. ASLR ist nicht perfekt. Durch die Nutzung von weiteren Lücken kann ein Angreifer Speicheradressen erfahren, das sogenannte Heap Spraying setzt darauf, bösartigen Code möglichst oft im Speicher zu wiederholen, so dass bei einem zufälligen Sprung die Chance besteht, den entsprechenden Code zu erreichen. Doch auch wenn ASLR nicht alle Angriffe verhindert, gilt es als wichtiger Baustein moderner Sicherheitskonzepte.

Linux war Pionier in Sachen ASLR

Linux war eigentlich einst Pionier in Sachen Speicherrandomisierung. Das PaX-Projekt hatte bereits 2002 mittels eines Kernel-Patches die Möglichkeit von ASLR eingeführt. Ein Jahr später führte OpenBSD als erstes Betriebssystem ASLR als Standardfunktion ein. PaX existiert noch heute und ist Teil des Grsecurity-Projekts, das einen Kernel-Patch mit zahlreichen zusätzlichen Sicherheitsfunktionen für den Linux-Kernel bereitstellt. Doch PaX wurde nie Teil des offiziellen Linux-Kernels. Mit der Version 2.6.12 führte Linux eine eigene Implementierung von ASLR ein. Doch das Problem dabei: In vielen Fällen greift diese überhaupt nicht. Während unter Windows, Mac OS X, Android und iOS ASLR inzwischen Standard ist, wird es unter Linux nach wie vor nur mangelhaft genutzt.

Der Hintergrund ist, dass nicht jedes Programm automatisch an beliebige Speicherbereiche geladen werden kann. Klassischerweise können Sprungbefehle in Software auf feste Adressen verweisen. Damit der Code an beliebige Speicherbereiche geladen werden kann, muss dies bereits bei der Kompilierung berücksichtigt werden. Der gcc-Compiler bietet hierfür die Option -fpic (pic steht für “Position Independent Code”), für den Linker muss die Option -pie (für “Position Independent Executable”) angegeben werden. Und genau hier hapert es: Alle großen Distributionen nutzen standardmäßig noch Programme, die nicht mit den entsprechenden Optionen für positionsunabhängigen Code kompiliert wurden.

Geringe Auswirkungen auf die Leistungen

Die Nutzung von positionsunabhängigem Code hat Auswirkungen auf die Performance. Insbesondere auf alten PC-Systemen mit 32 Bit ist das ein Problem, denn hier ist die Zahl der Prozessorregister knapp und für den positionsunabhängigen Code wird ein zusätzliches Register benötigt. Auf 64-Bit-Systemen sind die Performanceeinbußen hingegen sehr gering. Bei einem Test von uns mit der Codierung eines Videos mit dem Programm ffmpeg betrug der Unterschied etwa 1,5 Prozent. Es gibt Patches für den gcc-Compiler und Binutils, welche die Leistungseinbußen noch weiter reduzieren und die in den kommenden Versionen der entsprechenden Tools enthalten sein werden.Auch ohne positionsunabhängigen Code ist die Adressrandomisierung nicht völlig nutzlos. Der Stack- und der Heap-Speicher landen trotzdem an zufälligen Adressen und Bibliotheken werden generell mit positionsunabhängigem Code kompiliert. Aber für einen wirklichen Schutz reicht das nicht. Insbesondere um vor sogenannten Return-Oriented-Programming-Angriffen zu schützen, ist eine Randomisierung des eigentlichen Programmcodes wichtig.

Firefox hat ASLR nach Problemen wieder deaktiviert

Mozilla hatte vor kurzem versucht, Firefox für Linux mit den entsprechenden Optionen zu kompilieren. Dabei trat ein unerwartetes Problem auf: Der GNOME-Dateimanager Nautilus erkannte die entsprechend kompilierten ausführbaren Dateien nicht als solche und Firefox ließ sich über den Dateimanager nicht starten. Firefox schaltete daraufhin die entsprechende Funktion wieder ab.

Der Grund für die Nautilus-Probleme, die bei einem Test von Golem.de unter dem KDE-Dateimanager Dolphin in genau derselben Form auftraten: Der Dateimanager greift zur Erkennung von ausführbaren Dateien auf die Bibliothek libmagic zurück, die Teil des Tools file ist. Die libmagic-Bilbiothek wiederum kann positionsunabhängige Linux-Binaries nicht von Bibliotheken unterscheiden und liefert den MIME-Type für Bibliotheken zurück. Sowohl Binaries als auch Bibliotheken verwenden unter Linux das Elf-Dateiformat.

Chrome wird standardmäßig mit Adressrandomisierung ausgeliefert, ebenso der auf Firefox basierende Tor-Browser. Anders als Mozilla liefern diese beiden Browser ein Shellskript zum Starten mit, sie sind somit von dem Problem in den Dateimanagern nicht betroffen.

In Linux-Distributionen kein Standard

Bei den Linux-Distributionen ist die Situation in Sachen ASLR sehr gemischt. Fedora und Debian aktivieren das Feature nur für einzelne Tools, die als besonders sicherheitskritisch gelten. Gleiches gilt auch für andere auf Debian basierende Distributionen wie Ubuntu. Selbst Tails, ein auf Datenschutzeinstellungen und Sicherheit getrimmtes Linux-System, nutzt ASLR nicht standardmäßig. Es gibt auch immer wieder generelle Probleme mit der ASLR-Implementierung von Linux. Mitglieder von Google's Projekt Zero entdeckten beim Versuch, eine Glibc-Sicherheitslücke auszunutzen, dass man zumindest unter 32-Bit-Systemen die Speicherrandomisierung von Suid-Binaries mit Hilfe des Befehls ulimit weitgehend deaktivieren kann.

offset2lib-Schwäche entdeckt

Zuletzt hatten die Sicherheitsforscher Hector Marco-Gisbert und Ismael Ripoll auf der Deepsec-Konferenz in Wien eine ausführliche Analyse des ASLR-Konzepts von Linux vorgestellt und ein weiteres Problem entdeckt, das sie offset2lib getauft haben: Linux legt zwar den Programmcode an einer zufälligen Stelle im Speicher ab, aber der Hauptprogrammcode und der Code von nachgeladenen Bibliotheken wird immer im selben Abstand abgelegt. Das bedeutet, dass ein Angreifer, der im Hauptprogramm aufgrund eines Fehlers möglicherweise Kenntnis von einer Speicheradresse erlangt, damit eine Sicherheitslücke in einer Bibliothek ausnutzen kann.

Android ist von der offset2lib-Schwäche ebenfalls betroffen. Anders als unter gängigen Linux-Distributionen kommt unter Android in aller Regel auch Adressrandomisierung zum Einsatz. Nicht betroffen sind Linux-Systeme, die Pax benutzen. Die Forscher haben einen Patch vorgelegt, der zur Zeit auf der Kernel-Mailingliste diskutiert wird.

Solange die meisten Linux-Distributionen aber keine Dateien mit positionsunabhängigem Code ausliefern, hilft das alles nicht viel. Die Distributionen sollten hier dringend handeln und die Speicherrandomisierung mittels ASLR auch unter Linux zum Standard machen.

ASLR

Speicher-Randomisierung unter Linux mangelhaft

Die Randomisierung des Speicherlayouts (ASLR) gilt als wichtige Maßnahme, um die Ausnutzung von Sicherheitslücken zu erschweren. Unter Linux hat das Konzept Mängel, aber viel gravierender ist, dass vielfach ASLR überhaupt nicht eingesetzt wird.

Zu den häufigsten Sicherheitslücken gehören Fehler in der Speicherverwaltung von C-Programmen, beispielsweise klassische Buffer Overflows. Moderne Betriebssysteme haben inzwischen eine Reihe von Schutzmaßnahmen implementiert, um die Ausnutzung von solchen Fehlern zu erschweren. Eine Möglichkeit ist die sogenannte Address Space Layout Randomisation (ASLR).

Eine Strategie zur Ausnutzung von Sicherheitslücken ist es häufig, das System des Opfers dazu zu bringen, an eine bestimmte Stelle im Speicher zu springen und dort Code auszuführen. Damit derartige Angriffe jedoch funktionieren, muss der Angreifer wissen, an welchen Speicheradressen sich was befindet. Hier setzt ASLR an: Durch die zufällige Verteilung von Code, Heap und Stack im Speicher werden solche Angriffe enorm erschwert. ASLR ist nicht perfekt. Durch die Nutzung von weiteren Lücken kann ein Angreifer Speicheradressen erfahren, das sogenannte Heap Spraying setzt darauf, bösartigen Code möglichst oft im Speicher zu wiederholen, so dass bei einem zufälligen Sprung die Chance besteht, den entsprechenden Code zu erreichen. Doch auch wenn ASLR nicht alle Angriffe verhindert, gilt es als wichtiger Baustein moderner Sicherheitskonzepte.

Linux war Pionier in Sachen ASLR

Linux war eigentlich einst Pionier in Sachen Speicherrandomisierung. Das PaX-Projekt hatte bereits 2002 mittels eines Kernel-Patches die Möglichkeit von ASLR eingeführt. Ein Jahr später führte OpenBSD als erstes Betriebssystem ASLR als Standardfunktion ein. PaX existiert noch heute und ist Teil des Grsecurity-Projekts, das einen Kernel-Patch mit zahlreichen zusätzlichen Sicherheitsfunktionen für den Linux-Kernel bereitstellt. Doch PaX wurde nie Teil des offiziellen Linux-Kernels. Mit der Version 2.6.12 führte Linux eine eigene Implementierung von ASLR ein. Doch das Problem dabei: In vielen Fällen greift diese überhaupt nicht. Während unter Windows, Mac OS X, Android und iOS ASLR inzwischen Standard ist, wird es unter Linux nach wie vor nur mangelhaft genutzt.

Der Hintergrund ist, dass nicht jedes Programm automatisch an beliebige Speicherbereiche geladen werden kann. Klassischerweise können Sprungbefehle in Software auf feste Adressen verweisen. Damit der Code an beliebige Speicherbereiche geladen werden kann, muss dies bereits bei der Kompilierung berücksichtigt werden. Der gcc-Compiler bietet hierfür die Option -fpic (pic steht für "Position Independent Code"), für den Linker muss die Option -pie (für "Position Independent Executable") angegeben werden. Und genau hier hapert es: Alle großen Distributionen nutzen standardmäßig noch Programme, die nicht mit den entsprechenden Optionen für positionsunabhängigen Code kompiliert wurden.

PaX liefert eine deutlich bessere Speicherrandomisierung als der Standard-Linux-Kernel. (Bild: PaX)

Artikel: ASLR Speicher-Randomisierung unter Linux mangelhaft

Inhalt: Firefox hat ASLR nach Problemen wieder deaktiviert

Datum: 8.12.2014, 16:00

Autor: Hanno Böck

Themen: Linux, Sicherheitslücke, Mozilla, Technologie, Applikationen, Open Source, Security

Geringe Auswirkungen auf die Leistungen

Die Nutzung von positionsunabhängigem Code hat Auswirkungen auf die Performance. Insbesondere auf alten PC-Systemen mit 32 Bit ist das ein Problem, denn hier ist die Zahl der Prozessorregister knapp und für den positionsunabhängigen Code wird ein zusätzliches Register benötigt. Auf 64-Bit-Systemen sind die Performanceeinbußen hingegen sehr gering. Bei einem Test von uns mit der Codierung eines Videos mit dem Programm *ffmpeg* betrug der Unterschied etwa 1,5 Prozent. Es gibt Patches für den gcc-Compiler und Binutils, welche die Leistungseinbußen noch weiter reduzieren und die in den kommenden Versionen der entsprechenden Tools enthalten sein werden.

Auch ohne positionsunabhängigen Code ist die Adressrandomisierung nicht völlig nutzlos. Der Stack- und der Heap-Speicher landen trotzdem an zufälligen Adressen und Bibliotheken werden generell mit positionsunabhängigem Code kompiliert. Aber für einen wirklichen Schutz reicht das nicht. Insbesondere um vor sogenannten Return-Oriented-Programming-Angriffen zu schützen, ist eine Randomisierung des eigentlichen Programmcodes wichtig.

Firefox hat ASLR nach Problemen wieder deaktiviert

Mozilla hatte vor kurzem versucht, Firefox für Linux mit den entsprechenden Optionen zu kompilieren. Dabei trat ein unerwartetes Problem auf: Der GNOME-Dateimanager Nautilus erkannte die entsprechend kompilierten ausführbaren Dateien nicht als solche und Firefox ließ sich über den Dateimanager nicht starten. Firefox schaltete daraufhin die entsprechende Funktion wieder ab.

Der Grund für die Nautilus-Probleme, die bei einem Test von Golem.de unter dem KDE-Dateimanager Dolphin in genau derselben Form auftraten: Der Dateimanager greift zur Erkennung von ausführbaren Dateien auf die Bibliothek libmagic zurück, die Teil des Tools file ist. Die libmagic-Bilbiothek wiederum kann positionsunabhängige Linux-Binaries nicht von Bibliotheken unterscheiden und liefert den MIME-Type für Bibliotheken zurück. Sowohl Binaries als auch Bibliotheken verwenden unter Linux das Elf-Dateiformat.

Chrome wird standardmäßig mit Adressrandomisierung ausgeliefert, ebenso der auf Firefox basierende Tor-Browser. Anders als Mozilla liefern diese beiden Browser ein Shellskript zum Starten mit, sie sind somit von dem Problem in den Dateimanagern nicht betroffen.

In Linux-Distributionen kein Standard

Bei den Linux-Distributionen ist die Situation in Sachen ASLR sehr gemischt. Fedora und Debian aktivieren das Feature nur für einzelne Tools, die als besonders sicherheitskritisch gelten. Gleiches gilt auch für andere auf Debian basierende Distributionen wie Ubuntu. Selbst Tails, ein auf Datenschutzeinstellungen und Sicherheit getrimmtes Linux-System, nutzt ASLR nicht standardmäßig.

Es gibt auch immer wieder generelle Probleme mit der ASLR-Implementierung von Linux. Mitglieder von Google's Projekt Zero entdeckten beim Versuch, eine Glibc-Sicherheitslücke auszunutzen, dass man zumindest unter 32-Bit-Systemen die Speicherrandomisierung von Suid-Binaries mit Hilfe des Befehls ulimit weitgehend deaktivieren kann.

Videos

E-Fan fliegt über den Ärmelkanal - Airbus

Verwandte Artikel

ENTERPRISE-LINUX
CentOS bringt monatliche Rolling-Releases

PaX liefert eine deutlich bessere Speicherrandomisierung als der Standard-Linux-Kernel. (Bild: PaX)

Artikel: ASLR Speicher-Randomisierung unter Linux mangelhaft

Inhalt: Firefox hat ASLR nach Problemen wieder deaktiviert

Datum: 8.12.2014, 16:00

Autor: Hanno Böck

Themen: Linux, Sicherheitslücke, Mozilla, Technologie, Applikationen, Open Source, Security

Teilen: 5 8 18 5

Tools: Drucken

offset2lib-Schwäche entdeckt

Zuletzt hatten die Sicherheitsforscher Hector Marco-Gisbert und Ismael Ripoll auf der Deepsec-Konferenz in Wien eine ausführliche Analyse des ASLR-Konzepts von Linux vorgestellt und ein weiteres Problem entdeckt, das sie offset2lib getauft haben: Linux legt zwar den Programmcode an einer zufälligen Stelle im Speicher ab, aber der Hauptprogrammcode und der Code von nachgeladenen Bibliotheken wird immer im selben Abstand abgelegt. Das bedeutet, dass ein Angreifer, der im Hauptprogramm aufgrund eines Fehlers möglicherweise Kenntnis von einer Speicheradresse erlangt, damit eine Sicherheitslücke in einer Bibliothek ausnutzen kann.

Android ist von der offset2lib-Schwäche ebenfalls betroffen. Anders als unter gängigen Linux-Distributionen kommt unter Android in aller Regel auch Adressrandomisierung zum Einsatz. Nicht betroffen sind Linux-Systeme, die Pax benutzen. Die Forscher haben einen Patch vorgelegt, der zur Zeit auf der Kernel-Mailingliste diskutiert wird.

Solange die meisten Linux-Distributionen aber keine Dateien mit positionsunabhängigem Code ausliefern, hilft das alles nicht viel. Die Distributionen sollten hier dringend handeln und die Speicherrandomisierung mittels ASLR auch unter Linux zum Standard machen. ▪

1 2

ASLR: Speicher-Randomisierung unter Linux mangelhaft

http://oe1.orf.at/programm/390557

matrix - computer & neue medien

Sonntag

30. November 2014

22:30

1. Hacker-Training Die DeepSec 2014

2. Ist Privatsphäre wirklich so wichtig? Über Bürgerrechte und Lippenbekenntnisse

EPA/PETER STEFFEN

Menschen vor einem bunten Weltkartenbild

1. Die im September geleakten Nacktbilder von US-Prominenten, die aus dem Online-Speicherdienst iCloud gestohlen wurden, zeigen ein weiteres Mal, dass im Netz nichts und niemand sicher ist. Manchmal sind es nur zu einfach gesetzte Passwörter, die es Kriminellen leicht machen, Fotos, Kreditkartendetails oder ganze Identitäten zu stehlen.

Um die Sicherheits-Herausforderungen der IT zu beleuchten und aus den Fehlern der Vergangenheit zu lernen, holt die "DeepSec"-Konferenz auch dieses Jahr internationale Vortragende Ende November nach Wien. Ein erklärtes Ziel dieser Internationalen Konferenz ist es, Akademiker, Regierungs- und Wirtschaftsvertreter, sowie die Hacking-Community zusammenzubringen und den Dialog rund um das Thema Sicherheit zu intensivieren, wie Sarah Kriesche berichtet.

2. Wie stehen die Europäerinnen und Europäer zum Thema Überwachung, Privatsphäre und Regulierung des Internet? Das wollte die EU-Kommission wissen und initiierte drei Bürgerbeteiligungsprojekte namens SURPRISE, PRISMS und PACT. Mitte November trafen sich Expertinnen und Experten auf Einladung des Instituts für Technikfolgenabschätzung ITA an der Akademie der Wissenschaften in Wien, um die Ergebnisse zu diskutieren. Entgegen allen Klischees sorgen sich junge Leute zum Beispiel mehr um die Privatsphäre als ältere. Mariann Unterluggauer war dabei und hat die Anwesenheit von Gästen wie Ben Hayes von Statewatch und Peter Hustinx, ehemals Datenschutzbeauftragter in der Barroso-Kommission, dazu genutzt, um der Frage nachzugehen, warum es so schwer ist, das Bedürfnis der Bevölkerung nach Datenschutz, Privatheit und Kommunikationsfreiheit politisch umzusetzen.

Standort: oe1.ORF.at

OE1 ORF.at

Navigation

matrix - computer & neue medien

Sonntag
30. November 2014
22:30

1. Hacker-Training Die DeepSec 2014
2. Ist Privatsphäre wirklich so wichtig? Über Bürgerrechte und Lippenbekenntnisse

EPA/PETER STEFFEN

1. Die im September geleakten Nacktbilder von US-Prominenten, die aus dem Online-Speicherdienst

iCloud gestohlen wurden, zeigen ein weiteres Mal, dass im Netz nichts und niemand sicher ist. Manchmal sind es nur zu einfach gesetzte Passwörter, die es Kriminellen leicht machen, Fotos, Kreditkartendetails oder ganze Identitäten zu stehlen.
Um die Sicherheits-Herausforderungen der IT zu beleuchten und aus den Fehlern der Vergangenheit zu lernen, holt die "DeepSec"-Konferenz auch dieses Jahr internationale Vortragende Ende November nach Wien. Ein erklärtes Ziel dieser Internationalen Konferenz ist es, Akademiker, Regierungs- und Wirtschaftsvertreter, sowie die Hacking-Community zusammenzubringen und den Dialog rund um das Thema Sicherheit zu intensivieren, wie Sarah Kriesche berichtet.

2. Wie stehen die Europäerinnen und Europäer zum Thema Überwachung, Privatsphäre und Regulierung des Internet? Das wollte die EU-Kommission wissen und initiierte drei Bürgerbeteiligungsprojekte namens SURPRISE, PRISMS und PACT. Mitte November trafen sich Expertinnen und Experten auf Einladung des Instituts für Technikfolgenabschätzung ITA an der Akademie der Wissenschaften in Wien, um die Ergebnisse zu diskutieren. Entgegen allen Klischees sorgen sich junge Leute zum Beispiel mehr um die Privatsphäre als ältere. Mariann Unterluggauer war dabei und hat die Anwesenheit von Gästen wie Ben Hayes von Statewatch und Peter Hustinx, ehemals Datenschutzbeauftragter in der Barroso-Kommission, dazu genutzt, um der Frage nachzugehen, warum es so schwer ist, das Bedürfnis der Bevölkerung nach Datenschutz, Privatheit und Kommunikationsfreiheit politisch umzusetzen.

zurück

zur Sendereihe

Kategorie: Wissen

Programm

Mo	Di	Mi	Do	Fr	Sa	So
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Dezember
Gestern
Morgen
Heute
Wissen Downloads

Social Media

http://oe1.orf.at/programm/390226

Digital.Leben

Donnerstag

27. November 2014

16:55

Hacker mit Ethos

Gestaltung: Sarah Kriesche

Moderation und Redaktion: Franz Zeller

EPA/JOCHENLUEBKE

Frau hält Laptop

Sicherheitsexperten haben oft etwas Paranoides an sich - sie wittern allerorts Überwachung. Und das häufig zu Recht: Webseiten versuchen mit Cookies unser Surf-Verhalten aufzuzeichnen, Fitnessgadgets speichern unseren Körperzustand - und melden ihn weiter.

Mit Themen wie diesen beschäftigte sich letzte Woche die Sicherheitskonferenz "Deepsec" in Wien. Der Nachwuchs in der IT-Sicherheitsszene konnte sich tags darauf bei den sogenannten B-Sides austoben. Sarah Kriesche hat dort einen "ethischen Hacker" zum Interview getroffen.

zur Sendereihe

Standort: oe1.ORF.at

Digital.Leben

Donnerstag
27. November 2014
16:55

Hacker mit Ethos
Gestaltung: Sarah Kriesche

Moderation und Redaktion: Franz Zeller

EPA/JOCHENLUEBKE

Sicherheitsexperten haben oft etwas Paranoides an sich - sie wittern allerorts Überwachung. Und das häufig zu Recht: Webseiten versuchen mit Cookies unser Surf-Verhalten aufzuzeichnen, Fitnessgadgets speichern unseren Körperzustand - und melden ihn weiter.

Mit Themen wie diesen beschäftigte sich letzte Woche die Sicherheitskonferenz "Deepsec" in Wien. Der Nachwuchs in der IT-Sicherheitsszene konnte sich tags darauf bei den sogenannten B-Sides austoben. Sarah Kriesche hat dort einen "ethischen Hacker" zum Interview getroffen.

zurück

zur Sendereihe

Kategorie: Wissen

Programm

Mo	Di	Mi	Do	Fr	Sa	So
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Dezember
Gestern
Morgen
Heute
Wissen Downloads

Social Media

http://fm4.orf.at/stories/1749883/

Freie Programme gegen "Staatstrojaner"

23. 11. 2014 - 19:22

Erich Möchel

Neben neuen Verschlüsselungsprogrammen sind auch ein Tool gegen Staatstrojaner und eine mächtige Netzwerksuite zur Abwehr von Angriffen nun frei verfügbar.

Die Ankündigung von WhatsApp, ihr populäres, aber bis dato kaum gesichertes Chatprogramm künftig zu verschlüsseln, markiert den ersten Höhepunkt eines Trends, der seit Monaten sichtbar ist. Sichere Protokolle und Methoden, die aus der Hackersphäre stammen und nur von einer Minderheit benutzt wurden, ziehen in weit verbreitete Anwendungen ein. Im Falle von WhatsApp wurde das Protokoll von TextSecure übernommen, das Chats so verschlüsselt, dass auch der Betreiber selbst nicht mitlesen kann.

Zu einer großen Anzahl neuer, einfach zu bedienender Chat-Verschlüsselungsprogramme wie TextSecure oder Cryptocat kommen nun auch spezialisierte und komplexere Anwendungen. Am Donnerstag wurde mit "Detekt" der erste, auf sogenannte "Staatstrojaner" spezialisierte Virenscanner veröffentlicht. Derartige Schadsoftware wird von Firmen vor allem aus der EU den USA für Geheimdienste und Polizeibehörden produziert und auch an Diktaturen geliefert, die damit Oppositionelle ausspionieren. Zur Früherkennung von Angriffen auf Netzwerke generell wird mit der freien "Suricata"-Suite auch ein mächtiges Abwehrinstrument für fortgeschrittene Anwender benutzbar, das sich mit teuren kommerziellen Produkten für Unternehmensnetze messen kann.

Immer mehr einfach zu bedienende, neue und freie Kryptoprogramme kommen als bloße Plug-ins für gängige Webbrowser daher. Prototypisch für diese Entwicklung steht Cryptocat, das auch als iPhone-App und bald auch für Android erhältlich ist.

Die Gemeinsamkeiten

Diese drei, von ihren Funktionen völlig unterschiedlichen Tools weisen jedoch eine ganze Reihe von Gemeinsamkeiten auf. Zum einen liegt bei allen der Quellcode offen, denn nur dann lässt sich von unabhängiger Seite überprüfen, ob der Code auch wirklich keine Hintertüren enthält. Zweitens stammen all diese Programme von Entwicklergemeinschaften, die ihre Arbeit über Stiftungen und Spenden finanzieren.

TextSecure wurde von einer Gruppe von Open-Source-Programmierern rund um den bekannten Hacker Moxie Marlinspike entwickelt. TextSecure bietet sicher verschlüsselten Chat sowohl für Androids und iPhones und ist aber mit mehreren, anderen Chatprogrammen - etwa Pidgin (Windows, Linux) oder Adium (Mac) - kompatibel, die ebenfalls das "Off the Record"-Protokoll beherrschen. Daneben haben Marlinspike und Co auch die Redphone-App für verschlüsselte Telefonate entwickelt. RedPhone nützt das von Kryptopionier Phil Zimmermann entwickelte ZRTP-Protokoll zur Sprachverschlüsselung. Wie TextSecure hat auch Redphone in allen Sicherheitstests bis dato hervorragend abgeschnitten.

Scorecard sicherer ChatEFF

Die Tabelle der Electronic Frontier Foundation zeigt noch den derzeitigen Unterschied an Sicherheit zwischen TextSecure und WhatsApp

Macht durch Offenheit

Die neuen Services, für die auch die Anbieter keine Nachschlüssel haben, veranlasste die Behörden bereits zur Beschwörung "dunkler, dunkler Zeiten". Anlass für diese Unkenrufe war, dass die neuen iPhones mit Passwortschutz ausgeliefert werden

Die eigentliche Macht dieser Programme liegt in der Offenheit ihres Quellcodes begründet. Da die berühmte "Kette der Sicherheit" insgesamt nur so stark ist, wie ihr schwächstes Glied, lässt sie sich nur dann auch lückenlos überprüfen. Am sichersten ist sie natürlich, wenn darunter ein Betriebssystem werkt, dessen Quellcode ebenfalls offenliegt, doch auch unter Windows oder Mac ist der Sicherheitsgewinn für die Benutzer beträchtlich.

Wer diese TextSecure-Server auch betreibt, hat weder eine Möglichkeit, die Konversationen mitzuschneiden, noch kann er Schlüssel an Behörden herausgeben, weil die Schlüssel nicht auf dem Server, sondern auf den Clients der Benutzer gespeichert sind. Dasselbe gilt bald auch für die weltweit auf 600 Millionen geschätzten Nutzer von WhatsApp.

Wachsame Erdmännchen

Während TextSecure gerade in kommerzielle Anwendungen für Endbenutzer wie WhatsApp integriert werden, wird die quelloffene "Suricata"-Suite schon seit geraumer Zeit in Firmen eingesetzt. Anders als TextSecure ist Suricata kein Tool für Endanwender, vielmehr wurde es für Administratoren entwickelt, die damit Angriffe auf ihr Netz frühzeitig erkennen können. Die Entwicklung von Suricata wurde bereits vor sieben Jahren begonnen, ein eigenes graphisches Benutzerinterface hatte dabei keine besondere Priorität. Offenbar war das Projekt von den

Sponsoren (siehe unten) zur Integration in eigene Benutzeroberflächen vorgesehen.

"Natürlich gibt es da einiges zu konfigurieren, so müssen etwa die Parameter des jeweiligen Netzes - Gateways, Routeradressen usw. - eingegeben werden, damit sich Suricata orientieren kann", sagte Victor Julien, der Entwicklungschef von Suricata zu ORF.at. "Wir arbeiten im Moment vor allem daran, die Konfigurierbarkeit zu vereinfachen und Prozesse, bei denen dies auch möglich ist, zu automatisieren." Ziel sei es dabei, sagte Julien, dass Suricata auch von weniger geübten Administratoren oder auch fortgeschrittenen Usern eingesetzt werden könne. Die Software läuft auf allen drei großen Betriebssystemen, für den Betrieb genügt ein einfacher PC.

Die Entwickler von Suricata hielten auf der DeepSec Konferenz, die am Freitag in Wien zu Ende ging, Suricata-Workshops für Nutzer aus Industrie und Behörden ab. Dieselbe Suricata-Suite ist allerdings als Tool für die Kommandozeile in allen Linuxdistributionen schon enthalten.

Mächtiges Verteidigungsinstrument

Damit steht auch kleineren Firmen wie finanzschwachen Organisationen ein mächtiges Instrument zu Überwachung ihrer eigenen Netze auf Angriffe von außen zur Verfügung. Anders als bei Virenscannern werden hier nicht bloß Dateien auf die jeweils charakteristischen Zeichenfolgen bekannter Schadsoftware durchsucht. Vielmehr werden die Vorgänge im gesamten Datenverkehr beobachtet und nach Mustern gesucht, die auf einen Angriff von außen hinweisen.

Screenshot von SuricataCC Suricata

Im Grunde macht Suricata ganz genau dasselbe, wie alle kommerziellen - und entsprechend teuren - "Intrusion Detection Suites" für Netzwerke von Großkonzernen. In den Netzen von Geheimdiensten und Militärs gehören solche Softwaretools seit jeher zum Sicherheitsstandard und genau von dort kommt Suricata eigentlich her, von der "dunklen Seite der Macht".

Heimatschutz und Sternenkrieger

Die Stiftung, die diese Suite zur Identifikation und Abwehr von Angriffen finanziert, gehört zum "Homeland Open Security Program" des US-Ministeriums für Heimatschutz und dem "Space and Naval Warfare Systems Command" (SPAWAR) der US Navy. Das erscheint paradox, hat aber dennoch einen völlig rationalen Hintergrund.

Dass nur quelloffene Sicherheitssysteme vertrauenswürdig, weil auch überprüfbar sind, gilt im Militärbereich schon weitaus länger als in der Sphäre ziviler Kommunikation. Zudem sind Open-Source-Systeme viel schneller zu entwickeln, wenn nämlich andere Interessenten für dieselbe Art von Software dazustoßen. Obendrein hängt der Sicherheitsgrad noch völlig davon ab, wieviele Coder mit entsprechender Erfahrung den Quellcode laufend überprüfen. Gerade im Sicherheitsbereich geht der Trend fast unaufhaltsam in Richtung Open Source, der NSA-Spionageskandal hat hier natürlich einen entscheidenden Schub geliefert.

Detekt AlarmmeldungCC

Staatstrojaner und ihre Lieferanten

Die Veröffentlichung von "Detekt" ist natürlich auch als politischer Akt zu sehen. Das Programm ist dazu angetan, die Kosten für die Entwicklung bestimmter Spionage-Suites in die Höhe zu treiben

Mit Amnesty International, Privacy International, der Digitalen Gesellschaft und der Electronic Frontier Foundation stehen hinter dem Staatstrojaner-Scanner "Detekt" ebenfalls gemeinnützige Organisationen. Die erste Version von "Detekt" ist ein vergleichsweise einfaches, aber hochspezialisiertes Tool, das eine selektive Zielgruppe bedient. Es richtet sich an Menschen, die wichtige Gründe haben, derartige staatliche Angriffe auf ihre Kommunikation zu befürchten.

Detekt soll in erster Linie Dissidenten und Journalisten schützen, die von Geheimdiensten und politischer Polizei in nichtdemokratischen Staaten angegriffen werden. Die bekanntesten dieser Spionagesuites sind die Produkte der deutsch-britischen Gamma International namens "FinFisher", sowie jene der italienischen Hacking Team RCS, die ebenfalls Behörden rund um die Welt mit Schadsoftware beliefert.

Aktivisten, Journalisten

Seit März läuft in Großbritannien ein von Privacy International und anderen unterstützter Prozess gegen Gamma International und Hacking Team RSC. Die Anzeige selbst stammt von einem britischen Staatsbürger, der aus Bahrain stammt.

Die Spionagesuites dieser beiden Firmen waren während des Arabischen Frühlings wiederholt aufgefallen, weil sie von den regierenden Diktatoren gegen Oppositionelle eingesetzt wurden. Der Zeitpunkt der Veröffentlichung von "Detekt" direkt vor den ersten Wahlen in Bahrain nach dem Volksaufstand von 2011 am Samstag war nicht zufällig. Eines der ersten nachgewiesenen Opfer von FinFisher war eine Aktivistin aus der Demokratiebewegung

in Bahrain, auf deren Rechner Spuren der deutsch-britischen Spionagesoftware FinFisher gefunden wurden.

Die Zielgruppe von Detekt ist allerdings nicht auf autoritär regierte Staaten wie Bahrain beschränkt. Am Freitag hatte AP gemeldet, die britische Journalistengewerkschaft habe Klage gegen die Londoner Metropolitan Police und das britische Innenministerium eingereicht. Anfragen von Journalisten nach dem Gesetz zur Informationsfreiheit hatten ergeben, dass eine ganze Reihe britischer Journalisten systematisch und jahrelang in ihrem persönlichen Umfeld bespitzelt wurde.

SPAWAR, TOR

Warum fördern das Außenministerium der USA, die See- und Sternenkrieger der US Navy, zu der auch die NSA gehört und weniger auffällige Stiftungen aus den USA Projekte wie etwa TOR? Zum einen, weil Bürger und Armeen der Weltmacht USA auch rund um die Welt sichere Kommunikation benötigen. Zum anderen muss man als Supermacht führend dabei sein, weil sich dieser ebenso globale wie mächtige Trend zur quelloffenen sicheren Verschlüsselung ohnehin nicht stoppen lässt.

Erstellt am: 23. 11. 2014 - 19:22 Uhr

Freie Programme gegen "Staatstrojaner"

Neben neuen Verschlüsselungsprogrammen sind auch ein Tool gegen Staatstrojaner und eine mächtige Netzwerksuite zur Abwehr von Angriffen nun frei verfügbar.

Die Ankündigung von WhatsApp, ihr populäres, aber bis dato kaum gesichertes Chatprogramm künftig zu verschlüsseln, markiert den ersten Höhepunkt eines Trends, der seit Monaten sichtbar ist. Sichere Protokolle und Methoden, die aus der Hackersphäre stammen und nur von einer Minderheit benutzt wurden, ziehen in weit verbreitete Anwendungen ein. Im Falle von WhatsApp wurde das Protokoll von TextSecure übernommen, das Chats so verschlüsselt, dass auch der Betreiber selbst nicht mitlesen kann.

Zu einer großen Anzahl neuer, einfach zu bedienender Chat-Verschlüsselungsprogramme wie TextSecure oder Cryptocat kommen nun auch spezialisierte und komplexere Anwendungen. Am Donnerstag wurde mit "Detekt" der erste, auf sogenannte "Staatstrojaner" spezialisierte Virenscanner veröffentlicht. Derartige Schadsoftware wird von Firmen vor allem aus der EU den USA für Geheimdienste und Polizeibehörden produziert und auch an Diktaturen geliefert, die damit Oppositionelle ausspionieren. Zur Früherkennung von Angriffen auf Netzwerke generell wird mit der freien "Suricata"-Suite auch ein mächtiges Abwehrinstrument für fortgeschrittene Anwender benutzbar, das sich mit teuren kommerziellen Produkten für Unternehmensnetze messen kann.

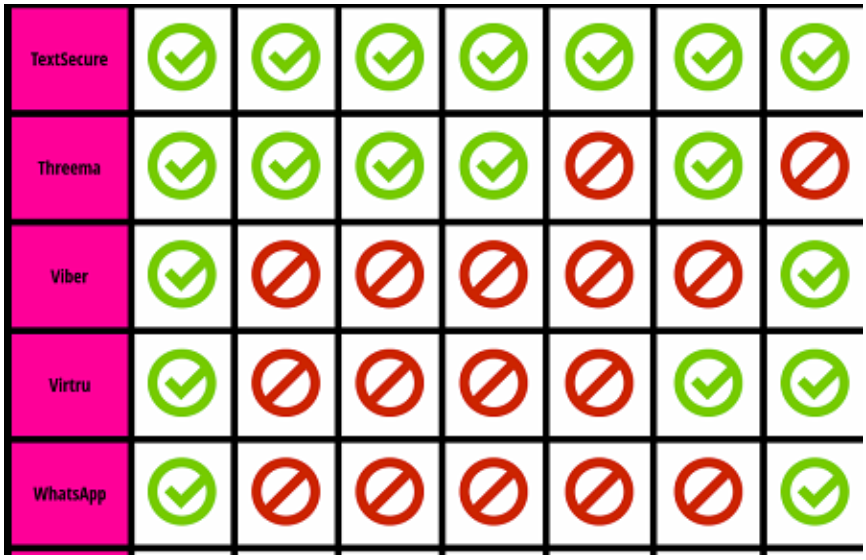
Immer mehr einfach zu bedienende, neue und freie Kryptoprogramme kommen als bloße Plug-ins für gängige Webbrowser daher. Prototypisch für diese Entwicklung steht Cryptocat, das auch als iPhone-App und bald auch für Android erhältlich ist.

Die Gemeinsamkeiten

Diese drei, von ihren Funktionen völlig unterschiedlichen Tools weisen jedoch eine ganze Reihe von Gemeinsamkeiten auf. Zum einen liegt bei allen der Quellcode offen, denn nur dann lässt sich von unabhängiger Seite überprüfen, ob der Code auch wirklich keine Hintertüren enthält. Zweitens stammen all diese Programme von Entwicklergemeinschaften, die ihre Arbeit über Stiftungen und Spenden finanzieren.

TextSecure wurde von einer Gruppe von Open-Source-Programmierern rund um den bekannten Hacker Moxie Marlinspike entwickelt. TextSecure bietet sicher verschlüsselten Chat sowohl für Androids und iPhones und ist aber mit mehreren, anderen Chatprogrammen - etwa Pidgin (Windows, Linux) oder Adium (Mac) - kompatibel, die ebenfalls das "Off the Record"-Protokoll beherrschen. Daneben haben Marlinspike und Co auch die Redphone-App für verschlüsselte Telefonate entwickelt. RedPhone nützt das von Kryptopionier Phil Zimmermann entwickelte ZRTP-Protokoll zur Sprachverschlüsselung. Wie TextSecure hat auch Redphone in allen Sicherheitstests bis dato hervorragend abgeschnitten.

Die Scorecard der EFF für sichere Chats `( https://www.eff.org/de/secure-messaging-scorecard )`



EFF

Die Tabelle der Electronic Frontier Foundation zeigt noch den derzeitigen Unterschied an Sicherheit zwischen TextSecure und WhatsApp

Macht durch Offenheit

Die neuen Services, für die auch die Anbieter keine Nachschlüssel haben, veranlasste die Behörden bereits zur Beschwörung "dunkler, dunkler Zeiten". Anlass für diese Unkenrufe war, dass die neuen iPhones mit Passwortschutz ausgeliefert werden

Die eigentliche Macht dieser Programme liegt in der Offenheit ihres Quellcodes begründet. Da die berühmte "Kette der Sicherheit" insgesamt nur so stark ist, wie ihr schwächstes Glied, lässt sie sich nur dann auch lückenlos überprüfen. Am sichersten ist sie natürlich, wenn darunter ein Betriebssystem werkt, dessen Quellcode ebenfalls offenliegt, doch auch unter Windows oder Mac ist der Sicherheitsgewinn für die Benutzer beträchtlich.

Wer diese TextSecure-Server auch betreibt, hat weder eine Möglichkeit, die Konversationen mitzuschneiden, noch kann er Schlüssel an Behörden herausgeben, weil die Schlüssel nicht auf dem Server, sondern auf den Clients der Benutzer gespeichert sind. Dasselbe gilt bald auch für die weltweit auf 600 Millionen geschätzten Nutzer von WhatsApp.

Wachsame Erdmännchen

Während TextSecure gerade in kommerzielle Anwendungen für Endbenutzer wie WhatsApp

integriert werden, wird die quelloffene "Suricata"-Suite schon seit geraumer Zeit in Firmen eingesetzt. Anders als TextSecure ist Suricata kein Tool für Endanwender, vielmehr wurde es für Administratoren entwickelt, die damit Angriffe auf ihr Netz frühzeitig erkennen können. Die Entwicklung von Suricata wurde bereits vor sieben Jahren begonnen, ein eigenes graphisches Benutzerinterface hatte dabei keine besondere Priorität. Offenbar war das Projekt von den Sponsoren (siehe unten) zur Integration in eigene Benutzeroberflächen vorgesehen.

Sara&Joachim&Mebe / CC BY-SA 2.0

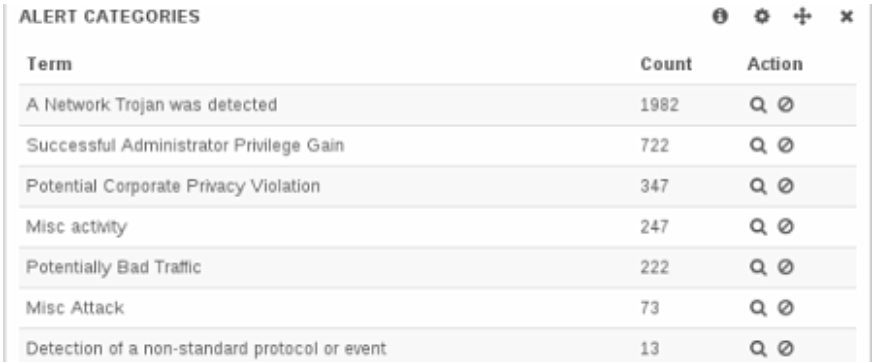
Die Wachsamkeit der Erdmännchen (lat. Suricata suricata) hat die Namensgebung von Suricata inspriert (CC BY-SA 2.0 (https://creativecommons.org/licenses/by-sa/2.0/))

"Natürlich gibt es da einiges zu konfigurieren, so müssen etwa die Parameter des jeweiligen Netzes - Gateways, Routeradressen usw. - eingegeben werden, damit sich Suricata orientieren kann", sagte Victor Julien, der Entwicklungschef von Suricata zu ORF.at. "Wir arbeiten im Moment vor allem daran, die Konfigurierbarkeit zu vereinfachen und Prozesse, bei denen dies auch möglich ist, zu automatisieren." Ziel sei es dabei, sagte Julien, dass Suricata auch von weniger geübten Administratoren oder auch fortgeschrittenen Usern eingesetzt werden könne. Die Software läuft auf allen drei großen Betriebssystemen, für den Betrieb genügt ein einfacher PC.

Die Entwickler von Suricata hielten auf der DeepSec Konferenz, die am Freitag in Wien (https://deepsec.net) zu Ende ging, Suricata-Workshops für Nutzer aus Industrie und Behörden ab. Dieselbe Suricata-Suite (https://redmine.openinfosecfoundation.org/projects/suricata/wiki) ist allerdings als Tool für die Kommandozeile in allen Linuxdistributionen schon enthalten.

Mächtiges Verteidigungsinstrument

Damit steht auch kleineren Firmen wie finanzschwachen Organisationen ein mächtiges Instrument zu Überwachung ihrer eigenen Netze auf Angriffe von außen zur Verfügung. Anders als bei Virenscannern werden hier nicht bloß Dateien auf die jeweils charakteristischen Zeichenfolgen bekannter Schadsoftware durchsucht. Vielmehr werden die Vorgänge im gesamten Datenverkehr beobachtet und nach Mustern gesucht, die auf einen Angriff von außen hinweisen.



ALERT CATEGORIES

Term	Count	Action
A Network Trojan was detected	1982	
Successful Administrator Privilege Gain	722	
Potential Corporate Privacy Violation	347	
Misc activity	247	
Potentially Bad Traffic	222	
Misc Attack	73	
Detection of a non-standard protocol or event	13	

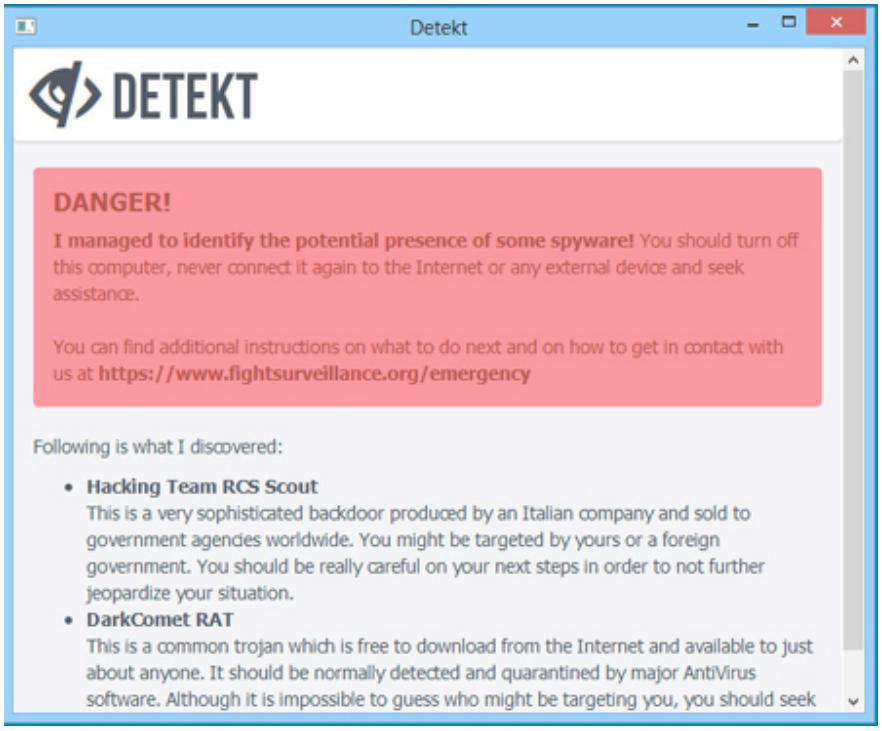
CC Suricata

Im Grunde macht Suricata ganz genau dasselbe, wie alle kommerziellen - und entsprechend teuren - "Intrusion Detection Suites" für Netzwerke von Großkonzernen. In den Netzen von Geheimdiensten und Militärs gehören solche Softwaretools seit jeher zum Sicherheitsstandard und genau von dort kommt Suricata eigentlich her, von der "dunklen Seite der Macht".

Heimatschutz und Sternenkrieger

Die Stiftung, die diese Suite zur Identifikation und Abwehr von Angriffen finanziert, gehört zum "Homeland Open Security Program" des US-Ministeriums für Heimatschutz und dem "Space and Naval Warfare Systems Command" (SPAWAR) der US Navy. Das erscheint paradox, hat aber dennoch einen völlig rationalen Hintergrund.

Dass nur quelloffene Sicherheitssysteme vertrauenswürdig, weil auch überprüfbar sind, gilt im Militärbereich schon weitaus länger als in der Sphäre ziviler Kommunikation. Zudem sind Open-Source-Systeme viel schneller zu entwickeln, wenn nämlich andere Interessenten für dieselbe Art von Software dazustoßen. Obendrein hängt der Sicherheitsgrad noch völlig davon ab, wieviele Coder mit entsprechender Erfahrung den Quellcode laufend überprüfen. Gerade im Sicherheitsbereich geht der Trend fast unaufhaltsam in Richtung Open Source, der NSA-Spionageskandal hat hier natürlich einen entscheidenden Schub geliefert.



CC

Staatstrojaner und ihre Lieferanten

Die Veröffentlichung von "Detekt" ist natürlich auch als politischer Akt zu sehen. Das Programm ist dazu angetan, die Kosten für die Entwicklung bestimmter Spionage-Suites in die Höhe zu treiben (`https://resistsurveillance.org/`)

Mit Amnesty International, Privacy International, der Digitalen Gesellschaft und der Electronic Frontier Foundation stehen hinter dem Staatstrojaner-Scanner "Detekt" ebenfalls gemeinnützige Organisationen. Die erste Version von "Detekt" ist ein vergleichsweise einfaches, aber hochspezialisiertes Tool, das eine selektive Zielgruppe bedient. Es richtet sich an Menschen, die wichtige Gründe haben, derartige staatliche Angriffe auf ihre Kommunikation zu befürchten.

Detekt soll in erster Linie Dissidenten und Journalisten schützen, die von Geheimdiensten und politischer Polizei in nichtdemokratischen Staaten angegriffen werden. Die bekanntesten dieser Spionagesuites sind die Produkte der deutsch-britischen Gamma International namens "FinFisher", sowie jene der italienischen Hacking Team RCS, die ebenfalls Behörden rund um die Welt mit Schadsoftware beliefert.

Aktivisten, Journalisten

Seit März läuft in Großbritannien ein von Privacy International und anderen unterstützter Prozess gegen Gamma International und Hacking Team RSC. Die Anzeige selbst stammt von einem britischen Staatsbürger, der aus Bahrain stammt.

Die Spionagesuites dieser beiden Firmen waren während des Arabischen Frühlings wiederholt aufgefallen, weil sie von den regierenden Diktatoren gegen Oppositionelle eingesetzt wurden. Der Zeitpunkt der Veröffentlichung von "Detekt" direkt vor den ersten Wahlen in Bahrain nach dem Volksaufstand von 2011 am Samstag war nicht zufällig. Eines der ersten nachgewiesenen Opfer von FinFisher war eine Aktivistin aus der Demokratiebewegung in Bahrain, auf deren Rechner Spuren der

deutsch-britischen Spionagesoftware FinFisher gefunden wurden.

Die Zielgruppe von Detekt ist allerdings nicht auf autoritär regierte Staaten wie Bahrain beschränkt. Am Freitag hatte AP gemeldet, die britische Journalistengewerkschaft habe Klage gegen die Londoner Metropolitan Police und das britische Innenministerium eingereicht. Anfragen von Journalisten nach dem Gesetz zur Informationsfreiheit hatten ergeben, dass eine ganze Reihe britischer Journalisten systematisch und jahrelang in ihrem persönlichen Umfeld bespitzelt wurde.

SPAWAR, TOR

Warum fördern das Außenministerium der USA, die See- und Sternenkrieger der US Navy, zu der auch die NSA gehört und weniger auffällige Stiftungen aus den USA Projekte wie etwa TOR? Zum einen, weil Bürger und Armeen der Weltmacht USA auch rund um die Welt sichere Kommunikation benötigen. Zum anderen muss man als Supermacht führend dabei sein, weil sich dieser ebenso globale wie mächtige Trend zur quelloffenen sicheren Verschlüsselung ohnehin nicht stoppen lässt.

http://futurezone.at/netzpolitik/white-hat-hacking-ist-nicht-lukrativ-genug/98.211.388

DEEPSEC

"White Hat Hacking ist nicht lukrativ genug"

Florian Christof 21.11.14, 11:24

Bei der DeepSec-Konferenz forderte Linus Neumann vom CCC, Anreize für das Aufdecken von Schwachstellen massiv zu erhöhen und sieht Interessenskonflikte im Innenministerium.

Die OpenSSL-Lücke Heartbleed bestand zwei Jahre, bis sie von der Öffentlichkeit entdeckt wurde. Der Shellshock-Bug, der Apple-, Linux- und Unix-Nutzer gefährdete, blieb überhaupt mehr als 20 Jahre unentdeckt. Dies sind nur zwei Beispiele, die Linus Neumann, ein Sprecher des Chaos Computer Clubs, bei der Pressekonferenz der Sicherheitskonferenz DeepSec in Wien für den katastrophalen Zustand der IT-Security anführte.

Problemfelder dabei sieht Neumann gleich an mehreren Orten und über verschiedene Ebenen verteilt. Ein wesentlicher Punkt ist, dass es für White Hat Hacker einfach nicht lukrativ genug sei, gefundene Sicherheitslücken offen zu legen.

Anreize für White Hats schaffen

"Bei den Bug-Bounties werden meist nur ein paar tausend Euro ausgeschrieben. Wer eine Schwachstelle entdeckt, kann sie allerdings am Schwarzmarkt um ein Vielfaches verkaufen", bemängelt Neumann. "Um Anreize zu schaffen, müssten die Prämien für das Aufspüren von Sicherheitslücken massiv erhöht werden, ganz besonders bei Open-Source-Software." Dabei sieht Neumann auch die Politik sowie branchen- und unternehmensübergreifende Initiativen gefordert.

Einen unüberbrückbaren Interessenskonflikt sieht Neumann in der Tatsache, dass IT-Sicherheitsthemen allesamt im Innenministerium angesiedelt sind. "Einerseits sind die Behörden mit Bewusstseinsarbeit, Aufklärung und Verbrechensaufdeckung beschäftigt und andererseits kauft dasselbe Ressort Zero Day Exploits um Schwachstellen, etwa für Spionage oder Überwachungstätigkeiten ausnutzen zu können", kritisiert Neumann. "Mit einer solchen Vorgehensweise kann man nicht für nachhaltige IT-Sicherheit sorgen."

BND will Zero Day Exploits kaufen

Für diesen Kauf von Zero Day Exploits hat der deutsche Bundesnachrichtendienst nach Informationen des Spiegel für die kommenden fünf Jahre 4,5 Millionen Euro budgetiert. Bis 2014 hatte die deutsche Bundesregierung einen Vertrag mit dem französischen Sicherheitsunternehmen Vupen, das auf den Handel mit Zero-Day-Schwachstellen spezialisiert ist.

Neumann kritisiert, dass Vupen-Mitarbeiter etwa bei Bug-Bounty-Events auftreten, Sicherheitslücken zeigen, aber die Schwachstellen weder dokumentieren noch erklären. "Nachdem sie ihren Hack gezeigt haben, packen sie zusammen und gehen, ohne sich ein Preisgeld abzuholen", sagt Neumann. Ein solches Verhalten signalisiere, dass woanders weit mehr Geld mit dem Aufdecken von Sicherheitslücken zu machen ist, wodurch auch der Handel mit Sicherheitslücken extrem angeheizt wird.

Daher forderte der CCC auch Anfang November, dass der Kauf von Zero Day Exploits durch deutsche Behörden verboten wird: "Sicherheitslücken gehören nach der Entdeckung geschlossen und nicht verkauft und geheim gehalten, solange es irgendwie geht."

Die Frage nach der Haftung

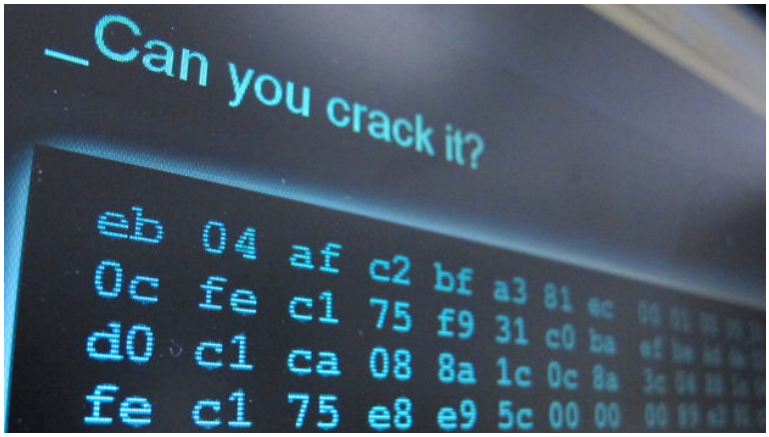
Abschließend stellte Neumann eine Frage in den Raum, die allerdings noch durchdiskutiert gehöre: "Warum haften Softwarehersteller eigentlich nicht für die Sicherheit ihres Produkts?" In keiner anderen Branche sei es möglich, ein Produkt zu verkaufen und dafür keine Haftung zu übernehmen. Wenn bei Fahrzeugen etwa Probleme mit den Bremsen auftreten, kann es sein, dass die komplette Serie zurückgerufen wird. Bei Software gebe es so etwas nicht. "Sollte nicht ein kommerzieller Anbieter für Sicherheitslücken haften", mutmaßt Neumann.

(FUTUREZONE) ERSTELLT AM 21.11.2014, 11:24

DEEPSEC

"White Hat Hacking ist nicht lukrativ genug"

von Florian Christof 21.11.14, 11:24 FlorianChristof Mail an Autor



Für White Hat Hacking sollten die Anreize massiv erhöht werden - Foto: AP/Cassandra Vinograd

DEEPSEC
"White Hat Hacking ist nicht lukrativ genug"
KOMMENTARE (2)
MEHR ZUM THEMA

Bei der DeepSec-Konferenz forderte Linus Neumann vom CCC, Anreize für das Aufdecken von Schwachstellen massiv zu erhöhen und sieht Interessenskonflikte im Innenministerium.

SICHERHEITSLÜCKE, HACKER, CCC, IT-SECURITY, DEEPSEC, IT-SICHERHEIT

Die OpenSSL-Lücke Heartbleed bestand zwei Jahre, bis sie von der Öffentlichkeit entdeckt wurde. Der Shellshock-Bug, der Apple-, Linux- und Unix-Nutzer gefährdete, blieb überhaupt mehr als 20 Jahre unentdeckt. Dies sind nur zwei Beispiele, die Linus Neumann, ein Sprecher des Chaos Computer Clubs, bei der Pressekonferenz der Sicherheitskonferenz DeepSec in Wien für den katastrophalen Zustand der IT-Security anführte.

Problemfelder dabei sieht Neumann gleich an mehreren Orten und über verschiedene Ebenen verteilt. Ein wesentlicher Punkt ist, dass es für White Hat Hacker einfach nicht lukrativ genug sei, gefundene Sicherheitslücken offen zu legen.

Anreize für White Hats schaffen

"Bei den Bug-Bounties werden meist nur ein paar tausend Euro ausgeschrieben. Wer eine Schwachstelle entdeckt, kann sie allerdings am Schwarzmarkt um ein Vielfaches verkaufen", bemängelt Neumann. "Um Anreize zu schaffen, müssten die Prämien für das Aufspüren von Sicherheitslücken massiv erhöht werden, ganz besonders bei Open-Source-Software." Dabei sieht Neumann auch die Politik sowie branchen- und unternehmensübergreifende Initiativen gefordert.

Einen unüberbrückbaren Interessenskonflikt sieht Neumann in der Tatsache, dass IT-Sicherheitsthemen allesamt im Innenministerium angesiedelt sind. "Einerseits sind die Behörden mit Bewusstseinsarbeit, Aufklärung und Verbrechensaufdeckung beschäftigt und andererseits kauft dasselbe Ressort Zero Day Exploits um Schwachstellen, etwa für Spionage oder Überwachungstätigkeiten ausnutzen zu können", kritisiert Neumann. "Mit einer solchen Vorgehensweise kann man nicht für nachhaltige IT-Sicherheit sorgen."

FEATURED

VERKEHR
Hier-Box holt bei Autounfällen automatisch Hilfe

REPORTAGE
Buffalo: „Stadt des Lichts" kämpft gegen den Rost

AKTION
Facebook-Video zeigt waghalsige Aktion im AKW Zwentendorf

BND will Zero Day Exploits kaufen

Für diesen Kauf von Zero Day Exploits hat der deutsche Bundesnachrichtendienst nach Informationen des Spiegel für die kommenden fünf Jahre 4,5 Millionen Euro budgetiert. Bis 2014 hatte die deutsche Bundesregierung einen Vertrag mit dem französischen Sicherheitsunternehmen Vupen, das auf den Handel mit Zero-Day-Schwachstellen spezialisiert ist.

Neumann kritisiert, dass Vupen-Mitarbeiter etwa bei Bug-Bounty-Events auftreten, Sicherheitslücken zeigen, aber die Schwachstellen weder dokumentieren noch erklären. "Nachdem sie ihren Hack gezeigt haben, packen sie zusammen und gehen, ohne sich ein Preisgeld abzuholen", sagt Neumann. Ein solches Verhalten signalisiere, dass woanders weit mehr Geld mit dem Aufdecken von Sicherheitslücken zu machen ist, wodurch auch der Handel mit Sicherheitslücken extrem angeheizt wird.

Daher forderte der CCC auch Anfang November, dass der Kauf von Zero Day Exploits durch deutsche Behörden verboten wird: "Sicherheitslücken gehören nach der Entdeckung geschlossen und nicht verkauft und geheim gehalten, solange es irgendwie geht."

Die Frage nach der Haftung

Abschließend stellte Neumann eine Frage in den Raum, die allerdings noch durchdiskutiert gehöre: "Warum haften Softwarehersteller eigentlich nicht für die Sicherheit ihres Produkts?" In keiner anderen Branche sei es möglich, ein Produkt zu verkaufen und dafür keine Haftung zu übernehmen. Wenn bei Fahrzeugen etwa Probleme mit den Bremsen auftreten, kann es sein, dass die komplette Serie zurückgerufen wird. Bei Software gebe es so etwas nicht. "Sollte nicht ein kommerzieller Anbieter für Sicherheitslücken haften", mutmaßt Neumann.

(FUTUREZONE) ERSTELLT AM 21.11.2014, 11:24

SICHERHEITSLÜCKE, HACKER, CCC, IT-SECURITY, DEEPSEC, IT-SICHERHEIT

Kommentare (2)

Ihr Kommentar
Bitte loggen Sie sich ein

Einloggen / Registrieren

ABSENDEN

a190 vor 7 monaten permalink | melden 0 0

Ich denke nicht, dass es notwendig ist, überhaupt "Prämien" für White Hacking zu zahlen.

Im Gegenteil: Wer eine Sicherheitslücke findet und diese verkauft, ist natürlich strafrechtlich voll in der Scheiße, wenn damit ein Schaden verursacht wird, und - zumindest teilweise - für den Schaden auch haftbar. Existenz, baba! Wer's nicht glaubt, versuche mal, die Information über eine versehentlich offene Tür an eine Einbrecherbande zu verkaufen.

Und Haftung für Software gibt's generell nicht. Dazu ist Software zu komplex, und auch zu abhängig von anderen Softwarekomponenten, Hardwaresystemen und zu vernetzt. Wo ist nun wirklich die Ursache für einen Schaden, und zu welchem Prozentsatz ist die Softwarelücke schuld? Diese Frage kann im Normalfall kein Gericht zweifelsfrei beantworten.

Haftung für Software wäre so: Ein Auto fährt durch ein Schlagloch; der Reifen platzt. Nun wäre der Autohersteller haftbar, weil er kein Schlaglochwarnsystem eingebaut hat, nicht etwa der Straßenerhalter oder der Lenker, der zu unaufmerksam war.

antworten

rhsraphael vor 7 monaten permalink | melden 0 0

Für Software wird viel zu wenig bezahlt, als dass man dann noch dafür haften könne...

antworten

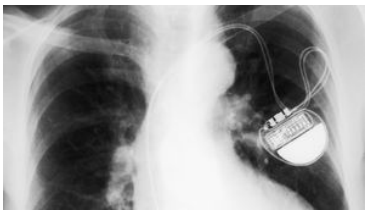
Mehr zum Thema

DEEPSEC

Forscher zeigt: So leicht lassen sich Medizingeräte hacken

Die IT-Sicherheit kommt bei vielen Medizingeräten zu kurz. Bei der Konferenz Deep Sec demonstrierte der Forscher Florian Grunow, wie man einen Patientenmonitor manipuliert.

von Barbara Wimmer



SICHERHEITSKONFERENZ

DeepSec: Vom Herzschrittmacher-Hack bis zum Profiling

Zur Sicherheitskonferenz DeepSec, die von 19. bis 22. November in Wien stattfindet, kommt unter anderem der IT-Sicherheitspionier Marcus J. Ranum.

KRITIK

CCC: Sicherheitslücken-Kauf durch Behörden verbieten

Der Chaos Computer Club kritisiert das Vorgehen der deutschen Bundesregierung scharf. Der Zukauf von "Zero Day Exploits" durch den Bund heize den Markt unnötig an.

Netzpolitik

15.07.2015 13:31 Uhr

JAHRESBERICHT 1

Europarat beklagt Zunahme von Hassreden im Internet

Laut Europarat gab es im Vorjahr eine "beunruhigenden Tendenz zu Hassreden und Ausländerfeindlichkeit im Internet", auch dank der Wahlerfolge populistischer Parteien.

SCHIKANE 1

Snowden-Dokumentarfilmerin Poitras verklagt US-Behörden

Die Filmschaffende verlangt von den US-Behörden Auskunft darüber, warum sie so häufig bei der Einreise in die USA zur Überprüfung festgehalten worden ist.

SICHERHEIT 8

US-Senator fordert Haftung für Verschlüsselung

Der demokratische Senator Sheldon Whitehouse fordert, dass Opfer eines Verbrechens Unternehmen verklagen können, sollte deren Verschlüsselung jemandem Schaden.

POLITIK 2

Hashtag #ThisIsACoup: Heftige Kritik an Griechenland-Deal

Die Forderungen der Gläubiger haben Kritik im Internet ausgelöst. Unter dem Hashtag #ThisIsACoup wurde vor allem über die Rolle Deutschlands in harschen Worten diskutiert.

EU 2

"Die Netzneutralität wird de facto abgeschafft"

Die geplanten EU-Regeln zur Gleichbehandlung aller Daten und Dienste im Internet stoßen auf harsche Kritik.

Featured

VERKEHR

Hier-Box holt bei Autounfällen automatisch Hilfe

Die Hier-Box, ein kleines Gerät zum Nachrüsten, kann bei einem Autounfall selbstständig einen Notruf absetzen. Die Reaktionszeit der Rettung soll so stark verkürzt werden.

von David Kotrba

REPORTAGE

http://www.golem.de/news/messenger-keine-kommunikation-zwischen-whatsapp-und-textsecure-1411-110718.html

Datum:21.11.2014, 12:15

Autor:Jörg Thoma

Messenger

Keine Kommunikation zwischen Whatsapp und Textsecure

Textsecure-Nutzer werden auch künftig nicht mit Whatsapp-Anwendern kommunizieren können. Textsecure soll als eigenständiges Produkt bestehen bleiben. Eine weitere Zusammenarbeit soll es dennoch geben.

Textsecure-Benutzer sollen auch künftig nicht direkt mit Whatsapp-Nutzern verschlüsselt kommunizieren können. Es gebe keine Pläne, das von Open Whispers Systems entwickelte und in Whatsapp integrierte Axolotl-Protokoll gemeinsam zu nutzen. Das sagte Christine Corbett von Open Whisper Systems zu Golem.de am Rande der IT-Sicherheitskonferenz Deepsec 2014 in Wien.

Technisch sei es zwar durchaus möglich, dass die Nutzer beider Messenger direkt kommunizieren könnten, es bestehe aber diesbezüglich von beiden Seiten kein Interesse. Open Whisper Systems wolle sein Axolotl-Protokoll weiterentwickeln und diese Änderungen nicht in Whatsapp erzwingen. Geplant sei jedoch, dass in Whatsapp auch der Gruppenchat künftig verschlüsselt wird. Daran arbeitet Open Whispers Systems gegenwärtig mit seinen etwa neun Kernentwicklern um Moxie Marlinspike.

Die Überraschung bei der Ankündigung, Whatsapp verwende jetzt das von Open Whisper Systems entwickelte Verschlüsselungsprotokoll, sei geplant. Dessen Integration habe bereits vor Monaten begonnen. Die Kryptographie sei aber so gut umgesetzt, dass es niemand gemerkt habe. Es habe keine Fehlermeldung durch Benutzer während der Umstellung gegeben, sagte Corbett.

Open Whisper Systems arbeite gerade vornehmlich an der Version von Textsecure in iOS. Wenn sie fertig ist, wird sie in Signal für iOS integriert. In Signal werden künftig der Messenger Textsecure und die verschlüsselte VoIP-Lösung Redphone vereint. Für Android wird es auch eine Version von Signal geben.

Von der Integration in Whatsapp habe Open Whisper Systems viel Erfahrung über die Skalierbarkeit seines Protokolls gesammelt. Sie soll künftig auch in weitere Funktionen einfließen. So sei beispielsweise geplant, die ge-

genwärtige Abhängigkeit von externen Cloud-Lösungen abzuschaffen. Das sei einer der größten Wünsche aus der Community, habe wegen Personalmangel aber aktuell nur eine niedrige Priorität.

Bislang ist der Markt der mobilen Messenger sehr zersplittert, in aller Regel sind die verschiedenen Systeme nicht miteinander kompatibel. Den Versuch, verschiedene Messenger-Systeme miteinander kompatibel zu gestalten, gab es bereits einmal: Jabber und das dahinterstehende Protokoll XMPP. Doch zuletzt hat Jabber einiges an Unterstützung eingebüßt. In Sachen Verschlüsselung kann das XMPP-Protokoll mit modernen Lösungen wie Textsecure nicht mithalten.

MESSENGER

Keine Kommunikation zwischen Whatsapp und Textsecure

Textsecure-Nutzer werden auch künftig nicht mit Whatsapp-Anwendern kommunizieren können. Textsecure soll als eigenständiges Produkt bestehen bleiben. Eine weitere Zusammenarbeit soll es dennoch geben.

Whatsapp-Nutzer werden nicht mit Textsecure-Anwendern kommunizieren können. (Bild: Stan Honda/AFP/Getty Images)

Datum: 21.11.2014, 12:15
Autor: Jörg Thoma
Themen: Whatsapp, Facebook, Instant Messenger, Jabber, Soziales Netz, Verschlüsselung, VoIP, XMPP, Applikationen, Internet

Textsecure-Benutzer sollen auch künftig nicht direkt mit Whatsapp-Nutzern verschlüsselt kommunizieren können. Es gebe keine Pläne, das von Open Whispers Systems entwickelte und in Whatsapp integrierte Axolotl-Protokoll gemeinsam zu nutzen. Das sagte Christine Corbett von Open Whisper Systems zu Golem.de am Rande der IT-Sicherheitskonferenz Deepsec 2014 in Wien.

Technisch sei es zwar durchaus möglich, dass die Nutzer beider Messenger direkt kommunizieren könnten, es bestehe aber diesbezüglich von beiden Seiten kein Interesse. Open Whisper Systems wolle sein Axolotl-Protokoll weiterentwickeln und diese Änderungen nicht in Whatsapp erzwingen. Geplant sei jedoch, dass in Whatsapp auch der Gruppenchat künftig verschlüsselt wird. Daran arbeitet Open Whispers Systems gegenwärtig mit seinen etwa neun Kernentwicklern um Moxie Marlinspike.

Die Überraschung bei der Ankündigung, Whatsapp verwende jetzt das von Open Whisper Systems entwickelte Verschlüsselungsprotokoll, sei geplant. Dessen Integration habe bereits vor Monaten begonnen. Die Kryptographie sei aber so gut umgesetzt, dass es niemand gemerkt habe. Es habe keine Fehlermeldung durch Benutzer während der Umstellung gegeben, sagte Corbett.

Open Whisper Systems arbeite gerade vornehmlich an der Version von Textsecure in iOS. Wenn sie fertig ist, wird sie in Signal für iOS integriert. In Signal werden künftig der Messenger Textsecure und die verschlüsselte VoIP-Lösung Redphone vereint. Für Android wird es auch eine Version von Signal geben.

Von der Integration in Whatsapp habe Open Whisper Systems viel Erfahrung über die Skalierbarkeit seines Protokolls gesammelt. Sie soll künftig auch in weitere Funktionen einfließen. So sei beispielsweise geplant, die gegenwärtige Abhängigkeit von externen Cloud-Lösungen abzuschaffen. Das sei einer der größten Wünsche aus der Community, habe wegen Personalmangel aber aktuell nur eine niedrige Priorität.

Bislang ist der Markt der mobilen Messenger sehr zersplittert, in aller Regel sind die verschiedenen Systeme nicht miteinander kompatibel. Den Versuch, verschiedene Messenger-Systeme miteinander kompatibel zu gestalten, gab es bereits einmal: Jabber und das dahinterstehende Protokoll XMPP. Doch zuletzt hat Jabber einiges an Unterstützung eingebüßt. In Sachen Verschlüsselung kann das XMPP-Protokoll mit modernen Lösungen wie Textsecure nicht mithalten. ▪

Link: http://derstandard.at/2000008419083/Das-Versagen-der-Politik-in-Fragen-IT-Sicherheit

Deepsec: Das Versagen der Politik bei IT-Sicherheit

ANDREAS PROSCHOFSKY

20. November 2014, 14:00

CCC-Sprecher Neumann attestiert fatalen Interessenskonflikt zwischen Schutzfunktion und Begehrlichkeiten der Geheimdienste

Zum mittlerweile achten Mal wird dieser Tage die IT-Sicherheitskonferenz Deepsec in Wien abgehalten. Neben vielen Fachvorträgen spielen dabei auch grundlegende Themen eine wichtige Rolle. So betont Linus Neumann, Sprecher des Chaos Computer Club, in einem Pressegespräch die gesellschaftspolitische Dimension.

Widerspruch

Durch ihr ambivalentes Verhältnis stünde die Politik der IT-Sicherheit derzeit eher im Wege als sie zu befördern. So sei es bezeichnend, dass dieser Bereich üblicherweise in den Innenministerien angesiedelt ist - und damit exakt dort, wo auch massive Anstrengungen unternommen werden, jegliche Computersicherheit zu unterwandern.

Finanzierung

Ein Beispiel: Der deutsche Bundesnachrichtendienst hat gerade erst angekündigt, in den kommenden Jahren 4,5 Millionen Euro für Zero-Day-Exploits zu Spionagezwecken ausgeben zu wollen. Damit werden aber genau jene Kreise finanziert, die solche Lücken aus finanziellen Motiven gezielt zurückhalten.

Selbstleger. Eine Doppelstrategie in IT-Sicherheitsfragen funktioniere aber schlicht nicht. Wer willentlich Sicherheitslücken in Kauf nehme, um einen Spionagevorteil zu haben, gefährde damit auch die eigene Infrastruktur. Ähnlich verhalte es sich mit Hintertüren wie jene zur "Lawful Interception" bei Telekomunternehmen: Jeder Angreifer wisse, dass es diese gebe, also sei sie ein lohnendes Ziel, da man an einem Punkt garantiert alle Daten bekomme.

Alternativen

Dabei könnten Staaten auch ganz anders agieren. Etwa indem mit öffentlichen Geldern Bug Bounties ausgeschrieben werden, um Sicherheitsforschern einen Anreiz zu geben, diese zu melden, anstatt sie gewinnbringend am Schwarzmarkt zu verkaufen. Immerhin werden aktuell bereits tausende Euros für Zero-Day-Exploits geboten. Den Wert einer Lücke wie Heartbleed würde Neumann gar ab einer Viertel Million Euro beziffern.

Fehlernder Wille

Hohe Preise für Bug Bounties würden zwar zweifellos auch die Preise am Schwarzmarkt steigen lassen, trotzdem zeigt sich der Sicherheitsexperte von den positiven Auswirkungen einer solchen Initiative überzeugt. Immerhin gebe es genügend Personen, die keine bösen Absichten hegen, und lieber auf diesem Weg ihr finanzielles Auskommen finden. Derzeit scheint aber der politische Wille für solche eine proaktive Sicherheitspolitik zu fehlen.

Investitionen

Zumindest ortet Neumann zarte Fortschritte im Unternehmensbereich. Nach dem "Super-GAU" mit Hearbleed und Shellshock hätten endlich die ersten Firmen damit begonnen in die Sicherheit von weit verbreiteten Open-Source-Programmen zu investieren. Aber auch hier gibt es natürlich noch viel Luft nach oben.

(apo, derStandard.at, 20.11.2014)

Deepsec: Das Versagen der Politik bei IT-Sicherheit

ANDREAS PROSCHOFSKY
20. November 2014, 14:02

foto: flickr.com/111692634@n04 (CC-Lizenz)

CCC-Sprecher Neumann attestiert fatalen Interessenskonflikt zwischen Schutzfunktion und Begehrlichkeiten der Geheimdienste

Zum mittlerweile achten Mal wird dieser Tage die IT-Sicherheitskonferenz Deepsec in Wien abgehalten. Neben vielen Fachvorträgen spielen dabei auch grundlegende Themen eine wichtige Rolle. So betont Linus Neumann, Sprecher des Chaos Computer Club, in einem Pressegespräch die gesellschaftspolitische Dimension.

Widerspruch

Durch ihr ambivalentes Verhältnis stünde die Politik der IT-Sicherheit derzeit eher im Wege als sie zu befördern. So sei es bezeichnend, dass dieser Bereich üblicherweise in den Innenministerien angesiedelt ist - und damit exakt dort, wo auch massive Anstrengungen unternommen werden, jegliche Computersicherheit zu unterwandern.

Finanzierung

Ein Beispiel: Der deutsche Bundesnachrichtendienst hat gerade erst angekündigt, in den kommenden Jahren 4,5 Millionen Euro für Zero-Day-Exploits zu Spionagezwecken ausgeben zu wollen. Damit werden aber genau jene Kreise finanziert, die solche Lücken aus finanziellen Motiven gezielt zurückhalten.

Selbstleger

Eine Doppelstrategie in IT-Sicherheitsfragen funktioniere aber schlicht nicht. Wer willentlich Sicherheitslücken in Kauf nehme, um einen Spionagevorteil zu haben, gefährde damit auch die eigene Infrastruktur. Ähnlich verhalte es sich mit Hintertüren wie jene zur "Lawful Interception" bei Telekomunternehmen: Jeder Angreifer wisse, dass es diese gebe, also sei sie ein lohnendes Ziel, da man an einem Punkt garantiert alle Daten bekomme.

Alternativen

Dabei könnten Staaten auch ganz anders agieren. Etwa indem mit öffentlichen Geldern Bug Bounties ausgeschrieben werden, um Sicherheitsforschern einen Anreiz zu geben, diese zu melden, anstatt sie gewinnbringend am Schwarzmarkt zu verkaufen. Immerhin werden aktuell bereits tausende Euros für Zero-Day-Exploits geboten. Den Wert einer Lücke wie Heartbleed würde Neumann gar ab einer Viertel Million Euro beziffern.

Fehlernder Wille

Hohe Preise für Bug Bounties würden zwar zweifellos auch die Preise am Schwarzmarkt steigen lassen, trotzdem zeigt sich der Sicherheitsexperte von den positiven Auswirkungen einer

solchen Initiative überzeugt. Immerhin gebe es genügend Personen, die keine bösen Absichten hegen, und lieber auf diesem Weg ihr finanzielles Auskommen finden. Derzeit scheint aber der politische Wille für solche eine proaktive Sicherheitspolitik zu fehlen.

Investitionen

Zumindest ortet Neumann zarte Fortschritte im Unternehmensbereich. Nach dem "Super-GAU" mit Hearbleed und Shellshock hätten endlich die ersten Firmen damit begonnen in die Sicherheit von weit verbreiteten Open-Source-Programmen zu investieren. Aber auch hier gibt es natürlich noch viel Luft nach oben. (apo, derStandard.at, 20.11.2014)

Link

Deepsec

Aktuelle Spiele finden Sie unter Rätsel & Sudoku

http://futurezone.at/netzpolitik/it-sicherheit-ist-kein-rein-technisches-thema/98.164.615

"IT-Sicherheit ist kein rein technisches Thema"

Florian Christofvon Florian Christof 20.11.14, 13:44

Auf der Sicherheitskonferenz DeepSec wird diagnostiziert, dass IT-Security darniederliegt. Das Thema gehöre breiter diskutiert und an Schulen vermittelt, so ein Vorschlag.

Die IT-Security liegt am Boden und kaum jemanden scheint es zu kümmern. Das war der Tenor bei der Pressekonferenz der diesjährigen Sicherheitskonferenz DeepSec in Wien. Um der IT-Sicherheit auf die Beine zu helfen, schlägt Stefan Schumacher vom Magdeburger Institut für Sicherheitsforschung vor, das Thema breiter zu diskutieren und es als Allgemeinbildung im Lehrplan zu verankern.

Er ist der Ansicht, es sei ein Fehler, zu glauben, IT-Security sei eine durch und durch technische Angelegenheit. Ein Grund für den katastrophalen Zustand der IT-Sicherheitsbranche sei daher, dass meist nur technische Details diskutiert werden, ohne nach langfristigen Lösungen zu suchen.

IT-Security breiter diskutieren

"Nur wenn man aus dem rein technischen Eck herauskommt und IT-Security breiter angeht, um psychologische, pädagogische, politische sowie soziologische Gesichtspunkte erweitert und mit Aspekten des Social Engineering verknüpft, kann es gelingen, nachhaltige Konzepte zu erarbeiten", sagte Schumacher. Daher setzt er sich dafür ein, dass IT-Sicherheit endlich auf wissenschaftlicher Ebene, Disziplin übergreifend diskutiert wird.

Dies sei für Schumacher auch der Ausgangspunkt dafür, dass Informatik im Allgemeinen und IT-Security im Speziellen, als Allgemeinbildung an den Schulen vermittelt wird. "Der heutige Informatikunterricht beschränkt sich meist auf ein bisschen MS Word erklären und eine bunte PowerPoint-Präsentation zu erstellen", kritisiert Schumacher, "Dabei wäre es höchst an der Zeit an den Schulen ein Verständnis für Informatik zu schaffen. Es müsste Grundlegendes gelehrt werden, etwa wie Computer und Netzwerke funktionieren und es müssten dringend auch netzpolitische Themen wie Datenschutz und Privacy vermittelt werden."

Kein Interesse vorhanden

Allerdings vermisst Schumacher dafür den politischen Willen und die Bereitschaft der Lehrer: "In Sachsen-Anhalt wollten wir bereits mehrfach eine Lehrerfortbildung für IT-Vermittlung im Schulunterricht anbieten. Leider ist diese Veranstaltung noch nie zustande gekommen, da das Interesse der Lehrpersonen einfach nicht vorhanden war."

(FUTUREZONE) ERSTELLT AM 20.11.2014, 13:44

DEEPSEC

"IT-Sicherheit ist kein rein technisches Thema"

von Florian Christof 20.11.14, 13:44 FlorianChristof Mail an Autor

Bei IT-Sicherheit gehe es nicht nur um Bits und Bytes - Foto: GETTY IMAGES/ISTOCKPHOTO
ISTOCKPHOTO/PN_Photo/thinkstock

DEEPSEC

"IT-Sicherheit ist kein rein technisches Thema"

KOMMENTARE ()

MEHR ZUM THEMA

Auf der Sicherheitskonferenz DeepSec wird diagnostiziert, dass IT-Security darniederliegt. Das Thema gehöre breiter diskutiert und an Schulen vermittelt, so ein Vorschlag.

SCHULE, IT-SECURITY, IT-SICHERHEIT

Die IT-Security liegt am Boden und kaum jemanden scheint es zu kümmern. Das war der Tenor bei der Pressekonferenz der diesjährigen Sicherheitskonferenz DeepSec in Wien. Um der IT-Sicherheit auf die Beine zu helfen, schlägt Stefan Schumacher vom Magdeburger Institut für Sicherheitsforschung vor, das Thema breiter zu diskutieren und es als Allgemeinbildung im Lehrplan zu verankern.

Er ist der Ansicht, es sei ein Fehler, zu glauben, IT-Security sei eine durch und durch technische Angelegenheit. Ein Grund für den katastrophalen Zustand der IT-Sicherheitsbranche sei daher, dass meist nur technische Details diskutiert werden, ohne nach langfristigen Lösungen zu suchen.

IT-Security breiter diskutieren

"Nur wenn man aus dem rein technischen Eck herauskommt und IT-Security breiter angeht, um psychologische, pädagogische, politische sowie soziologische Gesichtspunkte erweitert und mit Aspekten des Social Engineering verknüpft, kann es gelingen, nachhaltige Konzepte zu erarbeiten", sagte Schumacher. Daher setzt er sich dafür ein, dass IT-Sicherheit endlich auf wissenschaftlicher Ebene, Disziplin übergreifend diskutiert wird.

Dies sei für Schumacher auch der Ausgangspunkt dafür, dass Informatik im Allgemeinen und IT-Security im Speziellen, als Allgemeinbildung an den Schulen vermittelt wird. "Der heutige Informatikunterricht beschränkt sich meist auf ein bisschen MS Word erklären und eine bunte PowerPoint-Präsentation zu erstellen", kritisiert Schumacher, "Dabei wäre es höchst an der Zeit an den Schulen ein Verständnis für Informatik zu schaffen. Es müsste Grundlegendes gelehrt werden, etwa wie Computer und Netzwerke funktionieren und es müssten dringend auch netzpolitische Themen wie Datenschutz und Privacy vermittelt werden."

Kein Interesse vorhanden

FEATURED

VERKEHR
Hier-Box holt bei Autounfällen automatisch Hilfe

REPORTAGE
Buffalo: „Stadt des Lichts" kämpft gegen den Rost

AKTION
Facebook-Video zeigt waghalsige Aktion im AKW Zwentendorf

Allerdings vermisst Schumacher dafür den politischen Willen und die Bereitschaft der Lehrer: "In Sachsen-Anhalt wollten wir bereits mehrfach eine Lehrerfortbildung für IT-Vermittlung im Schulunterricht anbieten. Leider ist diese Veranstaltung noch nie zustande gekommen, da das Interesse der Lehrpersonen einfach nicht vorhanden war."

(FUTUREZONE) ERSTELLT AM 20.11.2014, 13:44

SCHULE, IT-SECURITY, IT-SICHERHEIT

Kommentare ()

Ihr Kommentar
Bitte loggen Sie sich ein

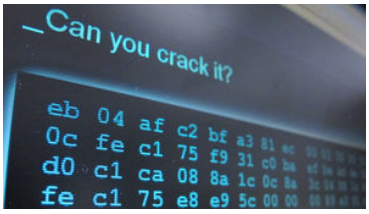
Mehr zum Thema

DEEPSEC

Forscher zeigt: So leicht lassen sich Medizingeräte hacken

Die IT-Sicherheit kommt bei vielen Medizingeräten zu kurz. Bei der Konferenz Deep Sec demonstrierte der Forscher Florian Grunow, wie man einen Patientenmonitor manipuliert.

von Barbara Wimmer



DEEPSEC

"White Hat Hacking ist nicht lukrativ genug"

Bei der DeepSec-Konferenz forderte Linus Neumann vom CCC, Anreize für das Aufdecken von Schwachstellen massiv zu erhöhen und sieht Interessenskonflikte im Innenministerium.

von Florian Christof

IT-SICHERHEIT

"Firmen müssen akzeptieren, dass Netzwerke knackbar sind"

Die IT-Infrastruktur von Firmen ist neuen Herausforderungen ausgesetzt. Thomas Hackner erläutert beim Security Forum des Hagenberger Kreises der FH Oberösterreich ...

von Markus Keßler

Netzpolitik

15.07.2015 13:38 Uhr

SICHERHEIT

US-Senator fordert Haftung für Verschlüsselung

8

Der demokratische Senator Sheldon Whitehouse fordert, dass Opfer eines Verbrechens Unternehmen verklagen können, sollte deren Verschlüsselung jemandem Schaden.

TELEKOM-PAKET

Kritik: Roaming-Abschaffung ist nur Formalität

EU-Parlamentarier der SPÖ, Grüne und ÖVP zeigen sich am Mittwoch - wenn auch aus unterschiedlichen Gründen - enttäuscht über die Entwicklungen bei Roaming und ...

SCHIKANE

Snowden-Dokumentarfilmerin Poitras verklagt US-Behörden

1

Die Filmschaffende verlangt von den US-Behörden Auskunft darüber, warum sie so häufig bei der Einreise in die USA zur Überprüfung festgehalten worden ist.

Featured

VERKEHR

Hier-Box holt bei Autounfällen automatisch Hilfe

Die Hier-Box, ein kleines Gerät zum Nachrüsten, kann bei einem Autounfall selbstständig einen Notruf absetzen. Die Reaktionszeit der Rettung soll so stark verkürzt werden.

von David Kotrba

Link: http://www.computerwelt.at/news/technologie-strategie/security/detail/artikel/106898-sicherheitskonferenz-deepsec-legt-fokus-auf-kommunikation-und-wissen/

Sicherheitskonferenz DeepSec legt Fokus auf Kommunikation und Wissen

03.11.2014 pi/Rudolf Felser

Bereits zum achten Mal versammelt die internationale Sicherheitskonferenz DeepSec vom 18. bis 21. November 2014 in Wien die Weltelite aus den Bereich der IT-Security.

Die Konferenz DeepSec versteht sich als neutrale Plattform die Hacker-Community, IT-/Security Unternehmen, Behördenvertreter sowie Forscher in Vorträgen und Workshops zum Gedanken- und Erfahrungsaustausch zusammenbringt. Wie kann man sich solch eine internationale IT-Sicherheitskonferenz vorstellen? "Die DeepSec funktioniert wie eine große Börse, auf der Lösungen und Abhilfe für brennende Sicherheitsprobleme diskutiert und ausgetauscht werden", so René Pfeiffer, Sicherheitsexperte und einer der Organisatoren der Konferenz. "Alles dreht sich um Informationen und Informationstechnologie: Man erhält kompetente Antworten von Experten, gepaart mit Demonstrationen von Schwachstellen, auf die Unternehmen reagieren müssen."

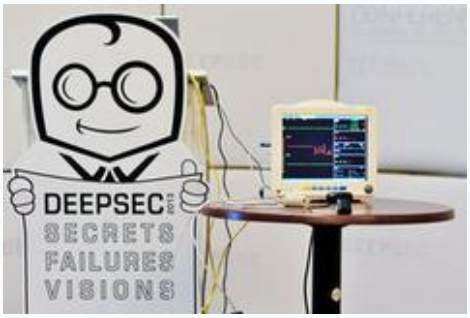
Die Highlights des Programms thematisieren Hintertüren in Serverhardware, Schwachstellen in kryptographischen Anwendungen, Schwächen im Internetprotokoll der nächsten Generation (IPv6), Aufspüren von Schadsoftware und neue Wege vernetzte Systeme zu kompromittieren. Teile der Inhalte haben ihre Premiere zur DeepSec und wurden bisher noch nicht öffentlich diskutiert.

Vor der Konferenz finden zweitägige Workshops statt, in denen Trainer mit den Teilnehmern ausgewählte Inhalte durchgehen. Die Trainings sind nicht nur passive Vorlesungstage sondern Unterricht zum Anfassen und Ausprobieren. Alle Teilnehmer lernen persönlich betreut an Beispiele aus der realen Welt. An den zwei darauf folgenden Tagen findet die eigentliche Konferenz statt. Über 30 Vorträgen zeigen aktuellen Bedrohungen im Bereich der Informationstechnologie und darüber hinaus. (pi)

03.11.2014 *pi/Rudolf Felser*

Sicherheitskonferenz DeepSec legt Fokus auf Kommunikation und Wissen

Bereits zum achten Mal versammelt die internationale Sicherheitskonferenz DeepSec vom 18. bis 21. November 2014 in Wien die Weltelite aus den Bereich der IT-Security.



DeepSec: Vortrag zu Schwachstellen medizinischer Geräte
© Joanna Pianka

Die Konferenz DeepSec versteht sich als neutrale Plattform die Hacker-Community, IT-/Security Unternehmen, Behördenvertreter sowie Forscher in Vorträgen und Workshops zum Gedanken- und Erfahrungsaustausch zusammenbringt. Wie kann man sich solch eine internationale IT-Sicherheitskonferenz vorstellen? "Die DeepSec funktioniert wie eine große Börse, auf der Lösungen und Abhilfe für brennende Sicherheitsprobleme diskutiert und ausgetauscht werden", so René Pfeiffer, Sicherheitsexperte und einer der Organisatoren der Konferenz. "Alles dreht sich um Informationen und Informationstechnologie: Man erhält kompetente Antworten von Experten, gepaart mit Demonstrationen von Schwachstellen, auf die Unternehmen reagieren müssen."

Die Highlights des Programms thematisieren Hintertüren in Serverhardware, Schwachstellen in kryptographischen Anwendungen, Schwächen im Internetprotokoll der nächsten Generation (IPv6), Aufspüren von Schadsoftware und neue Wege vernetzte Systeme zu kompromittieren. Teile der Inhalte haben ihre Premiere zur DeepSec und wurden bisher noch nicht öffentlich diskutiert.

Vor der Konferenz finden zweitägige Workshops statt, in denen Trainer mit den Teilnehmern ausgewählte Inhalte durchgehen. Die Trainings sind nicht nur passive Vorlesungstage sondern Unterricht zum Anfassen und Ausprobieren. Alle Teilnehmer lernen persönlich betreut an Beispiele aus der realen Welt. An den zwei darauf folgenden Tagen findet die eigentliche Konferenz statt. Über 30 Vorträgen zeigen aktuellen Bedrohungen im Bereich der Informationstechnologie und darüber hinaus. (pi)

http://oe1.orf.at/programm/372733

Radiokolleg - Schutz durch Spionage?

Montag

19. Mai 2014

09:05

Die Macht der Geheimdienste (1). Gestaltung: Sonja Bettel

René Pfeiffer, Dienstleister und Lektor für die Sicherheit von Informationstechnologien und Organisator der Wiener Sicherheitskonferenz DeepSec, über Angriffsmöglichkeiten durch Geheimdienste und Möglichkeiten und Grenzen des Schutzes vor Überwachung.

Zwischen Stasi und NSA

Viele Menschen lieben Bücher und Filme über Geheimdienste und vor allem über ihre Protagonisten, die Spione. Sie sind lässige Womanizer wie James Bond, eiskalte Killer wie Jason Bourne und überleben die schlimmsten Anschläge, wie Ethan Hunt in "Mission: Impossible". Spezialwaffen, schöne Frauen, schnelle Autos, Flugzeuge, versteckte Kameras und Tonbandgeräte, ein gestählter Körper und alle Psycho-Tricks der Welt sind selbstverständlich inbegriffen.

Doch wie sieht das Leben von Agenten und Agentinnen im wirklichen Leben aus? Warum und seit wann gibt es Geheimdienste und wie sind sie organisiert? Und was leisten sie überhaupt? Nach den Snowden-Enthüllungen über die NSA, die National Security Agency der USA, die lange Zeit so geheim war, dass sie ihre eigene Existenz leugnete, stellen sich dazu viele Fragen. Denn das Bild, das durch die Enthüllungen entstand, ist eher jenes von gelangweilten Beamt/innen, die in Hochsicherheitsgebäuden Computerprogramme und Server betreuen, die jeden Tag mehrere Petabyte an Kommunikationsdaten aus aller Welt absaugen, durchsuchen und speichern.

In den vergangenen Jahren sind aber auch Bilder von Geheimdiensten entstanden, die Menschen aus westlichen Demokratien entführen und in Diktaturen auf Auftrag foltern und verschwinden lassen. Es drängen sich unweigerlich Vergleiche auf zwischen der teils gefürchteten und teils belächelten Stasi der ehemaligen DDR und dem riesigen Überwachungs- und Spionageapparat der heutigen USA.

Sind Geheimdienste unvermeidlich? Können wir sie kontrollieren? Und wie viel "intelligence" liefern sie überhaupt angesichts der Datenflut heutiger elektronischer Kommunikation?

Gestaltung: Sonja Bettel · zur Sendereihe

Standort: oe1.ORF.at

OE1 ORF.at

Navigation

Radiokolleg - Schutz durch Spionage?

Montag
19. Mai 2014
09:05

Die Macht der Geheimdienste (1). Gestaltung: Sonja Bettel

(c) Schimmer, ORF

Audio als mp3

AUDIO 19:54
Externer Player

René Pfeiffer, Dienstleister und Lektor für die Sicherheit von Informationstechnologien und Organisator der Wiener Sicherheitskonferenz DeepSec, über Angriffsmöglichkeiten durch Geheimdienste und Möglichkeiten und Grenzen des Schutzes vor Überwachung.

Zwischen Stasi und NSA

Viele Menschen lieben Bücher und Filme über Geheimdienste und vor allem über ihre Protagonisten, die Spione. Sie sind lässige Womanizer wie James Bond, eiskalte Killer wie Jason Bourne und überleben die schlimmsten Anschläge, wie Ethan Hunt in "Mission: Impossible". Spezialwaffen, schöne Frauen, schnelle Autos, Flugzeuge, versteckte Kameras und Tonbandgeräte, ein gestählter Körper und alle Psycho-Tricks der Welt sind selbstverständlich inbegriffen.

Doch wie sieht das Leben von Agenten und Agentinnen im wirklichen Leben aus? Warum und seit wann gibt es Geheimdienste und wie sind sie organisiert? Und was leisten sie überhaupt? Nach den Snowden-Enthüllungen über die NSA, die National Security Agency der USA, die lange Zeit so geheim war, dass sie ihre eigene Existenz leugnete, stellen sich dazu viele Fragen. Denn das Bild, das durch die Enthüllungen entstand, ist eher jenes von gelangweilten Beamt/innen, die in Hochsicherheitsgebäuden Computerprogramme und Server betreuen, die jeden Tag mehrere Petabyte an Kommunikationsdaten aus aller Welt absaugen, durchsuchen und speichern.

(c) Gebert, DPA

In den vergangenen Jahren sind aber auch Bilder von Geheimdiensten entstanden, die Menschen aus westlichen Demokratien entführen und in Diktaturen auf Auftrag foltern und verschwinden lassen. Es drängen sich unweigerlich Vergleiche auf zwischen der teils gefürchteten und teils belächelten Stasi der ehemaligen DDR und dem riesigen Überwachungs- und Spionageapparat der heutigen USA.

Sind Geheimdienste unvermeidlich? Können wir sie kontrollieren? Und wie viel "intelligence" liefern sie überhaupt angesichts der Datenflut heutiger elektronischer Kommunikation?

zurück

Gestaltung: Sonja Bettel · zur Sendereihe

Kategorie: Wissen

http://fm4.orf.at/stories/1737330/

Der neueste Unsicherheitsstandard der NSA

Der aktuell beim Gremium für Internetstandards IETF eingereichte Entwurf der NSA für verschlüsselte Internettelefonie ist an Dreistigkeit kaum zu überbieten.

Langsam zeichnet sich hinter dem Agieren der NSA-Techniker in Standardisierungsgremien wie der "Internet Engineering Task Force" (IETF) eine Methodik ab. Die ist verblüffend einfach, geradlinig und strukturell ganz ähnlich auch in anderen Entwürfen der NSA anzutreffen. Auch der neueste Standardentwurf, den ein mittlerweile bekannter NSA-Techniker namens Kevin Igoe am 1. April 2014 bei der IETF eingereicht hatte, zeigt ein solches Muster.

Dieser aktuelle NSA-Entwurf betrifft das Protokoll zur Verschlüsselung von Internettelefonie. Der dafür vorgesehene Blockchiffre-Modus namens "Galois Counter Mode" (GCM) aber wurde bereits 2005 von einem namhaften Kryptografie-Eperten von Microsoft als generell angreifbar bezeichnet und vernichtend kritisiert. Speziell und eindringlich wurde davor gewarnt, diese Chiffre für Echtzeit-Protokolle einzusetzen, als negatives Praxisbeispiel dafür wurde die Verschlüsselung von Internettelefonie angeführt.

Die Methodik der NSA

Neun Jahre danach schlägt die NSA nun genau jenen Chiffriermodus GCM als Kernelement eines internationalen Verschlüsselungstandards für Internettelefonie vor. Und das, obwohl mehrere andere Chiffriermodi für diesen Zweck zur Verfügung stehen, die gerade diese Schwächen nicht aufweisen. Das entspricht der darunterliegenden, grundlegenden Methodik der NSA, die potentiell verheerende Wirkung dieser Vorgehensweise wurde von einem internationalen Forscherteam erst Ende März in der Praxis nachgewiesen.

TextCC IETF

Stets sind es zwei oder mehr verschiedene Komponenten des Verschlüsselungsvorgangs, die ihre Wirkung erst in ihrer Kombination entfalten. Und stets war mindestens eines dieser Elemente bereits davor in die Kritik der Fachwelt geraten, was die NSA jedoch nicht davon abgehalten hat, "verbesserte" Versionen davon erneut aufs Tapet zu bringen. Im Praxistest des Kryptografenteams, der nur einen Tag vor der Einreichung des aktuellen NSA-Standardvorschlags für verschlüsselte VoIP-Telefonie veröffentlicht wurde, wird dieses Muster ersichtlich.

Der aktuelle IETF-Entwurf für SRTP mit dem Blockchiffriermodus "Galois Counter Mode"

Wenn zwei Faktoren zusammentreffen

Der Test betraf den Zufallszahlengenerator "Dual EC DRBG", der von der NSA stammt und seit Anbeginn im Verdacht stand, letztlich berechenbare "Zufallszahlen" zu erzeugen. Mit der Qualität, also dem Grad der Zufälligkeit dieser Zahlen, aber steht und fällt jeder Verschlüsselungsvorgang. Ein im Vergleich zu NSA-Equipment mickriger Angriffsrechner mit 14 Prozessoren, der von den Forschern eingesetzt wurde, benötigte zwischen einer und drei Stunden um diesen in die BSAFe-Suite der Firma RSA integrierten Zahlengenerator zu knacken.

Im Rahmen des "Bullrun"-Programms, das gerade unter Netzwerkern für besondere Empörung gesorgt hat, schleusen NSA-nahe Techniker möglichst plausible Erweiterungen in bestehende Verschlüsselungsprotokolle ein, um diese auszuhebeln. Die Kombination von "Dual EC DRBG" und "Extended Random" im Detail.

Das eigentlich Verblüffende aber passierte, als in dieses Set-Up noch eine Erweiterung des für alle möglichen Arten von Verschlüsselung verwendeten Protokolls TLS/SSL integriert wurde. Diese ebenfalls von der NSA stammende Protokollerweiterung namens "Extended Random" beschleunigte den Entschlüsselungsvorgang um den Faktor 65.000. Damit dauerte es gerade noch vier Sekunden, um den Output von "Dual EC DRBG" zu berechnen.

Knackpunkt Chiffriermodus

Der neueste Entwurf der NSA bei der IETF weist strukturell ganz ähnliche Züge auf, auch wenn der Knackpunkt hier ein ganz anderes Element des Verschlüsselungsvorgangs betrifft, nämlich Blockchiffre-Modi und ihre Verkettung. Der aktuelle Entwurf Igoes bezieht sich auf Verschlüsselung und Authentifizierung im "Secure Real Time Protocol" (SRTP). Das ist die verschlüsselte Variante der herkömmlichen Internettelefonie (VoIP), die das RTP-Protokoll benutzt.

Das "Bullrun"-Projekt der NSA-Projekt sieht dem "Cloud-Überwachungsstandard" des European Telecom Standards Institute frappierend ähnlich. Erst seit den Enthüllungen Edward Snowdens sind Name und Mission dieses Projekts von NSA und GCHQ bekannt

Dabei soll nach dem Willen der NSA der "Galois Counter Mode" (GCM) als Modus zum Einsatz kommen, der als besonders schlank und schnell gilt und einen hohen Datendurchsatz verspricht. GCM hat deshalb bei Cloud-

Anwendungen Verbreitung, als Vorteil wird dabei hervorgehoben, dass GCM für Parallel-Computing gut geeignet ist. Ebenso ist ein Einsatz in rechenschwachen Umgebungen, also "Embedded"-Geräten denkbar. GCM hat also durchaus dort Meriten, wo Rechen- und Datendurchsatzzeiten absolut kritische Faktoren sind. Dafür wurde der Modus nämlich entwickelt. Die Schnelligkeit din diesem Chiffriermodus wird freilich dadurch erzielt, dass Authentifizierung und Verschlüsselung mit einer einzigen Funktion abgewickelt werden.

Zwei Anwendungen in einer

"Bei Anwendungen, die robuste Sicherheit verlangen, ist das unüblich", sagte der Wiener Sicherheitsexperte Michael Kafka zu ORF.at, "Man hat diese beiden Funktionen immer schon deshalb getrennt gehalten, weil Angriffe dadurch erschwert werden." Die durch die Schlankheit von GCM gewonnene Rechengeschwindigkeit könne bei VoIP-Telefonie so eher einem Angreifer zu Gute kommen, so Kafka weiter, während sich der Vorteil von GCM für die Abwicklung gerade von Internettelefonie in marginalen Grenzen halte.

Anders als etwa beim Cloud-Computing, wo gewaltige Datenmengen ver- und entschlüsselt werden müssen, nehmen sich die bei VoIP-Telefonie anfallenden Daten nachgerade verschwindend aus. Angesichts der Leistungsfähigkeit der Prozessoren in heute gängigen Smartphones falle dieser Gewinn an Performance deshalb in der Praxis überhaupt nicht mehr ins Gewicht, sagte Kafka.

"Galois Counter Mode"

Der grundsätzliche Vorteil der "Galois Counter Mode"-Methode, nämlich Effizienz und hoher Datendurchsatz kommt unter diesen Voraussetzungen also eben nicht zum Tragen, während sich die Nachteile gerade bei einem Echtzeitprotokoll wie SRTP multiplizieren. Auch hier gibt es auffällige Parallelen zum Fall des anrüchigen Zahlengenerators "Dual EC DRBG".

Eine 2008 von der NSA eingereichte Erweiterung des TLS/SSL-Protokolls namens "Extended Random" war von den in der IETF vertretenen, großteils zivilen Technikern letzlich deshalb abgelehnt worden, weil keine praktischen Vorteile dafür erkennbar waren. Wie der Feldversuch der Forscher nun zeigte, hatte "Extended Random" nur einen einzigen "Vorteil": Ein Angriff der NSA auf den Verschlüsselungsvorgang wurde um den Faktor 65.000 beschleunigt.

Negatives Musterbeispiel anno 2005

Bereits 2005 hatte der bekannte Kryptograf Niels Ferguson von Microsoft zwei grundlegende Schwächen gegenüber Angriffen in "Galois Counter Mode" nachgewiesen und vor dem Einsatz von GCM als universellem

Modus für kryptografische Blockchiffren gewarnt. Als negatives Musterbeispiel dafür führte Ferguson damals den möglichen Einsatz von GCM bei verschlüsselter Internettelefonie an.

TextMicrosoft

Das Gutachten Niels Fergusons im Volltext: "Authentication weaknesses in GCM"

Weil die Schwäche besonders eklatant zu Tage tritt, wenn zu kurze "Authentifizierungs-Tags" verwendet werden, riet Ferguson: "Wenn man umständehalber gezwungen ist, GCM einzusetzen, sollte man den Modus ausschließlich mit 128-Bit langen Tags benützen." Grundsätzlich riet der holländische Kryptograf vom Einsatz dieses Modus überhaupt ab und empfahl andere Blockchiffre-Modi zu benützen, die diese Schwächen eben nicht aufwiesen.

Wie GCM zum NIST-Standard wurde

2007 wurde GCM dennoch durch die US-Standardisierungsbehörde NIST in den Rang eines nationalen Standards erhoben, sieben Jahre danach, am 1. April 2014 schlug nun die NSA "Galois Counter Mode" ausgerechnet für jene Anwendung vor, für die man GCM laut Ferguson und einer Reihe anderer Fachleute auf keinen Fall einsetzen sollte.

Galois Counter Mode, NIST-Standard SP 800-38D

Wie auf dem Screenshot des aktuellen NSA-Entwurfs nun zu sehen ist, sind auch nicht wie 2005 empfohlen, ausschließlich 128-Bit sondern auch 64-Bit lange Tags für die Authentifizierung vorgesehen. Was auf den ersten Blick nur doppelt so viel ist, ergibt bei einer Exponentialrechnung doch deutlich mehr. "Der Unterschied zwischen 64 und 128 langen Tags ergibt eine Zahl mit 20 Nullen vor dem Komma. Ein solcher Faktor im Trillionenbereich macht dann doch einen gewaltigen Unterschied, wenn angegriffen wird" sagte Kafka.

TabelleCC IETF

Michael Kafka ist internationaler Sicherheitsexperte und Mitveranstalter der Wiener Deepsec-Konferenz deren Motto ist "Bleeding Edge Security"

Unangebrachte Schlüsse

Der aktuelle Entwurf für diesen internationalen Standard bei der IETF verzeichnet neben dem NSA-Mann Kevin Igoe noch einen zweiten Namen, nämlich den des Cisco-Technikers David McGrew. Die vorschnelle Annahme,

dass sich da Cisco mit der NSA zusammengetan hätte, um sichere Verschlüsselung zu sabotieren, wäre jedoch grundverkehrt.

Wie die Praxis in den Arbeitsgruppen der IETF zeigt, wird (nicht nur) bei kryptografiebezogenen Einreichungen dem jeweiligen Vertschlüsselungsexperten auch ein Spezialist für die Ebene der Protokolle beigestellt. Heißt die einreichende Partei dann NSA kommt eben auch ein ziviler Techniker zum Handkuss, der mit der Einreichung selbst eigentlich nichts zu tun hat, außer sie in die Protokolle zu integrieren. Im Falle von "Extended Random" kam zum Beispiel ein Protokollspezialist der Mozilla Foundation zur zweifelhaften Ehre, als Koautor einer Einreichung der hochrangigen NSA-Technikerin Margaret Salter zu firmieren.

Wie Techniker unter Druck geraten

Im Falle von McGrew erwies sich diese Vorgangsweise, die von der NSA benützt wird, als besonders perfid. McGrew ist nämlich Koautor von "Galois Counter Mode", um dessen Einsatz sich der gesamte NSA-Entwurf ja dreht. Hier sieht man, unter welchen Druck der weltweit insgesamt recht kleine Kreis von Verschlüsselungsspezialisten durch die NSA geraten ist. Im Dezember hatte einer Reihe ziviler Techniker in der IETF gegen diese Art von Einflussnahme durch die NSA rebelliert und die Absetzung Kevin Igoes als zweiten Vorsitzenden der IETF-Forschungsgruppe für Kryptografie gefordert.

Die Forderung nach Absetzung Igoes auf der Mailing-Liste, samt dem Thead mit den Antworten der anderen Techniker

Igoe hatte einen Entwurf für ein passwortbasiertes Protokoll zum Schlüsselaustausch namens "Dragonfly" präsentiert, das er als einziger, der in der Forschungsgruppe versammelten Techniker für gut befunden hatte. Während der Konsens dort lautete, Dragonfly sei "ein schlampig gearbeitetes und unseriöses Protokoll" hatte Igoe versucht, es der übergeordneten TLS-Arbeitsgruppe in der IETF als Konsens der Kryptospezialisten zu verkaufen.

Die Dreistigkeit der NSA

Mit dem aktuellen Vorschlag, ausgerechnet "Galois Counter Mode" für verschlüsselte Internettelefonie zu verwenden hat Igoe seine damalige Vorgangsweise an Dreistigkeit noch übertroffen. Den Kopf mit dafür hinhalten muss nun Cisco-Techniker McGrew, der GCM für völlig andere Zwecke miterfunden hat.

Dass vordergründige Konspirationsthesen hier überhaupt nicht greifen, zeigt die Erwähnung McGrews in der

Expertise des Microsoft-Technikers Niels Ferguson. Unter der Handvoll von Experten, bei denen sich Ferguson für die technische Unterstützung bei seiner vernichtenden Analyse von "Galois Counter Mode" bedankte, war auch der Koautor von GCM, David McGrew.

Parallelen zu SSH

Der finnische Kryptograf Markku-Juhani Saarinen hatte 2012 auf der Sicherheitskonferenz FSE 2012 in Washington ebenfalls vor dem Einsatz der Blockchiffre gewarnt. Gerade bei Echtzeitprotokollen wie Secure Shell für Virtual Private Networks sei von GCM dringend abzuraten. "Wenn tatsächlich rationale Gründe für den Einsatz von GCM vorlägen, etwa in Hochgeschwindigkeits-VPNs" dann sollte das nur geschehen, wenn vorher eine Risikoabschätzung stattgefunden haben, hieß es in Saarinens Vortrag.

RFC 5647 der IETF CC IETF 2009

Die NSA-Techniker Kevin Igoe und Jerry Salinas waren von solchen Überlegungen offenbar nicht geplagt. Im Frühjahr 2009 wurde von beiden der Entwurf RFC 5647 bei der IETF eingereicht und im August dort durchgewunken. Der Titel: "Galois Counter Mode" für das Secure Shell Layer Protocol".

Der Vortrag Saarinens auf der FSE-Konferenz 2009 und der RFC 5647 der IETF

Das Bombardierkäfer-Prinzip

Niels Ferguson wiederum war einer der beiden Microsoft-Spezialisten, die bereits 2007 vor dem anrüchigen NSA-Zufallszahlengenerator "Dual EC DRBG" gewarnt hatten. Eine wirklich verheerende Wirkung entfaltete der erst in Kombination mit der Erweiterung "Extended Random" von 2008. Der Wiener Sicherheitsexperte Michael Kafka nennt dies das "Bombardierkäfer-Prinzip".

Der Bombardierkäfer in der Wikipedia

Der Abwehrmechanismus dieser Laufkäferart besteht darin, zwei jeweils für sich gesehen harmlose Flüssigkeiten getrennt im Körper vorzuhalten. Wenn sie jedoch vermischt und ausgespritzt werden, erhitzt sich diese Mischung plötzlich auf etwa 100 Grad wobei sie obendrein noch stark ätzend wirkt.

Erstellt am: 21. 4. 2014 - 19:00 Uhr

Der neueste Unsicherheitsstandard der NSA

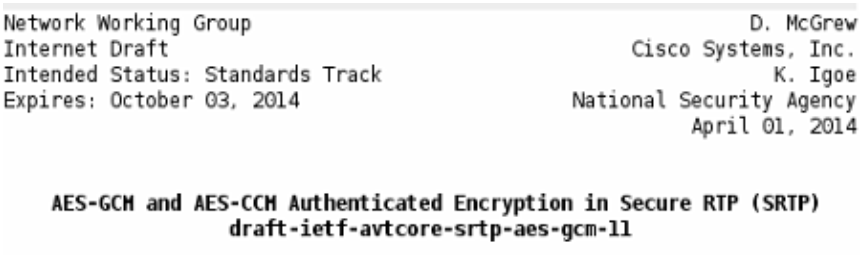
Der aktuell beim Gremium für Internetstandards IETF eingereichte Entwurf der NSA für verschlüsselte Internettelefonie ist an Dreistigkeit kaum zu überbieten.

Langsam zeichnet sich hinter dem Agieren der NSA-Techniker in Standardisierungsgremien wie der "Internet Engineering Task Force" (IETF) eine Methodik ab. Die ist verblüffend einfach, geradlinig und strukturell ganz ähnlich auch in anderen Entwürfen der NSA anzutreffen. Auch der neueste Standardentwurf, den ein mittlerweile bekannter NSA-Techniker namens Kevin Igoe am 1. April 2014 bei der IETF eingereicht hatte, zeigt ein solches Muster.

Dieser aktuelle NSA-Entwurf betrifft das Protokoll zur Verschlüsselung von Internettelefonie. Der dafür vorgesehene Blockchiffre-Modus namens "Galois Counter Mode" (GCM) aber wurde bereits 2005 von einem namhaften Kryptografie-Eperten von Microsoft als generell angreifbar bezeichnet und vernichtend kritisiert. Speziell und eindringlich wurde davor gewarnt, diese Chiffre für Echtzeit-Protokolle einzusetzen, als negatives Praxisbeispiel dafür wurde die Verschlüsselung von Internettelefonie angeführt.

Die Methodik der NSA

Neun Jahre danach schlägt die NSA nun genau jenen Chiffriermodus GCM als Kernelement eines internationalen Verschlüsselungstandards für Internettelefonie vor. Und das, obwohl mehrere andere Chiffriermodi für diesen Zweck zur Verfügung stehen, die gerade diese Schwächen nicht aufweisen. Das entspricht der darunterliegenden, grundlegenden Methodik der NSA, die potentiell verheerende Wirkung dieser Vorgehensweise wurde von einem internationalen Forscherteam erst Ende März in der Praxis nachgewiesen.



Network Working Group D. McGrew
Internet Draft Cisco Systems, Inc.
Intended Status: Standards Track K. Igoe
Expires: October 03, 2014 National Security Agency
April 01, 2014

AES-GCM and AES-CCM Authenticated Encryption in Secure RTP (SRTP)
draft-ietf-avtcore-srtp-aes-gcm-11

CC IETF

Stets sind es zwei oder mehr verschiedene Komponenten des Verschlüsselungsvorgangs, die ihre Wirkung erst in ihrer Kombination entfalten. Und stets war mindestens eines dieser Elemente bereits davor in die Kritik der Fachwelt geraten, was die NSA jedoch nicht davon abgehalten hat, "verbesserte" Versionen davon erneut aufs Tapet zu bringen. Im Praxistest des Kryptografenteams, der nur einen Tag vor der Einreichung des aktuellen NSA-Standardvorschlags für verschlüsselte VoIP-Telefonie veröffentlicht wurde, wird dieses Muster ersichtlich.

Der aktuelle IETF-Entwurf für SRTP mit dem Blockchiffriermodus "Galois Counter Mode" (http://tools.ietf.org/html/draft-ietf-avtcore-srtp-aes-gcm-11)

Wenn zwei Faktoren zusammentreffen

Der Test betraf den Zufallszahlengenerator "Dual EC DRBG", der von der NSA stammt und seit Anbeginn im Verdacht stand, letztlich berechenbare "Zufallszahlen" zu erzeugen. Mit der Qualität, also dem Grad der Zufälligkeit dieser Zahlen, aber steht und fällt jeder Verschlüsselungsvorgang. Ein im Vergleich zu NSA-Equipment mickriger Angriffsrechner mit 14 Prozessoren, der von den Forschern eingesetzt wurde, benötigte zwischen einer und drei Stunden um diesen in die BSAFe-Suite der Firma RSA integrierten Zahlengenerator zu knacken.

Im Rahmen des "Bullrun"-Programms, das gerade unter Netzwerkern für besondere Empörung gesorgt hat, schleusen NSA-nahe Techniker möglichst plausible Erweiterungen in bestehende Verschlüsselungsprotokolle ein, um diese auszuhebeln. Die Kombination von "Dual EC DRBG" und "Extended Random" im Detail.

Das eigentlich Verblüffende aber passierte, als in dieses Set-Up noch eine Erweiterung des für alle möglichen Arten von Verschlüsselung verwendeten Protokolls TLS/SSL integriert wurde. Diese ebenfalls von der NSA stammende Protokollerweiterung namens "Extended Random" beschleunigte den Entschlüsselungsvorgang um den Faktor 65.000. Damit dauerte es gerade noch vier Sekunden, um den Output von "Dual EC DRBG" zu berechnen.

Knackpunkt Chiffriermodus

Der neueste Entwurf der NSA bei der IETF weist strukturell ganz ähnliche Züge auf, auch wenn der Knackpunkt hier ein ganz anderes Element des Verschlüsselungsvorgangs betrifft, nämlich Blockchiffre-Modi und ihre Verkettung. Der aktuelle Entwurf Igoes bezieht sich auf Verschlüsselung und Authentifizierung im "Secure Real Time Protocol" (SRTP). Das ist die verschlüsselte Variante der herkömmlichen Internettelefonie (VoIP), die das RTP-Protokoll benutzt.

Das "Bullrun"-Projekt der NSA-Projekt sieht dem "Cloud-Überwachungsstandard" des European Telecom Standards Institute frappierend ähnlich. Erst seit den Enthüllungen Edward Snowdens sind Name und Mission dieses Projekts von NSA und GCHQ bekannt

Dabei soll nach dem Willen der NSA der "Galois Counter Mode" (GCM) als Modus zum Einsatz

kommen, der als besonders schlank und schnell gilt und einen hohen Datendurchsatz verspricht. GCM hat deshalb bei Cloud-Anwendungen Verbreitung, als Vorteil wird dabei hervorgehoben, dass GCM für Parallel-Computing gut geeignet ist. Ebenso ist ein Einsatz in rechenschwachen Umgebungen, also "Embedded"-Geräten denkbar. GCM hat also durchaus dort Meriten, wo Rechen- und Datendurchsatzzeiten absolut kritische Faktoren sind. Dafür wurde der Modus nämlich entwickelt. Die Schnelligkeit din diesem Chiffriermodus wird freilich dadurch erzielt, dass Authentifizierung und Verschlüsselung mit einer einzigen Funktion abgewickelt werden.

Zwei Anwendungen in einer

"Bei Anwendungen, die robuste Sicherheit verlangen, ist das unüblich", sagte der Wiener Sicherheitsexperte Michael Kafka zu ORF.at, "Man hat diese beiden Funktionen immer schon deshalb getrennt gehalten, weil Angriffe dadurch erschwert werden." Die durch die Schlankheit von GCM gewonnene Rechengeschwindigkeit könne bei VoIP-Telefonie so eher einem Angreifer zu Gute kommen, so Kafka weiter, während sich der Vorteil von GCM für die Abwicklung gerade von Internettelefonie in marginalen Grenzen halte.

Anders als etwa beim Cloud-Computing, wo gewaltige Datenmengen ver- und entschlüsselt werden müssen, nehmen sich die bei VoIP-Telefonie anfallenden Daten nachgerade verschwindend aus. Angesichts der Leistungsfähigkeit der Prozessoren in heute gängigen Smartphones falle dieser Gewinn an Performance deshalb in der Praxis überhaupt nicht mehr ins Gewicht, sagte Kafka.

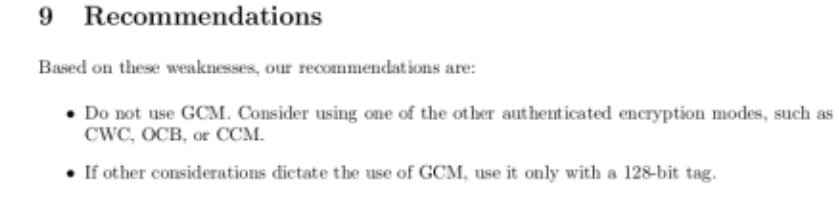
"Galois Counter Mode"

Der grundsätzliche Vorteil der "Galois Counter Mode"-Methode, nämlich Effizienz und hoher Datendurchsatz kommt unter diesen Voraussetzungen also eben nicht zum Tragen, während sich die Nachteile gerade bei einem Echtzeitprotokoll wie SRTP multiplizieren. Auch hier gibt es auffällige Parallelen zum Fall des anrüchigen Zahlengenerators "Dual EC DRBG".

Eine 2008 von der NSA eingereichte Erweiterung des TLS/SSL-Protokolls namens "Extended Random" war von den in der IETF vertretenen, großteils zivilen Technikern letzlich deshalb abgelehnt worden, weil keine praktischen Vorteile dafür erkennbar waren. Wie der Feldversuch der Forscher nun zeigte, hatte "Extended Random" nur einen einzigen "Vorteil": Ein Angriff der NSA auf den Verschlüsselungsvorgang wurde um den Faktor 65.000 beschleunigt.

Negatives Musterbeispiel anno 2005

Bereits 2005 hatte der bekannte Kryptograf Niels Ferguson von Microsoft zwei grundlegende Schwächen gegenüber Angriffen in "Galois Counter Mode" nachgewiesen und vor dem Einsatz von GCM als universellem Modus für kryptografische Blockchiffren gewarnt. Als negatives Musterbeispiel dafür führte Ferguson damals den möglichen Einsatz von GCM bei verschlüsselter Internettelefonie an.



9 Recommendations

Based on these weaknesses, our recommendations are:

- Do not use GCM. Consider using one of the other authenticated encryption modes, such as CWC, OCB, or CCM.
- If other considerations dictate the use of GCM, use it only with a 128-bit tag.

Microsoft

Das Gutachten Niels Fergusons im Volltext: "Authentication weaknesses in GCM" (http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/comments/CWC-GCM/Ferguson2.pdf)

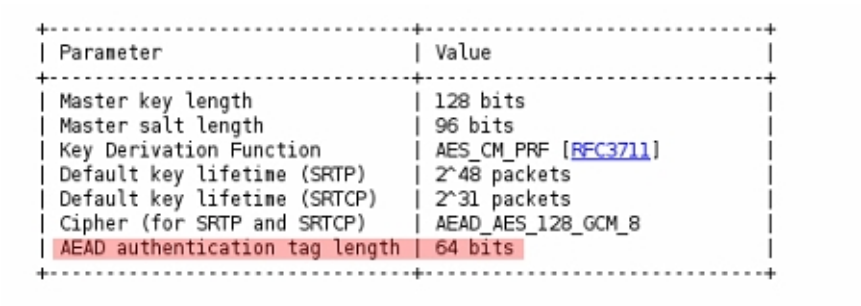
Weil die Schwäche besonders eklatant zu Tage tritt, wenn zu kurze "Authentifizierungs-Tags" verwendet werden, riet Ferguson: "Wenn man umständehalber gezwungen ist, GCM einzusetzen, sollte man den Modus ausschließlich mit 128-Bit langen Tags benützen." Grundsätzlich riet der holländische Kryptograf vom Einsatz dieses Modus überhaupt ab und empfahl andere Blockchiffre-Modi zu benützen, die diese Schwächen eben nicht aufwiesen.

Wie GCM zum NIST-Standard wurde

2007 wurde GCM dennoch durch die US-Standardisierungsbehörde NIST in den Rang eines nationalen Standards erhoben, sieben Jahre danach, am 1. April 2014 schlug nun die NSA "Galois Counter Mode" ausgerechnet für jene Anwendung vor, für die man GCM laut Ferguson und einer Reihe anderer Fachleute auf keinen Fall einsetzen sollte.

Galois Counter Mode, NIST-Standard SP 800-38D (http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf)

Wie auf dem Screenshot des aktuellen NSA-Entwurfs nun zu sehen ist, sind auch nicht wie 2005 empfohlen, ausschließlich 128-Bit sondern auch 64-Bit lange Tags für die Authentifizierung vorgesehen. Was auf den ersten Blick nur doppelt so viel ist, ergibt bei einer Exponentialrechnung doch deutlich mehr. "Der Unterschied zwischen 64 und 128 langen Tags ergibt eine Zahl mit 20 Nullen vor dem Komma. Ein solcher Faktor im Trillionenbereich macht dann doch einen gewaltigen Unterschied, wenn angegriffen wird" sagte Kafka.



Parameter	Value
Master key length	128 bits
Master salt length	96 bits
Key Derivation Function	AES_CM_PRF [RFC3711]
Default key lifetime (SRTP)	2^48 packets
Default key lifetime (SRTCP)	2^31 packets
Cipher (for SRTP and SRTCP)	AEAD_AES_128_GCM_8
AEAD authentication tag length	64 bits

CC IETF

Michael Kafka ist internationaler Sicherheitsexperte und Mitveranstalter der Wiener Deepsec-Konferenz deren Motto ist "Bleeding Edge Security" (https://deepsec.net)

Unangebrachte Schlüsse

Der aktuelle Entwurf für diesen internationalen Standard bei der IETF verzeichnet neben dem NSA-Mann Kevin Igoe noch einen zweiten Namen, nämlich den des Cisco-Technikers David McGrew. Die vorschnelle Annahme, dass sich da Cisco mit der NSA zusammengetan hätte, um sichere Verschlüsselung zu sabotieren, wäre jedoch grundverkehrt.

Wie die Praxis in den Arbeitsgruppen der IETF zeigt, wird (nicht nur) bei kryptografiebezogenen Einreichungen dem jeweiligen Vertschlüsselungsexperten auch ein Spezialist für die Ebene der Protokolle beigestellt. Heißt die einreichende Partei dann NSA kommt eben auch ein ziviler Techniker zum Handkuss, der mit der Einreichung selbst eigentlich nichts zu tun hat, außer sie in die Protokolle zu integrieren. Im Falle von "Extended Random" kam zum Beispiel ein Protokollspezialist der

Mozilla Foundation zur zweifelhaften Ehre, als Koautor einer Einreichung der hochrangigen NSA-Technikerin Margaret Salter zu firmieren.

Wie Techniker unter Druck geraten

Im Falle von McGrew erwies sich diese Vorgangsweise, die von der NSA benützt wird, als besonders perfid. McGrew ist nämlich Koautor von "Galois Counter Mode", um dessen Einsatz sich der gesamte NSA-Entwurf ja dreht. Hier sieht man, unter welchen Druck der weltweit insgesamt recht kleine Kreis von Verschlüsselungsspezialisten durch die NSA geraten ist. Im Dezember hatte einer Reihe ziviler Techniker in der IETF gegen diese Art von Einflussnahme durch die NSA rebelliert und die Absetzung Kevin Igoes als zweiten Vorsitzenden der IETF-Forschungsgruppe für Kryptografie gefordert.

Die Forderung nach Absetzung Igoes auf der Mailing-Liste, samt dem Thead mit den Antworten der anderen Techniker (http://www.ietf.org/mail-archive/web/cfrg/current/msg03554.html)

Igoe hatte einen Entwurf für ein passwortbasiertes Protokoll zum Schlüsselaustausch namens "Dragonfly" präsentiert, das er als einziger, der in der Forschungsgruppe versammelten Techniker für gut befunden hatte. Während der Konsens dort lautete, Dragonfly sei "ein schlampig gearbeitetes und unseriöses Protokoll" hatte Igoe versucht, es der übergeordneten TLS-Arbeitsgruppe in der IETF als Konsens der Kryptospezialisten zu verkaufen.

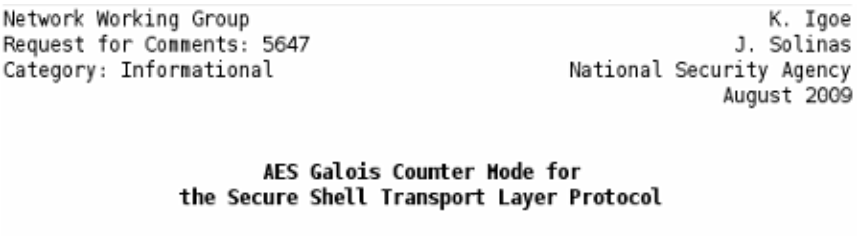
Die Dreistigkeit der NSA

Mit dem aktuellen Vorschlag, ausgerechnet "Galois Counter Mode" für verschlüsselte Internettelefonie zu verwenden hat Igoe seine damalige Vorgangsweise an Dreistigkeit noch übertroffen. Den Kopf mit dafür hinhalten muss nun Cisco-Techniker McGrew, der GCM für völlig andere Zwecke miterfunden hat.

Dass vordergründige Konspirationsthesen hier überhaupt nicht greifen, zeigt die Erwähnung McGrews in der Expertise des Microsoft-Technikers Niels Ferguson. Unter der Handvoll von Experten, bei denen sich Ferguson für die technische Unterstützung bei seiner vernichtenden Analyse von "Galois Counter Mode" bedankte, war auch der Koautor von GCM, David McGrew.

Parallelen zu SSH

Der finnische Kryptograf Markku-Juhani Saarinen hatte 2012 auf der Sicherheitskonferenz FSE 2012 in Washington ebenfalls vor dem Einsatz der Blockchiffre gewarnt. Gerade bei Echtzeitprotokollen wie Secure Shell für Virtual Private Networks sei von GCM dringend abzuraten. "Wenn tatsächlich rationale Gründe für den Einsatz von GCM vorlägen, etwa in Hochgeschwindigkeits-VPNs" dann sollte das nur geschehen, wenn vorher eine Risikoabschätzung stattgefunden haben, hieß es in Saarinens Vortrag.



Network Working Group — K. Igoe
Request for Comments: 5647 — J. Solinas
Category: Informational — National Security Agency
August 2009

AES Galois Counter Mode for the Secure Shell Transport Layer Protocol

Die NSA-Techniker Kevin Igoe und Jerry Salinas waren von solchen Überlegungen offenbar nicht geplagt. Im Frühjahr 2009 wurde von beiden der Entwurf RFC 5647 bei der IETF eingereicht und im August dort durchgewunken. Der Titel: "Galois Counter Mode" für das Secure Shell Layer Protocol".

Der Vortrag Saarinens (http://fse2012.inria.fr/SLIDES/36.pdf) auf der FSE-Konferenz 2009 und der RFC 5647 der IETF (https://tools.ietf.org/html/rfc5647)

Das Bombardierkäfer-Prinzip

Niels Ferguson wiederum war einer der beiden Microsoft-Spezialisten, die bereits 2007 vor dem anrüchigen NSA-Zufallszahlengenerator "Dual EC DRBG" gewarnt hatten. Eine wirklich verheerende Wirkung entfaltete der erst in Kombination mit der Erweiterung "Extended Random" von 2008. Der Wiener Sicherheitsexperte Michael Kafka nennt dies das "Bombardierkäfer-Prinzip".

Der Bombardierkäfer in der Wikipedia (http://de.wikipedia.org/wiki/Bombardierk%C3%A4fer)

Der Abwehrmechanismus dieser Laufkäferart besteht darin, zwei jeweils für sich gesehen harmlose Flüssigkeiten getrennt im Körper vorzuhalten. Wenn sie jedoch vermischt und ausgespritzt werden, erhitzt sich diese Mischung plötzlich auf etwa 100 Grad wobei sie obendrein noch stark ätzend wirkt.

http://www.golem.de/news/medizinische-geraete-der-hackbare-patient-1312-103397.html

MEDIZINISCHE GERÄTE

Der hackbare Patient

Datum: 16.12.2013, 17:00

Autor:Jörg Thoma

Experten wie Florian Grunow zeigen sich besorgt über die mangelnde Sicherheit in medizinischen Geräten. Mit immer mehr Konnektivität steigen auch die Angriffsflächen. Die Sicherheit spielt bei Herstellern und Kunden kaum eine Rolle.

Das Szenario klingt nach einem Agentenfilm: Ein Vitaldatenmonitor wird so gehackt, dass er keinen Alarm mehr auslöst, wenn die Vitalfunktionen eines Patienten außerhalb der normalen Parameter erfasst werden. Über eine Man-in-the-Middle-Attacke werden dann falsche Daten an die Überwachungszentrale geschickt. Der Patient kann so getötet werden, ohne dass es jemand im Krankenhaus bemerkt. Reine Fiktion ist das aber nicht.

Solche Szenarien würden im Gegenteil immer wahrscheinlicher, sagte Sicherheitsexperte Florian Grunow von der Sicherheitsfirma ERNW auf der Sicherheitskonferenz Deepsec 2013 in Wien. Der Hacker Barnaby Jack manipulierte beispielsweise eine Insulinpumpe so, dass sie die gesamte Dosis auf einmal abgab. Für einen Patienten wäre das tödlich. Jack nutzte dafür die Funkschnittstelle des Geräts - aus bis zu 300 Meter Entfernung ist das möglich. Der Sicherheitsexperte Kevin Fu experimentierte mit einem Defibrilator, dessen abgehörte Funksignale genutzt werden können, um ihn ein- und auszuschalten. Auch das kann für einen Patienten tödlich sein. Mit zunehmender Konnektivität der diversen medizinischen Geräte erweitere sich auch die Angriffsfläche, sagte Grunow Golem.de. Gleichzeitig werde die Gefahr von den Herstellern aber immer weiter unterschätzt.

Unsichere Systeme können tödlich sein

Zwar stehe die gesundheitliche Sicherheit der Patienten bei Herstellern von medizinischen Geräten weiter an erster Stelle, die Sicherheit ihrer Geräte gerate aber immer mehr ins Abseits, sagte Grunow. Der ehemalige US-Verteidigungsminister Dick Cheney ließ daher aus Angst vor solchen Anschlägen die Kommunikationsschnittstelle seines Herzschrittmachers deaktivieren. Grunow hält das für berechtigt, wenn auch etwas übertrieben. Zwar müsse ein Angreifer bei vielen Herzschrittmachern fast direkt vor seinem Opfer stehen, um erfolgreich zu sein, denn die Schnittstelle werde durch Induktion aktiviert, um Akkulaufzeit zu sparen. Einmal erfolgreich manipuliert könnte ein fehlkonfigurierter Herzschrittmacher aber tödlich sein.

Auch die IT in Krankenhäusern veraltet laut Grunow immer mehr - eine Gefahr für die sicheren Netzwerke, in denen medizinische Geräte hängen sollten. Hinzu kommen immer mehr Geräte, die von ambulanten Patienten

Daten sammeln und sie über das Netzwerk an Ärzte und Krankenhäuser versenden.

Gefährdete Patientendaten

Seit längerem werden Vitalparameter aus Krankenwagen über GSM an das Krankenhaus übertragen, damit sich die Ärzte vorab ein Bild über den Zustand eines Patienten machen und sich notfalls über Funk beraten können. Die Daten aus den Vitaldatenmonitoren werden aber über das GSM-Netzwerk versendet, das meist unverschlüsselt ist. Dabei ist das direkte gesundheitliche Sicherheitsrisiko bei Überwachungsgeräten noch relativ gering. Mit ihnen lassen sich aber persönliche Daten eines Patienten abgreifen. Dem Patienten selbst können sie physisch kaum schaden - außer in dem Agentenszenario.

Gefährlicher sind da schon die Diagnosegeräte. Immerhin kann ein über das Netzwerk gesteuertes Blutdruckmessgerät so manipuliert werden, dass die Manschette über einen längeren Zeitraum aufgepumpt bleibt und dem Patienten Schmerzen bereiten kann.

Veraltete Software und gefährliche Funktionen

Grunow sagte, er habe medizinische Geräte gesehen, deren Software nur auf einem Server mit Windows NT 4.0 funktioniere. Die Software, die die Daten solcher Geräte verarbeite, sei nicht mehr für neue Windows-Versionen aktualisiert worden. Die damals teuren Geräte müssten durch noch teurere, aktuelle ersetzt werden, um solche Angriffsflächen zu vermeiden. Mit Geld, das den Krankenhäusern heute jedoch fehle.

Deshalb würden oftmals kostengünstige Geräte angeschafft. Deren Hardware bestehe meist aus billigen Platinen asiatischer Hersteller, in Serien hergestellt und in leicht variierenden Gehäusen verbaut. Es gebe bereits Patientenmonitore, die einen eingebetteten Webbrowser enthielten - mit Internetzugriff. Die Geräte haben dann zwei Netzwerkschnittstellen, eine für ein Trusted-Netzwerk, über das Patientendaten an eine zentrale Überwachungsstation laufen, und eine für ein Untrusted-Network für den Zugriff auf das Internet.

Viel, zu viel Netzwerk

Grunow ist aber davon überzeugt, dass es ein Leichtes sei, durch Hacking Daten von einem Netz zum anderen zu übertragen. Im Streit mit den Administratoren spannten Ärzte sogar ihr eigenes unsicheres WLAN auf, erzählt er, trotz oder gerade wegen des Einspruchs durch die Administratoren. Er habe von Fällen erfahren, bei denen Ärzte neue Maschinen angeschafft und ans Netzwerk angeschlossen hätten, ohne die IT-Abteilung zu informieren. Geräte, die von sich aus ein /8-Netzwerk eingerichtet hätten, fluteten das Netzwerk. Bei manchen Geräten wundert sich Grunow allerdings, warum sie überhaupt netzwerkfähig sind. Etwa bei den Narkosegeräten, die den Patienten während einer Operation ja auch am Leben halten. Welche Geräte das sind, will Grunow nicht ver-

raten. Besonders im Bereich der medizinischen Technik hält Grunow den Grundsatz des "responsible disclosure" für unerlässlich, also eine verantwortungsvolle Veröffentlichung von Sicherheitslücken, um Patienten nicht zu gefährden.

Vor allem die Hersteller hätten kaum eine Ahnung, wie viele Angriffsmöglichkeiten solche Geräte böten. Sie seien tatsächlich "Rocket Science", sagte Grunow, hochkomplexe Geräte voller proprietärer Protokolle und Software, die nur sehr schwer zu debuggen sei. Auch für den Patienten fatale Softwarefehler seien möglich. Die fälschliche Anzeige einer Asystolie, die den Tod eines Patienten bedeute, sei noch einer der harmlosen Fehler.

Warnungen vom FDA

Die beschriebenen Beispiele klingen zwar nach Horrorgeschichten aus Kinofilmen, aber selbst die US-Behörde FDA warnt inzwischen vor Cyberangriffen auf medizinische Geräte. Mitte des Jahres entdeckten Sicherheitsforscher hart-kodierte - also unveränderbare - Passwörter in netzwerkfähigen Infusionspumpen, die bei Operationen eingesetzt werden.

Das Problem sei ein grundlegendes, sagte Grunow: Wir als Patienten vertrauten diesen Geräten ebenso wie die Ärzte. Und die Hersteller stünden unter dem Konkurrenzdruck, immer bessere Geräte mit immer mehr Funktionen herzustellen. Mit der zunehmenden Vernetzung werde auch die Fernüberwachung bei Patienten zu Hause zunehmen. Sofern die Hersteller nicht von den Kunden - den fachkundigen Ärzten - unter Druck gesetzt würden, werde sich kaum was ändern, befürchtet Grunow.

Die Hersteller zeigten sich aber weitgehend wenig kooperativ. Erst wenn etwas furchtbar schieflaufe, seien sie bereit, mit den Sicherheitsexperten zu reden. Grunow sei aber auf die Zusammenarbeit angewiesen. Die Geräte, die er untersuchen wolle, kosteten meist mehrere zehntausend Euro - und seien zudem schwer zu beschaffen.

MEDIZINISCHE GERÄTE

Der hackbare Patient

Experten wie Florian Grunow zeigen sich besorgt über die mangelnde Sicherheit in medizinischen Geräten. Mit immer mehr Konnektivität steigen auch die Angriffsflächen. Die Sicherheit spielt bei Herstellern und Kunden kaum eine Rolle.

Herzschrittmacher mit unsicheren Schnittstellen können für Patienten tödlich sein. (Bild: Thomas Zimmermann)

Artikel: MEDIZINISCHE GERÄTE
Der hackbare Patient

Inhalt: . Veraltete Software und gefährliche Funktionen

Datum: 16.12.2013, 17:00

Autor: Jörg Thoma

Themen: Security, Induktion, Man-in-the-Middle, Medizin, Passwort, Sicherheitslücke, Server, Internet, Wissenschaft

Das Szenario klingt nach einem Agentenfilm: Ein Vitaldatenmonitor wird so gehackt, dass er keinen Alarm mehr auslöst, wenn die Vitalfunktionen eines Patienten außerhalb der normalen Parameter erfasst werden. Über eine Man-in-the-Middle-Attacke werden dann falsche Daten an die Überwachungszentrale geschickt. Der Patient kann so getötet werden, ohne dass es jemand im Krankenhaus bemerkt. Reine Fiktion ist das aber nicht.

Solche Szenarien würden im Gegenteil immer wahrscheinlicher, sagte Sicherheitsexperte Florian Grunow von der Sicherheitsfirma ERNW auf der Sicherheitskonferenz Deepsec 2013 in Wien. Der Hacker Barnaby Jack manipulierte beispielsweise eine Insulinpumpe so, dass sie die gesamte Dosis auf einmal abgab. Für einen Patienten wäre das tödlich. Jack nutzte dafür die Funkschnittstelle des Geräts - aus bis zu 300 Meter Entfernung ist das möglich. Der Sicherheitsexperte Kevin Fu experimentierte mit einem Defibrilator, dessen abgehörte Funksignale genutzt werden können, um ihn ein- und auszuschalten. Auch das kann für einen Patienten tödlich sein. Mit zunehmender Konnektivität der diversen medizinischen Geräte erweitere sich auch die Angriffsfläche, sagte Grunow Golem.de. Gleichzeitig werde die Gefahr von den Herstellern aber immer weiter unterschätzt.

Unsichere Systeme können tödlich sein

Zwar stehe die gesundheitliche Sicherheit der Patienten bei Herstellern von medizinischen Geräten weiter an erster Stelle, die Sicherheit ihrer Geräte gerate aber immer mehr ins Abseits, sagte Grunow. Der ehemalige US-Verteidigungsminister Dick Cheney ließ daher aus Angst vor solchen Anschlägen die Kommunikationsschnittstelle seines Herzschrittmachers deaktivieren. Grunow hält das für berechtigt, wenn auch etwas übertrieben. Zwar müsse ein Angreifer bei vielen Herzschrittmachern fast direkt vor seinem Opfer stehen, um erfolgreich zu sein, denn die Schnittstelle werde durch Induktion aktiviert, um Akkulaufzeit zu sparen. Einmal erfolgreich manipuliert könnte ein fehlkonfigurierter Herzschrittmacher aber tödlich sein.

Auch die IT in Krankenhäusern veraltet laut Grunow immer mehr - eine Gefahr für die sicheren Netzwerke, in denen medizinische Geräte hängen sollten. Hinzu kommen immer mehr Geräte, die von ambulanten Patienten Daten sammeln und sie über das Netzwerk an Ärzte und Krankenhäuser versenden.

Gefährdete Patientendaten

Seit längerem werden Vitalparameter aus Krankenwagen über GSM an das Krankenhaus übertragen, damit sich die Ärzte vorab ein Bild über den Zustand eines Patienten machen und sich notfalls über Funk beraten können. Die Daten aus den Vitaldatenmonitoren werden aber über das GSM-Netzwerk versendet, das meist unverschlüsselt ist. Dabei ist das direkte gesundheitliche Sicherheitsrisiko bei Überwachungsgeräten noch relativ gering. Mit ihnen lassen sich aber persönliche Daten eines Patienten abgreifen. Dem Patienten selbst können sie physisch kaum schaden - außer in dem Agentenszenario.

Gefährlicher sind da schon die Diagnosegeräte. Immerhin kann ein über das Netzwerk gesteuertes Blutdruckmessgerät so manipuliert werden, dass die Manschette über einen längeren Zeitraum aufgepumpt bleibt und dem Patienten Schmerzen bereiten kann.

1 2 ›

Veraltete Software und gefährliche Funktionen ›

Veraltete Software und gefährliche Funktionen

Herzschrittmacher mit unsicheren Schnittstellen können für Patienten tödlich sein. (Bild: Thomas Zimmermann)

Artikel: MEDIZINISCHE GERÄTE
Der hackbare Patient

Inhalt: Veraltete Software und gefährliche Funktionen

Datum: 16.12.2013, 17:00

Autor: Jörg Thoma

Themen: Security, Induktion, Man-in-the-Middle, Medizin, Passwort, Sicherheitslücke, Server, Internet, Wissenschaft

Grunow sagte, er habe medizinische Geräte gesehen, deren Software nur auf einem Server mit Windows NT 4.0 funktioniere. Die Software, die die Daten solcher Geräte verarbeite, sei nicht mehr für neue Windows-Versionen aktualisiert worden. Die damals teuren Geräte müssten durch noch teurere, aktuelle ersetzt werden, um solche Angriffsflächen zu vermeiden. Mit Geld, das den Krankenhäusern heute jedoch fehle.

Deshalb würden oftmals kostengünstige Geräte angeschafft. Deren Hardware bestehe meist aus billigen Platinen asiatischer Hersteller, in Serien hergestellt und in leicht variierenden Gehäusen verbaut. Es gebe bereits Patientenmonitore, die einen eingebetteten Webbrowser enthielten - mit Internetzugriff. Die Geräte haben dann zwei Netzwerkschnittstellen, eine für ein Trusted-Netzwerk, über das Patientendaten an eine zentrale Überwachungsstation laufen, und eine für ein Untrusted-Network für den Zugriff auf das Internet.

Viel, zu viel Netzwerk

Grunow ist aber davon überzeugt, dass es ein Leichtes sei, durch Hacking Daten von einem Netz zum anderen zu übertragen. Im Streit mit den Administratoren spannten Ärzte sogar ihr eigenes unsicheres WLAN auf, erzählt er, trotz oder gerade wegen des Einspruchs durch die Administratoren. Er habe von Fällen erfahren, bei denen Ärzte neue Maschinen angeschafft und ans Netzwerk angeschlossen hätten, ohne die IT-Abteilung zu informieren. Geräte, die von sich aus ein /8-Netzwerk eingerichtet hätten, fluteten das Netzwerk. Bei manchen Geräten wundert sich Grunow allerdings, warum sie überhaupt netzwerkfähig sind. Etwa bei den Narkosegeräten, die den Patienten während einer Operation ja auch am Leben halten. Welche Geräte das sind, will Grunow nicht verraten. Besonders im Bereich der medizinischen Technik hält Grunow den Grundsatz des *"responsible disclosure"* für unerlässlich, also eine verantwortungsvolle Veröffentlichung von Sicherheitslücken, um Patienten nicht zu gefährden.

Vor allem die Hersteller hätten kaum eine Ahnung, wie viele Angriffsmöglichkeiten solche Geräte böten. Sie seien tatsächlich "Rocket Science", sagte Grunow, hochkomplexe Geräte voller proprietärer Protokolle und Software, die nur sehr schwer zu debuggen sei. Auch für den Patienten fatale Softwarefehler seien möglich. Die fälschliche Anzeige einer Asystolie, die den Tod eines Patienten bedeute, sei noch einer der harmlosen Fehler.

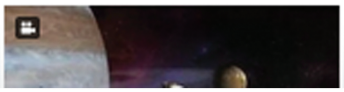
Warnungen vom FDA

Die beschriebenen Beispiele klingen zwar nach Horrorgeschichten aus Kinofilmen, aber selbst die US-Behörde FDA warnt inzwischen vor Cyberangriffen auf medizinische Geräte. Mitte des Jahres entdeckten Sicherheitsforscher hart-kodierte - also unveränderbare - Passwörter in netzwerkfähigen Infusionspumpen, die bei Operationen eingesetzt werden.

Das Problem sei ein grundlegendes, sagte Grunow: Wir als Patienten vertrauten diesen Geräten ebenso wie die Ärzte. Und die Hersteller stünden unter dem Konkurrenzdruck, immer bessere Geräte mit immer mehr Funktionen herzustellen. Mit der zunehmenden Vernetzung werde auch die Fernüberwachung bei Patienten zu Hause zunehmen. Sofern die Hersteller nicht von den Kunden - den fachkundigen Ärzten - unter Druck gesetzt würden, werde sich kaum was ändern, befürchtet Grunow.

Die Hersteller zeigten sich aber weitgehend wenig kooperativ. Erst wenn etwas furchtbar schieflaufe, seien sie bereit, mit den Sicherheitsexperten zu reden. Grunow sei aber auf die Zusammenarbeit angewiesen. Die Geräte, die er untersuchen wolle, kosteten meist mehrere zehntausend Euro - und seien zudem schwer zu beschaffen. ▪

1 2



http://oe1.orf.at/programm/356151

matrix - computer & neue medien

Sonntag

01. Dezember 2013

22:30

Geheimnisse, Pleiten und Visionen

Die DeepSec 2013

Gestaltung: Sarah Kriesche

Bereits zum 7. Mal findet von 19.-22. November die DeepSec-Konferenz in Wien statt. Die IT-Sicherheitskonferenz steht dieses Jahr unter dem Motto: "Secrets, Failures and Visions". Das Themenspektrum reicht von der Überwachung durch Geheimdienste, über die Analyse und Bewertung von Datenlecks, bis hin zu Zukunftsszenarien der Informationsgesellschaft. Mit dabei sind Vortragende aus den USA, Russland, Asien und Südamerika. Ein Bericht von Sarah Kriesche.

zur Sendereihe

Standort: oe1.ORF.at

matrix - computer & neue medien

Sonntag
01. Dezember 2013
22:30

Geheimnisse, Pleiten und Visionen
Die DeepSec 2013
Gestaltung: Sarah Kriesche

Bereits zum 7. Mal findet von 19.-22. November die DeepSec-Konferenz in Wien statt. Die IT-Sicherheitskonferenz steht dieses Jahr unter dem Motto: "Secrets, Failures and Visions". Das Themenspektrum reicht von der Überwachung durch Geheimdienste, über die Analyse und Bewertung von Datenlecks, bis hin zu Zukunftsszenarien der Informationsgesellschaft. Mit dabei sind Vortragende aus den USA, Russland, Asien und Südamerika. Ein Bericht von Sarah Kriesche.

zurück

zur Sendereihe

Kategorie: Wissen

Programm

Mo Di Mi Do Fr Sa So
1

http://www.golem.de/news/security-verfolgungsjagd-per-bluetooth-1311-103040.html

SECURITY

Verfolgungsjagd per Bluetooth

Datum:29.11.2013, 12:24

Autor:Jörg Thoma

Ausgestattet mit einem Raspberry Pi samt Bluetooth-Dongle haben sich Sicherheitsexperten auf die Suche nach Geräten mit aktivierter Bluetooth-Schnittstelle gemacht. Es waren erstaunlich viele, die zudem viele Informationen über ihren Besitzer verraten.

Bluetooth ist inzwischen in fast jedem mobilen und immobilen Gerät verbaut - und oftmals unbemerkt vom den Besitzern aktiviert. Smartphone-Nutzer telefonieren etwa über Bluetooth-Headsets, und die Entertainmentelektronik in Fahrzeugen sucht nach Bluetooth-Geräten, die sie einbinden kann. Selbst Prothesen haben inzwischen Bluetooth-Schnittstellen.

Video: Bluedriving (0:50)
http://video.golem.de/mobil/12095/bluedriving.html

Grund genug für die beiden Sicherheitsexperten Verónica Valeros und Sebastián García aus Argentinien, bei Spaziergängen nach Bluetooth-Geräten zu gucken und die Ergebnisse ihrer Suche in einer Datenbank zu speichern. Tools habe es schon vorher gegeben, sagten sie auf der Sicherheitskonferenz Deepsec 2013 in Wien. Allerdings erweiterten sie die von ihnen entwickelte Werkzeugsammlung so, dass die Informationen auch GPS-Daten enthalten. So entstanden etwa Bewegungsprofile von Menschen, die ihre Mobiltelefone mit aktiviertem Bluetooth nutzten. Mit ihrem Werkzeug könnten Diebe aber auch eine Positionsliste erstellen, etwa von für den Diebstahl lohnenswerten Objekten. Denn inzwischen haben selbst digitale Fernseher eine Bluetooth-Schnittstelle und bei manchen enthält der Gerätename auch gleich die Bildschirmgröße. Das Fazit der Sicherheitsforscher: lieber Bluetooth ausschalten und auch in Geräten nachsehen, in denen Bluetooth nicht einmal vermutet wird. Zumindest sollte der Name des Geräts keinen Hinweis auf den Besitzer oder das Gerät geben.

Bluetooth überall

Etwa in einem Gerät zur Messung der Lungenfunktionen, das viele Patienten mit Asthma mit sich tragen. Inzwischen werden auch Prothesen mit einer Bluetooth-Schnittstelle versehen. Bei Patienten mit zwei Beinprothesen kommunizieren die beiden künstlichen Gliedmaßen, um die Bewegung des Patienten besser zu koordinieren.

Eigentlich eine sinnvolle Funktion, wären da nicht die zwangsweise nach außen hin sichtbare MAC-Adresse und der Gerätename.

Mit ihrem Werkzeug wollten Valeros und García in erster Linie zeigen, wie einfach es ist, mit den gesammelten Daten Bewegungsprofile zu erstellen. Aus den Metadaten konnten die Sicherheitsexperten ziemlich genaue Mutmaßungen über die von ihnen Verfolgten machen. Wiederholte sich beispielsweise der Weg jeden Tag in der Früh zur gleichen Uhrzeit, gingen die Forscher davon aus, dass das Opfer auf dem Weg zur Arbeit war.

Bis zu 100 Meter

Allerdings ist die Reichweite bei Bluetooth begrenzt. Per Standard definiert liegt der Radius bei etwa zehn Metern. Das gilt für Bluetooth-Geräte der Klasse 2, die 2,5 mW verbrauchen und einen Leistungspegel von 4 dBm haben. Im Freien können sie aber aus bis zu 50 Metern Entfernung noch erkannt werden. Die selteneren Geräte der Klasse 1 können mit einem Leistungspegel von 20 dBm eine Reichweite drinnen und draußen von 100 Metern erreichen, benötigen dafür aber auch 100 mW. Gegenwärtig liegen Geräte mit Bluetooth der Klasse 3 im Trend. Mit einer Leistungsaufnahme von 1 mW und einem Leistungspegel von 0 dBm sind sie nur für den Einsatz bei kurzen Strecken und in Geräten mit langer Akkulaufzeit gedacht, wie etwa Headsets, Hörgeräten oder Pulsmessern, die beispielsweise ihre Daten an Smartphones weitergeben. Durchschnittlich liegt deren Reichweite bei etwa einem Meter, maximal sind es zehn.

Valeros und García haben sich ein Raspberry Pi als Wardriving-Gerät eingerichtet. Zunächst besorgten sie sich einen Akku, damit der kleine Rechner auch unterwegs mit Strom versorgt wird. An die beiden USB-Schnittstellen hängten sie einen Bluetooth-Dongle und ein GPS-Modul. Ein Laptop mit Bluetooth tut es natürlich auch. Die GPS-Daten lassen sich über Bluetooth aber auch von einem Mobiltelefon holen.

Mit Python Bluetooth-Daten sammeln

Python-Skripte sammeln die Daten über den Bluetooth-Dongle und speichern sie in einer Sqlite-Datenbank. Die kann dann per Skript ausgewertet werden. Alternativ macht das auch ein Webserver, der die Daten optisch aufbereitet und gleich noch die Position der erfassten Geräte im Kartenmaterial anzeigt. Den Code haben Valeros und García auf Github veröffentlicht.

Mit ihrem Experiment wollten Valeros und García die Aufmerksamkeit auf eine mögliche Schwachstelle lenken, die viele Menschen unbemerkt mit sich herumtragen, sagten sie zu Golem.de. Es gebe aber auch Hersteller, die

es dem Nutzer gar nicht ermöglichen, Bluetooth auszuschalten, etwa Audiogeräte in einigen Autos und sogar auf Laptops. Bluetooth biete als Schnittstelle zahlreiche Möglichkeiten, könne aber auch sehr einfach dazu missbraucht werden, die Privatsphäre zu verletzen. Vor allem mit der zunehmenden Verbreitung von Bluetooth in medizinischen Geräten steige auch die Gefahr für die Anwender nochmals deutlich.

Die Werkzeugsammlung liegt auf Github und läuft gegenwärtig nur unter Linux.

SECURITY

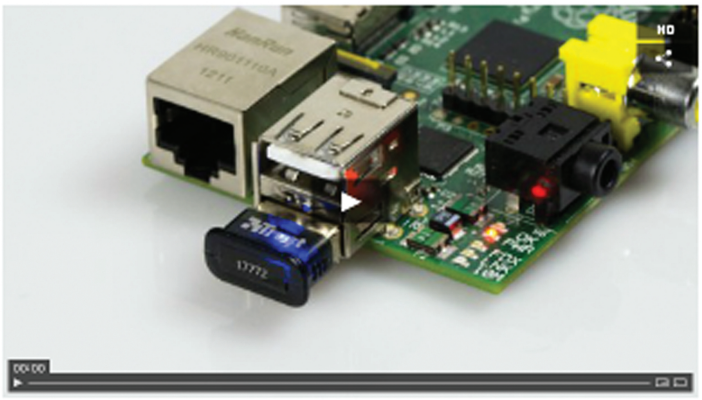
Verfolgungsjagd per Bluetooth

Ausgestattet mit einem Raspberry Pi samt Bluetooth-Dongle haben sich Sicherheitsexperten auf die Suche nach Geräten mit aktivierter Bluetooth-Schnittstelle gemacht. Es waren erstaunlich viele, die zudem viele Informationen über ihren Besitzer verraten.

Bluetooth-Geräte gepaart mit GPS-Daten sind gute Tracking-Geräte. (Bild: Verónica Valeros und Sebastián García)

Datum: 29.11.2013, 12:24
Autor: Jörg Thoma
Themen: Bluetooth, Raspberry Pi, Applikationen, PC-Hardware, Security

Bluetooth ist inzwischen in fast jedem mobilen und immobilen Gerät verbaut - und oftmals unbemerkt vom den Besitzern aktiviert. Smartphone-Nutzer telefonieren etwa über Bluetooth-Headsets, und die Entertainmentelektronik in Fahrzeugen sucht nach Bluetooth-Geräten, die sie einbinden kann. Selbst Prothesen haben inzwischen Bluetooth-Schnittstellen.



Video: Bluedriving (0:50)

Grund genug für die beiden Sicherheitsexperten Verónica Valeros und Sebastián García aus Argentinien, bei Spaziergängen nach Bluetooth-Geräten zu gucken und die Ergebnisse ihrer Suche in einer Datenbank zu speichern. Tools habe es schon vorher gegeben, sagten sie auf der Sicherheitskonferenz Deepsec 2013 in Wien. Allerdings erweiterten sie die von ihnen entwickelte Werkzeugsammlung so, dass die Informationen auch GPS-Daten enthalten. So entstanden etwa Bewegungsprofile von Menschen, die ihre Mobiltelefone mit aktiviertem Bluetooth nutzten. Mit ihrem Werkzeug könnten Diebe aber auch eine Positionsliste erstellen, etwa von für den Diebstahl lohnenswerten Objekten. Denn inzwischen haben selbst digitale Fernseher eine Bluetooth-Schnittstelle und bei manchen enthält der Gerätename auch gleich die Bildschirmgröße. Das Fazit der Sicherheitsforscher: lieber Bluetooth ausschalten und auch in Geräten nachsehen, in denen Bluetooth nicht einmal vermutet wird. Zumindest sollte der Name des Geräts keinen Hinweis auf den Besitzer oder das Gerät geben.

Bluetooth überall

Etwa in einem Gerät zur Messung der Lungenfunktionen, das viele Patienten mit Asthma mit sich tragen. Inzwischen werden auch Prothesen mit einer Bluetooth-Schnittstelle versehen. Bei Patienten mit zwei Beinprothesen kommunizieren die beiden künstlichen Gliedmaßen, um die Bewegung des Patienten besser zu koordinieren. Eigentlich eine sinnvolle Funktion, wären da nicht die zwangsweise nach außen hin sichtbare MAC-Adresse und der Gerätename.

Mit ihrem Werkzeug wollten Valeros und García in erster Linie zeigen, wie einfach es ist, mit den gesammelten Daten Bewegungsprofile zu erstellen. Aus den Metadaten konnten die Sicherheitsexperten ziemlich genaue Mutmaßungen über die von ihnen Verfolgten machen. Wiederholte sich beispielsweise der Weg jeden Tag in der Früh zur gleichen Uhrzeit, gingen die Forscher davon aus, dass das Opfer auf dem Weg zur Arbeit war.

Bis zu 100 Meter

Allerdings ist die Reichweite bei Bluetooth begrenzt. Per Standard definiert liegt der Radius bei etwa zehn Metern. Das gilt für Bluetooth-Geräte der Klasse 2, die 2,5 mW verbrauchen und einen Leistungspegel von 4 dBm haben. Im Freien können sie aber aus bis zu 50 Metern Entfernung noch erkannt werden. Die selteneren Geräte der Klasse 1 können mit einem Leistungspegel von 20 dBm eine Reichweite drinnen und draußen von 100 Metern erreichen, benötigen dafür aber auch 100 mW. Gegenwärtig liegen Geräte mit Bluetooth der Klasse 3 im Trend. Mit einer Leistungsaufnahme von 1 mW und einem Leistungspegel von 0 dBm sind sie nur für den Einsatz bei kurzen Strecken und in Geräten mit langer Akkulaufzeit gedacht, wie etwa Headsets, Hörgeräten oder Pulsmessern, die beispielsweise ihre Daten an Smartphones weitergeben. Durchschnittlich liegt deren Reichweite bei etwa einem Meter, maximal sind es zehn.

Valeros und García haben sich ein Raspberry Pi als Wardriving-Gerät eingerichtet. Zunächst besorgten sie sich einen Akku, damit der kleine Rechner auch unterwegs mit Strom versorgt wird. An die beiden USB-Schnittstellen hängten sie einen Bluetooth-Dongle und ein GPS-Modul. Ein Laptop mit Bluetooth tut es natürlich auch. Die GPS-Daten lassen sich über Bluetooth aber auch von einem Mobiltelefon holen.

Mit Python Bluetooth-Daten sammeln

Python-Skripte sammeln die Daten über den Bluetooth-Dongle und speichern sie in einer Sqlite-Datenbank. Die kann dann per Skript ausgewertet werden. Alternativ macht das auch ein Webserver, der die Daten optisch aufbereitet und gleich noch die Position der erfassten Geräte im Kartenmaterial anzeigt. Den Code haben Valeros und García auf Github veröffentlicht.

Mit ihrem Experiment wollten Valeros und García die Aufmerksamkeit auf eine mögliche Schwachstelle lenken, die viele Menschen unbemerkt mit sich herumtragen, sagten sie zu Golem.de. Es gebe aber auch Hersteller, die es dem Nutzer gar nicht ermöglichen, Bluetooth auszuschalten, etwa Audiogeräte in einigen Autos und sogar auf Laptops. Bluetooth biete als Schnittstelle zahlreiche Möglichkeiten, könne aber auch sehr einfach dazu missbraucht werden, die Privatsphäre zu verletzen. Vor allem mit der zunehmenden Verbreitung von Bluetooth in medizinischen Geräten steige auch die Gefahr für die Anwender nochmals deutlich.

Die Werkzeugsammlung liegt auf Github und läuft gegenwärtig nur unter Linux. ▪

Videos

New Horizons' Mission Pluto und der Kuipergürtel - Nasa

Verwandte Artikel

WLAN-HACKING
Pakete einschleusen mit Packets in Packets

IOS UND ANDROID
Auto entriegeln mit dem Smartphone

SPÄHATTACKE
EU-Parlament schaltet öffentliches WLAN ab

IMPROV
Eine Platine - nicht nur - für Mer-Entwickler

INTELLIGENTE STROMZÄHLER
Versorger fordern 170 Euro jährlich von Verbrauchern

Meistgelesen | Meistkommentiert

NEMO'S GARDEN
Erdbeeren und Basilikum wachsen im Meer

COMMODORE PET
Das Smartphone mit dem großen Namen

SPIELEENTWICKLER
Star Citizen schließt Kritiker aus Unterstützerkreis aus

SPIONAGESOFTWARE
Hacking Team nutzt UEFI-Rootkit

KICKSTARTER
Kerze lädt Smartphone

Ticker

RECHT AUF VERGESSEN
Google veröffentlicht versehentlich Details zu Löschanträgen

http://futurezone.at/science/medizingeraete-lassen-sich-leicht-hacken/37.040.304

DEEPSEC

Forscher zeigt: So leicht lassen sich Medizingeräte hacken

Barbara Wimmer 25.11.13, 00:00

Die IT-Sicherheit kommt bei vielen Medizingeräten zu kurz. Bei der Konferenz Deep Sec demonstrierte der Forscher Florian Grunow, wie man einen Patientenmonitor manipuliert.

Eigentlich war der Patient tot. Am Monitor, der zur Überwachung seiner Vitalparameter eingesetzt wurde, lebte er jedoch noch. Bei der Sicherheitskonferenz DeepSec in Wien zeigte der Sicherheitsanalyst Florian Grunow live, wie man Patientenmonitore, die man im Krankenhaus zur Überwachung des Zustands von Patienten einsetzt, manipulieren kann. Grunow manipulierte dabei zuerst den Bildschirm des Monitors, in Folge spielte er aber auch im zentralen Netzwerk falsche Daten ein. Das Ganze dauerte nur wenige Minuten. Der futurezone erzählte der Sicherheitsforscher, der für das Unternehmen ERNW in Heidelberg an einem entsprechenden Research-Projekt beteiligt ist, wie das möglich wird und warum Hersteller den Aspekt der IT-Security von medizinischen Geräten sträflich vernachlässigen.

Futurezone: Herr Grunow, Sie erforschen die Sicherheit von Medizingeräten. War es einfach, an die entsprechenden Geräte heranzukommen?

Florian Grunow: Nein, es ist nicht ganz einfach, an die Geräte zu kommen. Entweder man braucht dafür Lizenzen z.B. wenn man sich ein Röntgengerät anschauen möchte. Das darf man auch nicht ohne spezielle Ausbildung und Berechtigungsscheine betreiben. Da wir das als IT-Security-Unternehmen nicht aufweisen können, haben wir beim Patientenmonitoring angefangen. Die Daten, die man aus dem Patientenmonitor gewinnt, sind für den Arzt auch Grundlage, um Entscheidungen über seine nächsten Schritte zu treffen.

Was genau haben Sie bei Ihren Forschungen rausgefunden und auf der DeepSec demonstriert?

Die Idee ist, den Überwachungsbildschirm, der die Vitalzeichen des Patienten anzeigt, so zu manipulieren, dass es halt einen lebenden Patienten anzeigt, obwohl der Patient gerade Probleme hat oder möglicherweise schon verstorben ist. Der Monitor ist dabei mit einem Netzwerkkabel am internen Netzwerk angeschlossen und sendet seine Daten an die Zentralstation. Wir haben getestet, ob man diese Zentralstation so angreifen kann, dass ich ihr vorgauklen kann, dass es dem Patienten wunderbar geht, obwohl er gerade Probleme hat. Das haben wir bei den Modellen von Monitoren, die wir uns bisher angesehen haben, geschafft.

Wie haben Sie das bewerkstelligt?

Wir konnten sowohl den Bildschirm als auch die Zentralstation so manipulieren, dass angezeigt wird, was wir wollen und zwar auch im laufenden Betrieb. Wir haben einen Weg gefunden, uns im Kommunikationsprozess dazwischen zu schalten und den Monitor aus der Kommunikation auszuklinken und selbst Daten an die Zentralstation zu schicken. Wie wir das genau gemacht haben, haben wir den Herstellern übermittelt.

In der Regel müssen die Hersteller dann in einem bestimmten Zeitraum reagieren. Wird das bei Medizingeräten auch gehandhabt?

Stimmt, normalerweise gibt man eine Deadline an, um den Hersteller unter Druck zu setzen, damit er die Sicherheitslücken behebt. In dem Fall muss man da ein bisschen vorsichtiger sein, weil man das Druckmittel gar nicht in der Hand hat. Da hängen Menschenleben dran und in so einem Fall kann man nicht einfach rausposaunen, wie man es gemacht hat.

Das heißt, Sie veröffentlichen auch nicht den Namen des Monitor-Herstellers?

Nein. Bei medizinischen Geräten haben wir das Problem, dass die Hersteller die Geräte ganz schlecht patchen können, weil diese in den Kliniken stehen und dort Patches auszurollen ist extrem schwer. Das braucht Zeit. Verraten kann ich lediglich, dass der Monitor, mit dem ich den Hack demonstriert habe, extrem häufig benutzt wird – und zwar mit unterschiedlicher Optik, aber dem gleichen Einbau.

Sind die Hersteller von Medizingeräten kooperativ, wenn Sie Probleme melden?

Das ist extrem unterschiedlich. Es gibt auch im Medizinbereich Hersteller, die begrüßen das sehr, wenn man Schwachstellen gefunden hat. Es gibt aber auch Hersteller, die blockieren. Was wir allerdings bemerken ist, dass die Bereitschaft der Hersteller im Vorhinein was zu tun, relativ gering ist. Es kristallisiert sich stark heraus, dass das Thema Security bei ihnen gar nicht auf der Agenda steht.

Die Food & Drug Administration (FDA), die in den USA unter anderem dafür zuständig ist, unter welchen Bedingungen solche Geräte zum Einsatz kommen dürfen, hat im Sommer eine Empfehlung herausgegeben, die besagt, dass die Hersteller dazu angehalten sind, etwas gegen Cyberangriffe auf ihre Geräte zu tun. Wenn eine Zertifizierungsbehörde jemanden im Jahr 2013 sagen muss, dass er auf Security zu achten hat, liegt wohl einiges im Argen. Das konnten wir mit unseren Forschungen bisher bestätigen.

Wie kann man die Geräte, jetzt speziell die Patientenmonitore, sicherer machen?

In dem Bereich könnte man mit der verschlüsselten Kommunikation anfangen. Über eine verschlüsselte Kommunikation findet man dann auch Wege, die Geräte untereinander zu authentifizieren. Im Moment ist es nämlich so, dass wir als Angreifer uns einfach auf einem Patientenmonitor anmelden und als anderes Gerät ausgeben können und es wird uns immer geglaubt. Da ist keinerlei Mechanismus implementiert, der schaut, ob das wirklich

ein Gerät ist, dem ich vertrauen kann. Das muss man auch historisch betrachten. Vor zehn Jahren waren die Monitore noch etwas schwach auf der Brust, da zählte jede Zeile Code. Mittlerweile ist das aber aus technischer Sicht überhaupt kein Problem mehr. Doch so etwas kostet etwas, ist aufwendig und deswegen bleibt es oft auf der Strecke.

Das klingt absurd, wenn man bedenkt, dass es dabei um Menschenleben geht.

Wenn wir an kritische Infrastrukturen denken, reden wir immer über Atomkraftwerke oder die Scada-Steuerung. Aber wenn es darum geht, dass ein Angriff auf ein System ein Menschenleben kosten kann, ist das die wohl kritischste Infrastruktur. Deswegen ist es erschreckend, dass die Hersteller da nicht mehr investieren.

Warum wird so wenig in die IT-Security von Medizingeräten investiert?

Sowohl die Hersteller als auch die Kliniken geben sich damit zufrieden, dass sich die Geräte in einem geschlossenen Netzwerk befinden, in das von außen keiner rein kommt. Das ist aber relativ einfach. Wenn man durch eine Klinik geht, sieht man überall LAN-Steckdosen, die Geräte selbst haben LAN-Buchsen. Im Zweifelsfall hält einem wenig davon ab, ein Gerät so umzuprogrammieren, dass man sich damit in das Netzwerk der Klinik hängen kann. Wenn man ein Gerät unter Kontrolle hat, kann man auch das Netz kontrollieren.

Wie kann man ein Umdenken bei den Herstellern und Kliniken erreichen?

Durch viele Publikationen. Die FDA hat einen Anfang gemacht. Auch wir als Security-Analysten sind gefragt, in dem wir uns gezielt Geräte anschauen müssen, um ein bisschen Druck auszuüben. Wenn IT-Security auch von den Kliniken eingefordert wird, wird es auch helfen. Über die Kliniken lässt sich auch leichter Druck ausüben, denn letztendlich sind sie verantwortlich, wenn etwas passiert. Hier sind wir auch auf der Suche nach Kooperationspartnern. Die Kliniken haben auch ein viel höheres Interesse an IT-Security. Bisher haben ausschließlich Hersteller reagiert, die schon einmal ein Problem hatten.

Kann man Herstellerversäumnisse in einem Krankenhausnetzwerk überhaupt ausbügeln?

Das ist schwierig. Bei den Geräten, die wir uns angesehen haben, kann ich nicht empfehlen, sie ans Netzwerk zu hängen. Die sollte man nur vom Netzwerk abgekoppelt betreiben, weil die Schwachstellen schwerwiegend sind. Doch gerade dahin geht der neue Trend, wie ich zuletzt auf der Medizinmesse MEDICA in Düsseldorf beobachten konnte. Man hat künftig nur noch eine Warte, wo eine Person sitzt, die mehrere Patientenbildschirme über das Netzwerk beobachtet.

Was für Medizingeräte sind noch gefährdet, außer Patientenmonitore?

Am meisten gefährdet ist alles, was ein Feedback zum Patienten hat wie z.B. Spritzenpumpen. Wenn Patienten auf der Intensivstation mehr als ein Medikament verabreicht bekommen, hängen diese Medikamente in automatisierten Spritzenpumpen. Diese werden heutzutage auch mit Netzwerkschnittstellen gebaut, so dass man von der Leitwarte aus sehen kann, wie diese gerade eingestellt sind. Über Sicherheitslücken könnte man da aber

drankommen. Der verstorbene Sicherheitsspezialist Barnaby Jack hat das z.B. mit einer Insulinpumpe vorgeführt, indem er die komplette Dosis auf einmal abgeben konnte. Wenn die Hersteller sagen, dass man nichts manipulieren kann, heißt das noch lange nicht, dass das auch stimmt.

Barnaby Jack wollte zuletzt einen Herzschrittmacher-Hack demonstrieren, doch kurz zuvor ist er verstorben.

Ja, er hat Forschungen in dem Gebiet gemacht. Es gibt auch wissenschaftliche Analysen dazu mit interessanten und bedrohlichen Ergebnissen. Dick Cheney hatte in einem Interview gesagt, dass er sich seine Wireless-Schnittstelle in seinem Herzschrittmacher deaktivieren lässt, weil er Angst davor hat, dass ihm Terroristen über die Luftbrücke das Gerät ausschalten. Das ist eine absolut realistische Bedrohung. Die Hersteller vertrauen dabei immer darauf, dass sie proprietäre Protokolle einsetzen, die keiner kennt und gehen davon aus, dass die Hürde für den Angreifer so hoch ist, dass er nicht auf die Idee kommt, sich das genauer anzusehen und Schwachstellen zu suchen. Das ist aber ein Trugschluss.

Würden Sie sich noch in ein Krankenhaus legen mit dem Wissen, das Sie haben?

Natürlich. Wenn es um das eigene Leben geht, dann denkt man in der Regel nicht darüber nach. Da möchte man, dass einem geholfen wird und da geht man das Risiko ein. Das würde ich auch jedem raten.

Nicht nur in Krankenhäusern kommt viel neue Medizintechnik zum Einsatz, sie ist auch für den Heimgebrauch stark im Steigen. Wo liegen hier die Gefahren?

Ja, Ambient Assistent Living (AAL) ist ein großer Bereich. Die Technik wird halt immer billiger. Die Kommunikationsmöglichkeiten ebenso. Gerade für ältere Leute kann das durchaus von Vorteil sein, wenn sie mit AAL kleine Helfer in der Umgebung haben. Solche Geräte werden nie dafür gebaut, dass sie sicher sind, sondern immer nur dazu, dass sie ihre primäre Funktion erfüllen. Der Kosten- und Marktdruck ist hoch, IT-Security bleibt außen vor. Wenn man IT-Security gut macht, kann man das auch schlecht in Zahlen messen, denn man bemerkt sie nicht. Deswegen ist es schwer für Unternehmen, damit in der Chefetage zu argumentieren.

Wie lange ist Ihr Forschungsprojekt bei ERNW angelegt?

Open End. Es ist sehr zeitintensiv. Die Kliniken müssen Geräte bereitstellen. Die müssen aus einem Wartungszyklus herausgenommen werden. Dann muss sichergestellt sein, dass die Geräte nach den Tests genauso funktionieren wie vorher. Das ist alles extrem aufwendig und muss gut geplant werden. Medizingeräte sind komplexer als Heim-WLAN-Router.

(FUTUREZONE) ERSTELLT AM 25.11.2013, 00:00

DEEPSEC

Forscher zeigt: So leicht lassen sich Medizingeräte hacken

von Barbara Wimmer 25.11.13, 00:00 shroombab Mail an Autor

Florian Grunow hackte auf der DeepSec in Wien einen Patientenmonitor. - Foto: Joanna Pianka

DEEPSEC
Forscher zeigt: So leicht lassen sich Medizingeräte hacken
KOMMENTARE (8)
MEHR ZUM THEMA

Die IT-Sicherheit kommt bei vielen Medizingeräten zu kurz. Bei der Konferenz Deep Sec demonstrierte der Forscher Florian Grunow, wie man einen Patientenmonitor manipuliert.

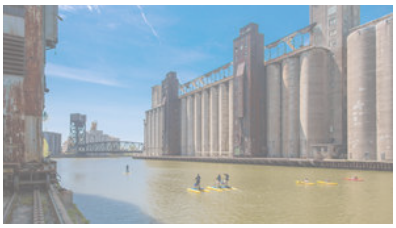
SICHERHEITSLÜCKE, SICHERHEIT, SICHERHEITSKONFERENZ, SICHERHEITSEXPERTEN, IT-SECURITY, DEEPSEC, HERZSCHRITTMACHER, PATIENTENMONITOR, INSULINPUMPE, MEDIZINTECHNIK

Eigentlich war der Patient tot. Am Monitor, der zur Überwachung seiner Vitalparameter eingesetzt wurde, lebte er jedoch noch. Bei der Sicherheitskonferenz DeepSec in Wien zeigte der Sicherheitsanalyst Florian Grunow live, wie man Patientenmonitore, die man im Krankenhaus zur Überwachung des Zustands von Patienten einsetzt, manipulieren kann. Grunow manipulierte dabei zuerst den Bildschirm des Monitors, in Folge spielte er aber auch im zentralen Netzwerk falsche Daten ein. Das Ganze dauerte nur wenige Minuten. Der futurezone erzählte der Sicherheitsforscher, der für das Unternehmen ERNW in Heidelberg an einem entsprechenden Research-Projekt beteiligt ist, wie das möglich wird und warum Hersteller den Aspekt der IT-Security von medizinischen Geräten sträflich vernachlässigen.

Futurezone: Herr Grunow, Sie erforschen die Sicherheit von Medizingeräten. War es einfach, an die entsprechenden Geräte heranzukommen?
Florian Grunow: Nein, es ist nicht ganz einfach, an die Geräte zu kommen. Entweder man braucht dafür Lizenzen z.B. wenn man sich ein Röntgengerät anschauen möchte. Das darf man auch nicht ohne spezielle Ausbildung und Berechtigungsscheine betreiben. Da wir das als IT-Security-Unternehmen nicht aufweisen können, haben wir beim Patientenmonitoring angefangen. Die Daten, die man aus dem Patientenmonitor

FEATURED

VERKEHR
Hier-Box holt bei Autounfällen automatisch Hilfe



REPORTAGE
Buffalo: „Stadt des Lichts" kämpft gegen den Rost

AKTION

gewinnt, sind für den Arzt auch Grundlage, um Entscheidungen über seine nächsten Schritte zu treffen.

Was genau haben Sie bei Ihren Forschungen rausgefunden und auf der DeepSec demonstriert?
Die Idee ist, den Überwachungsbildschirm, der die Vitalzeichen des Patienten anzeigt, so zu manipulieren, dass es halt einen lebenden Patienten anzeigt, obwohl der Patient gerade Probleme hat oder möglicherweise schon verstorben ist. Der Monitor ist dabei mit einem Netzwerkkabel am internen Netzwerk angeschlossen und sendet seine Daten an die Zentralstation. Wir haben getestet, ob man diese Zentralstation so angreifen kann, dass ich ihr vorgauklen kann, dass es dem Patienten wunderbar geht, obwohl er gerade Probleme hat. Das haben wir bei den Modellen von Monitoren, die wir uns bisher angesehen haben, geschafft.

Foto: Joanna Pianka

Wie haben Sie das bewerkstelligt?
Wir konnten sowohl den Bildschirm als auch die Zentralstation so manipulieren, dass angezeigt wird, was wir wollen und zwar auch im laufenden Betrieb. Wir haben einen Weg gefunden, uns im Kommunikationsprozess dazwischen zu schalten und den Monitor aus der Kommunikation auszuklinken und selbst Daten an die Zentralstation zu schicken. Wie wir das genau gemacht haben, haben wir den Herstellern übermittelt.

In der Regel müssen die Hersteller dann in einem bestimmten Zeitraum reagieren. Wird das bei Medizingeräten auch gehandhabt?
Stimmt, normalerweise gibt man eine Deadline an, um den Hersteller unter Druck zu setzen, damit er die Sicherheitslücken behebt. In dem Fall muss man da ein bisschen vorsichtiger sein, weil man das Druckmittel gar nicht in der Hand hat. Da hängen Menschenleben dran und in so einem Fall kann man nicht einfach rausposaunen, wie man es gemacht hat.

Das heißt, Sie veröffentlichen auch nicht den Namen des Monitor-Herstellers?
Nein. Bei medizinischen Geräten haben wir das Problem, dass die Hersteller die Geräte ganz schlecht patchen können, weil diese in den Kliniken stehen und dort Patches auszurollen ist extrem schwer. Das braucht Zeit. Verraten kann ich lediglich, dass der Monitor, mit dem ich den Hack demonstriert habe, extrem häufig benutzt wird – und zwar mit unterschiedlicher Optik, aber dem gleichen Einbau.

Facebook-Video zeigt waghalsige Aktion im AKW Zwentendorf

Foto: Joanna Pianka

Sind die Hersteller von Medizingeräten kooperativ, wenn Sie Probleme melden?
Das ist extrem unterschiedlich. Es gibt auch im Medizinbereich Hersteller, die begrüßen das sehr, wenn man Schwachstellen gefunden hat. Es gibt aber auch Hersteller, die blockieren. Was wir allerdings bemerken ist, dass die Bereitschaft der Hersteller im Vorhinein was zu tun, relativ gering ist. Es kristallisiert sich stark heraus, dass das Thema Security bei ihnen gar nicht auf der Agenda steht.

Die Food & Drug Administration (FDA), die in den USA unter anderem dafür zuständig ist, unter welchen Bedingungen solche Geräte zum Einsatz kommen dürfen, hat im Sommer eine Empfehlung herausgegeben, die besagt, dass die Hersteller dazu angehalten sind, etwas gegen Cyberangriffe auf ihre Geräte zu tun. Wenn eine Zertifizierungsbehörde jemanden im Jahr 2013 sagen muss, dass er auf Security zu achten hat, liegt wohl einiges im Argen. Das konnten wir mit unseren Forschungen bisher bestätigen.

Wie kann man die Geräte, jetzt speziell die Patientenmonitore, sicherer machen?
In dem Bereich könnte man mit der verschlüsselten Kommunikation anfangen. Über eine verschlüsselte Kommunikation findet man dann auch Wege, die Geräte untereinander zu authentifizieren. Im Moment ist es nämlich so, dass wir als Angreifer uns einfach auf einem Patientenmonitor anmelden und als anderes Gerät ausgeben können und es wird uns immer geglaubt. Da ist keinerlei Mechanismus implementiert, der schaut, ob das wirklich ein Gerät ist, dem ich vertrauen kann. Das muss man auch historisch betrachten. Vor zehn Jahren waren die Monitore noch etwas schwach auf der Brust, da zählte jede Zeile Code. Mittlerweile ist das aber aus technischer Sicht überhaupt kein Problem mehr. Doch so etwas kostet etwas, ist aufwendig und deswegen bleibt es oft auf der Strecke.

Das klingt absurd, wenn man bedenkt, dass es dabei um Menschenleben geht.
Wenn wir an kritische Infrastrukturen denken, reden wir immer über Atomkraftwerke oder die Scada-Steuerung. Aber wenn es darum geht, dass ein Angriff auf ein System ein Menschenleben kosten kann, ist das die wohl kritischste Infrastruktur. Deswegen ist es erschreckend, dass die Hersteller da nicht mehr investieren.

Warum wird so wenig in die IT-Security von Medizingeräten investiert?
Sowohl die Hersteller als auch die Kliniken geben sich damit zufrieden, dass sich die Geräte in einem geschlossenen Netzwerk befinden, in das von außen keiner rein kommt. Das ist aber relativ einfach. Wenn man durch eine Klinik geht, sieht man überall LAN-Steckdosen, die Geräte selbst haben LAN-Buchsen. Im Zweifelsfall hält einem wenig davon ab, ein Gerät so umzuprogrammieren, dass man sich damit in das Netzwerk der Klinik hängen kann. Wenn man ein Gerät unter Kontrolle hat, kann man auch das Netz kontrollieren.

Wie kann man ein Umdenken bei den Herstellern und Kliniken erreichen?

Durch viele Publikationen. Die FDA hat einen Anfang gemacht. Auch wir als Security-Analysten sind gefragt, in dem wir uns gezielt Geräte anschauen müssen, um ein bisschen Druck auszuüben. Wenn IT-Security auch von den Kliniken eingefordert wird, wird es auch helfen. Über die Kliniken lässt sich auch leichter Druck ausüben, denn letztendlich sind sie verantwortlich, wenn etwas passiert. Hier sind wir auch auf der Suche nach Kooperationspartnern. Die Kliniken haben auch ein viel höheres Interesse an IT-Security. Bisher haben ausschließlich Hersteller reagiert, die schon einmal ein Problem hatten.

Foto: Joanna Pianka

Kann man Herstellerversäumnisse in einem Krankenhausnetzwerk überhaupt ausbügeln?
Das ist schwierig. Bei den Geräten, die wir uns angesehen haben, kann ich nicht empfehlen, sie ans Netzwerk zu hängen. Die sollte man nur vom Netzwerk abgekoppelt betreiben, weil die Schwachstellen schwerwiegend sind. Doch gerade dahin geht der neue Trend, wie ich zuletzt auf der Medizinmesse MEDICA in Düsseldorf beoachten konnte. Man hat künftig nur noch eine Warte, wo eine Person sitzt, die mehrere Patientenbildschirme über das Netzwerk beobachtet.

Was für Medizingeräte sind noch gefährdet, außer Patientenmonitore?
Am meisten gefährdet ist alles, was ein Feedback zum Patienten hat wie z.B. Spritzenpumpen. Wenn Patienten auf der Intensivstation mehr als ein Medikament verabreicht bekommen, hängen diese Medikamente in automatisierten Spritzenpumpen. Diese werden heutzutage auch mit Netzwerkschnittstellen gebaut, so dass man von der Leitwarte aus sehen kann, wie diese gerade eingestellt sind. Über Sicherheitslücken könnte man da aber drankommen. Der verstorbene Sicherheitsspezialist Barnaby Jack hat das z.B. mit einer Insulinpumpe vorgeführt, indem er die komplette Dosis auf einmal abgeben konnte. Wenn die Hersteller sagen, dass man nichts manipulieren kann, heißt das noch lange nicht, dass das auch stimmt.

Barnaby Jack wollte zuletzt einen Herzschrittmacher-Hack demonstrieren, doch kurz zuvor ist er verstorben.
Ja, er hat Forschungen in dem Gebiet gemacht. Es gibt auch wissenschaftliche Analysen dazu mit interessanten und bedrohlichen Ergebnissen. Dick Cheney hatte in einem Interview gesagt, dass er sich seine Wireless-Schnittstelle in seinem Herzschrittmacher deaktivieren lässt, weil er Angst davor hat, dass ihm Terroristen über die Luftbrücke das Gerät ausschalten. Das ist eine absolut realistische Bedrohung. Die Hersteller vertrauen dabei immer darauf, dass sie proprietäre Protokolle einsetzen, die keiner kennt und gehen davon aus, dass die Hürde für den Angreifer so hoch ist, dass er nicht auf die Idee kommt, sich das genauer anzusehen und Schwachstellen zu suchen. Das ist aber ein Trugschluss.

Würden Sie sich noch in ein Krankenhaus legen mit dem Wissen, das Sie haben?
Natürlich. Wenn es um das eigene Leben geht, dann denkt man in der Regel nicht darüber nach. Da möchte man, dass einem geholfen wird und da geht man das Risiko ein. Das würde ich auch

jedem raten.

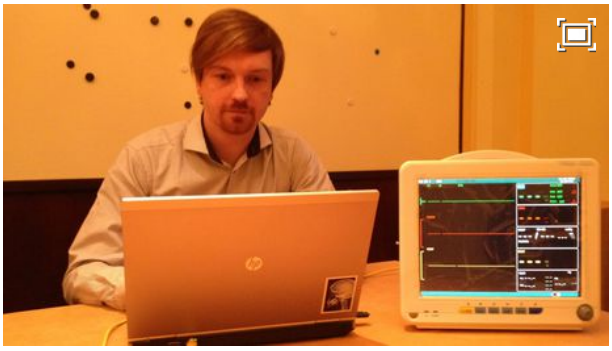


Foto: Barbara Wimmer

Nicht nur in Krankenhäusern kommt viel neue Medizintechnik zum Einsatz, sie ist auch für den Heimgebrauch stark im Steigen. Wo liegen hier die Gefahren?
Ja, Ambient Assistent Living (AAL) ist ein großer Bereich. Die Technik wird halt immer billiger. Die Kommunikationsmöglichkeiten ebenso. Gerade für ältere Leute kann das durchaus von Vorteil sein, wenn sie mit AAL kleine Helfer in der Umgebung haben. Solche Geräte werden nie dafür gebaut, dass sie sicher sind, sondern immer nur dazu, dass sie ihre primäre Funktion erfüllen. Der Kosten- und Marktdruck ist hoch, IT-Security bleibt außen vor. Wenn man IT-Security gut macht, kann man das auch schlecht in Zahlen messen, denn man bemerkt sie nicht. Deswegen ist es schwer für Unternehmen, damit in der Chefetage zu argumentieren.

Wie lange ist Ihr Forschungsprojekt bei ERNW angelegt?
Open End. Es ist sehr zeitintensiv. Die Kliniken müssen Geräte bereitstellen. Die müssen aus einem Wartungszyklus herausgenommen werden. Dann muss sichergestellt sein, dass die Geräte nach den Tests genauso funktionieren wie vorher. Das ist alles extrem aufwendig und muss gut geplant werden. Medizingeräte sind komplexer als Heim-WLAN-Router.

(FUTUREZONE) ERSTELLT AM 25.11.2013, 00:00

SICHERHEITSLÜCKE, SICHERHEIT, SICHERHEITSKONFERENZ, SICHERHEITSEXPERTEN, IT-SECURITY, DEEPSEC, HERZSCHRITTMACHER, PATIENTENMONITOR, INSULINPUMPE, MEDIZINTECHNIK

Kommentare (8)

Ihr Kommentar
Bitte loggen Sie sich ein

rasierklingenritterin vor einem jahrpermalink | melden 0 0

Dank an die Autorin für den Themenfokus.

http://m.kurier.at/lebensart/technik/medizingeraete-lassen-sich-leicht-hacken/37.040.304

DEEPSEC

Forscher zeigt: So leicht lassen sich Medizingeräte hacken

Barbara Wimmer

FUTUREZONE

Letztes Update am 25.11.2013, 00:00

Die IT-Sicherheit kommt bei vielen Medizingeräten zu kurz. Bei der Konferenz Deep Sec demonstrierte der Forscher Florian Grunow, wie man einen Patientenmonitor manipuliert.

Eigentlich war der Patient tot. Am Monitor, der zur Überwachung seiner Vitalparameter eingesetzt wurde, lebte er jedoch noch. Bei der Sicherheitskonferenz DeepSec in Wien zeigte der Sicherheitsanalyst Florian Grunow live, wie man Patientenmonitore, die man im Krankenhaus zur Überwachung des Zustands von Patienten einsetzt, manipulieren kann. Grunow manipulierte dabei zuerst den Bildschirm des Monitors, in Folge spielte er aber auch im zentralen Netzwerk falsche Daten ein. Das Ganze dauerte nur wenige Minuten. Der futurezone erzählte der Sicherheitsforscher, der für das Unternehmen ERNW in Heidelberg an einem entsprechenden Research-Projekt beteiligt ist, wie das möglich wird und warum Hersteller den Aspekt der IT-Security von medizinischen Geräten sträflich vernachlässigen.

Futurezone: Herr Grunow, Sie erforschen die Sicherheit von Medizingeräten. War es einfach, an die entsprechenden Geräte heranzukommen?

Florian Grunow: Nein, es ist nicht ganz einfach, an die Geräte zu kommen. Entweder man braucht dafür Lizenzen z.B. wenn man sich ein Röntgengerät anschauen möchte. Das darf man auch nicht ohne spezielle Ausbildung und Berechtigungsscheine betreiben. Da wir das als IT-Security-Unternehmen nicht aufweisen können, haben wir beim Patientenmonitoring angefangen. Die Daten, die man aus dem Patientenmonitor gewinnt, sind für den Arzt auch Grundlage, um Entscheidungen über seine nächsten Schritte zu treffen.

Was genau haben Sie bei Ihren Forschungen rausgefunden und auf der DeepSec demonstriert?

Die Idee ist, den Überwachungsbildschirm, der die Vitalzeichen des Patienten anzeigt, so zu manipulieren, dass es halt einen lebenden Patienten anzeigt, obwohl der Patient gerade Probleme hat oder möglicherweise schon verstorben ist. Der Monitor ist dabei mit einem Netzwerkkabel am internen Netzwerk angeschlossen und sendet seine Daten an die Zentralstation. Wir haben getestet, ob man diese Zentralstation so angreifen kann, dass ich ihr vorgauklen kann, dass es dem Patienten wunderbar geht, obwohl er gerade Probleme hat. Das ha-

ben wir bei den Modellen von Monitoren, die wir uns bisher angesehen haben, geschafft.

Wie haben Sie das bewerkstelligt?

Wir konnten sowohl den Bildschirm als auch die Zentralstation so manipulieren, dass angezeigt wird, was wir wollen und zwar auch im laufenden Betrieb. Wir haben einen Weg gefunden, uns im Kommunikationsprozess dazwischen zu schalten und den Monitor aus der Kommunikation auszuklinken und selbst Daten an die Zentralstation zu schicken. Wie wir das genau gemacht haben, haben wir den Herstellern übermittelt.

In der Regel müssen die Hersteller dann in einem bestimmten Zeitraum reagieren. Wird das bei Medizingeräten auch gehandhabt?

Stimmt, normalerweise gibt man eine Deadline an, um den Hersteller unter Druck zu setzen, damit er die Sicherheitslücken behebt. In dem Fall muss man da ein bisschen vorsichtiger sein, weil man das Druckmittel gar nicht in der Hand hat. Da hängen Menschenleben dran und in so einem Fall kann man nicht einfach rausposaunen, wie man es gemacht hat.

Das heißt, Sie veröffentlichen auch nicht den Namen des Monitor-Herstellers?

Nein. Bei medizinischen Geräten haben wir das Problem, dass die Hersteller die Geräte ganz schlecht patchen können, weil diese in den Kliniken stehen und dort Patches auszurollen ist extrem schwer. Das braucht Zeit. Verraten kann ich lediglich, dass der Monitor, mit dem ich den Hack demonstriert habe, extrem häufig benutzt wird – und zwar mit unterschiedlicher Optik, aber dem gleichen Einbau.

Sind die Hersteller von Medizingeräten kooperativ, wenn Sie Probleme melden?

Das ist extrem unterschiedlich. Es gibt auch im Medizinbereich Hersteller, die begrüßen das sehr, wenn man Schwachstellen gefunden hat. Es gibt aber auch Hersteller, die blockieren. Was wir allerdings bemerken ist, dass die Bereitschaft der Hersteller im Vorhinein was zu tun, relativ gering ist. Es kristallisiert sich stark heraus, dass das Thema Security bei ihnen gar nicht auf der Agenda steht.

Die Food & Drug Administration (FDA), die in den USA unter anderem dafür zuständig ist, unter welchen Bedingungen solche Geräte zum Einsatz kommen dürfen, hat im Sommer eine Empfehlung herausgegeben, die besagt, dass die Hersteller dazu angehalten sind, etwas gegen Cyberangriffe auf ihre Geräte zu tun. Wenn eine Zertifizierungsbehörde jemanden im Jahr 2013 sagen muss, dass er auf Security zu achten hat, liegt wohl einiges im Argen. Das konnten wir mit unseren Forschungen bisher bestätigen.

Wie kann man die Geräte, jetzt speziell die Patientenmonitore, sicherer machen?

In dem Bereich könnte man mit der verschlüsselten Kommunikation anfangen. Über eine verschlüsselte Kommunikation findet man dann auch Wege, die Geräte untereinander zu authentifizieren. Im Moment ist es nämlich so, dass wir als Angreifer uns einfach auf einem Patientenmonitor anmelden und als anderes Gerät ausgeben können und es wird uns immer geglaubt. Da ist keinerlei Mechanismus implementiert, der schaut, ob das wirklich

ein Gerät ist, dem ich vertrauen kann. Das muss man auch historisch betrachten. Vor zehn Jahren waren die Monitore noch etwas schwach auf der Brust, da zählte jede Zeile Code. Mittlerweile ist das aber aus technischer Sicht überhaupt kein Problem mehr. Doch so etwas kostet etwas, ist aufwendig und deswegen bleibt es oft auf der Strecke.

Das klingt absurd, wenn man bedenkt, dass es dabei um Menschenleben geht.

Wenn wir an kritische Infrastrukturen denken, reden wir immer über Atomkraftwerke oder die Scada-Steuerung. Aber wenn es darum geht, dass ein Angriff auf ein System ein Menschenleben kosten kann, ist das die wohl kritischste Infrastruktur. Deswegen ist es erschreckend, dass die Hersteller da nicht mehr investieren.

Warum wird so wenig in die IT-Security von Medizingeräten investiert?

Sowohl die Hersteller als auch die Kliniken geben sich damit zufrieden, dass sich die Geräte in einem geschlossenen Netzwerk befinden, in das von außen keiner rein kommt. Das ist aber relativ einfach. Wenn man durch eine Klinik geht, sieht man überall LAN-Steckdosen, die Geräte selbst haben LAN-Buchsen. Im Zweifelsfall hält einem wenig davon ab, ein Gerät so umzuprogrammieren, dass man sich damit in das Netzwerk der Klinik hängen kann. Wenn man ein Gerät unter Kontrolle hat, kann man auch das Netz kontrollieren.

Wie kann man ein Umdenken bei den Herstellern und Kliniken erreichen?

Durch viele Publikationen. Die FDA hat einen Anfang gemacht. Auch wir als Security-Analysten sind gefragt, in dem wir uns gezielt Geräte anschauen müssen, um ein bisschen Druck auszuüben. Wenn IT-Security auch von den Kliniken eingefordert wird, wird es auch helfen. Über die Kliniken lässt sich auch leichter Druck ausüben, denn letztendlich sind sie verantwortlich, wenn etwas passiert. Hier sind wir auch auf der Suche nach Kooperationspartnern. Die Kliniken haben auch ein viel höheres Interesse an IT-Security. Bisher haben ausschließlich Hersteller reagiert, die schon einmal ein Problem hatten.

Kann man Herstellerversäumnisse in einem Krankenhausnetzwerk überhaupt ausbügeln?

Das ist schwierig. Bei den Geräten, die wir uns angesehen haben, kann ich nicht empfehlen, sie ans Netzwerk zu hängen. Die sollte man nur vom Netzwerk abgekoppelt betreiben, weil die Schwachstellen schwerwiegend sind. Doch gerade dahin geht der neue Trend, wie ich zuletzt auf der Medizinmesse MEDICA in Düsseldorf beobachten konnte. Man hat künftig nur noch eine Warte, wo eine Person sitzt, die mehrere Patientenbildschirme über das Netzwerk beobachtet.

Was für Medizingeräte sind noch gefährdet, außer Patientenmonitore?

Am meisten gefährdet ist alles, was ein Feedback zum Patienten hat wie z.B. Spritzenpumpen. Wenn Patienten auf der Intensivstation mehr als ein Medikament verabreicht bekommen, hängen diese Medikamente in automatisierten Spritzenpumpen. Diese werden heutzutage auch mit Netzwerkschnittstellen gebaut, so dass man von der Leitwarte aus sehen kann, wie diese gerade eingestellt sind. Über Sicherheitslücken könnte man da aber

drankommen. Der verstorbene Sicherheitsspezialist Barnaby Jack hat das z.B. mit einer Insulinpumpe vorgeführt, indem er die komplette Dosis auf einmal abgeben konnte. Wenn die Hersteller sagen, dass man nichts manipulieren kann, heißt das noch lange nicht, dass das auch stimmt.

Barnaby Jack wollte zuletzt einen Herzschrittmacher-Hack demonstrieren, doch kurz zuvor ist er verstorben.

Ja, er hat Forschungen in dem Gebiet gemacht. Es gibt auch wissenschaftliche Analysen dazu mit interessanten und bedrohlichen Ergebnissen. Dick Cheney hatte in einem Interview gesagt, dass er sich seine Wireless-Schnittstelle in seinem Herzschrittmacher deaktivieren lässt, weil er Angst davor hat, dass ihm Terroristen über die Luftbrücke das Gerät ausschalten. Das ist eine absolut realistische Bedrohung. Die Hersteller vertrauen dabei immer darauf, dass sie proprietäre Protokolle einsetzen, die keiner kennt und gehen davon aus, dass die Hürde für den Angreifer so hoch ist, dass er nicht auf die Idee kommt, sich das genauer anzusehen und Schwachstellen zu suchen. Das ist aber ein Trugschluss.

Würden Sie sich noch in ein Krankenhaus legen mit dem Wissen, das Sie haben?

Natürlich. Wenn es um das eigene Leben geht, dann denkt man in der Regel nicht darüber nach. Da möchte man, dass einem geholfen wird und da geht man das Risiko ein. Das würde ich auch jedem raten.

Nicht nur in Krankenhäusern kommt viel neue Medizintechnik zum Einsatz, sie ist auch für den Heimgebrauch stark im Steigen. Wo liegen hier die Gefahren?

Ja, Ambient Assistent Living (AAL) ist ein großer Bereich. Die Technik wird halt immer billiger. Die Kommunikationsmöglichkeiten ebenso. Gerade für ältere Leute kann das durchaus von Vorteil sein, wenn sie mit AAL kleine Helfer in der Umgebung haben. Solche Geräte werden nie dafür gebaut, dass sie sicher sind, sondern immer nur dazu, dass sie ihre primäre Funktion erfüllen. Der Kosten- und Marktdruck ist hoch, IT-Security bleibt außen vor. Wenn man IT-Security gut macht, kann man das auch schlecht in Zahlen messen, denn man bemerkt sie nicht. Deswegen ist es schwer für Unternehmen, damit in der Chefetage zu argumentieren.

Wie lange ist Ihr Forschungsprojekt bei ERNW angelegt?

Open End. Es ist sehr zeitintensiv. Die Kliniken müssen Geräte bereitstellen. Die müssen aus einem Wartungszyklus herausgenommen werden. Dann muss sichergestellt sein, dass die Geräte nach den Tests genauso funktionieren wie vorher. Das ist alles extrem aufwendig und muss gut geplant werden. Medizingeräte sind komplexer als Heim-WLAN-Router.

Erstellt am 25.11.2013 00:00 Uhr

Florian Grunow hackte auf der DeepSec in Wien einen Patientenmonitor. - Foto: Joanna Pianka

DEEPSEC

Forscher zeigt: So leicht lassen sich Medizingeräte hacken

Letztes Update am 25.11.2013, 00:00

Die IT-Sicherheit kommt bei vielen Medizingeräten zu kurz. Bei der Konferenz Deep Sec demonstrierte der Forscher Florian Grunow, wie man einen Patientenmonitor manipuliert.

Barbara Wimmer
FUTUREZONE

Eigentlich war der Patient tot. Am Monitor, der zur Überwachung seiner Vitalparameter eingesetzt wurde, lebte er jedoch noch. Bei der Sicherheitskonferenz DeepSec in Wien zeigte der Sicherheitsanalyst Florian Grunow live, wie man Patientenmonitore, die man im Krankenhaus zur Überwachung des Zustands von Patienten einsetzt, manipulieren kann. Grunow manipulierte dabei zuerst den Bildschirm des Monitors, in Folge spielte er aber auch im zentralen Netzwerk falsche Daten ein. Das Ganze dauerte nur wenige Minuten. Der futurezone erzählte der Sicherheitsforscher, der für das Unternehmen ERNW in Heidelberg an einem entsprechenden Research-Projekt beteiligt ist, wie das möglich wird und warum Hersteller den Aspekt der IT-Security von medizinischen Geräten sträflich vernachlässigen.

…geräten. War

…. Entweder man …öchte. Das darf man auch nicht ohne spezielle Ausbildung und Berechtigungsscheine betreiben. Da wir das als IT-Security-Unternehmen nicht aufweisen können, haben wir beim Patientenmonitoring angefangen. Die Daten, die man aus dem Patientenmonitor gewinnt, sind für den Arzt auch Grundlage, um Entscheidungen über seine nächsten Schritte zu treffen.

Was genau haben Sie bei Ihren Forschungen rausgefunden und auf der DeepSec demonstriert?
Die Idee ist, den Überwachungsbildschirm, der die Vitalzeichen des Patienten anzeigt, so zu manipulieren, dass es halt einen lebenden Patienten anzeigt, obwohl der Patient gerade Probleme hat oder möglicherweise schon verstorben ist. Der Monitor ist dabei mit einem Netzwerkkabel am internen Netzwerk angeschlossen und sendet seine Daten an die Zentralstation. Wir haben getestet, ob man diese Zentralstation so angreifen kann, dass ich ihr vorgauklen kann, dass es dem Patienten wunderbar geht, obwohl er gerade Probleme hat. Das haben wir bei den Modellen von Monitoren, die wir uns bisher angesehen haben, geschafft.

Foto: Joanna Pianka

Wie haben Sie das bewerkstelligt?
Wir konnten sowohl den Bildschirm als auch die Zentralstation so manipulieren, dass angezeigt wird, was wir wollen und zwar auch im laufenden Betrieb. Wir haben einen Weg gefunden, uns im Kommunikationsprozess dazwischen zu schalten und den Monitor aus der Kommunikation auszuklinken und selbst Daten an die Zentralstation zu schicken. Wie wir das genau gemacht haben, haben wir den Herstellern übermittelt.

In der Regel müssen die Hersteller dann in einem bestimmten Zeitraum reagieren. Wird das bei Medizingeräten auch gehandhabt?
Stimmt, normalerweise gibt man eine Deadline an, um den Hersteller unter Druck zu setzen, damit er die Sicherheitslücken behebt. In dem Fall muss man da ein bisschen

vorsichtiger sein, weil man das Druckmittel gar nicht in der Hand hat. Da hängen Menschenleben dran und in so einem Fall kann man nicht einfach rausposaunen, wie man es gemacht hat.

Das heißt, Sie veröffentlichen auch nicht den Namen des Monitor-Herstellers?
Nein. Bei medizinischen Geräten haben wir das Problem, dass die Hersteller die Geräte ganz schlecht patchen können, weil diese in den Kliniken stehen und dort Patches auszurollen ist extrem schwer. Das braucht Zeit. Verraten kann ich lediglich, dass der Monitor, mit dem ich den Hack demonstriert habe, extrem häufig benutzt wird – und zwar mit unterschiedlicher Optik, aber dem gleichen Einbau.

Foto: Joanna Pianka

Sind die Hersteller von Medizingeräten kooperativ, wenn Sie Probleme melden?
Das ist extrem unterschiedlich. Es gibt auch im Medizinbereich Hersteller, die begrüßen das sehr, wenn man Schwachstellen gefunden hat. Es gibt aber auch Hersteller, die blockieren. Was wir allerdings bemerken ist, dass die Bereitschaft der Hersteller im Vorhinein was zu tun, relativ gering ist. Es kristallisiert sich stark heraus, dass das Thema Security bei ihnen gar nicht auf der Agenda steht.

Die Food & Drug Administration (FDA), die in den USA unter anderem dafür zuständig ist, unter welchen Bedingungen solche Geräte zum Einsatz kommen dürfen, hat im Sommer eine Empfehlung herausgegeben, die besagt, dass die Hersteller dazu angehalten sind, etwas gegen Cyberangriffe auf ihre Geräte zu tun. Wenn eine Zertifizierungsbehörde jemanden im Jahr 2013 sagen muss, dass er auf Security zu achten hat, liegt wohl einiges im Argen. Das konnten wir mit unseren Forschungen bisher bestätigen.

Wie kann man die Geräte, jetzt speziell die Patientenmonitore, sicherer machen?
In dem Bereich könnte man mit der verschlüsselten Kommunikation anfangen. Über eine verschlüsselte Kommunikation findet man dann auch Wege, die Geräte untereinander zu authentifizieren. Im Moment ist es nämlich so, dass wir als Angreifer uns einfach auf einem Patientenmonitor anmelden und als anderes Gerät ausgeben können und es wird uns immer geglaubt. Da ist keinerlei Mechanismus implementiert, der schaut, ob das wirklich ein Gerät ist, dem ich vertrauen kann. Das muss man auch historisch betrachten. Vor zehn Jahren waren die Monitore noch etwas schwach auf der Brust, da zählte jede Zeile Code. Mittlerweile ist das aber aus technischer Sicht überhaupt kein Problem mehr. Doch so etwas kostet etwas, ist aufwendig und deswegen bleibt es oft auf der Strecke.

Das klingt absurd, wenn man bedenkt, dass es dabei um Menschenleben geht.
Wenn wir an kritische Infrastrukturen denken, reden wir immer über Atomkraftwerke oder die Scada-Steuerung. Aber wenn es darum geht, dass ein Angriff auf ein System ein Menschenleben kosten kann, ist das die wohl kritischste Infrastruktur. Deswegen ist es erschreckend, dass die Hersteller da nicht mehr investieren.

Warum wird so wenig in die IT-Security von Medizingeräten investiert?
Sowohl die Hersteller als auch die Kliniken geben sich damit zufrieden, dass sich die Geräte in einem geschlossenen Netzwerk befinden, in das von außen keiner rein kommt. Das ist aber relativ einfach. Wenn man durch eine Klinik geht, sieht man überall LAN-Steckdosen, die Geräte selbst haben LAN-Buchsen. Im Zweifelsfall hält einem wenig davon ab, ein Gerät so umzuprogrammieren, dass man sich damit in das Netzwerk der Klinik hängen kann. Wenn man ein Gerät unter Kontrolle hat, kann man auch das Netz kontrollieren.

Wie kann man ein Umdenken bei den Herstellern und Kliniken erreichen?
Durch viele Publikationen. Die FDA hat einen Anfang gemacht. Auch wir als Security-Analysten sind gefragt, in dem wir uns gezielt Geräte anschauen müssen, um ein bisschen Druck auszuüben. Wenn IT-Security auch von den Kliniken eingefordert wird, wird es auch helfen. Über die Kliniken lässt sich auch leichter Druck ausüben, denn letztendlich sind sie verantwortlich, wenn etwas passiert. Hier sind wir auch auf der Suche nach Kooperationspartnern. Die Kliniken haben auch ein viel höheres Interesse an IT-Security. Bisher haben ausschließlich Hersteller reagiert, die schon einmal ein Problem hatten.

Foto: Joanna Pianka

Kann man Herstellerversäumnisse in einem Krankenhausnetzwerk überhaupt ausbügeln?
Das ist schwierig. Bei den Geräten, die wir uns angesehen haben, kann ich nicht empfehlen, sie ans Netzwerk zu hängen. Die sollte man nur vom Netzwerk abgekoppelt betreiben, weil die Schwachstellen schwerwiegend sind. Doch gerade dahin geht der neue Trend, wie ich zuletzt auf der Medizinmesse MEDICA in Düsseldorf beoachten konnte. Man hat künftig nur noch eine Warte, wo eine Person sitzt, die mehrere Patientenbildschirme über das Netzwerk beobachtet.

Was für Medizingeräte sind noch gefährdet, außer Patientenmonitore?
Am meisten gefährdet ist alles, was ein Feedback zum Patienten hat wie z.B. Spritzenpumpen. Wenn Patienten auf der Intensivstation mehr als ein Medikament verabreicht bekommen, hängen diese Medikamente in automatisierten Spritzenpumpen. Diese werden heutzutage auch mit Netzwerkschnittstellen gebaut, so dass man von der Leitwarte aus sehen kann, wie diese gerade eingestellt sind. Über Sicherheitslücken könnte man da aber drankommen. Der verstorbene Sicherheitsspezialist Barnaby Jack hat das z.B. mit einer Insulinpumpe vorgeführt, indem er die komplette Dosis auf einmal abgeben konnte. Wenn die Hersteller sagen, dass man nichts manipulieren kann, heißt das noch lange nicht, dass das auch stimmt.

Barnaby Jack wollte zuletzt einen Herzschrittmacher-Hack demonstrieren, doch kurz zuvor ist er verstorben.
Ja, er hat Forschungen in dem Gebiet gemacht. Es gibt auch wissenschaftliche Analysen dazu mit interessanten und bedrohlichen Ergebnissen. Dick Cheney hatte in einem Interview gesagt, dass er sich seine Wireless-Schnittstelle in seinem Herzschrittmacher deaktivieren lässt, weil er Angst davor hat, dass ihm Terroristen über die Luftbrücke das Gerät ausschalten. Das ist eine absolut realistische Bedrohung. Die Hersteller vertrauen dabei immer darauf, dass sie proprietäre Protokolle einsetzen, die keiner kennt und gehen davon aus, dass die Hürde für den Angreifer so hoch ist, dass er nicht auf die Idee kommt, sich das genauer anzusehen und Schwachstellen zu suchen. Das ist aber ein Trugschluss.

Würden Sie sich noch in ein Krankenhaus legen mit dem Wissen, das Sie haben?
Natürlich. Wenn es um das eigene Leben geht, dann denkt man in der Regel nicht darüber nach. Da möchte man, dass einem geholfen wird und da geht man das Risiko ein. Das würde ich auch jedem raten.

Foto: Barbara Wimmer

Nicht nur in Krankenhäusern kommt viel neue Medizintechnik zum Einsatz, sie ist auch für den Heimgebrauch stark im Steigen. Wo liegen hier die Gefahren?
Ja, Ambient Assistent Living (AAL) ist ein großer Bereich. Die Technik wird halt immer billiger. Die Kommunikationsmöglichkeiten ebenso. Gerade für ältere Leute kann das durchaus von Vorteil sein, wenn sie mit AAL kleine Helfer in der Umgebung haben. Solche Geräte werden nie dafür gebaut, dass sie sicher sind, sondern immer nur dazu, dass sie

ihre primäre Funktion erfüllen. Der Kosten- und Marktdruck ist hoch, IT-Security bleibt außen vor. Wenn man IT-Security gut macht, kann man das auch schlecht in Zahlen messen, denn man bemerkt sie nicht. Deswegen ist es schwer für Unternehmen, damit in der Chefetage zu argumentieren.

Wie lange ist Ihr Forschungsprojekt bei ERNW angelegt?
Open End. Es ist sehr zeitintensiv. Die Kliniken müssen Geräte bereitstellen. Die müssen aus einem Wartungszyklus herausgenommen werden. Dann muss sichergestellt sein, dass die Geräte nach den Tests genauso funktionieren wie vorher. Das ist alles extrem aufwendig und muss gut geplant werden. Medizingeräte sind komplexer als Heim-WLAN-Router.

STICHWORTE: › SICHERHEITSLÜCKE › SICHERHEIT › SICHERHEITSKONFERENZ › SICHERHEITSEXPERTEN › IT-SECURITY › DEEPSEC › HERZSCHRITTMACHER › PATIENTENMONITOR › INSULINPUMPE › MEDIZINTECHNIK

Erstellt am 25.11.2013 00:00 Uhr

DISKUSSION

IHRE MEINUNG ZUM THEMA

EINLOGGEN / REGISTRIEREN

SENDEN

ALEX SORGHI | VOR EINEM JAHR PERMALINK | MELDEN 0 0

Dank an die Autorin für den Themenfokus.

ANTWORTEN

MICHAEL SABRANSKY | VOR EINEM JAHR PERMALINK | MELDEN 0 0

Eine Bedrohung gibt es hier sehr wohl.
1.) Erpressung: Jemand bekommt böswillig Zugriff auf ein solches System und schreibt dann Krankenhaus/Hersteller an: Es gibt einen Bug in Ihrem System. Wir können Ihn für €

xy beheben. Um zu Zeigen, dass dieser besteht prüfen Sie doch mal das Gerät mit MAC

http://www.deutschlandfunk.de/it-sicherheit-konferenz-deep-sec-hinterfragt-den-cyberwar.684.de.html?dram:article_id=269932

IT-Sicherheit

Konferenz Deep Sec hinterfragt den Cyberwar

Von Mariann Unterluggauer

23.11.2013

Die diesjährige Fachkonferenz für IT-Sicherheit "Deep Sec" in Wien hatte es in sich. Statt den immer wiederkehrenden Kanon von besserer Verschlüsselung und sicherem Abspeichern herunterzubeten, hinterfragten die Informatiker Grundsätzliches wie: Gibt es überhaupt einen Cyberwar?

Ein Computerbildschirm zeigt Programmcode-Zeilen. (picture alliance / dpa - Oliver Berg)

Der Cyberwar ist kein klassischer Krieg mit neuen Mitteln, sagen die Sicherheitsexperten auf der Deep Sec – und lehnen den Begriff deshalb ab. (picture alliance / dpa - Oliver Berg)

Rund 160 internationale Sicherheitsexperten trafen sich auf der "Deep Sec", um darüber zu reden, wie Computersysteme sicherer gemacht werden können. Um dies zu erreichen, brauche es vor allem eine offene Diskussion über Fehlschläge, sagt René Pfeiffer, Sicherheitsberater und einer der Veranstalter.

"Fehlschläge sind ein Teil von IT-Security, weil man es nicht immer schafft. Es gibt Einbrüche, es gibt Kompromittierungen. Wir wollten einfach nur klarmachen, dass dies völlig in Ordnung ist, dass man über alles offen reden kann. Das hat nichts mit Preisgabe zu tun, sondern ist ein Zugeben: Ja, ich habe welche. Ja, es gelingt mir nicht immer und wie können wir das in Zukunft besser machen."

Ein Credo der Sicherheitsbranche lautet: Fehler lassen sich vermeiden, indem man sie oft genug begeht.

"Wir haben das in unserem Motto drinnen, ja. Dieser Spruch: 'If you want to fail less, fail often' heißt letztendlich: Hier muss man die geeignete Portion lernen, damit man etwas verbessern kann. Das Problem, das in der IT-Security oft stattfindet, ist: Wenn nicht passiert, glaubt man, dass alles in Ordnung ist. Erst dann, wenn etwas passiert, fängt man an, die Konfigurationen zu hinterfragen und zu verbessern. Übersetzt heißt das einfach: Wenn ich weniger Fehlschläge haben will, muss ich oft etwas verbessern. Denn die Fehlschläge sind der Anlass, wo man was macht, denn normalerweise macht man ohne Anlass nichts."

Ein altbekanntes Problem: Sicherungen werden meist erst dann erstellt, wenn Daten bereits verloren gegangen sind. Und auch die Auslagerung der Daten in eine Cloud ist keine Lösung - auch nicht für die NASA. In einem Vortrag wurde darauf hingewiesen, dass es der NASA keineswegs billiger kommt, wenn sie ihre Daten in entfernte Rechenzentren auslagert. Ein Grund dafür ist, dass nicht nur ein Cloud-Service genutzt werden kann, sondern

mehrere. Dabei die Übersicht nicht zu verlieren ist ein Mehraufwand für die Administratoren. Michael Kafka, einer der Veranstalter der Deep Sec und in der Community unter dem Pseudonym Mika bekannt, hält von derartigen Trends generell wenig.

"Wir aus der Security werden auf Themen geworfen wie: 'bring your own device', Smartphones und Cloud. Lauter unwichtiges Zeug. Wir haben momentan noch kaum die Basis im Griff! Wir haben kaum eine Kontrolle darüber, wer in unserem System herumspaziert. Wir hören es in unseren Vorträgen, dass teilweise ein halbes bis ein Jahr lang Backdoors existieren. Das ist wirklich problematisch."

Anstatt solche Hintertüren - Backdoors - zu schließen, werden durch die Auslagerung neue geöffnet. Bereits seit Jahren wird auf der Deep Sec der Begriff Cyberwar hinterfragt. Ein Krieg, der vermehrt von militärischen Organisationen, Politikern und Medien heraufbeschworen wird. Krieg ist ein todbringendes Handwerk, das strikten Regeln zu folgen hat. So steht es im Völkerrecht: Ein Krieg hat einen eindeutigen Anfang - die Kriegserklärung eines Staates -, und er hat ein eindeutiges Ende, an dem ein Friedenschluss oder auch eine Staatenbildung steht. Beides trifft auf einen Cyberwar, der mit Software geführt werden soll, nicht zu. Die Sicherheitsexperten auf der Deep Sec lehnen diesen Begriff daher ab. Ein Cyber-Krieg ist kein klassischer Krieg mit neuen Mitteln, sondern etwas ganz anderes.

Michael Kafka: "In unseren Kreisen spricht man nicht von auf- oder abrüsten, das ist nicht der übliche Jargon."

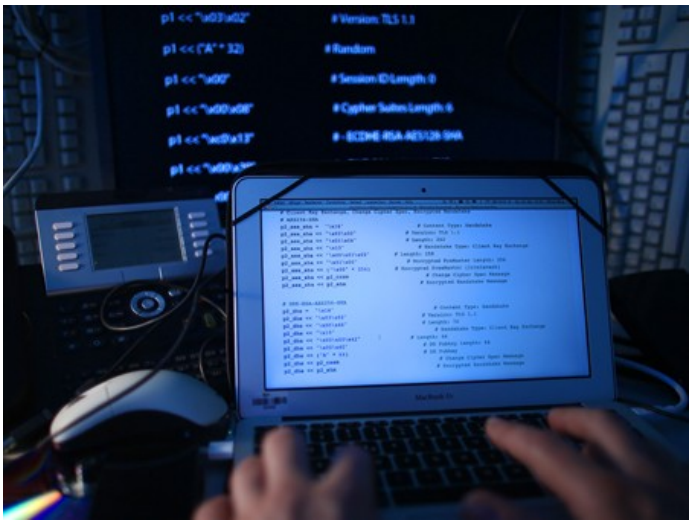
René Pfeiffer: "Also das große Problem da ist, dass oft mithilfe von Analogien diskutiert wird. Das heißt, man verwendet Metaphern, man verwendet 'Cyberwar'. Wenn ich 'Krieg' sage, dann habe ich plötzlich Waffen, und dann hat der eine mehr und der andere weniger. Das sind alles Analogien. Die klingen zwar gut, aber wenn ich wieder zurück gehe zur Security, dann kann ich damit nichts anfangen. Wenn ich mir jetzt überlege: Was ist eine Cyber-Waffe? Was ist eine digitale Waffe? Das ist nichts anderes als Code. Das sind Zahlen. Das heißt, ich müsste zu den Mathematikern gehen und ihnen sagen: Ihr müsst abrüsten. Was heißt das dann? Das macht überhaupt keinen Sinn."

IT-Sicherheit

Konferenz Deep Sec hinterfragt den Cyberwar

Die diesjährige Fachkonferenz für IT-Sicherheit "Deep Sec" in Wien hatte es in sich. Statt den immer wiederkehrenden Kanon von besserer Verschlüsselung und sicherem Abspeichern herunterzubeten, hinterfragten die Informatiker Grundsätzliches wie: Gibt es überhaupt einen Cyberwar?

Von Mariann Unterluggauer



Der Cyberwar ist kein klassischer Krieg mit neuen Mitteln, sagen die Sicherheitsexperten auf der Deep Sec – und lehnen den Begriff deshalb ab. (picture alliance / dpa - Oliver Berg)

Rund 160 internationale Sicherheitsexperten trafen sich auf der "Deep Sec", um darüber zu reden, wie Computersysteme sicherer gemacht werden können. Um dies zu erreichen, brauche es vor allem eine offene Diskussion über Fehlschläge, sagt René Pfeiffer, Sicherheitsberater und einer der Veranstalter.

"Fehlschläge sind ein Teil von IT-Security, weil man es nicht immer schafft. Es gibt Einbrüche, es gibt Kompromittierungen. Wir wollten einfach nur klarmachen, dass dies völlig in Ordnung ist, dass man über alles offen reden kann. Das hat nichts mit Preisgabe zu tun, sondern ist ein Zugeben: Ja, ich habe welche. Ja, es gelingt mir nicht immer und wie können wir das in Zukunft besser machen."

Ein Credo der Sicherheitsbranche lautet: Fehler lassen sich vermeiden, indem man sie oft genug begeht.

"Wir haben das in unserem Motto drinnen, ja. Dieser Spruch: 'If you want to fail less, fail often' heißt letztendlich: Hier muss man die geeignete Portion lernen, damit man etwas verbessern kann. Das Problem, das in der IT-Security

MEHR ZUM THEMA

Zum Themenportal "Risiko Internet"

Das Internet dem Volke - Computer und Kommunikation - 2013-11-09

oft stattfindet, ist: Wenn nicht passiert, glaubt man, dass alles in Ordnung ist. Erst dann, wenn etwas passiert, fängt man an, die Konfigurationen zu hinterfragen und zu verbessern. Übersetzt heißt das einfach: Wenn ich weniger Fehlschläge haben will, muss ich oft etwas verbessern. Denn die Fehlschläge sind der Anlass, wo man was macht, denn normalerweise macht man ohne Anlass nichts."

Ein altbekanntes Problem: Sicherungen werden meist erst dann erstellt, wenn Daten bereits verloren gegangen sind. Und auch die Auslagerung der Daten in eine Cloud ist keine Lösung - auch nicht für die NASA. In einem Vortrag wurde darauf hingewiesen, dass es der NASA keineswegs billiger kommt, wenn sie ihre Daten in entfernte Rechenzentren auslagert. Ein Grund dafür ist, dass nicht nur ein Cloud-Service genutzt werden kann, sondern mehrere. Dabei die Übersicht nicht zu verlieren ist ein Mehraufwand für die Administratoren. Michael Kafka, einer der Veranstalter der Deep Sec und in der Community unter dem Pseudonym Mika bekannt, hält von derartigen Trends generell wenig.

"Wir aus der Security werden auf Themen geworfen wie: 'bring your own device', Smartphones und Cloud. Lauter unwichtiges Zeug. Wir haben momentan noch kaum die Basis im Griff! Wir haben kaum eine Kontrolle darüber, wer in unserem System herumspaziert. Wir hören es in unseren Vorträgen, dass teilweise ein halbes bis ein Jahr lang Backdoors existieren. Das ist wirklich problematisch."

Anstatt solche Hintertüren - Backdoors - zu schließen, werden durch die Auslagerung neue geöffnet. Bereits seit Jahren wird auf der Deep Sec der Begriff Cyberwar hinterfragt. Ein Krieg, der vermehrt von militärischen Organisationen, Politikern und Medien heraufbeschworen wird. Krieg ist ein todbringendes Handwerk, das strikten Regeln zu folgen hat. So steht es im Völkerrecht: Ein Krieg hat einen eindeutigen Anfang - die Kriegserklärung eines Staates -, und er hat ein eindeutiges Ende, an dem ein Friedenschluss oder auch eine Staatenbildung steht. Beides trifft auf einen Cyberwar, der mit Software geführt werden soll, nicht zu. Die Sicherheitsexperten auf der Deep Sec lehnen diesen Begriff daher ab. Ein Cyber-Krieg ist kein klassischer Krieg mit neuen Mitteln, sondern etwas ganz anderes.

Michael Kafka: "In unseren Kreisen spricht man nicht von auf- oder abrüsten, das ist nicht der übliche Jargon."

René Pfeiffer: "Also das große Problem da ist, dass oft mithilfe von Analogien diskutiert wird. Das heißt, man verwendet Metaphern, man verwendet 'Cyberwar'. Wenn ich 'Krieg' sage, dann habe ich plötzlich Waffen, und dann hat der eine mehr und der andere weniger. Das sind alles Analogien. Die klingen zwar gut, aber wenn ich wieder zurück gehe zur Security, dann kann ich damit nichts anfangen. Wenn ich mir jetzt überlege: Was ist eine Cyber-Waffe? Was ist eine digitale Waffe? Das ist nichts anderes als Code. Das sind Zahlen. Das heißt, ich müsste zu den Mathematikern gehen und ihnen sagen: Ihr müsst abrüsten. Was heißt das dann? Das macht überhaupt keinen Sinn."

http://derstandard.at/1381373841474/Europaeische-Netze-sind-reine-Augenauswischerei

"Europäische Netze sind reine Augenauswischerei"

INTERVIEW | ANDREAS PROSCHOFSKY

22. November 2013, 11:30

DeepSec-Organisator René Pfeiffer erklärt im Interview, warum die NSA-Enthüllungen wenig überraschend und doch hilfreich sind

Durch die Enthüllungen des ehemaligen NSA-Mitarbeiters Edward Snowden ist die Diskussion über Sicherheit oder Unsicherheit von Computersystemen in den vergangenen Monaten zunehmend in den Fokus der Öffentlichkeit gekommen. In mit diesen Fragen vertrauten Kreisen zeigt man sich hingegen wenig überrascht über all die Enthüllungen. Einige der Szenarien seien schon in den Neunziger Jahren des letzten Jahrhunderts diskutiert worden, so René Pfeiffer, Co-Organisator der derzeit in Wien abgehaltenen Sicherheitskonferenz DeepSec. Warum der Zukunftsausblick kaum erfreulicher ist, und die Enthüllungen trotzdem einen positiven Effekt haben könnten, erläutert er im Gespräch mit Andreas Proschofsky.

derStandard.at: Die vergangenen Monate waren von Schlagzeilen über die massive Überwachung von Internet- und Telekommunikationsverbindungen durch den US-Geheimdienst NSA und sein britisches Pendant GCHQ dominiert. War das Ausmaß dieser Überwachung für Sicherheitsexperten überraschend?

René Pfeiffer: Sicherheitsexperten haben in diesen Belangen durch ihren Blick hinter die Kulissen eine andere Sicht der Dinge. Wir haben uns auch intensiv mit dem Spionageskandal beschäftigt und keinerlei Überraschungen bei Kollegen entdecken können. Die jetzt in der Presse veröffentlichten Szenarien wurden schon lange auf Sicherheitskonferenzen diskutiert. Man kann sogar noch einen Schritt zurückgehen und die Cypherpunk-Bewegung zitieren, die seit Anfang der 1990er Jahre starke Kryptographie propagiert hat, um digitale Kommunikation, sei es von Firmen oder Privatpersonen, zu schützen. Damals war das Internet längst nicht so weit verbreitet wie jetzt, dennoch hatten einige Experten Schreckensvisionen, die sich jetzt bewahrheitet haben.

derStandard.at: Bislang gibt es zwar einige Empörung über spezielle Details der Enthüllungen - etwa die Überwachung des Mobiltelefons der deutschen Kanzlerin - aber wenig konkrete Konsequenzen. Was müsste passieren, um die Daten der Nutzer besser vor dem scheinbar beinahe uneingeschränkten Zugriff von Geheimdiensten zu schützen? Oder ist dieser Kampf angesichts der Möglichkeiten solcher Organisationen bereits verloren?

René Pfeiffer: Die Konsequenzen wären eine Verbesserung der Sicherheit, und da schlägt bei vielen eine einfache Risikoanalyse verbunden mit Resignation zu: Kaum eine Firma und keine Privatperson kann das Budget der Geheimdienste schlagen. Selbst große Firmen wurden kompromittiert, teilweise ohne ihr Wissen, und das ist

die psychologische Kehrseite der Spionageaffäre. Es schleicht sich trotz Empörung eine Machtlosigkeit ein, da man scheinbar gegen eine Übermacht steht. Das stimmt nicht ganz, und daher gehen auch einige der betroffenen Firmen gegen die Bedrohung des Ausspionierens vor (zwar viel zu spät, aber immerhin). Der positivste Aspekt in diesem Zusammenhang für die IT Sicherheitsexperten ist die Tatsache, dass man die Risiken nun endlich offen diskutieren kann ohne in die Ecke der Verschwörungstheoretiker gestellt zu werden. Das ist ein guter Anfang und die Branche darf diesen nicht verspielen.

derStandard.at: Aktuell werden immer wieder Ideen über rein europäische bzw. nationale Netze zirkuliert. Ist dies überhaupt realistisch?

René Pfeiffer: Diese Gedanken sind reine Augenauswischerei und Marketing Gags. Wer mitverfolgt hat, welche Dienste mit welchen in anderen Ländern kooperieren, der weiß, dass rein europäische oder nationale Netzwerke nicht mehr Sicherheit bieten. Alleine die Tatsache, dass der GCHQ in Europa sitzt, macht diesen Umstand deutlich. Das Internet und das eigene Netzwerk ab dem eigenen Gerät muss als vertrauensunwürdig angesehen werden. Mit dieser Prämisse beginnen IT-Sicherheitsexperten Designs für neue Systeme oder die Absicherung der Alten. So sollten auch Entwickler und Administratoren denken. Alle anderen Ansätze stützen sich auf Annahmen, die dann in sich zusammenbrechen, wenn man am Fundament rüttelt.

derStandard.at: Eines der großen Probleme scheint die rechtlich schwierige Situation von Cloud-Services zu sein, die durch ihre globale Verteilung viele Angriffspunkte bieten. Immerhin ist es kein Zufall, dass die Überwachung der Kommunikation zwischen den Rechenzentren von Google in Großbritannien vorgenommen wurde - da dies in den USA schlicht illegal gewesen wäre. Besteht hier Nachbesserungsbedarf? Oder hilft ohnehin nur die Abkehr von solchen Systemen?

René Pfeiffer: Die Cloud-Anbieter haben sich selbst ein Bein gestellt, weil sie ihre Systeme nicht richtig abgesichert haben und kaum Auskunft über ihre Infrastruktur geben. Darüber hinaus hat man sich aus europäischer Hinsicht mit dem "Safe Harbor"-Abkommen zwischen der EU und den USA auch auf bloße Versprechungen verlassen. In anderen Branchen geht das nicht so einfach. Wenn die Lebensmittelindustrie im Supermarkt "Cloud-Eier" von Hühnern verkaufen möchte, so muss man erklären, wie das sein kann, und woher die kommen. Bei der IT-Cloud ist das anscheinend egal, weil man nicht mal angeben muss, dass Benutzerdaten munter fröhlich im Klartext zwischen Rechenzentren hin- und herkopiert werden. Cloud-Anbieter verkaufen letztlich Vertrauen, und neben den rechtlichen Aspekten, die sicher auch nachgebessert werden müssen, muss sich jeder Anbieter der Vertrauensfrage stellen. IT Sicherheitsexperten empfehlen Cloud-Lösungen vor Verwendung eingehend zu prüfen, weil die Technologien einfach da sind. Teilweise wird das mittlerweile getan, mehr als vor dem Spionageskandal.

derStandard.at: Können einzelne Nutzer überhaupt etwas tun, um sich besser vor Überwachung zu schützen?

René Pfeiffer: Ja, das können sie. Weder Privatpersonen noch kleine Firmen sind zur Gänze machtlos. Man kann mit der Geldbörse abstimmen und nicht vertrauenswürdige Dienstleistungen (ob Cloud oder andere) gegen andere austauschen. Man kann Lieferanten unbequeme Fragen stellen, und man kann versuchen seine eigenen Daten nicht einem Einzelnen anzuvertrauen. Darüber hinaus kann man das Verhalten hinterfragen, wie mit Daten umgegangen wird. Das ist der schwerste Schritt, denn oft muss man Gewohnheiten umstellen. Es ist eine Vielzahl von Möglichkeiten, die zur Verfügung stehen. Leider ist der "NSA off" Schalter oder die "Anti-NSA-App" nicht dabei.

derStandard.at: Seit Jahren prangern Sicherheitsexperten auf Konferenzen wie der DeepSec grundlegende Probleme in Mobilfunkstandards wie GSM an. Ändern scheint sich daran bislang aber wenig. Warum?

René Pfeiffer: Die weite Verbreitung von Standards ist im Fall von Mobilfunk das größte Problem. Kaum ein Anbieter kann es sich leisten, das komplette Netz auszutauschen. Speziell in Anbetracht der Tatsache, dass kein Mobilfunkanbieter mehr das eigene Netz selbst verwaltet (Outsourcing lässt grüßen), sind solche Änderungen kaum finanzierbar. Man behilft sich da mit zusätzlicher Technologie, die bekannte Schwächen vermeidet. Das ist aber nicht nur im Mobilfunk so. Es gibt viele Zeitbomben wie alte Betriebssysteme oder nicht gewartete Software. Der beste Zeitpunkt für drastische Änderungen sind leider immer noch drastische Vorfälle.

derStandard.at: Mit LTE wird derzeit nach und nach die nächste Mobilfunkgeneration ausgeliefert. Sieht es bei dieser in Sicherheitsbelangen besser aus?

René Pfeiffer: LTE bietet einige Verbesserungen, aber auch hier stehen Agenden im Weg. Der Markt drängt nach LTE, also muss man es schnell umsetzen. Um Zeit und Geld zu sparen, ist zu erwarten, dass nicht alle Sicherheits-Features von Anfang an eingesetzt und auch nicht nachgerüstet werden. Immerhin haben die Frequenzen viel Geld gekostet, und das Geld muss wieder verdient werden. Sicherheitsforscher haben sich mit LTE schon beschäftigt, und wir gehen davon aus, dass es nicht weniger Sicherheitsprobleme geben wird. Wir hatten dazu schon 2010 auf der DeepSec einen Ausblick von einem Vortragenden. Bisher sind wir nicht enttäuscht worden.

derStandard.at: In den vergangenen ein bis zwei Jahren wurden immer öfter Sicherheitslücken in den für den privaten Internetzugang nötigen Routern diskutiert. Ein großes Problem scheint hier das Fehlen von Softwareupdates zu sein, die einmal aufgetauchte Sicherheitslücken auch beheben. Wieso reagieren die Hersteller hier nicht?.

René Pfeiffer: Das ist eine Kombination aus "never change a running system" und dem "Black Box Problem". Gerade bei Internetanbietern mit sehr vielen Anschlüssen können missglückte Upgrades zu vermehrten Supportanfragen führen, die dann Geld kosten. Dazu kommt, dass Hersteller verschieden gut im Beheben von Schwachstellen sind und gerne "Black Boxes" ausliefern, in die man nicht reinschauen sollte. Das Problem wird

in Deutschland gerade diskutiert, wo man den Routerzwang des Anbieters abschaffen möchte. Das halten wir für eine gute Idee, weil dann die Router-/Modemlandschaft weniger eine Monokultur darstellt und man den Herstellern, die gute Qualität liefern, den Vorzug geben kann.

derStandard.at: Muss man sich angesichts solcher Erfahrungen nicht Sorgen darüber machen, dass die Zahl jener Geräte, die mit dem Internet verbunden sind - vom Auto bis zur Waschmaschine - rasant zunimmt?

René Pfeiffer: Das "Internet der Dinge" ist definitiv eine Herausforderung an die Sicherheit und wird uns in der Zukunft noch sehr viele Überraschungen bescheren. Man findet auch jetzt schon sehr seltsame Geräte im Internet (sei es IPv4 oder IPv6). Es sollte nicht verwundern, wenn die IT-Sicherheit auf der Strecke bleibt, weil die Sicherheitstests für die IPv6-fähige Glühbirne bestimmt nicht ganz so streng ausfallen wie solche für die neueste Firewall. Solchen Umgebungen kann man nur mit Risikoanalyse und Abschottung begegnen – wenn etwas passiert, dann sollte nicht die Kompromittierung der Beleuchtung oder des Kühlschranks ausreichen, um das ganze Netzwerk zu übernehmen.

derStandard.at: Mittlerweile findet die DeepSec bereits zum siebten Mal statt. Wie hat sich in all den Jahren der thematische Fokus verändert? Welche großen Themenblöcke kommen in den kommenden Jahren auf uns zu?

René Pfeiffer: Die DeepSec versucht jedes Jahr einen bestimmten Fokus vorzugeben. Wir haben schon den ganzen Mobilbereich (Geräte, Apps und Netzwerke), Infrastruktur, "Cloud" Technologien, moderne Netzwerke (IPv6) und Softwareentwicklung adressiert. In diesem Jahr haben wir den Fokus erstmals aufgebrochen, indem wir die Konferenz unter das Motto "Secrets, Failures, and Visions" gestellt haben. Wir sehen die Entwicklung der IT-Sicherheit technikagnostisch. Jede Software, jedes Gerät und jedes Protokoll hat Schwachstellen. Oft kann man seine Schätze ("secrets") nicht schützen, erleidet Fehlschläge ("failures") und lernt hoffentlich daraus ("visions"). Wir vermuten allerdings, dass marktbedingt die Infrastruktur ("Cloud" inklusive) und der Mobilbereich auch 2014 eine große Rollen spielen wird. Vielleicht führt uns LTE dann auch schon zu den Schwachstellen der 4. Generation. (Andreas Proschofsky, derStandard.at, 22.11.13)

René Pfeiffer ist Organisator der seit 2007 jährlich in Wien abgehaltenen Sicherheitskonferenz DeepSec, selbstständiger IT-Dienstleister und Lektor am Technikum Wien.

"Europäische Netze sind reine Augenauswischerei"

INTERVIEW | ANDREAS PROSCHOFSKY
22. November 2013, 11:30

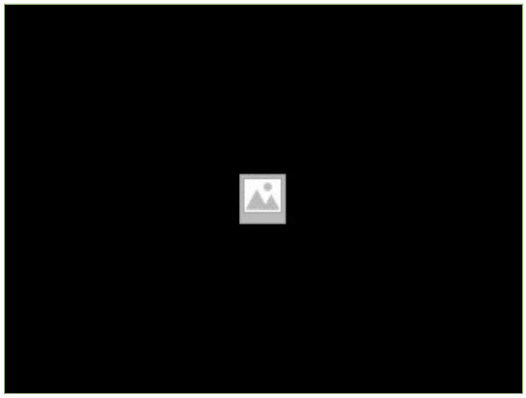


foto: joanna pianka / ap
DeepSec-Co-Organisator René Pfeiffer.

DeepSec-Organisator René Pfeiffer erklärt im Interview, warum die NSA-Enthüllungen wenig überraschend und doch hilfreich sind

Durch die Enthüllungen des ehemaligen NSA-Mitarbeiters Edward Snowden ist die Diskussion über Sicherheit oder Unsicherheit von Computersystemen in den vergangenen Monaten zunehmend in den Fokus der Öffentlichkeit gekommen. In mit diesen Fragen vertrauten Kreisen zeigt man sich hingegen wenig überrascht über all die Enthüllungen. Einige der Szenarien seien schon in den Neunziger Jahren des letzten Jahrhunderts diskutiert worden, so René Pfeiffer, Co-Organisator der derzeit in Wien abgehaltenen Sicherheitskonferenz DeepSec. Warum der Zukunftsausblick kaum erfreulicher ist, und die Enthüllungen trotzdem einen positiven Effekt haben könnten, erläutert er im Gespräch mit Andreas Proschofsky.

derStandard.at: Die vergangenen Monate waren von Schlagzeilen über die massive Überwachung von Internet- und Telekommunikationsverbindungen durch den US-Geheimdienst NSA und sein britisches Pendant GCHQ dominiert. War das Ausmaß dieser Überwachung für Sicherheitsexperten überraschend?

René Pfeiffer: Sicherheitsexperten haben in diesen Belangen durch ihren Blick hinter die Kulissen eine andere Sicht der Dinge. Wir haben uns auch intensiv mit dem Spionageskandal beschäftigt und keinerlei Überraschungen bei Kollegen entdecken können. Die jetzt in der Presse veröffentlichten Szenarien wurden schon lange auf Sicherheitskonferenzen diskutiert. Man kann sogar noch einen Schritt zurückgehen und die Cypherpunk-Bewegung zitieren, die seit Anfang der 1990er Jahre starke Kryptographie propagiert hat, um digitale Kommunikation, sei es von Firmen oder Privatpersonen, zu schützen. Damals war das Internet längst nicht so weit verbreitet wie jetzt, dennoch hatten einige Experten Schreckensvisionen, die sich jetzt bewahrheitet haben.

derStandard.at: Bislang gibt es zwar einige Empörung über spezielle Details der Enthüllungen - etwa die Überwachung des Mobiltelefons der deutschen Kanzlerin - aber wenig konkrete Konsequenzen. Was müsste passieren, um die Daten der Nutzer besser vor dem scheinbar beinahe uneingeschränkten Zugriff von Geheimdiensten zu schützen? Oder ist dieser Kampf angesichts der Möglichkeiten solcher Organisationen bereits verloren?

René Pfeiffer: Die Konsequenzen wären eine Verbesserung der Sicherheit, und da schlägt bei vielen eine einfache Risikoanalyse verbunden mit Resignation zu: Kaum eine Firma und keine Privatperson kann das Budget der Geheimdienste

schlagen. Selbst große Firmen wurden kompromittiert, teilweise ohne ihr Wissen, und das ist die psychologische Kehrseite der Spionageaffäre. Es schleicht sich trotz Empörung eine Machtlosigkeit ein, da man scheinbar gegen eine Übermacht steht. Das stimmt nicht ganz, und daher gehen auch einige der betroffenen Firmen gegen die Bedrohung des Ausspionierens vor (zwar viel zu spät, aber immerhin). Der positivste Aspekt in diesem Zusammenhang für die IT Sicherheitsexperten ist die Tatsache, dass man die Risiken nun endlich offen diskutieren kann ohne in die Ecke der Verschwörungstheoretiker gestellt zu werden. Das ist ein guter Anfang und die Branche darf diesen nicht verspielen.

derStandard.at: Aktuell werden immer wieder Ideen über rein europäische bzw. nationale Netze zirkuliert. Ist dies überhaupt realistisch?

René Pfeiffer: Diese Gedanken sind reine Augenauswischerei und Marketing Gags. Wer mitverfolgt hat, welche Dienste mit welchen in anderen Ländern kooperieren, der weiß, dass rein europäische oder nationale Netzwerke nicht mehr Sicherheit bieten. Alleine die Tatsache, dass der GCHQ in Europa sitzt, macht diesen Umstand deutlich. Das Internet und das eigene Netzwerk ab dem eigenen Gerät muss als vertrauensunwürdig angesehen werden. Mit dieser Prämisse beginnen IT-Sicherheitsexperten Designs für neue Systeme oder die Absicherung der Alten. So sollten auch Entwickler und Administratoren denken. Alle anderen Ansätze stützen sich auf Annahmen, die dann in sich zusammenbrechen, wenn man am Fundament rüttelt.

derStandard.at: Eines der großen Probleme scheint die rechtlich schwierige Situation von Cloud-Services zu sein, die durch ihre globale Verteilung viele Angriffspunkte bieten. Immerhin ist es kein Zufall, dass die Überwachung der Kommunikation zwischen den Rechenzentren von Google in Großbritannien vorgenommen wurde - da dies in den USA schlicht illegal gewesen wäre. Besteht hier Nachbesserungsbedarf? Oder hilft ohnehin nur die Abkehr von solchen Systemen?

René Pfeiffer: Die Cloud-Anbieter haben sich selbst ein Bein gestellt, weil sie ihre Systeme nicht richtig abgesichert haben und kaum Auskunft über ihre Infrastruktur geben. Darüber hinaus hat man sich aus europäischer Hinsicht mit dem "Safe Harbor"-Abkommen zwischen der EU und den USA auch auf bloße Versprechungen verlassen. In anderen Branchen geht das nicht so einfach. Wenn die Lebensmittelindustrie im Supermarkt "Cloud-Eier" von Hühnern verkaufen möchte, so muss man erklären, wie das sein kann, und woher die kommen. Bei der IT-Cloud ist das anscheinend egal, weil man nicht mal angeben muss, dass Benutzerdaten munter fröhlich im Klartext zwischen Rechenzentren hin- und herkopiert werden. Cloud-Anbieter verkaufen letztlich Vertrauen, und neben den rechtlichen Aspekten, die sicher auch nachgebessert werden müssen, muss sich jeder Anbieter der Vertrauensfrage stellen. IT Sicherheitsexperten empfehlen Cloud-Lösungen vor Verwendung eingehend zu prüfen, weil die Technologien einfach da sind. Teilweise wird das mittlerweile getan, mehr als

derStandard.at: Können einzelne Nutzer überhaupt etwas tun, um sich besser vor Überwachung zu schützen?

René Pfeiffer: Ja, das können sie. Weder Privatpersonen noch kleine Firmen sind zur Gänze machtlos. Man kann mit der Geldbörse abstimmen und nicht vertrauenswürdige Dienstleistungen (ob Cloud oder andere) gegen andere austauschen. Man kann Lieferanten unbequeme Fragen stellen, und man kann versuchen seine eigenen Daten nicht einem Einzelnen anzuvertrauen. Darüber hinaus kann man das Verhalten hinterfragen, wie mit Daten umgegangen wird. Das ist der schwerste Schritt, denn oft muss man Gewohnheiten umstellen. Es ist eine Vielzahl von Möglichkeiten, die zur Verfügung stehen. Leider ist der "NSA off" Schalter oder die "Anti-NSA-App" nicht dabei.

derStandard.at: Seit Jahren prangern Sicherheitsexperten auf Konferenzen wie der DeepSec grundlegende Probleme in Mobilfunkstandards wie GSM an. Ändern scheint sich daran bislang aber wenig. Warum?

René Pfeiffer: Die weite Verbreitung von Standards ist im Fall von Mobilfunk das größte Problem. Kaum ein Anbieter kann es sich leisten, das komplette Netz auszutauschen. Speziell in Anbetracht der Tatsache, dass kein Mobilfunkanbieter mehr das eigene Netz selbst verwaltet (Outsourcing lässt grüßen), sind solche Änderungen kaum finanzierbar. Man behilft sich da mit zusätzlicher Technologie, die bekannte Schwächen vermeidet. Das ist aber nicht nur im Mobilfunk so. Es gibt viele Zeitbomben wie alte Betriebssysteme oder nicht gewartete Software. Der beste Zeitpunkt für drastische Änderungen sind leider immer noch drastische Vorfälle.

derStandard.at: Mit LTE wird derzeit nach und nach die nächste Mobilfunkgeneration ausgeliefert. Sieht es bei dieser in Sicherheitsbelangen besser aus?

René Pfeiffer: LTE bietet einige Verbesserungen, aber auch hier stehen Agenden im Weg. Der Markt drängt nach LTE, also muss man es schnell umsetzen. Um Zeit und Geld zu sparen, ist zu erwarten, dass nicht alle Sicherheits-Features von Anfang an eingesetzt und auch nicht nachgerüstet werden. Immerhin haben die Frequenzen viel Geld gekostet, und das Geld muss wieder verdient werden. Sicherheitsforscher haben sich mit LTE schon beschäftigt, und wir gehen davon aus, dass es nicht weniger Sicherheitsprobleme geben wird. Wir hatten dazu schon 2010 auf der DeepSec einen Ausblick von einem Vortragenden. Bisher sind wir nicht enttäuscht worden.

derStandard.at: In den vergangenen ein bis zwei Jahren wurden immer öfter Sicherheitslücken in den für den privaten Internetzugang nötigen Routern diskutiert. Ein großes Problem scheint hier das Fehlen von Softwareupdates zu sein, die einmal aufgetauchte Sicherheitslücken auch beheben. Wieso reagieren die Hersteller hier nicht?.

René Pfeiffer: Das ist eine Kombination aus "never change a running system" und dem "Black Box Problem". Gerade bei Internetanbietern mit sehr vielen Anschlüssen können missglückte Upgrades zu vermehrten Supportanfragen führen, die dann Geld kosten. Dazu kommt, dass Hersteller verschieden gut im Beheben von Schwachstellen sind und gerne "Black

Boxes" ausliefern, in die man nicht reinschauen sollte. Das Problem wird in Deutschland gerade diskutiert, wo man den Routerzwang des Anbieters abschaffen möchte. Das halten wir für eine gute Idee, weil dann die Router-/Modemlandschaft weniger eine Monokultur darstellt und man den Herstellern, die gute Qualität liefern, den Vorzug geben kann.

derStandard.at: Muss man sich angesichts solcher Erfahrungen nicht Sorgen darüber machen, dass die Zahl jener Geräte, die mit dem Internet verbunden sind - vom Auto bis zur Waschmaschine - rasant zunimmt?

René Pfeiffer: Das "Internet der Dinge" ist definitiv eine Herausforderung an die Sicherheit und wird uns in der Zukunft noch sehr viele Überraschungen bescheren. Man findet auch jetzt schon sehr seltsame Geräte im Internet (sei es IPv4 oder IPv6). Es sollte nicht verwundern, wenn die IT-Sicherheit auf der Strecke bleibt, weil die Sicherheitstests für die IPv6-fähige Glühbirne bestimmt nicht ganz so streng ausfallen wie solche für die neueste Firewall. Solchen Umgebungen kann man nur mit Risikoanalyse und Abschottung begegnen – wenn etwas passiert, dann sollte nicht die Kompromittierung der Beleuchtung oder des Kühlschranks ausreichen, um das ganze Netzwerk zu übernehmen.

derStandard.at: Mittlerweile findet die DeepSec bereits zum siebten Mal statt. Wie hat sich in all den Jahren der thematische Fokus verändert? Welche großen Themenblöcke kommen in den kommenden Jahren auf uns zu?

René Pfeiffer: Die DeepSec versucht jedes Jahr einen bestimmten Fokus vorzugeben. Wir haben schon den ganzen Mobilbereich (Geräte, Apps und Netzwerke), Infrastruktur, "Cloud" Technologien, moderne Netzwerke (IPv6) und Softwareentwicklung adressiert. In diesem Jahr haben wir den Fokus erstmals aufgebrochen, indem wir die Konferenz unter das Motto "Secrets, Failures, and Visions" gestellt haben. Wir sehen die Entwicklung der IT-Sicherheit technikagnostisch. Jede Software, jedes Gerät und jedes Protokoll hat Schwachstellen. Oft kann man seine Schätze ("secrets") nicht schützen, erleidet Fehlschläge ("failures") und lernt hoffentlich daraus ("visions"). Wir vermuten allerdings, dass marktbedingt die Infrastruktur ("Cloud" inklusive) und der Mobilbereich auch 2014 eine große Rollen spielen wird. Vielleicht führt uns LTE dann auch schon zu den Schwachstellen der 4. Generation. (Andreas Proschofsky, derStandard.at, 22.11.13)

René Pfeiffer ist Organisator der seit 2007 jährlich in Wien abgehaltenen Sicherheitskonferenz DeepSec, selbstständiger IT-Dienstleister und Lektor am Technikum Wien.

Link

DeepSec

http://futurezone.at/digital-life/deepsec-falsches-vertrauen-in-facebook-freunde/36.875.293

SICHERHEITSKONFERENZ

DeepSec: Falsches Vertrauen in Facebook-Freunde

Barbara Wimmer 21.11.13, 16:11

Auf der Sicherheitskonferenz DeepSec erklärte der IT-Forscher Ashar Javed, warum man seinen Facebook-Freunden nicht uneingeschränkt vertrauen sollte.

Im Netz sollte man generell nicht zu vertrauensseelig sein. Das gilt gleichermaßen für Nutzer wie für Unternehmen. Um diese Aussage zu beweisen, hat sich der IT-Sicherheitsforscher Ashar Javed von der Universität in Bochum 50 populäre Social Media-Websites näher angesehen. Javed probierte dabei aus, ob es ihm gelingt, sich mit einfachen Mitteln Zugriff zu Passwörtern von Nutzern zu erschleichen und deren Profile zu übernehmen. Er konnte.

"Passwort verloren"

Von den 50 Social Networks gelang es ihm bei sieben – und zwar mit relativ einfachen Mitteln, ohne großes technische Know-How. Er gab sich einfach als Nutzer eines bestimmten Profils aus und schickte eine Support-Anfrage an das Team mit dem Betreff: „Passwort verloren“ und der Bitte, ihm ein Neues zuzusenden. Sieben Netzwerke kamen dieser Bitte nach, ohne seine Identität und seine Anfrage zu hinterfragen. „Erschütternd ist, dass sechs Unternehmen gar nicht reagiert haben, als ich sie mit diesem Sicherheits-Faux-Pas konfrontiert habe. Auch auf meine zweite E-Mail bekam ich keine Antwort“, erzählte Javed bei der Sicherheitskonferenz DeepSec in Wien.

Auf der DeepSec kommen seit jeher weltweit renommierte Sicherheitsexperten von Universitäten, Regierungen und der Industrie zusammen, um sich über das „Leben im global vernetzten Dorf“ auszutauschen. Javed ist einer von zahlreichen Speakern, rund 160 Personen besuchen die Konferenz, die noch bis Freitag Abend im Imperial Riding School Renaisscance Vienna Hotel im 3. Bezirk läuft.

Javed spricht in seinem Vortrag auch über die „Trusted Friends“-Attacke, die er auf Facebook verübt hat. „Bei Facebook funktioniert die Methode, die ich bei den anderen Netzwerken angewandt habe, nicht. Dafür gibt es das Trusted Friends-Prinzip, das Facebook im Oktober 2011 eingeführt hat, um die Sicherheit des Netzwerkes zu erhöhen.

"Trusted Friends" manipulierbar

Doch auch das „Trusted Friends“-Prinzip von Facebook lässt sich laut Javed überlisten. Auf Facebook geht

es vielen Nutzern nämlich darum, möglichst viele Freunde zu sammeln. Viele Nutzer akzeptieren daher auch Personen als Freunde, die sie gar nicht persönlich aus dem „echten Leben“ kennen. Javed legte drei Facebook-Profile an, befreundete sich mit seinen 250 „echten“ Freunden, um die Attacke zu erproben. Das Ergebnis: Er konnte elf Accounts übernehmen.

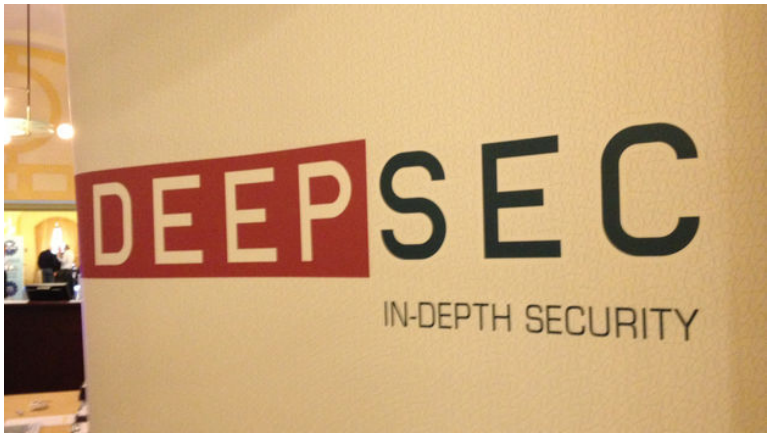
„Ich habe dieses Problem an Facebook gemeldet. Derzeit gibt es allerdings keine Lösung dafür, man muss damit leben“, so Javed, der gerade die Übernahme von Facebook-Profilen für besonders schlimm hält. „Facebook dient für viele als Single-Sign-On-Account bei anderen Diensten. User loggen sich mit ihrem Facebook-Profil zur Identifikation bei vielen anderen Services ein. Das heißt, dass dann nicht nur ein Profil betroffen ist, sondern viele.“

Dem Problem Abhilfe schaffen kann man laut Javed nur, wenn sich User bewusst werden, was sie im Netz im Generellen und auf Facebook im Speziellen tun und wen sie in ihre Freundesliste aufnehmen und wen besser nicht. Vertrauen will auch im Netz verdient sein.

SICHERHEITSKONFERENZ

DeepSec: Falsches Vertrauen in Facebook-Freunde

von Barbara Wimmer 21.11.13, 16:11 shroombab Mail an Autor



Derzeit in Wien: Die Sicherheitskonferenz DeepSec - Foto: Barbara Wimmer

SICHERHEITSKONFERENZ
DeepSec: Falsches Vertrauen in Facebook-Freunde
KOMMENTARE (1)
MEHR ZUM THEMA

Auf der Sicherheitskonferenz DeepSec erklärte der IT-Forscher Ashar Javed, warum man seinen Facebook-Freunden nicht uneingeschränkt vertrauen sollte.

FACEBOOK, IT, SECURITY

Im Netz sollte man generell nicht zu vertrauensseelig sein. Das gilt gleichermaßen für Nutzer wie für Unternehmen. Um diese Aussage zu beweisen, hat sich der IT-Sicherheitsforscher Ashar Javed von der Universität in Bochum 50 populäre Social Media-Websites näher angesehen. Javed probierte dabei aus, ob es ihm gelingt, sich mit einfachen Mitteln Zugriff zu Passwörtern von Nutzern zu erschleichen und deren Profile zu übernehmen. Er konnte.

"Passwort verloren"

Von den 50 Social Networks gelang es ihm bei sieben – und zwar mit relativ einfachen Mitteln, ohne großes technische Know-How. Er gab sich einfach als Nutzer eines bestimmten Profils aus und schickte eine Support-Anfrage an das Team mit dem Betreff: „Passwort verloren" und der Bitte, ihm ein Neues zuzusenden. Sieben Netzwerke kamen dieser Bitte nach, ohne seine Identität und seine Anfrage zu hinterfragen. „Erschütternd ist, dass sechs Unternehmen gar nicht reagiert haben, als ich sie mit diesem Sicherheits-Faux-Pas konfrontiert habe. Auch auf meine zweite E-Mail bekam ich keine Antwort", erzählte Javed bei der Sicherheitskonferenz DeepSec in Wien.

Auf der DeepSec kommen seit jeher weltweit renommierte Sicherheitsexperten von Universitäten, Regierungen und der Industrie zusammen, um sich über das „Leben im global vernetzten Dorf" auszutauschen. Javed ist einer von zahlreichen Speakern, rund 160 Personen besuchen die Konferenz, die noch bis Freitag Abend im Imperial Riding School Renaisscance Vienna Hotel im 3. Bezirk läuft.

Javed spricht in seinem Vortrag auch über die „Trusted Friends"-Attacke, die er auf Facebook verübt hat. „Bei Facebook funktioniert die Methode, die ich bei den anderen Netzwerken angewandt habe, nicht. Dafür gibt es das Trusted Friends-Prinzip, das Facebook im Oktober 2011 eingeführt hat, um die Sicherheit des Netzwerkes zu erhöhen.

"Trusted Friends" manipulierbar

Doch auch das „Trusted Friends"-Prinzip von Facebook lässt sich laut Javed überlisten. Auf Facebook geht es vielen Nutzern nämlich darum, möglichst viele Freunde zu sammeln. Viele Nutzer akzeptieren daher auch Personen als Freunde, die sie gar nicht persönlich aus dem „echten Leben" kennen. Javed legte drei Facebook-Profile an, befreundete sich mit seinen 250 „echten" Freunden, um die Attacke zu erproben. Das Ergebnis: Er konnte elf Accounts übernehmen.

„Ich habe dieses Problem an Facebook gemeldet. Derzeit gibt es allerdings keine Lösung dafür, man muss damit leben", so Javed, der gerade die Übernahme von Facebook-Profilen für besonders schlimm hält. „Facebook dient für viele als Single-Sign-On-Account bei anderen Diensten. User loggen sich mit ihrem Facebook-Profil zur Identifikation bei vielen anderen Services ein. Das heißt, dass dann nicht nur ein Profil betroffen ist, sondern viele."

Dem Problem Abhilfe schaffen kann man laut Javed nur, wenn sich User bewusst werden, was sie im Netz im Generellen und auf Facebook im Speziellen tun und wen sie in ihre Freundesliste aufnehmen und wen besser nicht. Vertrauen will auch im Netz verdient sein.

(FUTUREZONE) ERSTELLT AM 21.11.2013, 16:12

6

FACEBOOK, IT, SECURITY

Kommentare (1)

Ihr Kommentar
Bitte loggen Sie sich ein

Einloggen / Registrieren

ABSENDEN

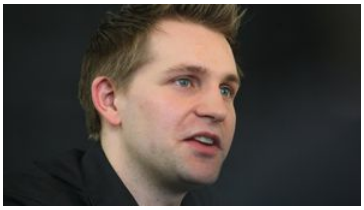
wolfgangh.wã¶gerer vor einem jahr

Wie der Duden glaubhaft ausweist, ist Fauxpas EIN Wort. Ansonsten gibt's dazu wohl nix zu kommentieren.

permalink | melden 0 0

antworten

Mehr zum Thema

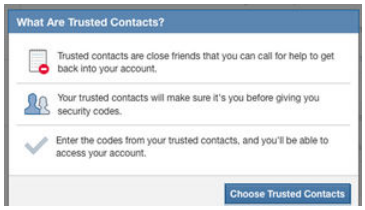


KAMPF GEGEN FACEBOOK

Schlag ins Gesicht für Aktivisten

Darf man große Konzerne als Aktivist nicht mehr anprangern? Diese Frage stellt sich, wenn man sich den Beschluss im Fall Max Schrems gegen Facebook näher anschaut.

von Barbara Wimmer



SICHERHEIT

Facebook bringt Notfall-Schlüssel für Freunde

Das Social Network stellt "Zuverlässige Kontake" ("trusted contacts") vor, eine Funktion, mit der man seinen verlorenen Facebook-Zugang zurückerhalten kann. Bis zu fünf ...

SICHERHEIT

Facebook: Freunde sollen Account entsperren

Rund 600.000 Login-Versuche bei Facebook täglich sind kompromittiert. Das bestätigte das soziale Netzwerk vor kurzem. Um das Netzwerk sicherer zu machen hat Facebook ein ...

http://futurezone.at/digital-life/deepsec-vom-herzschrittmacher-hack-bis-zum-profiling/32.427.591

SICHERHEITSKONFERENZ

DeepSec: Vom Herzschrittmacher-Hack bis zum Profiling

Letztes Update am 24.10.13, 14:35

Zur Sicherheitskonferenz DeepSec, die von 19. bis 22. November in Wien stattfindet, kommt unter anderem der IT-Sicherheitspionier Marcus J. Ranum.

Auf der DeepSec kommen seit jeher weltweit renommierte Sicherheitsexperten von Universitäten, Regierungen und der Industrie zusammen, um sich über das „Leben im global vernetzten Dorf" auszutauschen. Das diesjährige Motto der Konferenz, die von 19. bis 22. November im Imperial Riding School Renaisscance Vienna Hotel im 3. Bezirk stattfindet, lautet: „All about Secrets, Failures and Vision".

Die Keynote hält Marcus J. Ranum, der sich mit der Vorherrschaft der USA im Internet beschäftigt und den Auswirkungen dessen für die gesamte mobile Welt. Ranum hält sich seit den 1980ern in Top-Positionen in IT-Sicherheitsfirmen und publizierte das Sachbuch „The Myth of Homeland Security".

Vorträge über Online-Betrug und Profiling

Zudem wird Stefan Schumacher vom Magdeburger Institut für Sicherheitsforschung darüber sprechen, warum es Betrügern dermaßen leicht gelingt via Porno-Apps oder Sexbildern ganze Unternehmen auszuspionieren. Frank Ackermann beschreibt in seinem nicht technischen Talk, wie viel Online-Identitäten wert sind und wie die damit verbundenen Informationen von den Internetplattformen verarbeitet werden. Er leitet daraus Bedrohungen und Risiken für unsere Datenprofile ab: Neben dem durchaus bekannten Aspekt des „gläsernen Surfers" bieten Online-Identitäten ein hohes Missbrauchspotential unterschiedlicher Art.

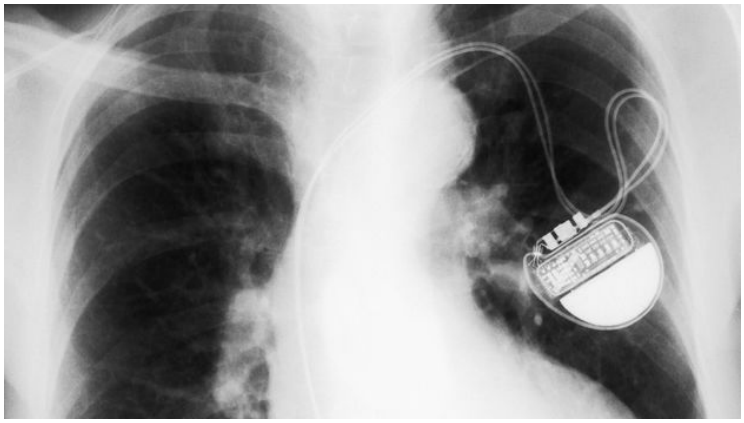
Der Forscher und Security-Analyst Florian Grunow aus Heidelberg beschäftigt sich unter anderem damit, wie sich die Wireless-Funktionen von Herzschrittmachern ausschalten lassen. Insulinpumpen oder Herzschrittmacher sind schon lang mit Wireless-Zugangsfunktionen ausgestattet, doch genau über diese Funktion können sie auch angegriffen werden. Grunow geht es weniger um einen tatsächlichen Angriff auf das Leben des Patienten, als vielmehr darum, Werksspionage und wirtschaftlich motivierte Angriffe auf einen Hersteller durch Sicherheitslücken in seinen Computersystemen aufzuzeigen.

Das detailliierte Programm zu allen Sessions findet sich hier.

SICHERHEITSKONFERENZ

DeepSec: Vom Herzschrittmacher-Hack bis zum Profiling

Letztes Update am 24.10.13, 14:35 Mail an die Redaktion



Florian Grunow beschäftigt sich damit, wie man mit Herzschrittmachern wirtschaftlich motivierte Angriffe tätigen kann. - Foto: Dario Sabljak/Fotolia

SICHERHEITSKONFERENZ

DeepSec: Vom Herzschrittmacher-Hack bis zum Profiling

KOMMENTARE ()

MEHR ZUM THEMA

Zur Sicherheitskonferenz DeepSec, die von 19. bis 22. November in Wien stattfindet, kommt unter anderem der IT-Sicherheitspionier Marcus J. Ranum.

Auf der DeepSec kommen seit jeher weltweit renommierte Sicherheitsexperten von Universitäten, Regierungen und der Industrie zusammen, um sich über das „Leben im global vernetzten Dorf" auszutauschen. Das diesjährige Motto der Konferenz, die von 19. bis 22. November im Imperial Riding School Renaisscance Vienna Hotel im 3. Bezirk stattfindet, lautet: „All about Secrets, Failures and Vision".

Die Keynote hält Marcus J. Ranum, der sich mit der Vorherrschaft der USA im Internet beschäftigt und den Auswirkungen dessen für die gesamte mobile Welt. Ranum hält sich seit den 1980ern in Top-Positionen in IT-Sicherheitsfirmen und publizierte das Sachbuch „The Myth of Homeland Security".

Vorträge über Online-Betrug und Profiling

Zudem wird Stefan Schumacher vom Magdeburger Institut für Sicherheitsforschung darüber sprechen, warum es Betrügern dermaßen leicht gelingt via Porno-Apps oder Sexbildern ganze Unternehmen auszuspionieren. Frank Ackermann beschreibt in seinem nicht technischen Talk, wie viel Online-Identitäten wert sind und wie die damit verbundenen Informationen von den Internetplattformen verarbeitet werden. Er leitet daraus Bedrohungen und Risiken für unsere Datenprofile ab: Neben dem durchaus bekannten Aspekt des „gläsernen Surfers" bieten Online-Identitäten ein hohes Missbrauchspotential unterschiedlicher Art.

Der Forscher und Security-Analyst Florian Grunow aus Heidelberg beschäftigt sich unter anderem damit, wie sich die Wireless-Funktionen von Herzschrittmachern ausschalten lassen. Insulinpumpen oder Herzschrittmacher sind schon lang mit Wireless-Zugangsfunktionen ausgestattet, doch genau über diese Funktion können sie auch angegriffen werden. Grunow geht es weniger um einen tatsächlichen Angriff auf das Leben des Patienten, als vielmehr darum, Werksspionage und wirtschaftlich motivierte Angriffe auf einen Hersteller durch Sicherheitslücken in seinen Computersystemen aufzuzeigen.

FEATURED

VERKEHR
Hier-Box holt bei Autounfällen automatisch Hilfe

REPORTAGE
Buffalo: „Stadt des Lichts" kämpft gegen den Rost

AKTION
Facebook-Video zeigt waghalsige Aktion im AKW Zwentendorf

Das detailliierte Programm zu allen Sessions findet sich hier.

(FUTUREZONE) ERSTELLT AM 24.10.2013, 14:35

1 2

Kommentare ()

Ihr Kommentar
Bitte loggen Sie sich ein

Einloggen / Registrieren

ABSENDEN

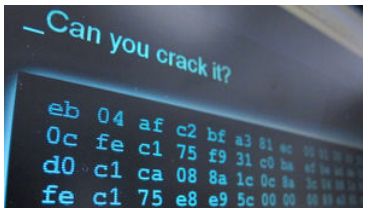
Mehr zum Thema

DEEPSEC

Forscher zeigt: So leicht lassen sich Medizingeräte hacken

Die IT-Sicherheit kommt bei vielen Medizingeräten zu kurz. Bei der Konferenz Deep Sec demonstrierte der Forscher Florian Grunow, wie man einen Patientenmonitor manipuliert.

von Barbara Wimmer



DEEPSEC

"White Hat Hacking ist nicht lukrativ genug"

Bei der DeepSec-Konferenz forderte Linus Neumann vom CCC, Anreize für das Aufdecken von Schwachstellen massiv zu erhöhen und sieht Interessenskonflikte im Innenministerium.

von Florian Christof

SICHERHEITSKONFERENZ

DeepSec: Falsches Vertrauen in Facebook-Freunde

Auf der Sicherheitskonferenz DeepSec erklärte der IT-Forscher Ashar Javed, warum man seinen Facebook-Freunden nicht uneingeschränkt vertrauen sollte.

von Barbara Wimmer

Digital-Life

15.07.2015 13:30 Uhr

REPORTAGE

Chinas mobile Medienrevolution hinter der virtuellen Mauer

Die chinesischen Medien haben den Trend der Zeit erkannt und werfen sich mit aller Kraft ins Smartphone-Zeitalter. Daneben steht Zensur auf der Tagesordnung.

PLÄNE

EU überlegt neue Energie-Kennzeichnung für Elektrogeräte

Beim Kauf von Elektrogeräten sollen Verbraucher künftig leichter erkennen können, wie energiehungrig die Produkte sind.

DER NEUE JOKER

Erster Trailer zu Suicide Squad veröffentlicht

Jetzt gibt es einen ersten, offiziellen Blick auf den Bösewicht-Film und der bereits im Vorfeld stark kritisierten, neuen Version des Jokers.

DATENSCHUTZ 3

Google Fotos lädt Bilder auch nach Löschen der App hoch

Will man Googles Foto-App nicht mehr nutzen, muss das automatische Hochladen der Bilder separat deaktiviert werden. Ein Deinstallieren der Anwendung genügt nicht.

Featured

VERKEHR

Hier-Box holt bei Autounfällen automatisch Hilfe

Die Hier-Box, ein kleines Gerät zum Nachrüsten, kann bei einem Autounfall selbstständig einen Notruf absetzen. Die Reaktionszeit der Rettung soll so stark verkürzt werden.

von David Kotrba

http://fm4.orf.at/stories/1718934/

Datenschutz hilft, Cyberspionage abzuwehren

Firmen, in denen Datenschutz ein Thema ist, haben in der Regel auch ein generell überdurchschnittliches Sicherheitsniveau, sagen drei namhafte Sicherheitsberater aus Österreich.

Wenn der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) am kommenden Donnerstag zusammentritt, dann wird dort ein Thema mit abgehandelt, das nicht auf der Tagesordnung steht. Nach Ansicht dreier unabhängiger Sicherheitsexperten, die von ORF.at befragt wurden, wird bei dieser ersten Beratung über Maßnahmen gegen Cyberangeriffe automatisch auch über die heftig umstrittene Novelle zum EU-Datenschutzpaket diskutiert.

"Firmen, in denen das Thema Datenschutz hoch angesiedelt ist, haben praktisch immer auch ein überdurchschnittlich hohes Sicherheitsniveau. Beides geht ja Hand in Hand", sagte Joe Pichlmayr zu ORF.at. Erst wenn quer durch die Belegschaft ein Bewusstsein dafür da sei, dass Daten einen Wert darstellen, der von existenzieller Bedeutung für ihr Unternehmen sei, könne auch ein "vitales Interesse entstehen, diese Daten auch zu schützen"; Mit dieser Ansicht steht der Geschäftsführer des österreichischen Sicherheitsunternehmens Ikarus nicht allein.

Datenschutz, Informationssicherheit

"Das kann ich nur unterschreiben. Wer die Aufgabe hat, was auch immer an Informationen zu schützen, der muss sich auch intensiv mit Sicherheitsfragen beschäftigten", so IT-Sicherheitexperte Rene Pfeiffer, der aus der Hackerszene kommt.

"Das ist nur logisch" sekundiert Sicherheitsberater Gert-Rene Polli, was in der allgemeinen Öffentlichkeit nämlich unter "Datenschutz" verstanden werde, sei doch nur Teil des Komplexes "Informationssicherheit". Dieser Begriff stammt aus der militärischen Welt, seit jeher ist "Information Assurance" neben der Spionage ("Signals Intelligence") eine der beiden Kernaufgaben des fortgeschrittensten aller Militärgeheimdienste, der National Security Agency der USA.

HNA, Hacker, Wirtschaft

Der nunmehrige Sicherheitsberater Polli war mehr als zwei Jahrzehnte für das Heeresnachrichtenamt (HNA) tätig und wurde 2002 Direktor des damals neu gegründeten Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT) im Innenministerium. Dass ein gelernter Geheimdienstmann derselben Ansicht zu diesem Thema ist, wie ein gelernter Hacker und der Geschäftsführer einer mittelständischen Anti-Virusfirma klingt nur für Außenstehende befremdlich.

In der Sicherheitsbranche ist es "Common Sense", dass die absolut wichtigste Linie der Verteidigung gegen die überbordenden Spionageangriffe auf Unternehmen das Sicherheitsbewusstssein der Mitarbeiter ist. Dieser Aspekt wurde im Zusammenhang mit dem EU-Datenschutzpaket bis jetzt noch überhaupt nicht diskutiert.

Ein Bärendienst

Im EU-Ministerrat, wo die Meinungsbildung von großen Mitgliedsstatten wie England, Frankreich oder Spanien überproportional geprägt ist, wird der Parlamentsentwurf zum Datenschutzpaket regelrecht demontiert. Österreich hat deshalb generellen Vorbehalt eingelegt .

Dieser wichtige Aspekt der EU-Datenschutznovelle aus dem Blickwinkel der Datensicherheit ist in die Diskussionen von EU-Parlament und Ministerrat bis jetzt noch überhaupt nicht eingeflossen. Jene EU-Parlamentarier, die erklärtermaßen die Interessen der Wirtschaft schützen wollen, indem sie Partei gegen grundlegende Maßnahmen zum Datenschutz ergreifen, erweisen der Wirtschaft damit einen Bärendienst, meint Pfeiffer.

Jede Hebung des betrieblichen Datenschutz- und damit des Sicherheitsniveaus bringe einen "wirtschaftlichen Benefit mit sich, der überhaupt nicht abstrakt sondern in konkreten Zahlen darstellbar ist."

"Geistiges Eigentum der KMUs"

"Betroffen sind vor allem kleine und mittelständische Unternehmen, bei denen in Österreich Innovation und Knowhow zuhause sind", sagt Polli, "Es geht hier um den Schutz des geistigen Eigentums dieser Firmen." Und das sei schon jetzt ziemlich gefährdet, denn "dieser Bereich ist leider so offen wie ein Scheunentor."

Angesichts der kleinteiligen Struktur der österreichischen Wirtschaft sei es gerade für innovative und obendrein neu gegründete Firmen gar nicht erschwinglich, von vornherein eine entsprechend dimensionierte Sicherheitsabteilung mit einem "Chief Security Officer" einzurichten, so Polli weiter.

"Authentizität, Integrität und Vertraulichkeit"

Solche "Targeted Attacks" oder "Spear Phishing" genannten Angriffsformen zielen auf einen definierten Personenkreis. Im Fall von Cyberspionage zum wirtschaftlichen Vorteil werden etwa die Mitarbeiter einer Firma in Sozialen Netzen beobachtet und dann kontaktiert. Sobald eine gewisse Vertraulichkeit gegegeben ist, kommen die Angriffsmails, deren Anhänge eine bis dahin nicht bekannte Sicherheitslücke angreifen. Damit ist man im Firmennetzwerk.

Wer unter "Schutzmaßnahmen für betriebliche Daten" die bloße Einrichtung von Firewalls und Virenscannern verstehe, sei in der globalsierten Welt der Informationstechnologie mehr gefährdet, als er vielleicht glaube, sagt Pichlmayr. Um ein akzeptables Niveau an Datensicherheit zu erreichen, gelte es zuerst einmal, einen Masterplan zu erstellen, der auf den "drei Säulen der Informationssicherheit aufgebaut sein muss: Authentizität, Integrität und Vertraulichkeit".

Von diesen drei Prinzipien der Informationssicherheit, die lange vor dem World Wide Web schon galten, sind auch die Prinzipien des Datenschutzes hergeleitet. Alle in den Datenschutzgesetzen quer durch Europa vorgeschriebenen Mechanismen und Regeln zum Schutz der persönlichen Daten von Privatpersonen finden sich hier wieder.

Das Prinzip in der Praxis

So ist seit der ersten EU-Datenschutzrichtlinie von 1995 ein Recht auf Einsicht in die eigenen Datensätze und deren allfällige Korrektur durch den Eigentümer dieser Daten selbst gesetzlich festgeschrieben. Das Recht, bei Falschangaben in den eigenen, persönlichen Datensätzen eine Richtigstellung erzwingen zu können, fällt unter "Integrität".

"Authentizität" wiederum bedeutet mehr als nur diese Daten auf ihren Eigentümer zurückzuführen, also ihre Echtheit zu überprüfen, sondern auch den Abfragenden selbst. Wer auf personenbezogene Datensätze zugreift, muss sich daher authentifizieren, während in Punkt "Vertraulichkeit" der Regelsatz definiert ist, wer aller unter welchen Umständen auf Daten zugreifen darf und wie dieser Zugriff dokumentiert werden muss.

Historische Datenskandale

Josef Pichlmayr ist Geschäftsführer der 1993 gegründeten IT-Security-Firma Ikarus. Die Ikarus war einer der ersten europäischen Firmen überhaupt, die einen eigenen Virenscanner entwickelt hat.

In der jüngeren österreichischen Geschichte finden sich sich zuhauf Beispiel dafür, was unweigerlich passiert, wenn diese Regeln nicht beachtet werden. Weil man die Polizeibeamten nicht durch "unnötige bürokratische Hürden" - wie es damals hieß - in ihrer Ermittlungstätigkeit behindern wollte, wurden jahrelang keine internen Regeln für Protokollierung und Überprüfung dieser Zugriffe auf die Datenbanken des Innenministeriums festgelegt.

Die Folge war eine Serie von Datenskandalen im genannten Ministerium. 1998 flog eine Reihe von Beamten auf, die Meldedaten und solche aus den kriminalpolizeilichen Ermittlungsakten auf eigene Faust an Datenhändler weiterverkauft hatten.

Gert-Rene Polli war 25 Jahre lang Offizier, davon die längste Zeit im österreichischen Heeresnachrichtenamt. 2002 bis 2008 war Polli Direktor des damals neugegründeten Bundesamts für Verfassungssdchutz und Terrorbekämpfung Im Innenministerium.

Dann wieder kam heraus, dass Beamte nach Lust und Laune in den Datenbanken gefuhrwerkt hatten, etwa um die Identität der "feschen Blonden im Mercedes-Cabrio" über die KFZ-Halterdatenbank zu ermitteln. Dann wieder wurden im Auftrag von Detektivbüros Daten von Privatpersonen abgezogen und weitergegeben oder es wurde im eigenen, weiteren Familienbereich spioniert.

Die Crux mit dem Verwendungszweck

All diesen Fällen gemeinsam war, dass Daten zu anderen Zwecken als für jene verwendet wurden, für die sie erhoben worden waren: polizeiliche Ermittlungstätigkeit. Genau diese Zweckbindung ist einer der in Brüssel am heftigsten umstrittenen Punkte in der Novelle zum Datenschutzpaket. Wie nämlich weitere Verwendungszwecke, als jene, zu denen das Datensubjekt - eine Privatperson - zugestimmt hat, geregelt werden.

Neben seiner Tätigkeit als Sicherheitsberater ist Rene Pfeiffer einer der Veranstalter der jährlichen Security-Konferenz DeepSec. Dieser Event unterscheidet sich von anderen Sicherheitsveranstaltungen insofern stark, weil es eine Veranstaltung von Miglieder der Wiener IT-Security-Community ist und Open-Source-Lösungen im Mittelpunkt stehen.

Die US-amerikanischen Internetkonzerne wie der weitaus kleinteiligere, europäische Datenhandelssektor - Direktmarketer, Adressverlage, Bonitätsbüros und Internetfirmen - bekämpfen jede diesbezügliche Regelung mit allen Mitteln, die ihnen zur Verfügung stehen. Von "bürokratischen Hürden" ist da die Rede und Nachteilen im

Wettbewerb, weil den Unternehmen dadurch Mehrkosten aufgebürdet würden.

Die Position der EVP

Während vor allem deutsche EU-Parlamentarier von CDU/CSU und FDP in ihren Änderungsvorschlägen einander an solcher "Wirtschaftsfreundlichkeit" zu überbieten suchen, bezieht die EVP hier eine deutlich ausgewogenere Position. Auf Anfrage von ORF.at wurde der derzeitige Stand der Meinungsbildung zum EU-Datenschutzpaket vom für das Thema zuständigen EVP-Abgeordneten Hubert Pirker so zusammengefasst:

"Bei der Verwendung von persönlichen Daten ist es wichtig, dass der Grundsatz der Zweckbindung beachtet wird. Mit anderen Worten: ich bin gegen eine vollkommen zweckfremde Bearbeitung oder Weitergabe von Daten, die ich für einen bestimmten Zweck hergegeben habe. Die strengen Erfordernisse des europäischen Rechts zur Rechtmäßigkeit der Verarbeitung müssen auf jeden Fall erfüllt sein. Wird Vertrauen missbraucht, so muss es bei schwerwiegenden Verstößen auch Sanktionen geben, die weh tun."

Im Vergleich dazu die Positionen der SPE sowie der Grünen. Die übrigen EU-Parlamentarier - mit einer Ausnahme allesamt fraktionslos - folgen in einem der nächsten Artikel.

Meinungsbildung im EU-Parlament

Der Ausdruck "derzeitiger Stand der Meinungsbildung" entspricht der Brüsseler parlamentarischen Praxis. Abseits von Fraktionszwängen und regionalen Beschränkungen geht man die Dinge dort in der Regel weitaus pragmatischer, differenzierter und weniger ideologisch an, als dies auf den nationalen Ebenen passiert.

Gerade wenn das Thema wie hier einigermaßen komplex und sehr facettenreich ist, verläuft die Meinungsbildung der Parlamentarier in der Regel über Monate. Zum einen müssen sich die MEPs erst einmal in das Thema einarbeiten. Dann gilt es, Interessen und Widersprüche abzuwägen, nicht selten paart sich das mit der Erkenntnis, dass jene, die besonders lautstark lobbyieren, ihre Partikularinteressen einfach zu Interessen der gesamten Wirtschaft erklärt haben, während de facto das Gegenteil der Fall ist.

Besonders bei Lobbyisten im Dienst von US-Großkonzernen ist die Vorgangsweise besonders beliebt, ihre Konzerninteressen als solche von europäischen Mittelstandsunternehmen zu deklarieren, was in den allermeisten Fällen tatsachenwidrig ist.

Österreich und Irland im Vergleich

Was die Kette der Datenskandale im österreichischen Innenministerium betrifft, so rissen diese abrupt ab, nachdem eine einfache Maßnahme gesetzt wurde, die wiederum auf den drei Säulen der Informationssicherheit beruht. Es wurde schlicht und einfach protokolliert, wer wann intern auf welche Datensätze zugegriffen hat. Diese Protokolle werden seitdem routinemäßig einer Plausibilitätsprüfung unterzogen.

Laut Berichten der Irlandausgabe des "Independent" der "Irish Times" u.a. Medien war erst im Dezember 2012 Weisung an die "Garda" ergangen, die Zugriffe auf die Datenbanken zu protokollieren. Davor hatten irische Polizisten offenbar aus Neugier massenhaft Prominenten nachspioniert.

So gelagerte Fälle von Datenmissbrauch durch Polizeibeamte, die jahrelang an der Tagesordnung waren, sind in Österreich seither ausgesprochen selten geworden.

In Irland, wo der Datenschutz aus ökonomischen Gründen seitens der Politik systematisch unterlaufen wird, stehen aktuell mehrere Polizeibeamte vor Gericht. Sie werden beschuldigt, für private Zwecke systematisch Daten aus den Informationssystemen der Polizei abgezogen zu haben. Ganz offensichtlich wurde erst jüngst damit begonnen, die Zugriffe von Beamten der "Garda" zu protokollieren und in Stichproben zu überprüfen. In Österreich ist das bereits vor etwa einem Jahrzehnt passiert.

Erstellt am: 3. 6. 2013 - 10:41 Uhr

Datenschutz hilft, Cyberspionage abzuwehren

Firmen, in denen Datenschutz ein Thema ist, haben in der Regel auch ein generell überdurchschnittliches Sicherheitsniveau, sagen drei namhafte Sicherheitsberater aus Österreich.

Wenn der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) am kommenden Donnerstag zusammentritt, dann wird dort ein Thema mit abgehandelt, das nicht auf der Tagesordnung steht. Nach Ansicht dreier unabhängiger Sicherheitsexperten, die von ORF.at befragt wurden, wird bei dieser ersten Beratung über Maßnahmen gegen Cyberangeriffe automatisch auch über die heftig umstrittene Novelle zum EU-Datenschutzpaket diskutiert.

"Firmen, in denen das Thema Datenschutz hoch angesiedelt ist, haben praktisch immer auch ein überdurchschnittlich hohes Sicherheitsniveau. Beides geht ja Hand in Hand", sagte Joe Pichlmayr zu ORF.at. Erst wenn quer durch die Belegschaft ein Bewusstsein dafür da sei, dass Daten einen Wert darstellen, der von existenzieller Bedeutung für ihr Unternehmen sei, könne auch ein "vitales Interesse entstehen, diese Daten auch zu schützen"; Mit dieser Ansicht steht der Geschäftsführer des österreichischen Sicherheitsunternehmens Ikarus nicht allein.

Datenschutz, Informationssicherheit

"Das kann ich nur unterschreiben. Wer die Aufgabe hat, was auch immer an Informationen zu schützen, der muss sich auch intensiv mit Sicherheitsfragen beschäftigten", so IT-Sicherheitexperte Rene Pfeiffer, der aus der Hackerszene kommt.

"Das ist nur logisch" sekundiert Sicherheitsberater Gert-Rene Polli, was in der allgemeinen Öffentlichkeit nämlich unter "Datenschutz" verstanden werde, sei doch nur Teil des Komplexes "Informationssicherheit". Dieser Begriff stammt aus der militärischen Welt, seit jeher ist "Information Assurance" neben der Spionage ("Signals Intelligence") eine der beiden Kernaufgaben des fortgeschrittensten aller Militärgeheimdienste, der National Security Agency der USA.

HNA, Hacker, Wirtschaft

Der nunmehrige Sicherheitsberater Polli war mehr als zwei Jahrzehnte für das Heeresnachrichtenamt (HNA) tätig und wurde 2002 Direktor des damals neu gegründeten Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT) im Innenministerium. Dass ein gelernter Geheimdienstmann derselben Ansicht zu diesem Thema ist, wie ein gelernter Hacker und der Geschäftsführer einer mittelständischen Anti-Virusfirma klingt nur für Außenstehende befremdlich.

In der Sicherheitsbranche ist es "Common Sense", dass die absolut wichtigste Linie der Verteidigung gegen die überbordenden Spionageangriffe auf Unternehmen das Sicherheitsbewusstssein der Mitarbeiter ist. Dieser Aspekt wurde im Zusammenhang mit dem EU-Datenschutzpaket bis jetzt noch überhaupt nicht diskutiert.

Ein Bärendienst

Im EU-Ministerrat, wo die Meinungsbildung von großen Mitgliedsstatten wie England, Frankreich oder Spanien überproportional geprägt ist, wird der Parlamentsentwurf zum Datenschutzpaket regelrecht demontiert. Österreich hat deshalb generellen Vorbehalt eingelegt .

Dieser wichtige Aspekt der EU-Datenschutznovelle aus dem Blickwinkel der Datensicherheit ist in die Diskussionen von EU-Parlament und Ministerrat bis jetzt noch überhaupt nicht eingeflossen. Jene EU-Parlamentarier, die erklärtermaßen die Interessen der Wirtschaft schützen wollen, indem sie Partei gegen grundlegende Maßnahmen zum Datenschutz ergreifen, erweisen der Wirtschaft damit einen Bärendienst, meint Pfeiffer.

Jede Hebung des betrieblichen Datenschutz- und damit des Sicherheitsniveaus bringe einen "wirtschaftlichen Benefit mit sich, der überhaupt nicht abstrakt sondern in konkreten Zahlen darstellbar ist."

"Geistiges Eigentum der KMUs"

"Betroffen sind vor allem kleine und mittelständische Unternehmen, bei denen in Österreich Innovation und Knowhow zuhause sind", sagt Polli, "Es geht hier um den Schutz des geistigen Eigentums dieser Firmen." Und das sei schon jetzt ziemlich gefährdet, denn "dieser Bereich ist leider so offen wie ein Scheunentor."

Angesichts der kleinteiligen Struktur der österreichischen Wirtschaft sei es gerade für innovative und obendrein neu gegründete Firmen gar nicht erschwinglich, von vornherein eine entsprechend dimensionierte Sicherheitsabteilung mit einem "Chief Security Officer" einzurichten, so Polli weiter.

"Authentizität, Integrität und Vertraulichkeit"

Solche "Targeted Attacks" oder "Spear Phishing" genannten Angriffsformen zielen auf einen definierten Personenkreis. Im Fall von Cyberspionage zum wirtschaftlichen Vorteil werden etwa die Mitarbeiter einer Firma in Sozialen Netzen beobachtet und dann kontaktiert. Sobald eine gewisse Vertraulichkeit gegegeben ist, kommen die Angriffsmails, deren Anhänge eine bis dahin nicht bekannte Sicherheitslücke angreifen. Damit ist man im Firmennetzwerk.

Wer unter "Schutzmaßnahmen für betriebliche Daten" die bloße Einrichtung von Firewalls und Virenscannern verstehe, sei in der globalsierten Welt der Informationstechnologie mehr gefährdet, als er vielleicht glaube, sagt Pichlmayr. Um ein akzeptables Niveau an Datensicherheit zu erreichen, gelte es zuerst einmal, einen Masterplan zu erstellen, der auf den "drei Säulen der Informationssicherheit aufgebaut sein muss: Authentizität, Integrität und Vertraulichkeit".

Von diesen drei Prinzipien der Informationssicherheit, die lange vor dem World Wide Web schon galten, sind auch die Prinzipien des Datenschutzes hergeleitet. Alle in den Datenschutzgesetzen quer durch Europa vorgeschriebenen Mechanismen und Regeln zum Schutz der persönlichen Daten von Privatpersonen finden sich hier wieder.

Das Prinzip in der Praxis

So ist seit der ersten EU-Datenschutzrichtlinie von 1995 ein Recht auf Einsicht in die eigenen Datensätze und deren allfällige Korrektur durch den Eigentümer dieser Daten selbst gesetzlich festgeschrieben. Das Recht, bei Falschangaben in den eigenen, persönlichen Datensätzen eine Richtigstellung erzwingen zu können, fällt unter "Integrität".

"Authentizität" wiederum bedeutet mehr als nur diese Daten auf ihren Eigentümer zurückzuführen, also ihre Echtheit zu überprüfen, sondern auch den Abfragenden selbst. Wer auf personenbezogene Datensätze zugreift, muss sich daher authentifizieren, während in Punkt "Vertraulichkeit" der Regelsatz definiert ist, wer aller unter welchen Umständen auf Daten zugreifen darf und wie dieser Zugriff dokumentiert werden muss.

Historische Datenskandale

Josef Pichlmayr ist Geschäftsführer der 1993 gegründeten IT-Security-Firma Ikarus (http://www.ikarus.at) . Die Ikarus war einer der ersten europäischen Firmen überhaupt, die einen eigenen Virenscanner entwickelt hat.

In der jüngeren österreichischen Geschichte finden sich sich zuhauf Beispiel dafür, was unweigerlich passiert, wenn diese Regeln nicht beachtet werden. Weil man die Polizeibeamten nicht durch "unnötige bürokratische Hürden" - wie es damals hieß - in ihrer Ermittlungstätigkeit behindern wollte, wurden jahrelang keine internen Regeln für Protokollierung und Überprüfung dieser Zugriffe auf die Datenbanken des Innenministeriums festgelegt.

Die Folge war eine Serie von Datenskandalen im genannten Ministerium. 1998 flog eine Reihe von Beamten auf, die Meldedaten und solche aus den kriminalpolizeilichen Ermittlungsakten auf eigene Faust an Datenhändler weiterverkauft hatten.

Gert-Rene Polli (http://www.polli-ips.com/) war 25 Jahre lang Offizier, davon die längste Zeit im österreichischen Heeresnachrichtenamt. 2002 bis 2008 war Polli Direktor des damals neugegründeten Bundesamts für Verfassungssdchutz und Terrorbekämpfung Im Innenministerium.

Dann wieder kam heraus, dass Beamte nach Lust und Laune in den Datenbanken gefuhrwerkt hatten, etwa um die Identität der "feschen Blonden im Mercedes-Cabrio" über die KFZ-Halterdatenbank zu ermitteln. Dann wieder wurden im Auftrag von Detektivbüros Daten von Privatpersonen abgezogen und weitergegeben oder es wurde im eigenen, weiteren Familienbereich spioniert.

Die Crux mit dem Verwendungszweck

All diesen Fällen gemeinsam war, dass Daten zu anderen Zwecken als für jene verwendet wurden, für die sie erhoben worden waren: polizeiliche Ermittlungstätigkeit. Genau diese Zweckbindung ist einer der in Brüssel am heftigsten umstrittenen Punkte in der Novelle zum Datenschutzpaket. Wie nämlich weitere Verwendungszwecke, als jene, zu denen das Datensubjekt - eine Privatperson - zugestimmt hat, geregelt werden.

Neben seiner Tätigkeit als Sicherheitsberater ist Rene Pfeiffer einer der Veranstalter der jährlichen

Security-Konferenz DeepSec (https://deepsec.net/) . Dieser Event unterscheidet sich von anderen Sicherheitsveranstaltungen insofern stark, weil es eine Veranstaltung von Miglieder der Wiener IT-Security-Community ist und Open-Source-Lösungen im Mittelpunkt stehen.

Die US-amerikanischen Internetkonzerne wie der weitaus kleinteiligere, europäische Datenhandelssektor - Direktmarketer, Adressverlage, Bonitätsbüros und Internetfirmen - bekämpfen jede diesbezügliche Regelung mit allen Mitteln, die ihnen zur Verfügung stehen. Von "bürokratischen Hürden" ist da die Rede und Nachteilen im Wettbewerb, weil den Unternehmen dadurch Mehrkosten aufgebürdet würden.

Die Position der EVP

Während vor allem deutsche EU-Parlamentarier von CDU/CSU und FDP in ihren Änderungsvorschlägen einander an solcher "Wirtschaftsfreundlichkeit" zu überbieten suchen, bezieht die EVP hier eine deutlich ausgewogenere Position. Auf Anfrage von ORF.at wurde der derzeitige Stand der Meinungsbildung zum EU-Datenschutzpaket vom für das Thema zuständigen EVP-Abgeordneten Hubert Pirker so zusammengefasst:

"Bei der Verwendung von persönlichen Daten ist es wichtig, dass der Grundsatz der Zweckbindung beachtet wird. Mit anderen Worten: ich bin gegen eine vollkommen zweckfremde Bearbeitung oder Weitergabe von Daten, die ich für einen bestimmten Zweck hergegeben habe. Die strengen Erfordernisse des europäischen Rechts zur Rechtmäßigkeit der Verarbeitung müssen auf jeden Fall erfüllt sein. Wird Vertrauen missbraucht, so muss es bei schwerwiegenden Verstößen auch Sanktionen geben, die weh tun."

Im Vergleich dazu die Positionen der SPE sowie der Grünen. Die übrigen EU-Parlamentarier - mit einer Ausnahme allesamt fraktionslos - folgen in einem der nächsten Artikel.

Meinungsbildung im EU-Parlament

Der Ausdruck "derzeitiger Stand der Meinungsbildung" entspricht der Brüsseler parlamentarischen Praxis. Abseits von Fraktionszwängen und regionalen Beschränkungen geht man die Dinge dort in der Regel weitaus pragmatischer, differenzierter und weniger ideologisch an, als dies auf den nationalen Ebenen passiert.

Gerade wenn das Thema wie hier einigermaßen komplex und sehr facettenreich ist, verläuft die Meinungsbildung der Parlamentarier in der Regel über Monate. Zum einen müssen sich die MEPs erst einmal in das Thema einarbeiten. Dann gilt es, Interessen und Widersprüche abzuwägen, nicht selten paart sich das mit der Erkenntnis, dass jene, die besonders lautstark lobbyieren, ihre Partikularinteressen einfach zu Interessen der gesamten Wirtschaft erklärt haben, während de facto das Gegenteil der Fall ist.

Besonders bei Lobbyisten im Dienst von US-Großkonzernen ist die Vorgangsweise besonders beliebt, ihre Konzerninteressen als solche von europäischen Mittelstandsunternehmen zu deklarieren, was in den allermeisten Fällen tatsachenwidrig ist.

Österreich und Irland im Vergleich

Was die Kette der Datenskandale im österreichischen Innenministerium betrifft, so rissen diese abrupt ab, nachdem eine einfache Maßnahme gesetzt wurde, die wiederum auf den drei Säulen der Informationssicherheit beruht. Es wurde schlicht und einfach protokolliert, wer wann intern auf welche Datensätze zugegriffen hat. Diese Protokolle werden seitdem routinemäßig einer

Plausibilitätsprüfung unterzogen.

Laut Berichten der Irlandausgabe des "Independent" (http://www.independent.ie/irish-news/report-finds-gardai-snooping-on-celebrities-and-sports-stars-29281086.html) der "Irish Times" u.a. Medien war erst im Dezember 2012 Weisung an die "Garda" ergangen, die Zugriffe auf die Datenbanken zu protokollieren. Davor hatten irische Polizisten offenbar aus Neugier massenhaft Prominenten nachspioniert.

So gelagerte Fälle von Datenmissbrauch durch Polizeibeamte, die jahrelang an der Tagesordnung waren, sind in Österreich seither ausgesprochen selten geworden.

In Irland, wo der Datenschutz aus ökonomischen Gründen seitens der Politik systematisch unterlaufen wird, stehen aktuell mehrere Polizeibeamte vor Gericht. Sie werden beschuldigt, für private Zwecke systematisch Daten aus den Informationssystemen der Polizei abgezogen zu haben. Ganz offensichtlich wurde erst jüngst damit begonnen, die Zugriffe von Beamten der "Garda" zu protokollieren und in Stichproben zu überprüfen. In Österreich ist das bereits vor etwa einem Jahrzehnt passiert.

http://www.golem.de/news/2012-die-verschwindetricks-der-social-engineers-1212-96455.html

Die Verschwindetricks der Social Engineers

Datum:26.12.2012, 09:25

Autor:Jörg Thoma

Per Social Engineering ist es Betrügern 2012 gelungen, die gesamte digitale Identität eines Wired-Journalisten verschwinden zu lassen. Im Real Life ließen sie sogar eine ganze Brücke mitgehen.

Jenseits von Phishing-Attacken, als Nacktfotos getarnter Malware im E-Mail-Postfach oder sprachlich unbeholfenen Aufforderungen, bei lukrativen Finanztransaktionen in Nigeria behilflich zu sein, gibt es Betrugsmaschen, auf die selbst Polizei und IT-Experten hereinfallen: Hacks auf Onlinekonten, Identitätsklau, Industriespionage, Diebstahl mit digitalen Unterschriften oder mit gefälschten Dokumenten. Die Social-Engineering-Expertin und Sicherheitsprüferin Sharon Conheady hat auf der Deepsec 2012 die spektakulärsten Scams 2012 präsentiert.

http://video.golem.de/internet/6440/interview-sharon-conheady.html

Video: Interview Sharon Conheady über Social Engineering (10:41)

Gesamtes digitales Leben gelöscht

Das komplette digitale Leben des Wired-Journalisten Matt Honan wurde von Angreifern gelöscht. Sie verschafften sich durch Social Engineering genügend Informationen, um sich bei einem Anruf beim Apple-Support als Honan zu authentifizieren und forderten ein neues Passwort für Honans Me.com-Account an. Damit ausgestattet, konnten sie gleich auch Honans Apple-ID ändern. Zuvor hatten sie noch die Bestätigungs-E-Mail in den Papierkorb verschoben. Kurz darauf setzten sie sein Gmail-Passwort und die Zugangsdaten zu seinem Konto bei Google zurück.

Kleinlaut musste Honan zugeben, dass es ein Fehler gewesen war, sämtliche E-Mail-Konten mit dem gleichen Namen zu versehen und sie auch mit verschiedenen Konten zu verknüpfen. Backups hatte er nicht. Hätte er seinen Google-Account mit zweifacher Authentifizierung abgesichert, wären die Hacker nicht weitergekommen, schreibt er in einem ausführlichen Bericht. Er kritisierte aber auch Apple, das mit nur wenigen Informationen das Zurücksetzen eines Passworts erlaubt.

Ziel der Scammer war das Twitter-Konto

Auch das Passwort für Honans Twitter-Account forderten die Hacker an und verbreiteten darüber rassistische Tweets. Über den iCloud-Account setzten sie iPhone, iPad und Macbook zurück und löschten schließlich auch

sein Google-Konto. E-Mails, Familienfotos, alles sei weg, beklagt Honan. Die Angreifer hatten es zwar nur auf sein Twitter-Konto abgesehen, löschten aber alles andere, damit Honan ihn nicht wieder zurückbekommen würde.

Letztendlich benötigt Apple nur die Rechnungsadresse und die letzten vier Zahlen der Kreditkarte, um einen Zugang zurückzusetzen, wie das Unternehmen auf Anfrage von Wired bestätigte. Wie die Betrüger daran gekommen waren, erfuhr Honan später von ihnen selbst. Sie tauschten sich über Honans neuen Twitter-Account aus.

Erst Amazon-, dann Google- und Apple-Konten

Honans Rechnungsadresse erfuhren die Hacker durch einen einfachen Whois-Lookup seiner privaten Domäne. Genauso gut hätten sie aber öffentliche Verzeichnisse im Internet durchforsten können, schreibt Honan. Den wiederkehrenden Namen "mhonan" in seinen diversen E-Mail-Adressen erfuhren sie über seinen Twitter-Account.

Die benötigten Ziffern seiner Kreditkartennummer holten sich die Hacker bei Amazon. Dort hatte Honan ebenfalls ein Konto. Zunächst riefen die Betrüger beim Support an und gaben die Rechnungsadresse, die E-Mail-Adresse und den Namen an. Nach erfolgreicher Authentifizierung verlangten sie, dem Konto eine zweite Kreditkartennummer hinzuzufügen, und gaben eine - natürlich gefälschte - Nummer durch.

Später riefen sie nochmals dort an, gaben an, keinen Zugang zum Konto mehr zu haben und gaben wieder Rechnungsadresse, Name, E-Mail-Adresse und die neue Kreditkartennummer an. Daraufhin konnten sie dem Konto eine zweite E-Mail-Adresse hinzufügen, an die dann ein neues Passwort versendet wurde. Damit ausgestattet, loggten sie sich ein und erfuhren die Ziffern, die sie für die Authentifizierung bei Apple benötigten.

Es war nicht persönlich gemeint

Sie hätten es nicht auf ihn persönlich abgesehen, schrieb ihm einer der Betrüger später. Sie hätten nur sein Twitter-Konto kapern wollen. Es hätte schlimmer kommen können, schrieb der zerknirschte Journalist, denn er habe zahlreiche einflussreiche Namen in seiner Kontaktliste, die ebenfalls hätten angegriffen werden können. Er trauere aber um die unwiederbringlich gelöschten Fotos seiner Familie, vor allem seiner kleinen Tochter, die er seit ihrer Geburt gesammelt hatte. Auch sein Ruf als IT-Journalist habe gelitten.

Dem Hacker habe sein Tun später leidgetan, schreibt Honan. Nicht er, sondern sein Kumpel habe Honans Daten gelöscht, teilte der Angreifer mit. Auf die Frage Honans, warum er den Hack eigentlich durchgeführt habe, antwortete er lapidar, er wolle auf die Schwachstelle hinweisen. Die Hackerethik besagt allerdings, dass öffentliche Daten genutzt und private Daten geschützt werden müssen.

Falscher Paul Allen verschafft sich Kontozugang

Stars oder Millionäre sind natürlich ein beliebtes Angriffsziel für Scammer, da über sie viel bekannt ist und das Hacken eine medienwirksame Aktion bedeutet - oder einfach, weil sie viel Geld haben.

Nicht besonders geschickt hat sich ein unerlaubt abwesender US-Soldat in den USA angestellt, der sich zunächst erfolgreich als der Millionär und Microsoft-Mitbegründer Paul Allen ausgab. Er rief bei Allens Bank an und erklärte, dass er seine Bankkarte daheim verlegt hätte. Er wolle die Karte zwar nicht als verloren melden, hätte aber gerne sobald wie möglich eine zweite. Der Citibank-Mitarbeiter war offensichtlich so hilfsbereit, dass er eine zusätzliche Adresse aufnahm, an die er die zweite Karte per Express rausschickte. Der US-Soldat gab auch gleich seine Telefonnummer an.

Viel Erfolg hatte der Soldat aber nicht. Ihm gelang zwar zunächst eine Überweisung in Höhe von etwa 600 US-Dollar mit der neuen Karte, eine zweite Überweisung in Höhe von 15.000 US-Dollar sowie Einkäufe in einem Computerspielgeschäft fielen aber der Betrugsabteilung in der Bank auf. Der Soldat wurde verhaftet und angeklagt. Wie der Betrüger den Bankmitarbeiter dazu überredete, die zweite Karte auszustellen, bleibt ein Geheimnis. Die Bank gab dazu keinen Kommentar ab.

Mit öffentlicher Unterschrift zu Millionen

Gleich mehrere Anläufe benötigten Scammer aus Hongkong, um etwa 2 Millionen US-Dollar zu erbeuten. Das Geld ergaunerten sie von Wells Fargo, das ein gemeinsames Treuhandkonto des US-Bezirks Merced und der Catholic Healthcare West verwaltet. Das Geld auf dem Treuhandkonto ist für das Medical Center in Merced im US-Bundesstaat Kalifornien gedacht.

Die Betrüger forderten zunächst einen Geldbetrag von 440.000 US-Dollar per Fax an. Ihre Anforderungen legitimierten sie mit der Unterschrift des Präsidenten der Stiftung. Diese hatten sie ausgerechnet von der Webseite der Stiftung selbst. Dort waren mehrere Dokumente verfügbar, die die Unterschrift enthielten.

Das Konto, auf das Wells Fargo das Geld überweisen sollte, gab es aber nicht. Möglicherweise wollten die Betrüger zunächst prüfen, ob ihr Scam überhaupt funktioniert. Wells Fargo kontaktierte den anonymen Betrüger, um die Kontonummer zu verifizieren. Auch eine zweite Überweisung klappte jedoch nicht. Erst Monate und mehrere Anfragen später schaffte es das Geldinstitut, etwa 1 Million US-Dollar auf ein tatsächlich vorhandenes Konto in Hongkong zu überweisen. Nach einer weiteren Anfrage transferierte Wells Fargo ein weiteres Mal etwa 1,1 Millionen US-Dollar. Erst, als Betrüger abermals 2,3 Millionen US-Dollar anforderten, schöpfte das Geldinstitut Verdacht. Es erstattete das fälschlich überwiesene Geld an die Stiftung zurück und Anzeige gegen unbekannt.

Der Klassiker: Industriespionage

Industriespionage gehört mit zu den ältesten und erfolgreichsten Maschen des Social Engineerings. Als legitim betrachtete Mitarbeiter können sich Zugang zu den geheimsten Labors verschaffen und Konkurrenten ausspionieren. Jüngst will die britische Staubsaugerfirma Dyson einen Spion von Bosch bei sich entdeckt haben, der dort Geschäftsgeheimnisse gesammelt und an die deutsche Firma Bosch weitergeben haben soll. Der Mitarbeiter, dessen Identität noch unbekannt ist, soll zwei Jahre lang in Dysons Entwicklungsabteilung für elektrische Motoren gearbeitet haben.

Die Abteilung ist laut Dyson in einem Gebäudetrakt mit höchster Sicherheit untergebracht, der Zugang nur per Fingerabdruckerkennung möglich. Bosch weist die Vorwürfe zurück. Der ehemalige Mitarbeiter habe bei Bosch in der Abteilung für Gartengeräte gearbeitet. Dyson hat gegen Bosch Klage vor einem britischen Gericht eingereicht.

Schon früher wurden deutsche Firmen beschuldigt, bei britischen Unternehmen abgekupfert zu haben. Im späten 19. Jahrhundert hatte Großbritannien einen derart großen Vorsprung bei Qualitätsprodukten vor dem Nachzügler auf dem Kontinent, dass reihenweise deutsche Facharbeiter zum "Anlernen" auf die Insel geschickt wurden. Damit die immer noch minderwertigen und fast identischen deutschen Produkte von den britischen Originalen zu unterscheiden waren, setzte Großbritannien damals die Bezeichnung "Made in Germany" durch.

...und eine ganze Brücke

Einer der Basistricks bei Social Engineering sind gefälschte Dokumente. Mit diesen konnten Diebe in der Nähe von Slavkov in Tschechien einen ganzen Fußgängerübergang abbauen und die darunterliegenden Bahngleise gleich mit. Die Metalldiebe rückten dafür sogar mit einem Kran an. Als die örtliche Polizei nach dem Rechten sehen wollte, präsentierten die Diebe offensichtlich gut gefälschte Genehmigungspapiere. Sie seien mit dem Abriss beauftragt worden, um Platz für einen neuen Fahrradweg zu machen.

Erst nachdem die Brücke verschwunden war, überprüften Mitarbeiter der örtlichen Bahnstation den vermeintlichen Auftrag. Angaben über die Höhe des Verlusts reichen von mehreren Tausend Euro an Materialkosten bis hin zu mehreren Millionen Euro für den Wiederaufbau der entwendeten Brücke. Die Gleisstrecke war aber laut Bahn bereits stillgelegt.

Metallabbau hat in der Gegend um Slavkov Tradition: Bereits im 2. Jahrtausend vor Christus wurde dort Zinnab- gebaut, die Region war bis ins 16. Jahrhundert für das Metall berühmt. Es wurde beispielsweise von der Familie Fugger aus Augsburg gehandelt.

Betrug ist nicht Hacken

Auch wenn sich einige Diebe wie im Fall des IT-Journalisten Honan selbst gerne Hacker nennen, verstoßen sie gegen die allgemein anerkannte Ethik, dass persönliche Daten geschützt werden müssen. Betrug durch Social Engineering hat nichts mit Hacking zu tun und kann auch furchtbare Konsequenzen für die Opfer haben. Das zeigt auch der tragische Fall der britischen Krankenschwester.

Sie war auf einen Trickanruf von zwei Radiomoderatoren hereingefallen, die sich als Queen Elisabeth II und Prince Charles ausgaben und Informationen über den Gesundheitszustand der schwangeren Herzogin Kate erbaten. Obwohl sie lediglich den Anruf durchgestellt hatte, beging die Krankenschwester Selbstmord, nachdem der Sender die so erschlichenen Informationen veröffentlicht hatte. Dem Sender wurden schwere Vorwürfe gemacht, weil er das Opfer nicht aufgeklärt und den Telefonscherz ohne dessen Erlaubnis veröffentlicht hatte.

Conheady hat viel Verständnis für die Opfer von Social Engineering, auch für ihre eigenen. Denn ihre Aufgabe ist es, mit Social-Engineering-Tricks in Unternehmen einzudringen und so Sicherheitslücken aufzudecken. Mitarbeiter, die auf Conheadys Tricks hereinfallen, werden meist aufgeklärt, aber nicht gescholten. Sie könne ihren Job ohne Mitgefühl oder Empathie für ihre potenziellen Opfer gar nicht machen, sagt sie. Sie müsse sich ja in diese Personen hineinversetzen können, um Wege zu finden, sie zu überlisten.

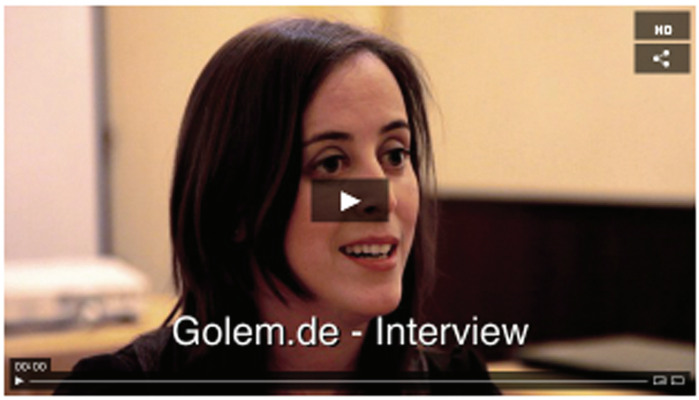
Nicht nur für die Opfer, auch für die Scammer selbst kann Betrug durch Social Engineering schwere Folgen haben. Das zeigt ein Fall in den USA. Dort wurde der selbsternannte Paparazzi-Hacker zu zehn Jahren Haft verurteilt. Er hatte prominente Opfer wie Scarlett Johansson jahrelang ausspioniert, deren private Daten veröffentlicht und damit geprahlt.

2012

Die Verschwindetricks der Social Engineers

Per Social Engineering ist es Betrügern 2012 gelungen, die gesamte digitale Identität eines Wired-Journalisten verschwinden zu lassen. Im Real Life ließen sie sogar eine ganze Brücke mitgehen.

Jenseits von Phishing-Attacken, als Nacktfotos getarnter Malware im E-Mail-Postfach oder sprachlich unbeholfenen Aufforderungen, bei lukrativen Finanztransaktionen in Nigeria behilflich zu sein, gibt es Betrugsmaschen, auf die selbst Polizei und IT-Experten hereinfallen: Hacks auf Onlinekonten, Identitätsklau, Industriespionage, Diebstahl mit digitalen Unterschriften oder mit gefälschten Dokumenten. Die Social-Engineering-Expertin und Sicherheitsprüferin Sharon Conheady hat auf der Deepsec 2012 die spektakulärsten Scams 2012 präsentiert.



Video: Interview Sharon Conheady über Social Engineering (10:41)

Gesamtes digitales Leben gelöscht

Das komplette digitale Leben des Wired-Journalisten Matt Honan wurde von Angreifern gelöscht. Sie verschafften sich durch Social Engineering genügend Informationen, um sich bei einem Anruf beim Apple-Support als Honan zu authentifizieren und forderten ein neues Passwort für Honans Me.com-Account an. Damit ausgestattet, konnten sie gleich auch Honans Apple-ID ändern. Zuvor hatten sie noch die Bestätigungs-E-Mail in den Papierkorb verschoben. Kurz darauf setzten sie sein Gmail-Passwort und die Zugangsdaten zu seinem Konto bei Google zurück.

Kleinlaut musste Honan zugeben, dass es ein Fehler gewesen war, sämtliche E-Mail-Konten mit dem gleichen Namen zu versehen und sie auch mit verschiedenen Konten zu verknüpfen. Backups hatte er nicht. Hätte er seinen Google-Account mit zweifacher Authentifizierung abgesichert, wären die Hacker nicht weitergekommen, schreibt er in einem ausführlichen Bericht. Er kritisierte aber auch Apple, das mit

Verschwindetrick auf traditionelle Art (Bild: George W. Hales/Getty Images)

Datum: 26.12.2012, 09:25

Autor: Jörg Thoma

Themen: Security, Deepsec, Hacker, Malware, Paul Allen, iCloud, Internet, Politik/Recht

nur wenigen Informationen das Zurücksetzen eines Passworts erlaubt.

Ziel der Scammer war das Twitter-Konto

Auch das Passwort für Honans Twitter-Account forderten die Hacker an und verbreiteten darüber rassistische Tweets. Über den iCloud-Account setzten sie iPhone, iPad und Macbook zurück und löschten schließlich auch sein Google-Konto. E-Mails, Familienfotos, alles sei weg, beklagt Honan. Die Angreifer hatten es zwar nur auf sein Twitter-Konto abgesehen, löschten aber alles andere, damit Honan ihn nicht wieder zurückbekommen würde.

Letztendlich benötigt Apple nur die Rechnungsadresse und die letzten vier Zahlen der Kreditkarte, um einen Zugang zurückzusetzen, wie das Unternehmen auf Anfrage von Wired bestätigte. Wie die Betrüger daran gekommen waren, erfuhr Honan später von ihnen selbst. Sie tauschten sich über Honans neuen Twitter-Account aus.

Erst Amazon-, dann Google- und Apple-Konten

Honans Rechnungsadresse erfuhren die Hacker durch einen einfachen Whois-Lookup seiner privaten Domäne. Genauso gut hätten sie aber öffentliche Verzeichnisse im Internet durchforsten können, schreibt Honan. Den wiederkehrenden Namen "mhonan" in seinen diversen E-Mail-Adressen erfuhren sie über seinen Twitter-Account.

Die benötigten Ziffern seiner Kreditkartennummer holten sich die Hacker bei Amazon. Dort hatte Honan ebenfalls ein Konto. Zunächst riefen die Betrüger beim Support an und gaben die Rechnungsadresse, die E-Mail-Adresse und den Namen an. Nach erfolgreicher Authentifizierung verlangten sie, dem Konto eine zweite Kreditkartennummer hinzuzufügen, und gaben eine - natürlich gefälschte - Nummer durch.

Später riefen sie nochmals dort an, gaben an, keinen Zugang zum Konto mehr zu haben und gaben wieder Rechnungsadresse, Name, E-Mail-Adresse und die neue Kreditkartennummer an. Daraufhin konnten sie dem Konto eine zweite E-Mail-Adresse hinzufügen, an die dann ein neues Passwort versendet wurde. Damit ausgestattet, loggten sie sich ein und erfuhren die Ziffern, die sie für die Authentifizierung bei Apple benötigten.

Es war nicht persönlich gemeint

Sie hätten es nicht auf ihn persönlich abgesehen, schrieb ihm einer der Betrüger später. Sie hätten nur sein Twitter-Konto kapern wollen. Es hätte schlimmer kommen können, schrieb der zerknirschte Journalist, denn er habe zahlreiche einflussreiche Namen in seiner Kontaktliste, die ebenfalls hätten angegriffen werden können. Er trauere aber um die unwiederbringlich gelöschten Fotos seiner Familie, vor allem seiner kleinen Tochter, die er seit ihrer Geburt gesammelt hatte. Auch sein Ruf als IT-Journalist habe gelitten.

Dem Hacker habe sein Tun später leidgetan, schreibt Honan. Nicht er, sondern sein Kumpel habe Honans Daten gelöscht, teilte der Angreifer mit. Auf die Frage Honans, warum er den Hack eigentlich durchgeführt habe, antwortete er lapidar, er wolle auf die Schwachstelle hinweisen. Die Hackerethik besagt allerdings, dass öffentliche Daten genutzt und private Daten geschützt werden müssen.

Verschwindetrick auf traditionelle Art (Bild: George W. Hales/Getty Images)

Artikel: 2012
Die Verschwindetricks der Social Engineers

Inhalt:
- Ziel der Scammer war das Twitter-Konto
- Falscher Paul Allen verschafft sich Kontozugang
- Der Klassiker: Industriespionage
- Betrug ist nicht Hacken

Datum: 26.12.2012, 09:25

Autor: Jörg Thoma

Themen: Security, Deepsec, Hacker, Malware, Paul Allen, iCloud, Internet, Politik/Recht

Falscher Paul Allen verschafft sich Kontozugang

Stars oder Millionäre sind natürlich ein beliebtes Angriffsziel für Scammer, da über sie viel bekannt ist und das Hacken eine medienwirksame Aktion bedeutet - oder einfach, weil sie viel Geld haben.

Nicht besonders geschickt hat sich ein unerlaubt abwesender US-Soldat in den USA angestellt, der sich zunächst erfolgreich als der Millionär und Microsoft-Mitbegründer Paul Allen ausgab. Er rief bei Allens Bank an und erklärte, dass er seine Bankkarte daheim verlegt hätte. Er wolle die Karte zwar nicht als verloren melden, hätte aber gerne sobald wie möglich eine zweite. Der Citibank-Mitarbeiter war offensichtlich so hilfsbereit, dass er eine zusätzliche Adresse aufnahm, an die er die zweite Karte per Express rausschickte. Der US-Soldat gab auch gleich seine Telefonnummer an.

Viel Erfolg hatte der Soldat aber nicht. Ihm gelang zwar zunächst eine Überweisung in Höhe von etwa 600 US-Dollar mit der neuen Karte, eine zweite Überweisung in Höhe von 15.000 US-Dollar sowie Einkäufe in einem Computerspielgeschäft fielen aber der Betrugsabteilung in der Bank auf. Der Soldat wurde verhaftet und angeklagt. Wie der Betrüger den Bankmitarbeiter dazu überredete, die zweite Karte auszustellen, bleibt ein Geheimnis. Die Bank gab dazu keinen Kommentar ab.

Mit öffentlicher Unterschrift zu Millionen

Gleich mehrere Anläufe benötigten Scammer aus Hongkong, um etwa 2 Millionen US-Dollar zu erbeuten. Das Geld ergaunerten sie von Wells Fargo, das ein gemeinsames Treuhandkonto des US-Bezirks Merced und der Catholic Healthcare West verwaltet. Das Geld auf dem Treuhandkonto ist für das Medical Center in Merced im US-Bundesstaat Kalifornien gedacht.

Die Betrüger forderten zunächst einen Geldbetrag von 440.000 US-Dollar per Fax an. Ihre Anforderungen legitimierten sie mit der Unterschrift des Präsidenten der Stiftung. Diese hatten sie ausgerechnet von der Webseite der Stiftung selbst. Dort waren mehrere Dokumente verfügbar, die die Unterschrift enthielten.

Das Konto, auf das Wells Fargo das Geld überweisen sollte, gab es aber nicht. Möglicherweise wollten die Betrüger zunächst prüfen, ob ihr Scam überhaupt funktioniert. Wells Fargo kontaktierte den anonymen Betrüger, um die Kontonummer zu verifizieren. Auch eine zweite Überweisung klappte jedoch nicht. Erst Monate und mehrere Anfragen später schaffte es das Geldinstitut, etwa 1 Million US-Dollar auf ein tatsächlich vorhandenes Konto in Hongkong zu überweisen. Nach einer weiteren Anfrage transferierte Wells Fargo ein weiteres Mal etwa 1,1 Millionen US-Dollar. Erst, als Betrüger abermals 2,3 Millionen US-Dollar anforderten, schöpfte das Geldinstitut Verdacht. Es erstattete das fälschlich überwiesene Geld an die Stiftung zurück und Anzeige gegen unbekannt.

‹ 1 2 3 4 5 ›

Verschwindetrick auf traditionelle Art (Bild: George W. Hales/Getty Images)

Artikel: 2012 Die Verschwindetricks der Social Engineers

Inhalt:
- Ziel der Scammer war das Twitter-Konto
- Falscher Paul Allen verschafft sich Kontozugang
- Der Klassiker: Industriespionage
- Betrug ist nicht Hacken

Datum: 26.12.2012, 09:25

Autor: Jörg Thoma

Themen: Security, Deepsec, Hacker, Malware, Paul Allen, iCloud, Internet, Politik/Recht

Der Klassiker: Industriespionage

Industriespionage gehört mit zu den ältesten und erfolgreichsten Maschen des Social Engineerings. Als legitim betrachtete Mitarbeiter können sich Zugang zu den geheimsten Labors verschaffen und Konkurrenten ausspionieren. Jüngst will die britische Staubsaugerfirma Dyson einen Spion von Bosch bei sich entdeckt haben, der dort Geschäftsgeheimnisse gesammelt und an die deutsche Firma Bosch weitergeben haben soll. Der Mitarbeiter, dessen Identität noch unbekannt ist, soll zwei Jahre lang in Dysons Entwicklungsabteilung für elektrische Motoren gearbeitet haben.

Die Abteilung ist laut Dyson in einem Gebäudetrakt mit höchster Sicherheit untergebracht, der Zugang nur per Fingerabdruckerkennung möglich. Bosch weist die Vorwürfe zurück. Der ehemalige Mitarbeiter habe bei Bosch in der Abteilung für Gartengeräte gearbeitet. Dyson hat gegen Bosch Klage vor einem britischen Gericht eingereicht.

Schon früher wurden deutsche Firmen beschuldigt, bei britischen Unternehmen abgekupfert zu haben. Im späten 19. Jahrhundert hatte Großbritannien einen derart großen Vorsprung bei Qualitätsprodukten vor dem Nachzügler auf dem Kontinent, dass reihenweise deutsche Facharbeiter zum "Anlernen" auf die Insel geschickt wurden. Damit die immer noch minderwertigen und fast identischen deutschen Produkte von den britischen Originalen zu unterscheiden waren, setzte Großbritannien damals die Bezeichnung "Made in Germany" durch.

...und eine ganze Brücke

Einer der Basistricks bei Social Engineering sind gefälschte Dokumente. Mit diesen konnten Diebe in der Nähe von Slavkov in Tschechien einen ganzen Fußgängerübergang abbauen und die darunterliegenden Bahngleise gleich mit. Die Metalldiebe rückten dafür sogar mit einem Kran an. Als die örtliche Polizei nach dem Rechten sehen wollte, präsentierten die Diebe offensichtlich gut gefälschte Genehmigungspapiere. Sie seien mit dem Abriss beauftragt worden, um Platz für einen neuen Fahrradweg zu machen.

Erst nachdem die Brücke verschwunden war, überprüften Mitarbeiter der örtlichen Bahnstation den vermeintlichen Auftrag. Angaben über die Höhe des Verlusts reichen von mehreren Tausend Euro an Materialkosten bis hin zu mehreren Millionen Euro für den Wiederaufbau der entwendeten Brücke. Die Gleisstrecke war aber laut Bahn bereits stillgelegt.

Metallabbau hat in der Gegend um Slavkov Tradition: Bereits im 2. Jahrtausend vor Christus wurde dort Zinn abgebaut, die Region war bis ins 16. Jahrhundert für das Metall berühmt. Es wurde beispielsweise von der Familie Fugger aus Augsburg gehandelt.

Verschwindetrick auf traditionelle Art (Bild: George W. Hales/Getty Images)

Datum: 26.12.2012, 09:25

Autor: Jörg Thoma

Themen: Security, Deepsec, Hacker, Malware, Paul Allen, iCloud, Internet, Politik/Recht

Betrug ist nicht Hacken

Auch wenn sich einige Diebe wie im Fall des IT-Journalisten Honan selbst gerne Hacker nennen, verstoßen sie gegen die allgemein anerkannte Ethik, dass persönliche Daten geschützt werden müssen. Betrug durch Social Engineering hat nichts mit Hacking zu tun und kann auch furchtbare Konsequenzen für die Opfer haben. Das zeigt auch der tragische Fall der britischen Krankenschwester.

Sie war auf einen Trickanruf von zwei Radiomoderatoren hereingefallen, die sich als Queen Elisabeth II und Prince Charles ausgaben und Informationen über den Gesundheitszustand der schwangeren Herzogin Kate erbaten. Obwohl sie lediglich den Anruf durchgestellt hatte, beging die Krankenschwester Selbstmord, nachdem der Sender die so erschlichenen Informationen veröffentlicht hatte. Dem Sender wurden schwere Vorwürfe gemacht, weil er das Opfer nicht aufgeklärt und den Telefonscherz ohne dessen Erlaubnis veröffentlicht hatte.

Conheady hat viel Verständnis für die Opfer von Social Engineering, auch für ihre eigenen. Denn ihre Aufgabe ist es, mit Social-Engineering-Tricks in Unternehmen einzudringen und so Sicherheitslücken aufzudecken. Mitarbeiter, die auf Conheadys Tricks hereinfallen, werden meist aufgeklärt, aber nicht gescholten. Sie könne ihren Job ohne Mitgefühl oder Empathie für ihre potenziellen Opfer gar nicht machen, sagt sie. Sie müsse sich ja in diese Personen hineinversetzen können, um Wege zu finden, sie zu überlisten.

Nicht nur für die Opfer, auch für die Scammer selbst kann Betrug durch Social Engineering schwere Folgen haben. Das zeigt ein Fall in den USA. Dort wurde der selbsternannte Paparazzi-Hacker zu zehn Jahren Haft verurteilt. Er hatte prominente Opfer wie Scarlett Johansson jahrelang ausspioniert, deren private Daten veröffentlicht und damit geprahlt. ▪

‹ 1 2 3 4 5

‹ Der Klassiker: Industriespionage

Verschwindetrick auf traditionelle Art (Bild: George W. Hales/Getty Images)

Artikel: 2012
Die Verschwindetricks der Social Engineers

Inhalt:
- Ziel der Scammer war das Twitter-Konto
- Falscher Paul Allen verschafft sich Kontozugang
- Der Klassiker: Industriespionage
- Betrug ist nicht Hacken

Datum: 26.12.2012, 09:25

Autor: Jörg Thoma

Themen: Security, Deepsec, Hacker, Malware, Paul Allen, iCloud, Internet, Politik/Recht

http://oe1.orf.at/programm/322335

matrix - computer & neue medien

Sonntag

09. Dezember 2012

22:30

Löcher im Netz. Die DeepSec 2012. Gestaltung: Sarah Kriesche

Die Sicherheitskonferenz DeepSec findet in diesem Jahr bereits zum 6. Mal statt. Die heurige Veranstaltung widmet sich den Schwerpunkten "Cyberwar", mobile Geräte und Infrastruktur. Nicht nur das Fachpublikum, sondern auch die Endverbraucher sollen auf dieser Veranstaltung, die längst internationale Beachtung gefunden hat, für die Bedeutung sicherer Netzwerke und ein sicheres Internet sensibilisiert werden. Sarah Kriesche berichtet über die Bedrohungen aus dem Netz.

zur Sendereihe

Standort: oe1.ORF.at

matrix - computer & neue medien

Sonntag
09. Dezember 2012
22:30

Löcher im Netz. Die DeepSec 2012. Gestaltung: Sarah Kriesche

Die Sicherheitskonferenz DeepSec findet in diesem Jahr bereits zum 6. Mal statt. Die heurige Veranstaltung widmet sich den Schwerpunkten "Cyberwar", mobile Geräte und Infrastruktur. Nicht nur das Fachpublikum, sondern auch die Endverbraucher sollen auf dieser Veranstaltung, die längst internationale Beachtung gefunden hat, für die Bedeutung sicherer Netzwerke und ein sicheres Internet sensibilisiert werden. Sarah Kriesche berichtet über die Bedrohungen aus dem Netz.

zurück

zur Sendereihe

Kategorie: Wissen

Programm

Mo	Di	Mi	Do	Fr	Sa	So
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16

http://fm4.orf.at/radio/stories/1708743

Connected (13-17)

mit Nina Hofer

Merry Clipmas! Der FM4 Video-Advent-Kalender

Deep Sec

Sicherheitskonferenz in Wien, Rückschau, IT ; Aufhänger ist der Hoax um eine Facebook-Gold-Mitgliedschaft, die es natürlich nicht gibt, und wie leicht man an Geld und Daten von leichtgläubigen Social Media Noobs kommt. (Sarah Kriesche)

Trauma

Eine junge Frau wacht nach einem Autounfall im Krankenhaus auf und versucht sich zu erinnern. In Form von Bildern und Photos reflektiert sie über ihr Leben. Der/die SpielerIn klickt sich durch eine menschenleere Welt, auf der Suche nach Hinweisen. Die Bilder von verlassenen Kölner Orten bei Nacht, dazu ein sphärischer Soundtrack und die unheimliche Erzählstimme der jungen Frau saugen einen in die melancholische Welt von „Trauma“, das eigentlich nur mehr als Computerspiel bezeichnet werden kann, weil es noch keinen besseren Begriff dafür gibt. Conny Lee hat die interaktiven Bilder von Trauma erforscht.

Cribs

In ihrer Heimat England sind sie die DIY-Vorzeigeband, die regelmässig Konzerte ausverkauft und heuer auch mit dem Q Magazin Spirit Of Independence Award ausgezeichnet wurde. Im Fm4 Blinddate mit Susi Ondrusova sprechen Ross Jarman und Gary Jarman u.a. über Queen, Beat Happening, Steve Albini und Beth Ditto.

Artist Of The Week: Interpol (Arthur Einöder) | Crystal Castles (Dani Derntl) |

Amadou & Mariam (Eva Umbauer) | Linus Volkmann - Kein Schlaf bis Langenselbold (David Pfister)

Connected (13-17)

mit Nina Hofer

Merry Clipmas! Der FM4 Video-Advent-Kalender

Deep Sec (https://deepsec.net/)
Sicherheitskonferenz in Wien, Rückschau, IT ; Aufhänger ist der Hoax um eine Facebook-Gold-Mitgliedschaft, die es natürlich nicht gibt, und wie leicht man an Geld und Daten von leichtgläubigen Social Media Noobs kommt. (Sarah Kriesche)

Trauma
Eine junge Frau wacht nach einem Autounfall im Krankenhaus auf und versucht sich zu erinnern. In Form von Bildern und Photos reflektiert sie über ihr Leben. Der/die SpielerIn klickt sich durch eine menschenleere Welt, auf der Suche nach Hinweisen. Die Bilder von verlassenen Kölner Orten bei Nacht, dazu ein sphärischer Soundtrack und die unheimliche Erzählstimme der jungen Frau saugen einen in die melancholische Welt von „Trauma“, das eigentlich nur mehr als Computerspiel bezeichnet werden kann, weil es noch keinen besseren Begriff dafür gibt. Conny Lee hat die interaktiven Bilder von Trauma erforscht.

Cribs (http://www.thecribs.com/official/)
In ihrer Heimat England sind sie die DIY-Vorzeigeband, die regelmässig Konzerte ausverkauft und heuer auch mit dem Q Magazin Spirit Of Independence Award (http://www.youtube.com/watch?v=4tHizgTRBAg) ausgezeichnet wurde. Im Fm4 Blinddate mit Susi Ondrusova sprechen Ross Jarman und Gary Jarman u.a. über Queen, Beat Happening, Steve Albini und Beth Ditto.

Artist Of The Week (/artistoftheweek) : Interpol (Arthur Einöder) | Crystal Castles (http://www.crystalcastles.com/) (Dani Derntl) |
Amadou & Mariam (http://www.amadou-mariam.com/?utm_source=Email+Campaign&utm_medium=email&utm_campaign=188866-Amadou+and+Mariam+) (Eva Umbauer) | Linus Volkmann - Kein Schlaf bis Langenselbold (David Pfister)

http://www.golem.de/news/vmware-esxi-5-uebernahme-des-hypervisors-ueber-ein-gastsystem-1211-96059.html

VMWARE ESXI 5

Übernahme des Hypervisors über ein Gastsystem

Datum:30.11.2012, 12:09

Autor:Jörg Thoma

Deepsec 2012 Mit modifizierter Firmware können Hacker mit einer Root-Shell auf den ESXi-5-Hypervisor von VMware zugreifen. Das haben die beiden Sicherheitsexperten Pascal Turbing und Hendrik Schmidt auf der Deepsec 2012 demonstriert.

Ohne großen Aufwand können Angreifer auf den Hypervisor von VMware zugreifen. Sie können dazu weitgehend unbekannte Parameter in den Beschreibungsdateien der virtuellen Festplatten für Gastsysteme nutzen, um sich schreibenden Zugriff auf das Root-Dateisystem des Hypervisors zu verschaffen. Da der Zugriff auf die virtuelle Infrastruktur in entfernten Systemen weitgehend vom Provider ungeprüft erfolgt, werten die Sicherheitsexperten Pascal Turbing und Hendrik Schmidt diese Lücke als gravierend. Sie demonstrierten auf der Deepsec 2012 erstmals auch einen Zugriff auf den Hypervisor mit einer Root-Shell.

Zunächst fiel den Sicherheitsexperten auf, dass sie mit eigenen Parametern im Abschnitt Disk Descriptor aus Gastsystemen heraus auf die Lodgdateien des Hypervisors zugreifen können. Dazu reicht beispielsweise der Eintrag VMFS "/scratch/log/vmkernel1.0.gz". Danach kann die Logdatei als Loopback-Device mit dem Befehl losetup in das Linux-Gastsystem eingebunden werden.

Erst Logdateien, dann ganze Verzeichnisse

Turbing und Schmidt gingen noch ein Schritt weiter. Mit dem Zugriff auf die Logdateien ließen sich auch weitere Informationen der virtuellen Umgebung auslesen, etwa der Name der von dem Hypervisor verwendeten Festplatten. Diese konnten sie dann mit dem Konfigurationseintrag RW 0 VMFSRAW "/dev/disk/Diskname" ebenfalls ins Gastsystem einbinden.

Das funktioniert auch deshalb, weil Linux Geräte als Dateien behandelt. Das Einbinden einzelner Verzeichnisse ist ebenfalls möglich. Lediglich Dateien in der Ramdisk des Hypervisors konnten sie zunächst nicht einbinden, denn sie wird dynamisch während des Starts des Hypervisors erzeugt und mit den Parametern aus der Bootbank-Partition gefüttert, aus der das Root-Dateisystem des Hypervisors generiert wird.

Zugriff auf die Konfigurationsdateien des Hypervisors

Also galt es, Zugriff auf das Bootbank-Verzeichnis zu erhalten. Es wurde wie bereits erwähnt mit Schreibzugriff im Gastsystem eingebunden. Die dort abgelegten Dateien sind mit einem speziellen Tar-Gz-Format gepackt. Sie können nur mit der Binärdatei Vmtar und der Bibliothek Libvmlibs.so erstellt werden, die jeder VMware-Installation beiliegen und in das Gastsystem kopiert werden können.

Die Hacker konnten so eine modifizierte Firewall-Konfigurationsdatei im Bootbank-Verzeichnis ablegen und beispielsweise per DoS-Angriff einen Neustart des Hypervisors erzwingen. Danach konnte sie sich in die Shell des Hypervisors einloggen.

Unbefugte Nutzer fernhalten

Ein solcher Angriff kann unter folgenden Voraussetzungen erfolgen: Das präparierte Gastsystem muss über das von VMware bereitgestellte API ohne Änderungen oder Verifizierung auf das System mit dem Hypervisor ESXi 5 übertragen werden. Die Dateien des Gastsystems müssen auf einer eigenständigen Partition liegen, die nicht vom Hypervisor genutzt wird.

Bislang weist der VMware-Hersteller lediglich darauf hin, dass grundsätzlich Unbefugten kein Zugang zum Hypervisor gewährt werden sollte. Von den vier kontaktierten Serviceprovidern, die virtuelle Umgebungen mit ESXi 5 anbieten, geben nur zwei an, die auf ihre Server hochgeladenen Dateien zu prüfen, sagten Turbing und Schmidt zu Golem.de.

Eine genaue Beschreibung des Angriffsvektors haben die Hacker in ihrem Blog veröffentlicht.

VMWARE ESXI 5

Übernahme des Hypervisors über ein Gastsystem

Deepsec 2012 Mit modifizierter Firmware können Hacker mit einer Root-Shell auf den ESXi-5-Hypervisor von VMware zugreifen. Das haben die beiden Sicherheitsexperten Pascal Turbing und Hendrik Schmidt auf der Deepsec 2012 demonstriert.

Die Hacker Pascal Turbing und Hendrik Schmidt demonstrierten die Übernahme des ESXi-Hypervisors von VMware. (Bild: Andreas Sebayang/Golem.de)

Datum: 30.11.2012, 12:09
Autor: Jörg Thoma
Themen: Deepsec, Cloud Computing, Dateisystem, Server-Applikationen, VMware, Virtualisierung, API, Server, Applikationen, Security

Ohne großen Aufwand können Angreifer auf den Hypervisor von VMware zugreifen. Sie können dazu weitgehend unbekannte Parameter in den Beschreibungsdateien der virtuellen Festplatten für Gastsysteme nutzen, um sich schreibenden Zugriff auf das Root-Dateisystem des Hypervisors zu verschaffen. Da der Zugriff auf die virtuelle Infrastruktur in entfernten Systemen weitgehend vom Provider ungeprüft erfolgt, werten die Sicherheitsexperten Pascal Turbing und Hendrik Schmidt diese Lücke als gravierend. Sie demonstrierten auf der Deepsec 2012 erstmals auch einen Zugriff auf den Hypervisor mit einer Root-Shell.

Zunächst fiel den Sicherheitsexperten auf, dass sie mit eigenen Parametern im Abschnitt *Disk Descriptor* aus Gastsystemen heraus auf die Lodgdateien des Hypervisors zugreifen können. Dazu reicht beispielsweise der Eintrag *VMFS "/scratch/log/vmkernel1.0.gz"*. Danach kann die Logdatei als Loopback-Device mit dem Befehl *losetup* in das Linux-Gastsystem eingebunden werden.

Erst Logdateien, dann ganze Verzeichnisse

Turbing und Schmidt gingen noch ein Schritt weiter. Mit dem Zugriff auf die Logdateien ließen sich auch weitere Informationen der virtuellen Umgebung auslesen, etwa der Name der von dem Hypervisor verwendeten Festplatten. Diese konnten sie dann mit dem Konfigurationseintrag *RW 0 VMFSRAW "/dev/disk/Diskname"* ebenfalls ins Gastsystem einbinden.

Das funktioniert auch deshalb, weil Linux Geräte als Dateien behandelt. Das Einbinden einzelner Verzeichnisse ist ebenfalls möglich. Lediglich Dateien in der Ramdisk des Hypervisors konnten sie zunächst nicht einbinden, denn sie wird dynamisch während des Starts des Hypervisors erzeugt und mit den Parametern aus der Bootbank-Partition gefüttert, aus der das Root-Dateisystem des Hypervisors generiert wird.

Zugriff auf die Konfigurationsdateien des Hypervisors

Also galt es, Zugriff auf das Bootbank-Verzeichnis zu erhalten. Es wurde wie bereits erwähnt mit Schreibzugriff im Gastsystem eingebunden. Die dort abgelegten Dateien sind mit einem speziellen Tar-Gz-Format gepackt. Sie können nur mit der Binärdatei Vmtar und der Bibliothek Libvmlibs.so erstellt werden, die jeder VMware-Installation beiliegen und in das Gastsystem kopiert werden können.

Die Hacker konnten so eine modifizierte Firewall-Konfigurationsdatei im Bootbank-Verzeichnis ablegen und beispielsweise per DoS-Angriff einen Neustart des Hypervisors erzwingen. Danach konnte sie sich in die Shell des Hypervisors einloggen.

Unbefugte Nutzer fernhalten

Ein solcher Angriff kann unter folgenden Voraussetzungen erfolgen: Das präparierte Gastsystem muss über das von VMware bereitgestellte API ohne Änderungen oder Verifizierung auf das System mit dem Hypervisor ESXi 5 übertragen werden. Die Dateien des Gastsystems müssen auf einer eigenständigen Partition liegen, die nicht vom Hypervisor genutzt wird.

Bislang weist der VMware-Hersteller lediglich darauf hin, dass grundsätzlich Unbefugten kein Zugang zum Hypervisor gewährt werden sollte. Von den vier kontaktierten Serviceprovidern, die virtuelle Umgebungen mit ESXi 5 anbieten, geben nur zwei an, die auf ihre Server hochgeladenen Dateien zu prüfen, sagten Turbing und Schmidt zu Golem.de.

Eine genaue Beschreibung des Angriffsvektors haben die Hacker in ihrem Blog veröffentlicht. ▪

Verwandte Artikel

VMsafe soll virtuelle Maschinen sichern

VMWARE

Apple soll Microsoft-Office-

http://www.golem.de/news/snoop-it-fuer-ios-sicherheitschecks-von-iphone-apps-fuer-fast-jeden-moeglich-1211-96034.html

SNOOP-IT FÜR IOS

Sicherheitschecks von iPhone-Apps für fast jeden möglich

Datum:29.11.2012, 15:08

Autor:Andreas Sebayang

Deepsec 2012 Die Snoop-It-App soll jedem eine Basisüberprüfung der Sicherheit von Apps ermöglichen. Das könnte dazu führen, dass viele iOS-Entwickler entdeckt werden, die auf fragwürdige Art und Weise Daten erheben.

Andreas Kurtz von den NESO Security Labs und der Universität Erlangen-Nürnberg arbeitet an einem einfach zu bedienenden Werkzeug, um iOS-Anwendungen auf ihre Sicherheit hin zu überprüfen. Die Snoop-It-App wird auf einem iPhone oder iPad installiert und dort über einen simplen Dialog konfiguriert. Kurtz demonstrierte die Anwendung, die sich noch in einem Vorversionsstatus befindet, auf der Deepsec in Wien. Dabei fiel auf, dass sie vergleichsweise einfach zu bedienen ist. Das Herumhacken auf der Kommandozeile ist nicht einmal notwendig. Stattdessen nutzt der Anwender einfach einen Browser und verbindet sich mit der Snoop-It-App, die gerade eine App untersucht.

Snoop-It-Demo

Über den Browser kann dann mit den Sicherheitstests begonnen werden. Einige dieser Tests sind sehr einfach gehalten. So ist es etwa möglich, der App einen anderen Ort vorzugaukeln. Die Auswahl geschieht über Google Maps. Interessant ist das, um etwa eine Kontrolle von Apps zu ermöglichen, die nur in bestimmten Arealen, etwa dem Firmengelände, benutzt werden dürfen. Auch der Netzwerkverkehr kann untersucht werden. So sieht der Anwender, ob und wie die App auf externe Server zugreift und erhobene Daten abliefert und ob dies verschlüsselt geschieht. Zugriffe auf Systemkomponenten (Schlüsselbund, Dateien, Kontakte und Fotos) werden ebenfalls aufgenommen.

Mit Hilfe eines Ampelsystems werden kritische Zugriffe außerdem schnell erfassbar gemacht. Zudem kann der Anwender Hardware-IDs (MACs und UDID) fälschen, um zu sehen, wie die App darauf reagiert. Bekanntlich nutzen einige Apps, darunter auch das populäre Whatsapp, diese als feste Passwörter.

Potenzial für eine umfassende Sicherheitsüberprüfung des App-Katalogs

Die Snoop-It-App hat das Potenzial, die App-Welt unter iOS zu verbessern. Zwar führt Apple eine Kontrolle aller eingereichten Apps durch, diese ist aber nicht nur lückenhaft, sondern greift auch bei Sicherheitslücken nicht. Schließlich befindet sich Whatsapp als Negativbeispiel noch immer im App Store, obwohl die Anwendung mehrfach durch Sicherheitsprobleme aufgefallen ist. Derartiges Testen von Apps ist aufwendig, und dementsprechend werden nur wenige Apps überhaupt umfassend untersucht. Außerdem dürften zahlreiche Entwickler entdeckt werden, die allzu viele Daten sammeln.

Snoop-It beherrscht auch Verschleierungstaktiken. So kann die Anwendung auch Apps untersuchen, die das System nach verräterischen Hinweisen auf einen Jailbreak überprüfen und somit nicht starten würden. Snoop-It verbirgt einige dieser Hinweise, wie etwa Symlinks, Cydia oder manipulierte Dateirechte, die durch das Jailbreaken entstanden sind.

Die App Snoop-It soll noch vor Ende des Jahres erscheinen. Sie wird voraussichtlich über den Cydia-Store und Github verteilt. Der Quellcode wird laut Kurtz erst im nächsten Jahr bereitgestellt. Snoop-It setzt ein iOS-Gerät voraus und der Anwender muss in der Lage sein, einen Jailbreak durchzuführen. Ein paar Grundkenntnisse sind also notwendig. Eine Umsetzung auf Android ist derzeit nicht geplant.

SNOOP-IT FÜR IOS

Sicherheitschecks von iPhone-Apps für fast jeden möglich

Deepsec 2012 Die Snoop-It-App soll jedem eine Basisüberprüfung der Sicherheit von Apps ermöglichen. Das könnte dazu führen, dass viele iOS-Entwickler entdeckt werden, die auf fragwürdige Art und Weise Daten erheben.

Andreas Kurtz von den NESO Security Labs und der Universität Erlangen-Nürnberg arbeitet an einem einfach zu bedienenden Werkzeug, um iOS-Anwendungen auf ihre Sicherheit hin zu überprüfen. Die Snoop-It-App wird auf einem iPhone oder iPad installiert und dort über einen simplen Dialog konfiguriert. Kurtz demonstrierte die Anwendung, die sich noch in einem Vorversionsstatus befindet, auf der Deepsec in Wien. Dabei fiel auf, dass sie vergleichsweise einfach zu bedienen ist. Das Herumhacken auf der Kommandozeile ist nicht einmal notwendig. Stattdessen nutzt der Anwender einfach einen Browser und verbindet sich mit der Snoop-It-App, die gerade eine App untersucht.

1 / 5

Snoop-It-Demo

Snoop-It kann auch Anwendungen untersuchen, die bei einem Jailbreak nicht mehr starten. (Bild: Andreas Sebayang/Golem.de)

Datum: 29.11.2012, 15:08

Autor: Andreas Sebayang

Themen: Deepsec, App, Cydia, Passwort, Sicherheitslücke, iOS, Server, Security, Softwareentwicklung

Teilen: 0 27 30 12

Tools: Drucken

Über den Browser kann dann mit den Sicherheitstests begonnen werden. Einige dieser Tests sind sehr einfach gehalten. So ist es etwa möglich, der App einen anderen Ort vorzugaukeln. Die Auswahl geschieht über Google Maps. Interessant ist das, um etwa eine Kontrolle von Apps zu ermöglichen, die nur in bestimmten Arealen, etwa dem Firmengelände, benutzt werden dürfen. Auch der Netzwerkverkehr kann untersucht werden. So sieht der Anwender, ob und wie die App auf externe Server zugreift und erhobene Daten abliefert und ob dies verschlüsselt geschieht. Zugriffe auf Systemkomponenten (Schlüsselbund, Dateien, Kontakte und Fotos) werden ebenfalls aufgenommen.

Mit Hilfe eines Ampelsystems werden kritische Zugriffe außerdem schnell erfassbar gemacht. Zudem kann der Anwender Hardware-IDs (MACs und UDID) fälschen, um zu sehen, wie die App darauf reagiert. Bekanntlich nutzen einige Apps, darunter auch das populäre Whatsapp, diese als feste Passwörter.

Potenzial für eine umfassende Sicherheitsüberprüfung des App-Katalogs

Die Snoop-It-App hat das Potenzial, die App-Welt unter iOS zu verbessern. Zwar führt Apple eine Kontrolle aller eingereichten Apps durch, diese ist aber nicht nur lückenhaft, sondern greift auch bei Sicherheitslücken nicht. Schließlich befindet sich Whatsapp als Negativbeispiel noch immer im App Store, obwohl die Anwendung mehrfach durch Sicherheitsprobleme aufgefallen ist. Derartiges Testen von Apps ist aufwendig, und dementsprechend werden nur wenige Apps überhaupt umfassend untersucht. Außerdem dürften zahlreiche Entwickler entdeckt werden, die allzu viele Daten sammeln.

Snoop-It beherrscht auch Verschleierungstaktiken. So kann die Anwendung auch Apps untersuchen, die das System nach verräterischen Hinweisen auf einen Jailbreak überprüfen und somit nicht starten würden. Snoop-It verbirgt einige dieser Hinweise, wie etwa Symlinks, Cydia oder manipulierte Dateirechte, die durch das Jailbreaken entstanden sind.

Die App Snoop-It soll noch vor Ende des Jahres erscheinen. Sie wird voraussichtlich über den Cydia-Store und Github verteilt. Der Quellcode wird laut Kurtz erst im nächsten Jahr bereitgestellt. Snoop-It setzt ein iOS-Gerät voraus und der Anwender muss in der Lage sein, einen Jailbreak durchzuführen. Ein paar Grundkenntnisse sind also notwendig. Eine Umsetzung auf Android ist derzeit nicht geplant. ▪

https://adainitiative.org/2012/10/conferences-are-not-intended-to-create-bad-memories-only-good-ones-deep-sec-organizer-ren-pfeiffer/

“Conferences are not intended to create bad memories, only good ones”

DeepSec organizer René Pfeiffer

Interviews on October 1, 2012 by Valerie Aurora.

DeepSec logoDeepSec is the second hacker conference to adopt a public, enforceable anti-harassment policy in response to the Ada Initiative’s article about pervasive harassment of women at several hacker conferences (which called out DeepSec’s existing reputation as one of the most welcoming conferences for women).

We interviewed René Pfeiffer, one of the organizers of DeepSec about the conference, why they adopted a policy, and what they are looking forward to at future DeepSec conferences. It sounds like a great conference from all reports!

Tell us a little about DeepSec.

DeepSec’s full name is “In-Depth Security Conference”. The focus is on information security, and we like to present content which is not purely driven by marketing purposes. We are not a simple tradeshow with a “IT security” sticker slapped on the schedule. We try to be a platform where members of the academic community, governments, industry and (underground) hacking community meet in order to talk about security and exchange ideas. We believe in keeping an open mind and tearing down artificial barriers between groups that have a lot to talk about, but can’t in their normal environment. Most security related problems get worse if communication breaks down, so talking to each other is an important aspect of dealing with security breaches. This is what CERTs are preaching and what DeepSec tries to implement on conference-level.

The advantage to meet in person and talk and discuss certain issues from each perspective will give everyone involved a brighter understanding about needs and topics in the vast field of IT security, combined by interesting talks and new business opportunities.

The DeepSec event itself consists of two days of trainings followed by a two-day conference. We organise a dinner for all speakers and staff, and we have a party at the Metalab, a local hacker space, after the conference.

How did DeepSec get started?

In 2007 Paul Böhm created the DeepSec conference from scratch because he felt that a security-related conference where everyone can attend and talk openly was missing. He selected Vienna, Austria, as location which has been traditionally a bridge between different regions. Paul put a lot of effort into the first DeepSec and did a terrific job to kick-start it into existence.

What made you decide to adopt an anti-harassment policy?

There were two motivations. The first one were the experiences from other events participants wrote about. While we don't feel that conferences and events turn into places of harassment in general, we like to do our part to work against this. It really doesn't matter if there was a case already or not. The second motivation stems from the place DeepSec wants to be. We have a very international audience with roots in four different continents. If we want to create an atmosphere where everyone feels relaxed and is treated with respect, then we have to actively maintain this environment. Trust, respect and safe places do not automatically exist, they have to be created; you need people who care and who make sure an event stays hospitable.

Fortunately our staff cares, so our anti-harassment policy is really a statement of what we have been doing and trying to create since the first conference anyway.

What would you like to see at the next DeepSec?

We would like to see more people holding presentations and workshops who are not sure if their skills are "in-depth" enough, or who are not sure if they can handle speaking on stage. We actively support students with bright ideas with our under 21 category, and we will maintain a mixture of seasoned security experts and those who like a chance to become one. Everyone needs a start. Fresh perspectives never hurt, and we will actively support you if you let us know about the work you have done or are doing.

And for all the companies that are listening, please do not always think in leads when dealing with IT security. Be part of the community instead and show this proudly. Companies can have open minds, too.

Anything else you'd like to say?

We are well aware that small conferences have a lot of advantages compared to big events when it comes to publishing and enforcing an anti-harassment policy or protecting all attendees. If you are part of a team organising one of these big events, please consider to signal everyone thinking about attending that you want everyone to enjoy the talks, to have fun and not to be harassed for any reason. While you cannot control every single

situation and second of your event, you can clearly state what you expect from everyone being there, and you can instruct your staff to do the same. It's a simple step. Conferences are not intended to create bad memories, only good ones.

The DeepSec and BruCON anti-harassment policies would not exist without the Ada Initiative's work. We are a non-profit funded primarily by donations from people like you. If you believe more women should attend hacker conferences, please become a supporting donor today.

Ada Initiative

Supporting women in open technology and culture

“Conferences are not intended to create bad memories, only good ones” DeepSec organizer René Pfeiffer

DeepSec is the second hacker conference to adopt a public, enforceable anti-harassment policy in response to the Ada Initiative’s article about pervasive harassment of women at several hacker conferences (which called out DeepSec’s existing reputation as one of the most welcoming conferences for women).

We interviewed René Pfeiffer, one of the organizers of DeepSec about the conference, why they adopted a policy, and what they are looking forward to at future DeepSec conferences. It sounds like a great conference from all reports!

Tell us a little about DeepSec.

DeepSec’s full name is “In-Depth Security Conference”. The focus is on information security, and we like to present content which is not purely driven by marketing purposes. **We are not a simple tradeshow with a “IT security” sticker slapped on the schedule.** We try to be a platform where members of the academic community, governments, industry and (underground) hacking community meet in order to talk about security and exchange ideas. We believe in keeping an open mind and tearing down artificial barriers between groups that have a lot to talk about, but can’t in their normal environment. Most security related problems get worse if communication breaks down, so talking to each other is an important aspect of dealing with security breaches. This is what CERTs are preaching and what DeepSec tries to implement on conference-level.

The advantage to meet in person and talk and discuss certain issues from each perspective will give everyone involved a brighter understanding about needs and topics in the vast field of IT security, combined by interesting talks and new business opportunities.

The DeepSec event itself consists of two days of trainings followed by a two-day conference. We organise a dinner for all speakers and staff, and we have a party at the Metalab, a local hacker space, after the conference.

How did DeepSec get started?

In 2007 Paul Böhm created the DeepSec conference from scratch because he felt that a security-related conference where everyone can attend and talk openly was missing. He selected Vienna, Austria, as location which has been traditionally a bridge between different regions. Paul put a lot of effort into the first DeepSec and did a terrific job to kick-start it into existence.

What made you decide to adopt an anti-harassment policy?

There were two motivations. The first one were the experiences from other events participants wrote about. While we don't feel that conferences and events turn into places of harassment in general, we like to do our part to work against this. It really doesn't matter if there was a case already or not. The second motivation stems from the place DeepSec wants to be. We have a very international audience with roots in four different continents. If we want to create an atmosphere where everyone feels relaxed and is treated with respect, then we have to actively maintain this environment. **Trust, respect and safe places do not automatically exist, they have to be created**; you need people who care and who make sure an event stays hospitable.

Fortunately our staff cares, so our anti-harassment policy is really a statement of what we have been doing and trying to create since the first conference anyway.

What would you like to see at the next DeepSec?

We would like to see more people holding presentations and workshops who are not sure if their skills are "in-depth" enough, or who are not sure if they can handle speaking on stage. We actively support students with bright ideas with our under 21 category, and we will maintain a mixture of seasoned security experts and those who like a chance to become one. Everyone needs a start. Fresh perspectives never hurt, and we will actively support you if you let us know about the work you have done or are doing.

And for all the companies that are listening, please do not always think in leads when dealing with IT security. Be part of the community instead and show this proudly. Companies can have open minds, too.

Anything else you'd like to say?

We are well aware that small conferences have a lot of advantages compared to big events when it comes to publishing and enforcing an anti-harassment policy or protecting all attendees. If you are part of a team organising one of these big events, please consider to signal everyone thinking about attending that you want everyone to enjoy the talks, to have fun and not to be harassed for any reason. While you cannot control every single situation and second of your event, you can clearly state what you expect from everyone being there, and

you can instruct your staff to do the same. It's a simple step. **Conferences are not intended to create bad memories, only good ones.**

The DeepSec and BruCON anti-harassment policies would not exist without the Ada Initiative's work. We are a non-profit funded primarily by donations from people like you. If you believe more women should attend hacker conferences, please become a supporting donor today.

This entry was posted in Ada Initiative resources in use, Anti-harassment policy, Interviews on October 1, 2012 [https://adainitiative.org/2012/10/conferences-are-not-intended-to-create-bad-memories-only-good-ones-deepsec-organizer-ren-pfeiffer/] by Valerie Aurora.

http://www.golem.de/news/paul-mockapetris-mit-dns-laesst-sich-noch-viel-machen-1208-94109.html

PAUL MOCKAPETRIS

“Mit DNS lässt sich noch viel machen”

27.8.2012, 15:43

Autor:Jörg Thoma

Das DNS-Protokoll ist noch nicht veraltet, könnte aber künftig durch neue Technik ersetzt werden, sagt dessen Erfinder Paul Mockapetris in einem Interview mit Golem.de. Und DNS sei der ideale Ort für Filter.

"Wer möchte schon auf einer Webseite mit Malware oder kinderpornografischem Material landen", fragt Paul Mockapetris zurück, als wir wissen wollen, ob er Filter per DNS immer noch befürworte. Und DNS habe noch viel Potenzial. Er könne sich beispielsweise dort eine integrierte Suche vorstellen, sagt er im Interview mit Golem.de.

Video: Paul Mockapetris über DNSSec, DNS Filtering und IPv6 (4:59)

Mockapetris geriet 2009 in die Kritik, als bekanntwurde, dass Nominum die Technik zur Filterung per DNS entwickeln würde, die in Deutschland geplant war, aber nach massiven Protesten wieder verworfen wurde.

Ganz nachvollziehen kann Mockapetris die Aufregung nicht: Die ISP sollten zwei Versionen von DNS anbieten, eine gefilterte, die gefährliche oder kriminelle Webseiten für diejenigen ausblendet, die gefahrlos surfen wollen, und eine für diejenigen, die aus Recherchegründen auch zweifelhafte Seiten ansteuern wollen.

DNSSec ist nicht genug

DNSSec eigne sich nur bedingt, die Sicherheitsprobleme im Internet zu lösen, denn es stelle nur sicher, dass Anfragen nicht gefälscht seien. Es gebe aber genügend Webseiten, die legitimiert von Kriminellen betrieben würden, sagt er.

Sir Tim Berners-Lee ist da anderer Meinung. DNS sei fast die einzige zentrale Instanz in einem sonst dezentralen Internet, sagte er in seiner Keynote-Ansprache auf der Campus Party Europe 2012. Berners-Lee setzte sich in seiner Rede für ein vollkommen freies, dezentrales und unzensiertes Internet ein. Er überlege, HTTP so zu erweitern, dass es bei Bedarf als Peer-to-Peer-Protokoll genutzt werden kann, auch um Zensur zu vermeiden.

DNS lässt sich noch erweitern

DNS habe aber noch sehr viel mehr Potenzial, als nur als Reputationsfilter eingesetzt zu werden, sagte Mockapetris. Es könne beispielsweise so erweitert werden, dass es als Suche verwendet werden könne.

In Kombination mit IPv6 stellt DNS aber kein Problem dar. DNS wurde so konzipiert, dass es bis zu 64.000 Datentypen nutzen kann, gegenwärtig werden aber nur etwa 60 genutzt. Es gebe andere Probleme mit dem neuen Internetprotokoll, etwa die gleichzeitige Nutzung von IPv4 und IPv6. Ähnlich äußerte sich auch der Netzwerkexperte Fernando Gont auf der Sicherheitskonferenz Deepsec im November 2011.

Er selbst wolle sich zukünftig der Weiterentwicklung von DNS im Zusammenhang mit Inhalten widmen, sagte Mockapetris. "Vielleicht ergibt sich daraus die nächste Generation von DNS."

PAUL MOCKAPETRIS

"Mit DNS lässt sich noch viel machen"

Das DNS-Protokoll ist noch nicht veraltet, könnte aber künftig durch neue Technik ersetzt werden, sagt dessen Erfinder Paul Mockapetris in einem Interview mit Golem.de. Und DNS sei der ideale Ort für Filter.

Paul Mockapetris sprach in einem Interview mit Golem.de über die Zukunft von DNS. (Bild: Daniel Pook/Golem.de)

Datum: 27.8.2012, 15:43
Autor: Jörg Thoma
Themen: DNS, Campus Party, IPv6, Malware, Server-Applikationen, Tim Berners-Lee, Zensur, Applikationen

"Wer möchte schon auf einer Webseite mit Malware oder kinderpornografischem Material landen", fragt Paul Mockapetris zurück, als wir wissen wollen, ob er Filter per DNS immer noch befürworte. Und DNS habe noch viel Potenzial. Er könne sich beispielsweise dort eine integrierte Suche vorstellen, sagt er im Interview mit Golem.de.

Video: Paul Mockapetris über DNSSec, DNS Filtering und IPv6 (4:59)

Mockapetris geriet 2009 in die Kritik, als bekanntwurde, dass Nominum die Technik zur Filterung per DNS entwickeln würde, die in Deutschland geplant war, aber nach massiven Protesten wieder verworfen wurde.

Ganz nachvollziehen kann Mockapetris die Aufregung nicht: Die ISP sollten zwei Versionen von DNS anbieten, eine gefilterte, die gefährliche oder kriminelle Webseiten für diejenigen ausblendet, die gefahrlos surfen wollen, und eine für diejenigen, die aus Recherchegründen auch zweifelhafte Seiten ansteuern wollen.

DNSSec ist nicht genug

DNSSec eigne sich nur bedingt, die Sicherheitsprobleme im Internet zu lösen, denn es stelle nur sicher, dass Anfragen nicht gefälscht seien. Es gebe aber genügend Webseiten, die legitimiert von Kriminellen betrieben würden, sagt er.

Sir Tim Berners-Lee ist da anderer Meinung. DNS sei fast die einzige zentrale Instanz in einem sonst dezentralen Internet, sagte er in seiner Keynote-Ansprache auf der Campus Party Europe 2012. Berners-Lee setzte sich in seiner Rede für ein vollkommen freies, dezentrales und unzensiertes Internet ein. Er überlege, HTTP so zu erweitern, dass es bei Bedarf als Peer-to-Peer-Protokoll genutzt werden kann, auch um Zensur zu vermeiden.

DNS lässt sich noch erweitern

DNS habe aber noch sehr viel mehr Potenzial, als nur als Reputationsfilter eingesetzt zu werden, sagte Mockapetris. Es könne beispielsweise so erweitert werden, dass es als Suche verwendet werden könne.

In Kombination mit IPv6 stellt DNS aber kein Problem dar. DNS wurde so konzipiert, dass es bis zu 64.000 Datentypen nutzen kann, gegenwärtig werden aber nur etwa 60 genutzt. Es gebe andere Probleme mit dem neuen Internetprotokoll, etwa die gleichzeitige Nutzung von IPv4 und IPv6. Ähnlich äußerte sich auch der Netzwerkexperte Fernando Gont auf der Sicherheitskonferenz Deepsec im November 2011.

Er selbst wolle sich zukünftig der Weiterentwicklung von DNS im Zusammenhang mit Inhalten widmen, sagte Mockapetris. *"Vielleicht ergibt sich daraus die nächste Generation von DNS."* ▪

Folgen Sie uns

Videos

Sapphire Radeon R9 Fury Tri-X (Hersteller-Trailer)

Verwandte Artikel

Droht Vista das DNS-System zu überlasten?

private blogs, personal experiences

http://ananalyticalapproach.blogspot.co.at/2014/11/thoughts-on-irisscon-and-deepsec.html

Thoughts on #IRISSCON and #DeepSec

MONDAY, NOVEMBER 24, 2014

Posted by Josh Goldfarb

at 3:51 AM

Last week, I was fortunate to have the opportunity to speak at both #IRISSCON and #DeepSec in Dublin and Vienna respectively. Both conferences were extremely well run, with a great crowd and interesting dialogue to go along with them. My conversations and observations at the conferences indicate to me that the paradigm shift from a focus solely on prevention to a mix between prevention and detection/response is indeed well under-way. Each conference I speak at, I find more and more people who are interested in better understanding the subject of incident response.

This is a good thing in my opinion. It shows that we as an industry are trending in the correct direction. People ask me many questions, but one of the most common is: "Where can I go to get good educational materials on incident response?" This is a tough question to answer because, while there are many, many good materials on the subject, there are unfortunately, quite a few not so good materials out there. Generally, I recommend finding a few trusted sources (I would be flattered if you would consider this blog one of them) as a beginning point. As time allows, sources can be expanded, perhaps with the help of a seasoned incident response veteran.

Those of us who have experience in incident response should continue to share our knowledge with those that are new to the field. Together, we can help organizations improve the state of their security operations function and their overall security posture. I am glad that the community is becoming more interested in what has for a long time been a very niche field. Let's continue to keep the knowledge and exchange of ideas flowing, while hopefully minimizing the influence of #FUD and bad ideas.

An Analytical Approach

MONDAY, NOVEMBER 24, 2014

Thoughts on #IRISSCON and #DeepSec

Last week, I was fortunate to have the opportunity to speak at both #IRISSCON and #DeepSec in Dublin and Vienna respectively. Both conferences were extremely well run, with a great crowd and interesting dialogue to go along with them. My conversations and observations at the conferences indicate to me that the paradigm shift from a focus solely on prevention to a mix between prevention and detection/response is indeed well underway. Each conference I speak at, I find more and more people who are interested in better understanding the subject of incident response.

This is a good thing in my opinion. It shows that we as an industry are trending in the correct direction. People ask me many questions, but one of the most common is: "Where can I go to get good educational materials on incident response?" This is a tough question to answer because, while there are many, many good materials on the subject, there are unfortunately, quite a few not so good materials out there. Generally, I recommend finding a few trusted sources (I would be flattered if you would consider this blog one of them) as a beginning point. As time allows, sources can be expanded, perhaps with the help of a seasoned incident response veteran.

Those of us who have experience in incident response should continue to share our knowledge with those that are new to the field. Together, we can help organizations improve the state of their security operations function and their overall security posture. I am glad that the community is becoming more interested in what has for a long time been a very niche field. Let's continue to keep the knowledge and exchange of ideas flowing, while hopefully minimizing the influence of #FUD and bad ideas.

Posted by Josh Goldfarb at 3:51 AM

No comments:

Post a Comment

https://www.securityninja.co.uk/hacking/deepsec-2013/

DeepSec 2013

DECEMBER 17, 2013 | WRITTEN BY SECURITY NINJA | APPLICATION SECURITY, HACKING, NINJA NEWS AND UPDATES | LEAVE A COMMENT

Hi everyone,

DeepSec is a security conference lauded by its fans as having the most interesting talks and inviting atmosphere. In its seventh year, it runs in Vienna, Austria, chosen for its central EU location, and not just because it's a beautiful city, with Christmas markets on at the same time as the conference – another good reason to visit. This was my first year going to DeepSec, thanks to the organizers offering a trip as the BSides London Rookie Track prize last April.

NSA Device

The morning after checking into the hotel and exploring Vienna on Wednesday night, the first thing I got my hands on was the magnetic badges. It was nice that I didn't have to put holes in my clothes to get in and made a nice difference to lanyards, and there was an added risk factor of wiping the hotels room cards magnetic strip (which happened to at least one of the speakers I chatted to).

The talks were all very interesting, and I was torn at times between which track to choose. I don't have the space to mention each talk I found impressive, but the best takeaway was an explanation of Session Puzzling by Shay Chen of Hacktics, who demonstrated how to use an applications functionality to populate server-side session variables in a way to bypass authorization checks, as one example. There were some great live demos, especially the root exploit on Cray supercomputers demonstrated by two researchers from MWR Infosecurity – exploited by hot patching a return statement using gdb.

Unlike other conferences where there was time to have quick breakout sessions in the hallways, I found myself hopping from room to room unable to take a break because of the quality of the talks.

The conference was rounded off with a meal at the aptly named "Hakka Cun":before rushing to MetaLab for the after party. The main classroom had been set up with decks, a couple of people mixing while "cyber cyber cyber" – the theme of DeepSec this year – scrolled across the projector screens over visualisations that would have made WinAmp envious.

DeepSec is a very welcoming conference, with great technical talks, located in a beautiful city. It's definitely a conference I want to revisit, and one I'd recommend to anyone who's involved in building or breaking security.

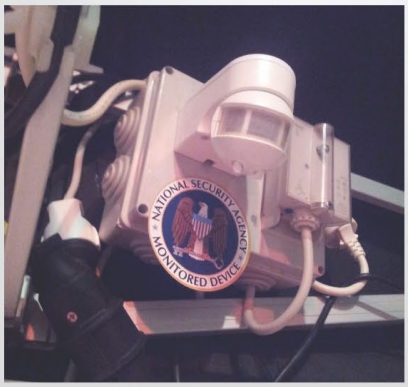
Diarmaid

DeepSec 2013

DECEMBER 17, 2013 | WRITTEN BY SECURITY NINJA | APPLICATION SECURITY, HACKING, NINJA NEWS AND UPDATES | LEAVE A COMMENT

Hi everyone,

DeepSec is a security conference lauded by its fans as having the most interesting talks and inviting atmosphere. In its seventh year, it runs in Vienna, Austria, chosen for its central EU location, and not just because it's a beautiful city, with Christmas markets on at the same time as the conference – another good reason to visit. This was my first year going to DeepSec, thanks to the organizers offering a trip as the BSides London Rookie Track prize last April.



The morning after checking into the hotel and exploring Vienna on Wednesday night, the first thing I got my hands on was the magnetic badges. It was nice that I didn't have to put holes in my clothes to get in and made a nice difference to lanyards, and there was an added risk factor of wiping the hotels room cards magnetic strip (which happened to at least one of the speakers I chatted to).

The talks were all very interesting, and I was torn at times between which track to choose. I don't have the space to mention each talk I found impressive, but the best takeaway was an explanation of Session Puzzling by Shay Chen of Hacktics, who demonstrated how to use an applications functionality to populate server-side session variables in a way to bypass authorization checks, as one example. There were some great live demos, especially the root exploit on Cray supercomputers demonstrated by two researchers from MWR Infosecurity – exploited by hot patching a return statement using gdb.

Unlike other conferences where there was time to have quick breakout sessions in the hallways, I found myself hopping from room to room unable to take a break because of the quality of the talks.

The conference was rounded off with a meal at the aptly named "Hakka Cun":

before rushing to MetaLab for the after party. The main classroom had been set up with decks, a couple of people mixing while "cyber cyber cyber" – the theme of DeepSec this year – scrolled across the projector screens over visualisations that would have made WinAmp envious.

DeepSec is a very welcoming conference, with great technical talks, located in a beautiful city. It's definitely a conference I want to revisit, and one I'd recommend to anyone who's involved in building or breaking security.

Diarmaid

This entry was posted on December 17, 2013 at 1:30 pm and is filed under Application Security, Hacking, Ninja News and Updates . You can follow any responses to this entry through the RSS 2.0 feed. You can leave a response, or trackback from your own site.

Leave a comment

Name *

Mail (will not be published) *

Website

Your Comment*

Submit

VIDEOS & SLIDESHARES
Look at our latest security Videos & SlideShares

EVENTS & SEMINARS
Upcoming Security Events & Seminars

PODCASTS & DOWNLOADS
Check out our Podcasts & White Papers

https://www.insinuator.net/2013/12/deepsec-2013/#more-2678

DeepSec 2013

0 Comments | Posted by Niklaus Schiess

09.12.2013

Last week Florian and I participated at this year's DeepSec in Vienna. We had a really good time, thanks again to the DeepSec staff for a nice conference. Although it might be a bit late, I want to share some impressions about various talks I enjoyed.

spin: Static Instrumentation For Binary Reverse-Engineering

This talk primarily covered a technique called binary instrumentation, which is used e.g. for performance evaluation, CPU emulation, tracing and profiling but also for malware- and threat-analysis. David Guillen Fandos proposed the application of this technique in the field of reverse engineering. Binary instrumentation is a technique which allows to modify and rewrite binaries during their execution by injecting instructions into the original code (pretty much like virtual machines do too). Therefore one could easily wrap instructions with logging/tracing functions, to observe the execution status before and after easy instruction step (and/or dump the output into a file). For the purpose of reversing, one could also create complex conditional breakpoints (retaining status across executions), which makes it possible to characterize functions.

David developed a tool called "spin" (a somehow static version of Intel's Pin tool) which is able to characterize and identify security-critical functions by applying conditions. Additionally, it can automatically hook functions by injecting DLL's during runtime. He demonstrated this in a little demo by hooking Winzip's serial verify function so it would accept any serial. Spin is still in early development but it's aid to the automation of reverse engineering seems really promising. Hopefully David will add support for API-Hooking, which isn't yet supported due to the lack of 2Byte-Opcode hooking.

Trusted Friend Attack: Guardian Angels Strike

Ashar Javed from the Ruhr University Bochum presented how an attacker can exploit social networks in order to gain access to user accounts. Especially functions where trusted third parties are involved, like Facebook's password recovery, are mostly vulnerable to those attacks. Ashar demonstrated that it's not the implementation of these functions that is vulnerable, but the logic behind. As those trusted third parties are just accounts that are in a users friend list, becoming one of them is a rather easy task, because most people confirm arbitrary friend-

ship requests anyway. The slides are available here.

The Boomerang Effect – Using Session Puzzling To Attack Apps From The Backend

Shay Chen presented a pretty interesting technique for web application hacking called session puzzling. Instead of directly sending payloads to a web application's front end, this technique aims at attacking the application from the back end by polluting session related memory in order to prepare payloads across multiple requests. Shay also demonstrated a few ways to attack an application via session puzzling (e.g. authentication bypass) at a self developed training platform called PuzzleMall. For further information, read the blog post as well as Shay's whitepaper.

Mutually Assured Pwange

This was the first anti cyber war talk I've every heard and I really liked it. Karin Kosina did a great job explaining why this so called "cyberwar" cannot be compared with the cold war. Those of you who are really interested in this topic should take a look at her master's thesis, which covers this topic as well. The slides are also available.

Applied Crypto Hardening

Aaron Kaplan and three others presented a project called Applied Crypto Hardening, which was initiated by CERT.at and Adi Kriegisch (VRVis). It aims at providing a paper for (mainly) system administrators with copy&paste-ready configuration examples for common applications like webservers (Apache, Nginx, …), mail transfer agents (like Postfix and Sendmail), SSHD and many others. So far those configuration examples only cover security related recommendations, mostly about choosing strong cipher suites for various tasks. It would be nice to see some performance related information for those configurations in the future (like suggested by an attendee after the talk) to further improve the quality of this paper. In my opinion this is a really important project but there is still a lot of work to do. I'm a little bit disappointed that there won't be a SSTP section. Instead they prefer to stick to PPTP. Furthermore I seriously doubt that a paper in PDF format is the right choice for content that's supposed to be copy&paste'd.

Hopefully the recordings won't take that long, so we can enjoy the other talks we missed during the conference.

Regards,

Niklaus

Insinuator

Some outright rants from a bunch of infosec practitioners.

Search this Blog

Search... Go

Tag Cloud

3G 4G Android attacks Cisco cloud conferences DHCPv6 ERNW Extension Headers Fragmentation fuzzing gsm gtp hacking Hardening HITB iOS IPv6 IPv6 Security Summit Loki LTE MitM MLD mobile newsletter pcap pentest python risk SAP slides TelcoSecDay tool TR14 TROOPERS TROOPERS12 TROOPERS13 TROOPERS15 video Virtualization vmdk vmware VoIP web application

Stay up-to-date

Twitter
Posts
Comments

NEW DATE: TROOPERS16 Conference March 14-18, 2016

Recent Comments

- Florian Grunow on RedStar OS Watermarking
- Jean-Christophe Manciot on Evasion of Cisco ACLs by (Ab)Using IPv6 – Part 2
- Isaias on Is IPv6 more Secure than IPv4? Or Less?
- witness digital on How to Get a BaseStation
- James Small on OS IPv6 Behavior in Conflicting Environments

Dec/13

9

DeepSec 2013

0 Comments | Posted by *Niklaus Schiess*

Last week Florian and I participated at this year's DeepSec in Vienna. We had a really good time, thanks again to the DeepSec staff for a nice conference. Although it might be a bit late, I want to share some impressions about various talks I enjoyed.

spin: Static Instrumentation For Binary Reverse-Engineering

This talk primarily covered a technique called *binary instrumentation*, which is used e.g. for performance evaluation, CPU emulation, tracing and profiling but also for malware- and threat-analysis. David Guillen Fandos proposed the application of this technique in the field of reverse engineering. Binary instrumentation is a technique which allows to modify and rewrite binaries during their execution by injecting instructions into the original code (pretty much like virtual machines do too). Therefore one could easily wrap instructions with logging/tracing functions, to observe the execution status before and after easy instruction step (and/or dump the output into a file). For the purpose of reversing, one could also create complex conditional breakpoints (retaining status across executions), which makes it possible to characterize functions.

David developed a tool called "spin" (a somehow static version of Intel's Pin tool) which is able to characterize and identify security-critical functions by applying conditions. Additionally, it can automatically hook functions by injecting DLL's during runtime. He demonstrated this in a little demo by hooking Winzip's serial verify function so it would accept any serial. Spin is still in early development but it's aid to the automation of reverse engineering seems really promising. Hopefully David will add support for API-Hooking, which isn't yet supported due to the lack of 2Byte-Opcode hooking.

Trusted Friend Attack: Guardian Angels Strike

Ashar Javed from the Ruhr University Bochum presented how an attacker can exploit social networks in order to gain access to user accounts. Especially functions where trusted third parties are involved, like Facebook's password recovery, are mostly vulnerable to those attacks. Ashar demonstrated that it's not the implementation of these functions that is vulnerable, but the logic behind. As those trusted

third parties are just accounts that are in a users friend list, becoming one of them is a rather easy task, because most people confirm arbitrary friendship requests anyway. The slides are available here.

The Boomerang Effect – Using Session Puzzling To Attack Apps From The Backend

Shay Chen presented a pretty interesting technique for web application hacking called session puzzling. Instead of directly sending payloads to a web application's front end, this technique aims at attacking the application from the back end by polluting session related memory in order to prepare payloads across multiple requests. Shay also demonstrated a few ways to attack an application via session puzzling (e.g. authentication bypass) at a self developed training platform called PuzzleMall. For further information, read the blog post as well as Shay's whitepaper.

Mutually Assured Pwange

This was the first anti cyber war talk I've every heard and I really liked it. Karin Kosina did a great job explaining why this so called "cyberwar" cannot be compared with the cold war. Those of you who are really interested in this topic should take a look at her master's thesis, which covers this topic as well. The slides are also available.

Applied Crypto Hardening

Aaron Kaplan and three others presented a project called Applied Crypto Hardening, which was initiated by CERT.at and Adi Kriegisch (VRVis). It aims at providing a paper for (mainly) system administrators with copy&paste-ready configuration examples for common applications like webservers (Apache, Nginx, …), mail transfer agents (like Postfix and Sendmail), SSHD and many others. So far those configuration examples only cover security related recommendations, mostly about choosing strong cipher suites for various tasks. It would be nice to see some performance related information for those configurations in the future (like suggested by an attendee after the talk) to further improve the quality of this paper. In my opinion this is a really important project but there is still a lot of work to do. I'm a little bit disappointed that there won't be a SSTP section. Instead they prefer to stick to PPTP. Furthermore I seriously doubt that a paper in PDF format is the right choice for content that's supposed to be copy&paste'd.

Hopefully the recordings won't take that long, so we can enjoy the other talks we missed during the conference.

Regards,
Niklaus

No tags

No comments yet.

Leave a comment!

Name* Mail* (will not be published) Website
Spam protection*: Sum of 3 + 7 ? Comment

http://www.alba13.com/2013/10/deepsec-effective-idsips-auditing-and.html

DeepSEC - Effective IDS/IPS Auditing And Testing With Finux – Arron 'f1nux' Finnon

Thursday, 24 October 2013

There comes a time in your life when you have to walk the walk! As a public speaker, I've done my share of talking the talk, and those that know me, know I have recently been conducting a lot of small training courses and workshops on effective NIDS/NIPS auditing and testing.

Truth be told, I've been doing this for two reasons. The first reason, is no matter how much I talk about this issue, nothing is going to help people more than sitting down and working with them. The second reason I've been on the road so much is getting myself in shape for DeepSEC training. Now, if you have to ask why getting myself fighting fit for DeepSEC is so important to me then you've either not been to the conference, or frankly you have no idea what on earth you're talking about.

I've always had a great love and respect for the crew of DeepSEC, and I have never hid that. I've been to a lot of conferences and frankly a lot of conferences like to boast about being the best in Europe, DeepSEC doesn't need to boast! I believe DeepSEC to be the best full-stop! The lack of egotistical babel; the beautiful city of Vienna; the amazing speakers and trainers; the warm and friendly family feeling you get there; and most importantly the crew that manages it, shows that bigging yourself up doesn't count for anything, doing it does!

So that being said, time to big up our training offering. So yes, of course ours is the best training offering ever! Of course you should hurry right now and purchase a ticket before they sell-out, in fact buy two or three, I mean every geek has at least one friend! Yeah, it will be biblical and we'll shove so much information into your brains that you'll be crying pcap files till new years day, blar, blar, blar. Seriously though, we have put together something special. Hand on my heart as I swear to God himself, we have taken everything we've learned about NIDS/NIPS testing and put together a course that will actually help. No silver bullets to be found here (we're based in Scotland, we sold the silver a very long time ago!), just what's needed to actually make a test of a NIDS/NIPS worthwhile. We cover everything in the Open Source Network Intrusion Framework (OSNIF) Top5, so NIDS/NIPS Evasion Techniques, False-Positive Issues, Protocol Ambiguities, Detection Rates, and Misconfiguration and Invisible Traffic Issues. We cover why sacrificial host testing with NIDS/NIPS has some serious flaws, and how to produce clean sample attack traffic to test attacks. However, we do have something very special indeed

planned for the second day of training.

Now this part is where I get to be mean, I'm not actually going to tell you the actual details of the second day. All I'm going to say is we're going to take an issue that faces enterprise networks everyday, and we're going to analyse and build an effective defence against it. Now the details are interesting, and without doubt everyone there will learn a lot. However, more importantly we'll show attendees how easy it is to take a threat, no matter how big the hype is, and actually defend against it.

This training course will be of benefit to testers as well as defenders. Whilst I'm here, I'm going to put this out there too. This is the début of our OSNIF Top5 training in Europe, it hasn't been done here, it has never been done, EVER, with a two day practical defence module. We will be dropping a new open source project on the second day too. So buy your tickets now for DeepSEC, come do the training, and come see me and Gavin's talk whilst you're there too.

Visit DeepSEC training pages for more information. http://deepsec.net/speaker.html#WSLOT96

alba 13 research labs

Thursday, 24 October 2013

DeepSEC - Effective IDS/IPS Auditing And Testing With Finux

DeepSEC - Effective IDS/IPS Auditing And Testing With Finux - Arron 'f1nux' Finnon

There comes a time in your life when you have to walk the walk! As a public speaker, I've done my share of talking the talk, and those that know me, know I have recently been conducting a lot of small training courses and workshops on effective NIDS/NIPS auditing and testing.

Truth be told, I've been doing this for two reasons. The first reason, is no matter how much I talk about this issue, nothing is going to help people more than sitting down and working with them. The second reason I've been on the road so much is getting myself in shape for DeepSEC training. Now, if you have to ask why getting myself fighting fit for DeepSEC is so important to me then you've either not been to the conference, or frankly you have no idea what on earth you're talking about.

I've always had a great love and respect for the crew of DeepSEC, and I have never hid that. I've been to a lot of conferences and frankly a lot of conferences like to boast about being the best in Europe, DeepSEC doesn't need to boast! I believe DeepSEC to be the best full-stop! The lack of egotistical babel; the beautiful city of Vienna; the amazing speakers and trainers; the warm and friendly family feeling you get there; and most importantly the crew that manages it, shows that bigging yourself up doesn't count for anything, doing it does!

So that being said, time to big up our training offering. So yes, of course ours is the best training offering ever! Of course you should hurry right now and purchase a ticket before they sell-out, in fact buy two or three, I mean every geek has at least one friend! Yeah, it will be biblical and we'll shove so much information into your brains that you'll be crying pcap files till new years day, blar, blar, blar. Seriously though, we have put together something special. Hand on my heart as I swear to God himself, we have taken everything we've learned about NIDS/NIPS testing and put together a course that will actually help. No silver bullets to be found here (we're based in Scotland, we sold the silver a very long time ago!), just what's needed to actually make a test of a NIDS/NIPS worthwhile. We cover everything in the Open Source Network Intrusion Framework (OSNIF) Top5, so NIDS/NIPS Evasion Techniques, False-Positive Issues, Protocol Ambiguities, Detection Rates, and Misconfiguration and Invisible Traffic Issues. We cover why sacrificial host testing with NIDS/NIPS has some serious flaws, and how to produce clean sample attack traffic to test attacks. However, we do have something very special indeed planned for the second day of training.

Now this part is where I get to be mean, I'm not actually going to tell you the actual details of the second day. All I'm going to say is we're going to take an issue that faces enterprise networks everyday, and we're going to analyse and build an effective defence against it. Now the details are interesting, and without doubt everyone there will learn a lot. However, more importantly we'll show attendees how easy it is to take a threat, no matter how big the hype is, and actually defend against it.

This training course will be of benefit to testers as well as defenders. Whilst I'm here, I'm going to put this out there too. This is the début of our OSNIF Top5 training in Europe, it hasn't been done here, it has never been done, EVER, with a two day practical defence module. We will be dropping a new open source project on the second day too. So buy your tickets now for DeepSEC, come do the training, and come see me and Gavin's talk whilst you're there too.

Visit DeepSEC training pages for more information.
http://deepsec.net/speaker.html#WSLOT96

Posted by Arron 'finux' Finnon at 09:18

Blog Archive

- ► 2014 (6)
- ▼ 2013 (6)
  - ▼ October (4)
    - DeepSEC - Effective IDS/IPS Auditing And Testing W...
    - Alba13 going deep with janet
    - Historical Tour Of IDS Evasion
    - The Economics of False Positives
  - ► July (2)

There was an error in this gadget

Contact Form

Name

Email *

Message *

Send

press release

PRESS RELEASE 01

DEEPSEC 2015

25.06.2015

DEEPSEC

Mission Statement

INTERNATIONAL, TRANS & INTERDISCIPLINARY

We believe that security problems need to be addressed by experts with interdisciplinary skills. We want to encourage individuals, organizations and countries to meet and exchange, to improve overall security and trust.

NEUTRAL GROUND

Our conference is an annual event where we can freely talk about ideas and points of view. It is the best place to get together informally, get new ideas, discuss a project, develop new contacts and meet new friends.

FOCUSED ON NOVELTY, QUALITY & IMPACT

We focus only on novelty, quality and relevance when selecting talks & workshops for our conference. We prefer to invite a newcomer to the stage if the content is more promising than the “safe choice” of well established truths.

HERE TO SCOUT & SUPPORT

We actively scout and contact women who do research and projects in the field of information security. And we launched our special U21 initiative to support young researchers and enable them to present their works and results in an appropriate manner.

USER FRIENDLY

Our web site states that DeepSec is a non-product, non-vendor-biased conference. DeepSec is all about facts not ads. We are looking for honest talks about security: If something breaks, tell us about it. If you can repair it, tell us about it. If you’ve discovered something, tell us about it. That’s our goal.

...about

René Pfeiffer

...is involved with cryptography and information security for over 20 years. He is one of the organizers of DeepSec, Vienna's very own IT-Security Conference, known for bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community.

...a little Q+A

Mr. Pfeiffer please tell us about your conference.

The DeepSec In-Depth Security Conference is an annual European two-day in-depth conference on computer, network, and application security. Our goal is to bring together the leading security experts from all over the world.

How did it all start?

DeepSec was founded in 2007. The vision was to create a IT security conference right in the heart of Europe and use it as a neutralground where professionals from academics, government, industry, and the underground hacking community can meet and exchange ideas.

What's special about DeepSec?

DeepSec is small compared to other events having thousands of participants. This is a dedicated advantage, because you can actually meet and talk to everyone. Furthermore we try to present a mix of talks connecting different aspects of information security. It's not always about technology. There's psychology, legal frameworks, human behaviour, and much more also at play.

Is there a matter particularly close to your heart?

We want to break down the barriers between technical and non-technical experts. While information security will always have a strong technical component, it is paramount to foster collaboration. Even decades ago network security wasn't implemented by one person alone. You need teams, you need to communicate, and you need creative ways of looking at your problems. If you want information security, you need to talk to others.

IT-Security is a very delicate matter. Aren't you afraid to offend someone?

DeepSec was the first conference to feature a talk about the broken GSM A5 encryption. When the talk went

live we were certainly a bit nervous. The GSM A5 algorithm family is responsible for encryption of the voice calls between mobile phones and the cells receiving their signals. GSM networks all over the world have billions of devices connected to it. Any vulnerability or design flaw affects a huge base of customers and companies, so having talks touching these big networks should not be taken lightly. However: We like a bit of controversy.

The next DeepSec is in November: What are you personally looking forward to the most?

Everything :) To meet our speakers, trainers and attendees and to discuss with them the state of affairs in information security. The world looks different after every DeepSec conference because of the many new perspectives and insights one gets while talking to creative and brilliant minds.

What about the future?

Information security has grown: it touches all aspects of our lifes.

Once networks enter home, office and recreational environments, so does information security. The Internet of Things is becoming a reality. We are confident that information security is here to stay. The same is true for the DeepSec conference.Year by year we adapt to the changes and include topics in the conference schedule. We have addressed mobile phone networks, Bluetooth connected devices, “cloud” technology, and many more issues in the past. In 2014 we have selected smartphones, devious backdoors in hardware, wireless networks, the new IPv6 technology, and how to educate “new” hackers. DeepSec 2015 is currently in preparation, and the Call for Papers is open.We’ll keep you posted and are already looking forward to this years event :) Stay tuned!

_____

…contact

DO YOU WANNA KNOW MORE?

DeepSec GmbH

eMail: deepsec@deepsec.net

Voice: +43 676 562 63 90

Web: http://deepsec.net

Blog: http://blog.deepsec.net

PRESS RELEASE 01

DEEPSEC 2015

DEEPSEC Mission Statement

INTERNATIONAL, TRANS & INTERDISCIPLINARY

We believe that security problems need to be addressed by experts with interdisciplinary skills. We want to encourage individuals, organizations and countries to meet and exchange, to improve overall security and trust.

NEUTRAL GROUND

Our conference is an annual event where we can freely talk about ideas and points of view. It is the best place to get together informally, get new ideas, discuss a project, develop new contacts and meet new friends.

FOCUSED ON NOVELTY, QUALITY & IMPACT

We focus only on novelty, quality and relevance when selecting talks & workshops for our conference. We prefer to invite a newcomer to the stage if the content is more promising than the “safe choice” of well established truths.

HERE TO SCOUT & SUPPORT

We actively scout and contact women who do research and projects in the field of information security. And we launched our special U21 initiative to support young researchers and enable them to present their works and results in an appropriate manner.

USER FRIENDLY

Our web site states that DeepSec is a non-product, non-vendor-biased conference. DeepSec is all about facts not ads. We are looking for honest talks about security: If something breaks, tell us about it. If you can repair it, tell us about it. If you’ve discovered something, tell us about it. That’s our goal.

...about

René Pfeiffer

…is involved with cryptography and information security for over 20 years.
He is one of the organizers of DeepSec, Vienna's very own IT-Security Conference, known for bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community.

...a little Q+A

Mr. Pfeiffer please tell us about your conference.

The DeepSec In-Depth Security Conference is an annual European two-day in-depth conference on computer, network, and application security. Our goal is to bring together the leading security experts from all over the world.

How did it all start?

DeepSec was founded in 2007. The vision was to create a IT security conference right in the heart of Europe and use it as a neutralground where professionals from academics, government, industry, and the underground hacking community can meet and exchange ideas.

What's special about DeepSec?

DeepSec is small compared to other events having thousands of participants. This is a dedicated advantage, because you can actually meet and talk to everyone. Furthermore we try to present a mix of talks connecting different aspects of information security. It's not always about technology. There's psychology, legal frameworks, human behaviour, and much more also at play.

Is there a matter particularly close to your heart?

We want to break down the barriers between technical and non-technical experts. While information security will always have a strong technical component, it is paramount to foster collaboration. Even decades ago network security wasn't implemented by one person alone. You need teams, you need to communicate, and you need creative ways of looking at your problems. If you want information security, you need to talk to others.

What about the future?

Information security has grown: it touches all aspects of our lifes. Once networks enter home, office and recreational environments, so does information security. The Internet of Things is becoming a reality.

We are confident that information security is here to stay. The same is true for the DeepSec conference.

Year by year we adapt to the changes and include topics in the conference schedule. We have addressed mobile phone networks, Bluetooth connected devices, “cloud” technology, and many more issues in the past. In 2014 we have selected smartphones, devious backdoors in hardware, wireless networks, the new IPv6 technology, and how to educate “new” hackers. DeepSec 2015 is currently in preparation, and the Call for Papers is open.
We’ll keep you posted and are already looking forward to this years event :) Stay tuned!

DeepSec GmbH
eMail: deepsec@deepsec.net
Voice: +43 676 562 63 90
Web: http://deepsec.net
Blog: http://blog.deepsec.net

...contact

Mon, 03.11.2014 08:15

http://www.pressetext.com/news/20141103007

Sicherheitskonferenz DeepSec legt Fokus auf Kommunikation und Wissen

Moderne Netzwerke lassen sich nur mit Information verteidigen

Wien (pts007/03.11.2014/08:15) -Wie kann man sich eine internationale IT-Sicherheitskonferenz vorstellen? "Die DeepSec funktioniert wie eine große Börse, auf der Lösungen und Abhilfe für brennende Sicherheitsprobleme diskutiert und ausgetauscht werden", so René Pfeiffer, Sicherheitsexperte und einer der Organisatoren der Konferenz. "Alles dreht sich um Informationen und Informationstechnologie: Man erhält kompetente Antworten von Experten, gepaart mit Demonstrationen von Schwachstellen, auf die Unternehmen reagieren müssen."

Gedankenaustausch und Aufklärungsarbeit

Bereits zum achten Mal versammelt die internationale Sicherheitskonferenz DeepSec (https://deepsec.net) vom 18. bis 21. November 2014 in Wien die Weltelite aus den Bereich der IT-Security. Die Konferenz versteht sich als neutrale Plattform die Hacker-Community, IT-/Security Unternehmen, Behördenvertreter sowie Forscher in Vorträgen und Workshops zum Gedanken- und Erfahrungsaustausch zusammenbringt.

Die Highlights des Programms thematisieren Hintertüren in Serverhardware, Schwachstellen in kryptographischen Anwendungen, Schwächen im Internetprotokoll der nächsten Generation (IPv6), Aufspüren von Schadsoftware und neue Wege vernetzte Systeme zu kompromittieren. Teile der Inhalte haben ihre Premiere zur DeepSec und wurden bisher noch nicht öffentlich diskutiert.

Sicherheit ist vielen ein Begriff, ganz besonders wenn es um Computer und Netzwerke geht. Leider wissen zuwenig Unternehmen was ihnen in der Wildnis "da draußen" wirklich passieren kann. Die internationale DeepSec Konferenz möchte diese Lücke schließen und Experten und Nutzer zusammenbringen. Die Konferenz will aber auch dem verbreiteten Vorurteil entgegen wirken, dass Hacker zwangsläufig Kriminelle sind: "Vielen geht es eher darum, Sicherheitslücken aufzuzeigen und bekannt zu machen. Erst dann können sie geschlossen werden", erklärt René Pfeiffer.

Informationen aus erster Hand

Vor der Konferenz finden zweitägige Workshops statt, in denen Trainer mit den Teilnehmern ausgewählte Inhalte durchgehen. Die Trainings sind nicht nur passive Vorlesungstage sondern Unterricht zum Anfassen und Ausprobieren. Bedrohungen sind schließlich keine Theorie. Alle Teilnehmer lernen persönlich betreut an Beispiele aus der realen Welt. An den zwei darauf folgenden Tagen findet die eigentliche Konferenz statt. Über 30 Vorträgen zeigen aktuellen Bedrohungen im Bereich der Informationstechnologie und darüber hinaus. Man hat damit die einmalige Gelegenheit aus erster Hand zu erfahren wie erfahrene Experten mit Risiken umgehen und welche Gegenmaßnahmen es gibt.

AUSSENDER

DEEPSEC

DeepSec GmbH
Ansprechpartner:
René Pfeiffer
Tel.: +43-676-5626390
E-Mail: deepsec@deepsec.net

Frühere Meldungen

- **DeepSec: IT-Sicherheit bei Online-Banking und Automobilen unzureichend**
- **Vom Auto zum "Zombie" - Datenangriffe auf Automobile**
- **DeepSec-Highlights: Terroristen-Verschlüsselung, Angriffe auf Mobilfunk und IPv6**

Schlagwörter:

- Computer und Informationstechnologie
- Computerkriminalität
- DeepSec
- Informatik
- Informationswissenschaft
- Internet

WETTER

Stadtname / PLZ

starten

AKTIENKURSE

Symbol | ISIN | Name STARTEN

HIGHTECH Mon, 03.11.2014 08:15

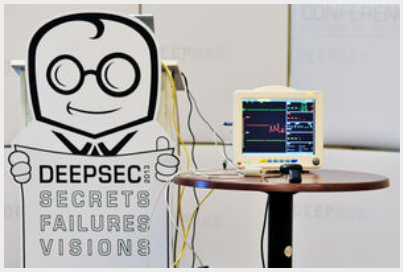
pts20141103007 Computer/Telekommunikation, Forschung/Technologie

Pressefach

Sicherheitskonferenz DeepSec legt Fokus auf Kommunikation und Wissen

Moderne Netzwerke lassen sich nur mit Information verteidigen

Wien (pts007/03.11.2014/08:15) - **Wie kann man sich eine internationale IT-Sicherheitskonferenz vorstellen? "Die DeepSec funktioniert wie eine große Börse, auf der Lösungen und Abhilfe für brennende Sicherheitsprobleme diskutiert und ausgetauscht werden", so René Pfeiffer, Sicherheitsexperte und einer der Organisatoren der Konferenz. "Alles dreht sich um Informationen und Informationstechnologie: Man erhält kompetente Antworten von Experten, gepaart mit Demonstrationen von Schwachstellen, auf die Unternehmen reagieren müssen."**



Vortrag zu Schwachstellen medizinischer Geräte (Foto: Joanna Pianka)

Gedankenaustausch und Aufklärungsarbeit

Bereits zum achten Mal versammelt die internationale Sicherheitskonferenz DeepSec (https://deepsec.net) vom 18. bis 21. November 2014 in Wien die Weltelite aus den Bereich der IT-Security. Die Konferenz versteht sich als neutrale Plattform die Hacker-Community, IT-/Security Unternehmen, Behördenvertreter sowie Forscher in Vorträgen und Workshops zum Gedanken- und Erfahrungsaustausch zusammenbringt.

Die Highlights des Programms thematisieren Hintertüren in Serverhardware, Schwachstellen in kryptographischen Anwendungen, Schwächen im Internetprotokoll der nächsten Generation (IPv6), Aufspüren von Schadsoftware und neue Wege vernetzte Systeme zu kompromittieren. Teile der Inhalte haben ihre Premiere zur DeepSec und wurden bisher noch nicht öffentlich diskutiert.

Sicherheit ist vielen ein Begriff, ganz besonders wenn es um Computer und Netzwerke geht. Leider wissen zuwenig Unternehmen was ihnen in der Wildnis "da draußen" wirklich passieren kann. Die internationale DeepSec Konferenz möchte diese Lücke schließen und Experten und Nutzer zusammenbringen. Die Konferenz will aber auch dem verbreiteten Vorurteil entgegen wirken, dass Hacker zwangsläufig Kriminelle sind: "Vielen geht es eher darum, Sicherheitslücken aufzuzeigen und bekannt zu machen. Erst dann können sie geschlossen werden", erklärt René Pfeiffer.

Informationen aus erster Hand

Vor der Konferenz finden zweitägige Workshops statt, in denen Trainer mit den Teilnehmern ausgewählte Inhalte durchgehen. Die Trainings sind nicht nur passive Vorlesungstage sondern Unterricht zum Anfassen und Ausprobieren. Bedrohungen sind schließlich keine Theorie. Alle Teilnehmer lernen persönlich betreut an Beispiele aus der realen Welt. An den zwei darauf folgenden Tagen findet die eigentliche Konferenz statt. Über 30 Vorträgen zeigen aktuellen Bedrohungen im Bereich der Informationstechnologie und darüber hinaus. Man hat damit die einmalige Gelegenheit aus erster Hand zu erfahren wie erfahrene Experten mit Risiken umgehen und welche Gegenmaßnahmen es gibt.

(Ende)

Aussender:	DeepSec GmbH
Ansprechpartner:	René Pfeiffer
Tel.:	+43-676-5626390
E-Mail:	deepsec@deepsec.net
Website:	www.deepsec.net

DEEPSEC

Press Release

Vienna/Austria, November 19th, 2013

Hackers sending out a message to managers: “Watch your risks!”

Vienna. On the occasion of the DeepSec Conference taking place in Vienna, the Scottish IT research company Alba 13 Research Labs reveals a new risk assessment system that is relevant to the business side of cyber crime.

While Alba 13 Research Labs developed the “Open Source Network Intrusion Framework” (OSNIF) and successfully implements the technological rule set already in various cooperations with international companies, the enlargement of the project now will support the risk assessment referring to the algorithms of the technical threats. This will help companies in their decision making whether an investigation or courntermeasures of all kind would be more cost effective than tolerating the level of risks.

The technical detection system with its proven alert system is therefore a component to the overall commercial controlling that is necessary for each corporation of significant value to mitigate cyber risks and protect their assets. “A technical rule set cannot 'make that decision', but a cost based one can! “, states Gavin Ewan, Chief Management Researcher at Alba 13 Research Labs.

Alba 13 Research Labs is founded in 2012 in Dundee/United Kingdom by Arron M. Finnon (Chief Technology Researcher) and Gavin Ewan (Chief Management Researcher). The foundation of the company was a result of successful research, presentation and training at various international Cyber Security Conferences in years. Focusing on the broader perspective involving IT Technology research as well as their impact for commercial risk assessment and decision making, Alba 13 Reserch Labs is unique in building bridges between managers and technical experts.

The DeepSec IDSC is an annual European two-day in-depth conference on computer, network, and application security. It is a non-product, non-vendor-biased conference event. The aim is to present the best research and experience from the fields' leading experts, bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community.

More information on: www.alba13.co.uk and www.deepsec.net

V.i.s.d.P. René Pfeiffer

Press Release

Vienna/Austria, November 19th, 2013

Hackers sending out a message to managers: “Watch your risks!”

Vienna. On the occasion of the DeepSec Conference taking place in Vienna, the Scottish IT research company Alba 13 Research Labs reveals a new risk assessment system that is relevant to the business side of cyber crime.

While Alba 13 Research Labs developed the “Open Source Network Intrusion Framework” (OSNIF) and successfully implements the technological rule set already in various cooperations with international companies, the enlargement of the project now will support the risk assessment referring to the algorithms of the technical threats. This will help companies in their decision making whether an investigation or courntermeasures of all kind would be more cost effective than tolerating the level of risks.

The technical detection system with its proven alert system is therefore a component to the overall commercial controlling that is necessary for each corporation of significant value to mitigate cyber risks and protect their assets. “A technical rule set cannot 'make that decision', but a cost based one can! “, states Gavin Ewan, Chief Management Researcher at Alba 13 Research Labs.

Alba 13 Research Labs is founded in 2012 in Dundee/United Kingdom by Arron M. Finnon (Chief Technology Researcher) and Gavin Ewan (Chief Management Researcher). The foundation of the company was a result of successful research, presentation and training at various international Cyber Security Conferences in years. Focusing on the broader perspective involving IT Technology research as well as their impact for commercial risk assessment and decision making, Alba 13 Reserch Labs is unique in building bridges between managers and technical experts.

The DeepSec IDSC is an annual European two-day in-depth conference on computer, network, and application security. It is a *non-product*, *non-vendor-biased* conference event. The aim is to present the best research and experience from the fields' leading experts, bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community.

More information on: www.alba13.co.uk and www.deepsec.net
V.i.s.d.P. René Pfeiffer

31.10.2013

P R E S S E I N F O R M A T I O N

Dicke Luft in Apples iCloud (oder: Dicke Luft in Daten Clouds)

Heitere Wölkchen versprechen Komfort – doch wer schützt meine Daten darin?
Bluetooth wurde massentauglich – aber deshalb auch sicherer?
Falschen Freunden vertraut - Social Media Dienste zeigen es vor

Wien, 31. Oktober 2013 – Diesmal Profis aus Russland, Argentinien und Deutschland zu Wort: Vladimir Katalov, Gründer von Elcomsoft, Veronica Valeros und Garcia Sebastian, und Ashar Javed, Ruhr Universität Bochum, sprechen auf der DeepSec - Depth Security Conference im Imperial Riding School Renaissance Vienna Hotel vom 19. bis 22.11.2013 über die globale Web-Wetterlage.

Cracking And Analyzing Apple iCloud von Vladimir Katalov, Begründer von Elcomsoft

Apples iCloud ist ein Dienst, mit dem Benutzer Daten speichern können. Gedacht war Apple iCloud dafür, Komfort und Flexibilität von iDevices Kunden zu erhöhen. Nicht bedacht wird oft, welche Möglichkeiten die Wolke bietet, Informationen über den Nutzer selbst herauszufinden.

Elcomsoft „rettet“ Passwörter durch ausprobieren bzw knacken. Das Unternehmen prüfte bereits unzählige Produkte auf Herz und Nieren. Bei Apples iCloud wurde aufgrund der nicht offengelegten Dokumentation des Protokolls die Interaktion zwischen der iCloud und den angeschlossenen Geräten ausgeforscht. Katalov nennt das „reverse engineering“.

Reverse Engineering bietet die Möglichkeit zu beliebig vielen Wechselwirkungen zwischen Applikationen der iCloud und des Nutzers. Vladimir Katalovs Arbeit leistet Grundlagenforschung, um die Funktionsweise und Sicherheit von Clouddiensten testen zu können. Katalov ist Russe, studierter Mathematiker und schrieb das erste Programm zur Passwortwiederherstellung. 1190 gründete er www.elcomsoft.com

Um Bluetooth Devices geht es im Vortrag der beiden Security Spezialisten Verónica Valeros & Sebastian Garcia: Privacy Issues of Bluetooth Devices

Bluetooth ist Teil unserer täglichen Welt. Drucker, Handys, Computer und viele andere Geräte haben eine Bluetooth-Schnittstelle. Ende der 90er Jahre, als die Technologie neu war, fanden Sicherheitsforscher rasch Schwächen in Implementierung und Protokoll. Es wurde erfolgreich am Bluetooth Standard nachgebessert.

Von „Sicher“ sind wir weit entfernt: Bluetooth bietet reichhaltige Möglichkeiten für Angreifer und birgt große Angriffsflächen für die Privatsphäre. Verónica Valeros & Garcia Sebastian stellen die Risikopotentiale der derzeitigen Bluetooth Implementierungen vor.

Veronica Valeros und Sebastian Garcia sind MatesLab Co-Gründer, des ersten Hackerspace in Mar del Plata, Argentina. Beide leben und arbeitet derzeit in Tschechien.

Traue niemanden....?

Ashar Javed probiert es aus: Trusted Friend Attack (Ashar Javed)

Wir alle haben schon mal Passwörter vergessen. Social Media Webseiten und andere Dienste bieten hierfür einfache Mechanismen, um den Zugang zu einem Konto auf alternativem Weg

wiederherzustellen. Ashar Javed hat sich 50 populäre Social Media Webseiten angesehen und dabei Erschreckendes festgestellt: Sechs Konten – das sind mehr als 10% - ließen sich kompromittieren, eines sogar blocken – und zwar nicht vom Inhaber.

Ein Angreifer kann dazu einfach das gute „trusted Friend“ Vertrauensverhältnis ausnutzen.

Klingt beunruhigend? Muss es nicht sein, wenn man einfache aber wirkungsvolle Ratschläge befolgt.

Ashar forscht als “Chair of Network & Data Security” an der Ruhr Universität in Bochum (D) und bereitet sich auf sein Doktorat vor. Sein Name wurde neun Mal in Google Security Hall of Fame genannt.

Bitte melden Sie Interview Anfragen bei uns an – wir organisieren gern vorab Gespräche.

Akkreditierungen für die Konferenz und die Workshops nehmen wir ab sofort entgegen:

Aufgrund limitierter Plätze bitten wir um rasche Anmeldungen:

info@deepsec.net oder René Pfeiffer: 043 676 /562 63 90

Das laufend aktualisierte Programm finden Sie auf http://deepsec.net/schedule.html

Übersicht aller Sprecher & Themen: http://deepsec.net/speaker.html

Kurzprofil DeepSec:

Die DeepSEC bildet die neutrale Plattform für ein unabhängiges Zusammentreffen von weltweit renommierten Sicherheitsexperten von Universitäten, Regierungen, der Industrie, sowie unabhängigen Wissenschaftlern, Autoren und der zumeist im Untergrund tätigen Hacker Community und interessierten Gäste aus der ganzen Welt, die sich im engeren oder weiteren Sinn mit Sicherheitsbelangen auseinandersetzen.

Die vielzitierte Vision „Leben im global vernetzten Dorf“ ist für die meisten von uns real und oft sogar Existenz bestimmend. Im selben Ausmaß wachsen auch die Bedeutung und somit die Teilnehmerbreite der DeepSec, die 2007 zum ersten Mal stattfand. Mittlerweile hat die Wiener Konferenz 200 Teilnehmer. Längst zählen nicht mehr nur Entwickler, Netzwerktechniker und Administratoren zum Besucherkreis.

DeepSec führt Interessierte aus unterschiedlichsten Bereichen wie Bildungseinrichtungen, Finanzinstitute oder Gesundheits- und Versicherungsorganisationen mit IT-Security Experten zusammen.

Kontakt / Pressekontakt

DeepSec GmbH

René Pfeiffer & Michael Kafka

Weyringergasse 30a/10

1040 Wien, Austria

rpfeiffer@deepsec.net

Mobiltelefon: +43/676/5626390

Bürotelefon: +43/720/349387

DEEPSEC

P R E S S E I N F O R M A T I O N

Dicke Luft in Apples iCloud *(oder: Dicke Luft in Daten Clouds)*

Heitere Wölkchen versprechen Komfort – doch wer schützt meine Daten darin?
Bluetooth wurde massentauglich – aber deshalb auch sicherer?
Falschen Freunden vertraut - Social Media Dienste zeigen es vor

Wien, 31. Oktober 2013 – Diesmal Profis aus Russland, Argentinien und Deutschland zu Wort: Vladimir Katalov, Gründer von Elcomsoft, Veronica Valeros und Garcia Sebastian, und Ashar Javed, Ruhr Universität Bochum, sprechen auf der DeepSec - Depth Security Conference im Imperial Riding School Renaissance Vienna Hotel vom 19. bis 22.11.2013 über die globale Web-Wetterlage.

Cracking And Analyzing Apple iCloud von Vladimir Katalov, Begründer von Elcomsoft

Apples iCloud ist ein Dienst, mit dem Benutzer Daten speichern können. Gedacht war Apple iCloud dafür, Komfort und Flexibilität von iDevices Kunden zu erhöhen. Nicht bedacht wird oft, welche Möglichkeiten die Wolke bietet, Informationen über den Nutzer selbst herauszufinden.

Elcomsoft „rettet“ Passwörter durch ausprobieren bzw knacken. Das Unternehmen prüfte bereits unzählige Produkte auf Herz und Nieren. Bei **Apples iCloud** wurde aufgrund der nicht offengelegten Dokumentation des Protokolls die Interaktion zwischen der iCloud und den angeschlossenen Geräten ausgeforscht. Katalov nennt das „reverse engineering“.
Reverse Engineering bietet die Möglichkeit zu beliebig vielen Wechselwirkungen zwischen Applikationen der iCloud und des Nutzers. Vladimir Katalovs Arbeit leistet Grundlagenforschung, um die Funktionsweise und Sicherheit von Clouddiensten testen zu können. Katalov ist Russe, studierter Mathematiker und schrieb das erste Programm zur Passwortwiederherstellung. 1190 gründete er www.elcomsoft.com

Um Bluetooth Devices geht es im Vortrag der beiden Security Spezialisten Verónica Valeros & Sebastian Garcia: **Privacy Issues of Bluetooth Devices**

Bluetooth ist Teil unserer täglichen Welt. Drucker, Handys, Computer und viele andere Geräte haben eine Bluetooth-Schnittstelle. Ende der 90er Jahre, als die Technologie neu war, fanden Sicherheitsforscher rasch Schwächen in Implementierung und Protokoll. Es wurde erfolgreich am Bluetooth Standard nachgebessert.

Von „Sicher“ sind wir weit entfernt: Bluetooth bietet reichhaltige Möglichkeiten für Angreifer und birgt große Angriffsflächen für die Privatsphäre. Verónica Valeros & Garcia Sebastian stellen die Risikopotentiale der derzeitigen Bluetooth Implementierungen vor.

Veronica Valeros und Sebastian Garcia sind MatesLab Co-Gründer, des ersten Hackerspace in Mar del Plata, Argentina. Beide leben und arbeitet derzeit in Tschechien.

Traue niemanden....?
Ashar Javed probiert es aus: Trusted Friend Attack (Ashar Javed)
Wir alle haben schon mal Passwörter vergessen. Social Media Webseiten und andere Dienste bieten hierfür einfache Mechanismen, um den Zugang zu einem Konto auf alternativem Weg wiederherzustellen. Ashar Javed hat sich 50 populäre Social Media Webseiten angesehen und dabei Erschreckendes festgestellt: Sechs Konten – das sind mehr als 10% - ließen sich kompromittieren, eines sogar blocken – und zwar nicht vom Inhaber.
Ein Angreifer kann dazu einfach das gute „trusted Friend“ Vertrauensverhältnis ausnutzen.
Klingt beunruhigend? Muss es nicht sein, wenn man einfache aber wirkungsvolle Ratschläge befolgt.

Ashar forscht als “Chair of Network & Data Security” an der Ruhr Universität in Bochum (D) und bereitet sich auf sein Doktorat vor. Sein Name wurde neun Mal in Google Security Hall of Fame genannt.

Bitte melden Sie **Interview Anfragen** bei uns an – wir organisieren gern vorab Gespräche.
Akkreditierungen für die Konferenz und die Workshops nehmen wir ab sofort entgegen:
Aufgrund limitierter Plätze bitten wir um rasche Anmeldungen:
info@deepsec.net oder René Pfeiffer: 043 676 /562 63 90

Das laufend aktualisierte Programm finden Sie auf http://deepsec.net/schedule.html

Übersicht aller Sprecher & Themen: http://deepsec.net/speaker.html

Kurzprofil DeepSec:
Die DeepSEC bildet die neutrale Plattform für ein unabhängiges Zusammentreffen von weltweit renommierten Sicherheitsexperten von Universitäten, Regierungen, der Industrie, sowie unabhängigen Wissenschaftlern, Autoren und der zumeist im Untergrund tätigen Hacker Community und interessierten Gäste aus der ganzen Welt, die sich im engeren oder weiteren Sinn mit Sicherheitsbelangen auseinandersetzen.
Die vielzitierte Vision „Leben im global vernetzten Dorf“ ist für die meisten von uns real und oft sogar Existenz bestimmend. Im selben Ausmaß wachsen auch die Bedeutung und somit die Teilnehmerbreite der DeepSec, die 2007 zum ersten Mal stattfand. Mittlerweile hat die Wiener Konferenz 200 Teilnehmer. Längst zählen nicht mehr nur Entwickler, Netzwerktechniker und Administratoren zum Besucherkreis.
DeepSec führt Interessierte aus unterschiedlichsten Bereichen wie Bildungseinrichtungen, Finanzinstitute oder Gesundheits- und Versicherungsorganisationen mit IT-Security Experten zusammen.

Kontakt / Pressekontakt
DeepSec GmbH
René Pfeiffer & Michael Kafka
Weyringergasse 30a/10
1040 Wien, Austria
rpfeiffer@deepsec.net
Mobiltelefon: +43/676/5626390
Bürotelefon: +43/720/349387

24.10.2013

P R E S S E I N F O R M A T I O N

Herzschrittmacher, Insulinpumpen und unser Wert im Web

Haben nichts miteinander zu tun? Im Gegenteil!

Auf der DeepSec diskutieren darüber:

• Hacking Medical Devices – Florian Grunow, ERNW GmbH

• Prism Break - The Value of Online Identities - Frank Ackermann

Wien, 24. Oktober 2013 – Es ist noch knapp ein Monat bis zur DeepSec ISDC -
In Depth Security Conference im Imperial Riding School Renaissance Vienna Hotel
(ehemals Penta Hotel Wien 3) vom 19. bis 22. November 2013.
René Pfeiffer und Michael Kafka präsentieren diesmal zwei deutsche Experten:
Florian Grunow, ERNW GmbH, und Frank Ackermann, passionierter IT-Security Profi.
Dick Cheney lässt Wireless Funktion im Herzschrittmacher ausschalten!
Schrieben Spiegel und englische Medien. „I found it credible“ meinte Cheney schon 2007, als er seinen Arzt bat, den Fernzugriff abzuschalten, um sich vor möglichen Terroranschlägen via Drahtlos-Funktion zu schützen. Dass er jetzt damit an die Öffentlichkeit geht, trifft sich zugegebenermaßen gut mit dem DeepSec Talk von Florian Grunow, der sich mit der Möglichkeit von Angriffen auf medizinische Gerätschaften beschäftigt.
Und es lässt die Meinung zu, Cheney muss wissen, wovor er Angst haben kann.
Insulinpumpen oder Herzschrittmacher sind schon lang mit Wireless-Zugangsfunktionen – für Ärzte oder Hersteller – ausgestattet. Dies macht viel Sinn, denn implantierte, oft lebensrettende Geräte müssen ohne operativen Aufwand von außen zu überwachen bzw. zu adjustieren sein.

Alle Geräte mit Wireless Funktion können auch angegriffen werden.
Das ist in der IT-Branche eine akzeptierte Tatsache.
Grunow geht es weniger um einen tatsächlichen Angriff auf das Leben des Patienten, als vielmehr darum, Werksspionage und wirtschaftlich motivierte Angriffe auf einen Hersteller durch Sicherheitslücken in seinen Computersystemen aufzuzeigen. Diese können enorme Auswirkungen auf Endgeräte wie Insulinpumpen, OP-Geräte, Überwachungsmonitore etc. haben.
Florian Grunow ist Security Analyst bei ERNW in Heidelberg, Deutschland, mit Fokus auf Application Security. Er besitzt ein Bachelor's Degree in Medical Computer Sciences und Master's Degree in Software Engineering und verfügt über Hintergrundwissen im Spitalwesen und in der täglichen Arbeit mit Informationstechnologien des medizinischen Personals.

Wie hoch ist mein Wert im Web? Prism Break

Frank Ackermann beschreibt in seinem nicht technischen Talk, wie viel Online Identitäten wert sind und wie die damit verbundenen Informationen von den Internetplattformen verarbeitet werden. Er leitet daraus Bedrohungen und Risiken für unsere Datenprofile ab: Neben dem durchaus bekannten Aspekt des „gläsernen Surfers“ bieten Online Identitäten ein hohes Missbrauchspotential unterschiedlicher Art. Das beginnt beim ‚Eintritt' in den Webdienst und den Wegen, dich ich im Netz wähle. Professionelle Schnüffler generieren daraus Muster, die dazu führen können, dass ich plötzlich in einer Weise und in einem Zusammenhang auffalle, der mir nicht bewusst war…

Ziel des Vortrages ist, den Teilnehmern ein besseres Verständnis davon zu geben, dass Prism, Suchmaschinen, Clouds, Big Data bei allen Online-Aktivitäten immer mitspielen und Informationen abgreifen können.

Frank Ackermann, Senior Security Professional in Düsseldorf. arbeitet seit über 13 Jahren in IT- und Information Security. Sein Credo lautet: 'Security is not my job – it is my passion'

Bitte melden Sie Interview Anfragen bei uns an – wir organisieren gern vorab Gespräche.

Akkreditierungen für die Konferenz und die Workshops nehmen wir ab sofort entgegen:

Aufgrund limitierter Plätze bitten wir um rasche Anmeldungen:

info@deepsec.net oder René Pfeiffer: 043 676 /562 63 90

Das laufend aktualisierte Programm finden Sie auf http://deepsec.net/schedule.html

Übersicht aller Sprecher & Themen: http://deepsec.net/speaker.html

Kurzprofil DeepSec:

Die DeepSEC bildet die neutrale Plattform für ein unabhängiges Zusammentreffen von weltweit renommierten Sicherheitsexperten von Universitäten, Regierungen, der Industrie, sowie unabhängigen Wissenschaftlern, Autoren und der zumeist im Untergrund tätigen Hacker Community und interessierten Gäste aus der ganzen Welt, die sich im engeren oder weiteren Sinn mit Sicherheitsbelangen auseinandersetzen.

Die vielzitierte Vision „Leben im global vernetzten Dorf“ ist für die meisten von uns real und oft sogar Existenz bestimmend. Im selben Ausmaß wachsen auch die Bedeutung und somit die Teilnehmerbreite der DeepSec, die 2007 zum ersten Mal stattfand. Mittlerweile hat die Wiener Konferenz 200 Teilnehmer. Längst zählen nicht mehr nur Entwickler, Netzwerktechniker und Administratoren zum Besucherkreis. DeepSec führt Interessierte aus unterschiedlichsten Bereichen wie Bildungseinrichtungen, Finanzinstitute oder Gesundheits- und Versicherungsorganisationen mit IT-Security Experten zusammen.

Kontakt / Pressekontakt

DeepSec GmbH

René Pfeiffer & Michael Kafka

Weyringergasse 30a/10

1040 Wien, Austria

rpfeiffer@deepsec.net

Mobiltelefon: +43/676/5626390

Bürotelefon: +43/720/349387

DEEPSEC

P R E S S E I N F O R M A T I O N

Herzschrittmacher, Insulinpumpen und unser Wert im Web

Haben nichts miteinander zu tun? Im Gegenteil!

Auf der DeepSec diskutieren darüber:

- ***Hacking Medical Devices – Florian Grunow, ERNW GmbH***
- ***Prism Break - The Value of Online Identities - Frank Ackermann***

Wien, 24. Oktober 2013 – Es ist noch knapp ein Monat bis zur DeepSec ISDC - In Depth Security Conference im Imperial Riding School Renaissance Vienna Hotel (ehemals Penta Hotel Wien 3) vom 19. bis 22. November 2013.
René Pfeiffer und Michael Kafka präsentieren diesmal zwei deutsche Experten: Florian Grunow, ERNW GmbH, und Frank Ackermann, passionierter IT-Security Profi.

Dick Cheney lässt Wireless Funktion im Herzschrittmacher ausschalten!

Schrieben Spiegel und englische Medien. „*I found it credible*“ meinte Cheney schon 2007, als er seinen Arzt bat, den Fernzugriff abzuschalten, um sich vor möglichen Terroranschlägen via Drahtlos-Funktion zu schützen. Dass er jetzt damit an die Öffentlichkeit geht, trifft sich zugegebenermaßen gut mit dem **DeepSec Talk von Florian Grunow,** der sich mit der Möglichkeit von Angriffen auf medizinische Gerätschaften beschäftigt.
Und es lässt die Meinung zu, Cheney muss wissen, wovor er Angst haben kann.

Insulinpumpen oder Herzschrittmacher sind schon lang mit Wireless-Zugangsfunktionen – für Ärzte oder Hersteller – ausgestattet. Dies macht viel Sinn, denn implantierte, oft lebensrettende Geräte müssen ohne operativen Aufwand von außen zu überwachen bzw. zu adjustieren sein.

Alle Geräte mit Wireless Funktion können auch angegriffen werden.
Das ist in der IT-Branche eine akzeptierte Tatsache.

Grunow geht es weniger um einen tatsächlichen Angriff auf das Leben des Patienten, als vielmehr darum, Werksspionage und wirtschaftlich motivierte Angriffe auf einen Hersteller durch Sicherheitslücken in seinen Computersystemen aufzuzeigen. Diese können enorme Auswirkungen auf Endgeräte wie Insulinpumpen, OP-Geräte, Überwachungsmonitore etc. haben.

Florian Grunow ist Security Analyst bei ERNW in Heidelberg, Deutschland, mit Fokus auf Application Security. Er besitzt ein Bachelor's Degree in Medical Computer Sciences und Master's Degree in Software Engineering und verfügt über Hintergrundwissen im Spitalwesen und in der täglichen Arbeit mit Informationstechnologien des medizinischen Personals.

Wie hoch ist mein Wert im Web? Prism Break

Frank Ackermann beschreibt in seinem nicht technischen Talk, wie viel Online Identitäten wert sind und wie die damit verbundenen Informationen von den Internetplattformen verarbeitet werden. Er leitet daraus Bedrohungen und Risiken für unsere Datenprofile ab: Neben dem durchaus bekannten Aspekt des „gläsernen Surfers“ bieten Online Identitäten ein hohes Missbrauchspotential unterschiedlicher Art. Das beginnt beim ‚Eintritt’ in den Webdienst und den Wegen, dich ich im Netz wähle. Professionelle Schnüffler generieren daraus Muster, die dazu führen können, dass ich plötzlich in einer Weise und in einem Zusammenhang auffalle, der mir nicht bewusst war…

Ziel des Vortrages ist, den Teilnehmern ein besseres Verständnis davon zu geben, dass Prism, Suchmaschinen, Clouds, Big Data bei allen Online-Aktivitäten immer mitspielen und Informationen abgreifen können.

Frank Ackermann, Senior Security Professional in Düsseldorf. arbeitet seit über 13 Jahren in IT- und Information Security. Sein Credo lautet: *'Security is not my job – it is my passion’*

Bitte melden Sie **Interview Anfragen** bei uns an – wir organisieren gern vorab Gespräche.

Akkreditierungen für die Konferenz und die Workshops nehmen wir ab sofort entgegen:

Aufgrund limitierter Plätze bitten wir um rasche Anmeldungen:

info@deepsec.net oder René Pfeiffer: 043 676 /562 63 90

Das laufend aktualisierte Programm finden Sie auf http://deepsec.net/schedule.html

Übersicht aller Sprecher & Themen: http://deepsec.net/speaker.html

Kurzprofil DeepSec:
Die DeepSEC bildet die neutrale Plattform für ein unabhängiges Zusammentreffen von weltweit renommierten Sicherheitsexperten von Universitäten, Regierungen, der Industrie, sowie unabhängigen Wissenschaftlern, Autoren und der zumeist im Untergrund tätigen Hacker Community und interessierten Gäste aus der ganzen Welt, die sich im engeren oder weiteren Sinn mit Sicherheitsbelangen auseinandersetzen.
Die vielzitierte Vision „Leben im global vernetzten Dorf“ ist für die meisten von uns real und oft sogar Existenz bestimmend. Im selben Ausmaß wachsen auch die Bedeutung und somit die Teilnehmerbreite der DeepSec, die 2007 zum ersten Mal stattfand. Mittlerweile hat die Wiener Konferenz 200 Teilnehmer. Längst zählen nicht mehr nur Entwickler, Netzwerktechniker und Administratoren zum Besucherkreis. DeepSec führt Interessierte aus unterschiedlichsten Bereichen wie Bildungseinrichtungen, Finanzinstitute oder Gesundheits- und Versicherungsorganisationen mit IT-Security Experten zusammen.

Kontakt / Pressekontakt
DeepSec GmbH
René Pfeiffer & Michael Kafka
Weyringergasse 30a/10
1040 Wien, Austria
rpfeiffer@deepsec.net
Mobiltelefon: +43/676/5626390
Bürotelefon: +43/720/349387

09.10.2013 1/3

P R E S S E I N F O R M A T I O N

Der Countdown zur DeepSec 2013 läuft

- Vom 19. bis 22.11.2013 referieren internationale Sicherheitsexperten in Wien

- Wir stellen Sprecher und Schwerpunkte vor

Wien, 9. Oktober 2012 – Vom 19. bis 22. November 2013 findet die DeepSec ISDC - In Depth Security Conference im Imperial Riding School Renaissance Vienna Hotel (ehemals Penta Hotel Wien 3) statt.

Heuriges Motto dieser 7. Konferenz ist “All about Secrets, Failures and Vision“.

Am 19.11. wird mit einem zweitägigen Workshop gestartet. Die Konferenz folgt am 21.11.2013.

Die Keynote hält Marcus J. Ranum. Am Anschluss daran findet die Pressekonferenz statt.

DeepSec Veranstalter René Pfeiffer und Michael Kafka gewannen auch 2013 wieder renommierte Experten aus Europa (u.a. Schweiz, Deutschland, Ungarn) sowie USA und Asien. Auf hohem Niveau diskutieren die Experten über Sicherheit in der mobilen Welt, welche Geheimnisse, Fehler und Visionen uns schon jetzt beschäftigen sollten, um auf die wachsenden Herausforderungen besser vorbereitet zu sein.

Geopolitics And The Internet: The Meaning Of "Hegemony", Marcus J. Ranum

Was die Vorherrschaft der USA im Internet und für die gesamte mobile Welt bedeutet, und was man ihr entgegensetzen kann und muss – darüber referiert Marcus J. Ranum (Tenable Network Security).

Der 1962 geborene US-Amerikaner gilt als IT-Sicherheits-Pionier, hält seit den 80er Jahren Top-Positionen in IT-Sicherheitsfirmen und publiziert regelmäßig Artikel sowie Sachbücher, u.a. „The Myth of Homeland Security“.

Ranum versteht das Internet als „Kolonie der US-Amerikaner“, in der sie ihre uneingeschränkte Machtposition laufend ausbauen – man denke beispielsweise an Stuxnet oder an den globalen Spionageskandal. Mittlerweile fordern einzelne europäische Regierungen ein Nachdenken über die Notwendigkeit einer europäischen ITK-Souveränität, um in der Informationstechnik nicht von den US-Amerikanern oder anderen Mächten abhängig zu sein.

09.10.2013 2/3

Auch die europäische Wirtschaft bildet sich langsam eine Meinung dazu: Politiker verstünden nichts von der Thematik und interessieren sich daher auch nicht für Sicherheit bzw. erkennen die Brisanz nicht. Dass Politiker von unzähligen Lobbyisten – Diener unterschiedlicher Herren – beraten werden, mache die Sache nicht einfacher; im Gegenteil.

Der menschlichen Psyche widmet sich Stefan Schumacher vom Magdeburger Institut für

Sicherheitsforschung: Psychology of Security - A Research Programme

Warum gelingt es Betrügern dermaßen leicht via Porno-Apps, Sexbildern und fingierter Partnersuche auf Webplattformen Menschen und ganze Unternehmen auszuspionieren, zu erpressen und zu schädigen?

Warum fallen Menschen immer wieder auf schlecht gemachte Passwort-Fischer herein?

Weil fast 50% aller Smartphone Nutzer weltweit ihre Handys in keinster Weise sichern und oft sogar Codes und Passwörter offen darin aufbewahren? (Zahlen: aktueller Norton Bericht 2013)

Weil IT-Security nur als technisches Problem angesehen wird, statt anzuerkennen, dass Entscheidungen von Menschen getroffen werden und somit Sicherheitsprobleme und –strategien auch mit psychologischen Methoden untersucht werden sollten?

Stefan Schumacher stellt Ergebnisse aus seinem aktuellen Forschungsprojekt vor:

Es geht dabei u.a. darum, wie Menschen IT-Security erleben, was sie motiviert? Wie lernen sie und warum machen viele immer wieder dieselben Fehler und wie kann dieser Kreislauf nachhaltig unterbrochen werden?

Des weiteren geht es um die psychologischen Profile der Angreifer, die neben ihren technischen Möglichkeiten genauso entscheidend für die Abwehr von Angriffen sind.

Kontroverse Themen wie diese diskutieren wir auf der DeepSec 2013.

Bitte melden Sie Interview Anfragen bei uns an – wir organisieren auch vorab Gespräche.

Akkreditierungen für die Konferenz und die Workshops nehmen wir ab sofort entgegen:

Aufgrund limitierter Plätze bitten wir um rasche Anmeldungen:

info@deepsec.net oder René Pfeiffer: 043 676 /562 63 90

Das laufend aktualisierte Programm finden Sie auf http://deepsec.net/schedule.html

Übersicht aller Sprecher & Themen: http://deepsec.net/speaker.html

09.10.2013 3/3

Kurzprofil DeepSec:

Die DeepSEC bildet die neutrale Plattform für ein unabhängiges Zusammentreffen von weltweit renommierten Sicherheitsexperten von Universitäten, Regierungen, der Industrie, sowie unabhängigen Wissenschaftlern, Autoren

und der zumeist im Untergrund tätigen Hacker Community und interessierten Gäste aus der ganzen Welt, die sich

im engeren oder weiteren Sinn mit Sicherheitsbelangen auseinandersetzen.

Die vielzitierte Vision „Leben im global vernetzten Dorf“ ist für die meisten von uns real und oft sogar Existenz bestimmend. Im selben Ausmaß wachsen auch die Bedeutung und somit die Teilnehmerbreite der DeepSec,

die2007 zum ersten Mal stattfand. Mittlerweile hat die Wiener Konferenz 200 Teilnehmer. Längst zählen nicht mehrnur Entwickler, Netzwerktechniker und Administratoren zum Besucherkreis. DeepSec führt Interessierte aus unterschiedlichsten Bereichen wie Bildungseinrichtungen, Finanzinstitute oder Gesundheits- und Versicherungs-organisationen mit IT-Security Experten zusammen.

Kontakt / Pressekontakt

DeepSec GmbH

René Pfeiffer & Michael Kafka

Weyringergasse 30a/10

1040 Wien, Austria

rpfeiffer@deepsec.net

Mobiltelefon: +43/676/5626390

Bürotelefon: +43/720/349387

DEEPSEC

P R E S S E I N F O R M A T I O N

Der Countdown zur DeepSec 2013 läuft

- ***Vom 19. bis 22.11.2013 referieren internationale Sicherheitsexperten in Wien***
- ***Wir stellen Sprecher und Schwerpunkte vor***

Wien, 9. Oktober 2012 – Vom 19. bis 22. November 2013 findet die DeepSec ISDC - In Depth Security Conference im Imperial Riding School Renaissance Vienna Hotel (ehemals Penta Hotel Wien 3) statt.
Heuriges Motto dieser 7. Konferenz ist "All about Secrets, Failures and Vision".
Am 19.11. wird mit einem zweitägigen Workshop gestartet. Die Konferenz folgt am 21.11.2013.
Die Keynote hält Marcus J. Ranum. Am Anschluss daran findet die Pressekonferenz statt.

DeepSec Veranstalter René Pfeiffer und Michael Kafka gewannen auch 2013 wieder renommierte Experten aus Europa (u.a. Schweiz, Deutschland, Ungarn) sowie USA und Asien. Auf hohem Niveau diskutieren die Experten über Sicherheit in der mobilen Welt, welche Geheimnisse, Fehler und Visionen uns schon jetzt beschäftigen sollten, um auf die wachsenden Herausforderungen besser vorbereitet zu sein.

Geopolitics And The Internet: The Meaning Of "Hegemony", Marcus J. Ranum
Was die Vorherrschaft der USA im Internet und für die gesamte mobile Welt bedeutet, und was man ihr entgegensetzen kann und muss – darüber referiert Marcus J. Ranum (Tenable Network Security).
Der 1962 geborene US-Amerikaner gilt als IT-Sicherheits-Pionier, hält seit den 80er Jahren Top-Positionen in IT-Sicherheitsfirmen und publiziert regelmäßig Artikel sowie Sachbücher, u.a. „The Myth of Homeland Security".

Ranum versteht das Internet als **„Kolonie der US-Amerikaner",** in der sie ihre uneingeschränkte Machtposition laufend ausbauen – man denke beispielsweise an Stuxnet oder an den globalen Spionageskandal. Mittlerweile fordern einzelne europäische Regierungen ein Nachdenken über die **Notwendigkeit einer europäischen ITK-Souveränität,** um in der Informationstechnik nicht von den US-Amerikanern oder anderen Mächten abhängig zu sein.

Auch die europäische Wirtschaft bildet sich langsam eine Meinung dazu: Politiker verstünden nichts von der Thematik und interessieren sich daher auch nicht für Sicherheit bzw. erkennen die Brisanz nicht. Dass Politiker von unzähligen Lobbyisten – Diener unterschiedlicher Herren – beraten werden, mache die Sache nicht einfacher; im Gegenteil.

Der menschlichen Psyche widmet sich Stefan Schumacher vom Magdeburger Institut für Sicherheitsforschung: Psychology of Security - A Research Programme

Warum gelingt es Betrügern dermaßen leicht via Porno-Apps, Sexbildern und fingierter Partnersuche auf Webplattformen Menschen und ganze Unternehmen auszuspionieren, zu erpressen und zu schädigen?
Warum fallen Menschen immer wieder auf schlecht gemachte Passwort-Fischer herein?
Weil fast 50% aller Smartphone Nutzer weltweit ihre Handys in keinster Weise sichern und oft sogar Codes und Passwörter offen darin aufbewahren? *(Zahlen: aktueller Norton Bericht 2013*)

Weil IT-Security nur als technisches Problem angesehen wird, statt anzuerkennen, dass Entscheidungen von Menschen getroffen werden und somit Sicherheitsprobleme und –strategien auch mit psychologischen Methoden untersucht werden sollten?

Stefan Schumacher stellt Ergebnisse aus seinem aktuellen Forschungsprojekt vor:

Es geht dabei u.a. darum, wie Menschen IT-Security erleben, was sie motiviert? Wie lernen sie und warum machen viele immer wieder dieselben Fehler und wie kann dieser Kreislauf nachhaltig unterbrochen werden?
Des weiteren geht es um die psychologischen Profile der Angreifer, die neben ihren technischen Möglichkeiten genauso entscheidend für die Abwehr von Angriffen sind.

Kontroverse Themen wie diese diskutieren wir auf der DeepSec 2013.

Bitte melden Sie **Interview Anfragen** bei uns an – wir organisieren auch vorab Gespräche.
Akkreditierungen für die Konferenz und die Workshops nehmen wir ab sofort entgegen:
Aufgrund limitierter Plätze bitten wir um rasche Anmeldungen:
info@deepsec.net oder René Pfeiffer: 043 676 /562 63 90

Das laufend aktualisierte Programm finden Sie auf http://deepsec.net/schedule.html

Übersicht aller Sprecher & Themen: http://deepsec.net/speaker.html

Kurzprofil DeepSec:
Die DeepSEC bildet die neutrale Plattform für ein unabhängiges Zusammentreffen von weltweit renommierten Sicherheitsexperten von Universitäten, Regierungen, der Industrie, sowie unabhängigen Wissenschaftlern, Autoren und der zumeist im Untergrund tätigen Hacker Community und interessierten Gäste aus der ganzen Welt, die sich im engeren oder weiteren Sinn mit Sicherheitsbelangen auseinandersetzen.
Die vielzitierte Vision „Leben im global vernetzten Dorf“ ist für die meisten von uns real und oft sogar Existenz bestimmend. Im selben Ausmaß wachsen auch die Bedeutung und somit die Teilnehmerbreite der DeepSec, die 2007 zum ersten Mal stattfand. Mittlerweile hat die Wiener Konferenz 200 Teilnehmer. Längst zählen nicht mehr nur Entwickler, Netzwerktechniker und Administratoren zum Besucherkreis.
DeepSec führt Interessierte aus unterschiedlichsten Bereichen wie Bildungseinrichtungen, Finanzinstitute oder Gesundheits- und Versicherungsorganisationen mit IT-Security Experten zusammen.

Kontakt / Pressekontakt
DeepSec GmbH
René Pfeiffer & Michael Kafka
Weyringergasse 30a/10
1040 Wien, Austria
rpfeiffer@deepsec.net
Mobiltelefon: +43/676/5626390
Bürotelefon: +43/720/349387

http://www.pressebox.de/inaktiv/deepsec-gmbh/Vorlaeufiges-DeepSec-Programm-veroeffentlicht-Cyberwar-und-Sicherheit-von-Mobilfunknetzwerken-im-Konferenz-Fokus/boxid/541775

Pressemitteilung BoxID 541775

Vorläufiges DeepSec-Programm veröffentlicht: Cyberwar und Sicherheit von Mobilfunknetzwerken im Konferenz-Fokus

Internationale Security-Expertise in 33 Vorträgen und acht Workshops

(PresseBox) (Wien, 25.09.2012) Vom 27. bis zum 30. November trifft sich die internationale Elite der Network-Security- und Hacking-Branche zum sechsten Mal auf der Wiener Sicherheitskonferenz DeepSec (https://deepsec.net/). 2012 liegen die Konferenzschwerpunkte auf der Sicherheit von mobilen Geräten, M obilfunknetzwerken und dem Cyberwar. 33 Vorträge und acht Workshops informieren Anwender, Forscher, IT- und Security-Unternehmen, Behörden sowie die Hacker-Community über die relevanten Cyber-Sicherheitsthemen der Gegenwart. "Für die sechste DeepSec konnten wir mit Felix Lindner und Babak Javadi internationale Spitzen-Referenten gewinnen und somit die Besten auf ihrem Gebiet in Wien vereinen", erklärt René Pfeiffer, Organisator der DeepSec.

Traditionell werden die ersten beiden Konferenztage aus acht Workshops bestehen. Mit Harald Welte und Dieter Spaar (Independent Researcher & HMW-Consulting) wird die DeepSec die führenden Experten für Mobilfunksicherheit nach Wien bringen. Ihr Workshop "Attacks on GSM Networks" beschäftigt sich mit den Schwächen aktueller GSM-Sicherheitssoftware und verdeutlicht, welche Probleme Sicherheitskräfte mit derzeit verfügbaren Tools haben. Die zweite Hälfte des Workshops wird aus Praxis-Ausflügen in GSM-Sicherheitstools wie OsmocomBB, OpenBSC, airprobe und SIMtrace bestehen.

Der zweitägige DeepSec-Workshop "Social Engineering Training for IT Security Professionals" der britischen Sicherheitsexperten Sharon Conheady und Martin Law der Firma First Defence Information Security Ltd., kommt DeepSec-Kennern sicher bekannt vor. Tatsächlich verliert die Gefahr sogenannter Social-Engineering-Angriffe gerade für größere Unternehmen nichts ihrer Bedrohlichkeit. Perfide Social Engineers versuchen dabei gezielt unsichere Mitarbeiter am Telefon auszuspionieren. Oft versuchen sie es mit der Telefon-Masche. Als vermeintliche Vorgesetzte fordern sie von Mitarbeitern sofort wichtige Auskünfte. Gerade gegenüber vermeintlichen Vorgesetzten ist die natürliche menschliche Reaktion eine konfliktvermeidende und kooperative. In Trainings erfahren Interessenten, wie sie sich selbst und ihre Mitarbeiter vor solchen Attacken schützen können. Der Workshop wird aus einem theoretischen und einem praktischen Teil bestehen.

Der Onapsis-Mitarbeiter Juan Pablo Perez Etchegoyen widmet sich in seinem SAP-Security-Workshop "SAP Security In-Depth" der Absicherung von SAP-Systemen in großen Firmen. Der CTO von Onapsis beschäftigt sich auch in seinem Vortrag "Inception of the SAP Platform's Brain: Attacks to SAP Solution Manager" mit der SAP-Sicherheit. Diese Themen sind von besonderem Interesse für alle SAP-Anwender und -Entwickler.

Etchegoyens Beitrag ist einer der am 29. November startenden 33 Vorträge. Die Keynote wird in diesem Jahr vom Leiter der Recurity Labs, Felix "FX" Lindner gehalten. Lindners Vortrag "We came in Peace - They don't: Hackers vs. CyberWar" thematisiert das derzeit kursierende Cyberwar-Gespenst im Zusammenhang mit Sicherheitslücken in der digitalen Waffenhandel-Industrie. Auch die Referenten Stefan Schumacher (Magdeburger Institut für Sicherheitsforschung) und Karin Kosina widmen sich dem Thema Cyberwar. Schumacher spricht in "The Vienna Programme: A Global Strategy for Cyber Security by the Global Cyber Defence Initiative" über Initiativen, Cyberwar durch Kommunikation in Krisensituationen zu vermeiden. Kosina setzt die Thematik Cyberwar mit "Wargames in the Fifth Domain" in einen internationalen Kontext, der stark die völker- und kriegsrechtliche Seite betont und verbindet diese Felder mit den verfügbaren technischen Möglichkeiten.

Mit Babak Javadi ist auch der Gründer der CORE Group in Wien zu Gast. In seinem Vortrag "4140 Ways Your Alarm System Can Fail" beschäftigt er sich mit der generellen Anfälligkeit herkömmlicher Alarmanlagen. Michael Niekamp und Florian Grunert von der Universität Osnabrück ergänzen das Thema mit ihrem Vortrag "A Non-Attribution-Dilemma and it's Impact on Legal Regulation of Cyberwar" durch eine rein rechtliche Situationsbetrachtung. Am 30. November kommt mit Robert M. Lee noch ein Angehöriger der US Air Force zu Wort: Sein Vortrag "The Interim Years of Cyberspace - Security in a Domain of Warfare" wirft einen Blick auf die Geschichte des Cyberwar. "Gerade den Cyberwar kennen selbst viele Computer-affine Menschen nur aus Kinofilmen oder Tom-Clancy-Videospielen. Wir wollen mit den Vorträgen auf der DeepSec 2012 einen Bezug zur Realität herstellen und das Thema sachlich diskutieren. Gerade beim Thema Infrastruktur und Sicherheit kommt es auf Fakten und Details an", erklärt Pfeiffer.

Die DeepSec versteht sich aber nicht nur als Expertenforum, sondern will gezielt Vorurteile gegenüber ihrer Zielgruppe abbauen. Weder seien DeepSec-Besucher kriminelle Hacker, noch Weltuntergangs-Nerds, so Pfeiffer. Zudem laden die DeepSec-Referenten ausdrücklich zum direkten Dialog ein. Während der ganzen DeepSec Konferenz werden die Besucher Zeit für persönliche Gespräche mit den Experten haben.

Weitere Informationen und das Programm der DeepSec finden Sie hier: https://deepsec.net/

Anmeldung zur DeepSec unter: https://deepsec.net/register.html

Vorläufiges DeepSec-Programm veröffentlicht: Cyberwar und Sicherheit von Mobilfunknetzwerken im Konferenz-Fokus

Internationale Security-Expertise in 33 Vorträgen und acht Workshops

(PresseBox) (Wien, 25.09.2012) Vom 27. bis zum 30. November trifft sich die internationale Elite der Network-Security- und Hacking-Branche zum sechsten Mal auf der Wiener Sicherheitskonferenz DeepSec (https://deepsec.net/). 2012 liegen die Konferenzschwerpunkte auf der Sicherheit von mobilen Geräten, M obilfunknetzwerken und dem Cyberwar. 33 Vorträge und acht Workshops informieren Anwender, Forscher, IT- und Security-Unternehmen, Behörden sowie die Hacker-Community über die relevanten Cyber-Sicherheitsthemen der Gegenwart. "Für die sechste DeepSec konnten wir mit Felix Lindner und Babak Javadi internationale Spitzen-Referenten gewinnen und somit die Besten auf ihrem Gebiet in Wien vereinen", erklärt René Pfeiffer, Organisator der DeepSec.

Traditionell werden die ersten beiden Konferenztage aus acht Workshops bestehen. Mit Harald Welte und Dieter Spaar (Independent Researcher & HMW-Consulting) wird die DeepSec die führenden Experten für Mobilfunksicherheit nach Wien bringen. Ihr Workshop "Attacks on GSM Networks" beschäftigt sich mit den Schwächen aktueller GSM-Sicherheitssoftware und verdeutlicht, welche Probleme Sicherheitskräfte mit derzeit verfügbaren Tools haben. Die zweite Hälfte des Workshops wird aus Praxis-Ausflügen in GSM-Sicherheitstools wie OsmocomBB, OpenBSC, airprobe und SIMtrace bestehen.

Der zweitägige DeepSec-Workshop "Social Engineering Training for IT Security Professionals" der britischen Sicherheitsexperten Sharon Conheady und Martin Law der Firma First Defence Information Security Ltd., kommt DeepSec-Kennern sicher bekannt vor. Tatsächlich verliert die Gefahr sogenannter Social-Engineering-Angriffe gerade für größere Unternehmen nichts ihrer Bedrohlichkeit. Perfide Social Engineers versuchen dabei gezielt unsichere Mitarbeiter am Telefon auszuspionieren. Oft versuchen sie es mit der Telefon-Masche. Als vermeintliche Vorgesetzte fordern sie von Mitarbeitern sofort wichtige Auskünfte. Gerade gegenüber vermeintlichen Vorgesetzten ist die natürliche menschliche Reaktion eine konfliktvermeidende und kooperative. In Trainings erfahren Interessenten, wie sie sich selbst und ihre Mitarbeiter vor solchen Attacken schützen können. Der Workshop wird aus einem theoretischen und einem praktischen Teil bestehen.

Der Onapsis-Mitarbeiter Juan Pablo Perez Etchegoyen widmet sich in seinem SAP-Security-Workshop "SAP Security In-Depth" der Absicherung von SAP-Systemen in großen Firmen. Der CTO von Onapsis beschäftigt sich auch in seinem Vortrag "Inception of the SAP Platform's Brain: Attacks to SAP Solution Manager" mit der SAP-Sicherheit. Diese Themen sind von besonderem Interesse für alle SAP-Anwender und -Entwickler.

Etchegoyens Beitrag ist einer der am 29. November startenden 33 Vorträge. Die Keynote wird in diesem Jahr vom Leiter der Recurity Labs, Felix "FX" Lindner gehalten. Lindners Vortrag "We came in Peace - They don't: Hackers vs. CyberWar" thematisiert das derzeit kursierende Cyberwar-Gespenst im Zusammenhang mit Sicherheitslücken in der digitalen Waffenhandel-Industrie. Auch die Referenten Stefan Schumacher (Magdeburger Institut für Sicherheitsforschung) und Karin Kosina widmen sich dem Thema Cyberwar. Schumacher spricht in "The Vienna Programme: A Global Strategy for Cyber Security by the Global Cyber Defence Initiative" über Initiativen, Cyberwar durch Kommunikation in Krisensituationen zu vermeiden. Kosina setzt die Thematik Cyberwar mit "Wargames in the Fifth Domain" in einen internationalen Kontext, der stark die völker- und kriegsrechtliche Seite betont und verbindet diese Felder mit den verfügbaren technischen Möglichkeiten.

Mit Babak Javadi ist auch der Gründer der CORE Group in Wien zu Gast. In seinem Vortrag "4140 Ways Your Alarm System Can Fail" beschäftigt er sich mit der generellen Anfälligkeit herkömmlicher Alarmanlagen. Michael Niekamp und Florian Grunert von der Universität Osnabrück ergänzen das Thema mit ihrem Vortrag "A Non-Attribution-Dilemma and it's Impact on Legal Regulation of Cyberwar" durch eine rein rechtliche Situationsbetrachtung. Am 30. November kommt mit Robert M. Lee noch ein Angehöriger der US Air Force zu Wort: Sein Vortrag "The Interim Years of Cyberspace - Security in a Domain of Warfare" wirft einen Blick auf die Geschichte des Cyberwar. "Gerade den Cyberwar kennen selbst viele Computer-affine Menschen nur aus Kinofilmen oder Tom-Clancy-Videospielen. Wir wollen mit den Vorträgen auf der DeepSec 2012 einen Bezug zur Realität herstellen und das Thema sachlich diskutieren. Gerade beim Thema Infrastruktur und Sicherheit kommt es auf Fakten und Details an", erklärt Pfeiffer.

Die DeepSec versteht sich aber nicht nur als Expertenforum, sondern will gezielt Vorurteile gegenüber ihrer Zielgruppe abbauen. Weder seien DeepSec-Besucher kriminelle Hacker, noch Weltuntergangs-Nerds, so Pfeiffer. Zudem laden die DeepSec-Referenten ausdrücklich zum direkten Dialog ein. Während der ganzen DeepSec Konferenz werden die Besucher Zeit für persönliche Gespräche mit den Experten haben.

Weitere Informationen und das Programm der DeepSec finden Sie hier: https://deepsec.net/

Anmeldung zur DeepSec unter: https://deepsec.net/register.html

3. DACH-Sicherheitsforum Österreich

Kontakt

DeepSec GmbH
Weyringergasse 30a/10
A-1040 Wien

Wed, 23.05.2012 07:35

http://www.pressetext.com/news/20120523006

Datenrettung: "Bei Daten-Gau sind alle Security-Regeln plötzlich außer Kraft"

Attingo und DeepSec warnen: Datenrettungspartner sollten vorab auditiert werden

Attingo Datenrettung - Labor

[Fotos]

Wien,Hamburg (pts006/23.05.2012/07:35) - Größere Unternehmen verfügen über ausgefeilte Security-Policies und Prozessbeschreibungen vom Backup bis zur Datenwiederherstellung. Was aber häufig unter den Tisch fällt, sind Notfallpläne für den Fall der Fälle: nämlich, wenn sich defekte Datenträger nicht hausintern wiederherstellen lassen und der Gang zum Datenretter erforderlich wird. "Bei kritischen Systemausfällen werden oft plötzlich zentrale Security-Regeln außer Acht gelassen und in Windeseile Server, RAID-Systeme oder Festplatten mit hochsensiblen Informationen an externe Dienstleister übergeben - ohne dass diese im Vorfeld auf Sicherheit geprüft wurden", berichtet René Pfeiffer, Geschäftsführer der Wiener Sicherheitskonferenz DeepSec.

Datendiebe zapfen Dritte an

Die Gefahr dabei: Einige Datenrettungsanbieter schicken defekte Medien an Recovery-Labore im benachbarten Ausland, ohne ihre Kunden explizit davon zu informieren. "Organisierte Datendiebe zapfen aber nicht selten Quellen über Dritte in Insider-Branchen an. Wenn auf diesem Weg Daten verloren gehen oder entwendet werden, hat das Unternehmen den doppelten Schaden", warnt Pfeiffer. Denn es kommt auch noch das Haftungsrisiko hinzu. "Laut Datenschutzgesetz haftet der Eigentümer dann voll für seine Informationen, wenn er es verabsäumt, die 'sichere Datenverarbeitung' durch seinen Dienstleister vorab zu prüfen", erklärt Nicolas Ehrschwendner, Geschäftsführer des heimischen Datenrettungsunternehmens Attingo. De facto fordert das DSG damit die Durchführung von Dienstleister-Audits.

Notfallplan für Datenrettung

Nach dem Motto: "Prüfe deinen Datenretter, so lange die IT-Welt noch in Ordnung ist", bietet Attingo seinen Kunden die gemeinsame Erarbeitung von Notfallplänen schon im Vorfeld an. Der Recovery-Spezialist betreibt sein Reinraumlabor in Wien, so dass ein Versand ins Ausland kein Thema ist. Aber mit seiner Strategie begegnet Attingo einer weiteren Gefahrenquelle: Bei Ausfall von Datenträgern liegt das größte technische Risiko in unsachgemäßen Wiederherstellungsversuchen. "In mehr als 80 Prozent aller Fälle, bei denen selbstständig Rettungsversuche unternommen werden, vergrößert sich der Schaden dadurch letztendlich", berichtet Ehrschwendner aus der täglichen Praxis.

Typische Fehler

"Bei Ausfall von Servern oder RAID-Systemen werden in der Hektik oft hausintern Schritte unternommen, die zwar logisch erscheinen, aber aufgrund der Komplexität gerade diesmal nicht funktionieren", führt er aus. Typische Fehler sind etwa: unkontrolliertes Tauschen defekter Festplatten, Löschen und neu-Anlegen von RAID-Konfigurationen, das Erzwingen des Online-Status von RAIDs oder Ausprobieren von unbekannten Funktionen. Generell sind die Daten auf einem defekten Speichermedium im Reinraumlabor bis zu 100 Prozent rekonstruierbar, solange die betreffenden Sektoren nicht durch falsch veranlasste Vorgänge im Betriebssystem überschrieben wurden. Ein schädigender Vorgang kann aber schon ein simpler Systemstart sein.

Recovery-Partner in die Policy

Vor allem Banken, Health-Care- und Forschungsunternehmen mit sensiblen Daten nutzen verstärkt die Möglichkeit, gemeinsam mit den Recovery-Spezialisten von Attingo eigene Notfallpläne für die Datenrettung auszuarbeiten. Ein wesentlicher Punkt dabei ist, dass der Datenrettungspartner schon auditiert wird, lange bevor eine Katastrophe eintritt. Auch DeepSec Geschäftsführer René Pfeiffer empfiehlt: "Die Auswahl des Datenrettungspartners gehört konsequenterweise in die Security-Policy integriert."

Über DeepSec

Die DeepSec bringt als neutrale Plattform Sicherheitsexperten aus allen Bereichen zum Gedanken- und Erfahrungsaustausch zusammen. Die Konferenz will aber auch dem verbreiteten Vorurteil entgegenwirken, dass Hacker zwangsläufig Kriminelle sind. "Ganz im Gegenteil. Vielen sogenannten Hackern geht es eher darum, Sicherheitslücken aufzuzeigen und bekannt zu machen. Man kann nur Gefahren beseitigen, die man kennt und die erforscht sind, ganz so wie in anderen Bereichen", so Pfeiffer.

Weitere Informationen zur DeepSec finden Sie hier: https://deepsec.net/

Über Attingo Datenrettung

Attingo Datenrettung ist ein führender, europäischer Anbieter von Datenrettungen. Die Datenrettung befasst sich mit der Rekonstruktion von Daten, die durch Löschung, Formatierung, technische Defekte, Manipulation, Sabotage oder äußere Einflüsse wie Wasser oder Feuer beeinträchtigt wurden. Attingo rettet diese Daten. Das Unternehmen betreibt dazu modernste Reinraumlaboratorien in Wien, Hamburg und Amsterdam und verfügt über Experten mit jahrelanger Erfahrung. Attingo ist in Notfällen für seine Klienten 24/7 erreichbar.

Weitere Informationen: http://www.attingo.com/

Rückfragehinweis: DI Nicolas Ehrschwendner: +43(1)2360101, +49(40)5488756-0, presse@attingo.com

Aussender: Attingo Datenrettung GmbH

Frühere Meldungen

Festplatten in der Notaufnahme - Datenrettung rund um die Uhr

Datenverlust-Fälle durch Sabotage verdoppeln sich zum Jahreswechsel

Bizarrste Datenverlust-Fälle: Rückblick 2011

Schlagwörter:

- Attingo
- Datenrekonstruktion
- Datenrettung
- DeepSec
- Sicherheit

HIGHTECH Wed, 23.05.2012 07:35

<< Zurück zu den Suchergebnissen

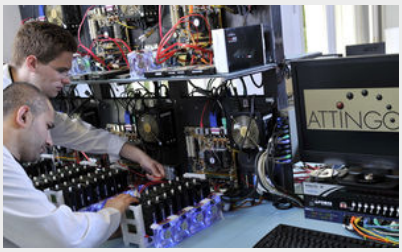
Link zu dieser Meldung

pts20120523006 Computer/Telekommunikation, Unternehmen/Finanzen

Pressefach

Datenrettung: "Bei Daten-Gau sind alle Security-Regeln plötzlich außer Kraft"

Attingo und DeepSec warnen: Datenrettungspartner sollten vorab auditiert werden



Attingo Datenrettung - Labor
[Fotos]

Wien,Hamburg (pts006/23.05.2012/07:35) - Größere Unternehmen verfügen über ausgefeilte Security-Policies und Prozessbeschreibungen vom Backup bis zur Datenwiederherstellung. Was aber häufig unter den Tisch fällt, sind Notfallpläne für den Fall der Fälle: nämlich, wenn sich defekte Datenträger nicht hausintern wiederherstellen lassen und der Gang zum Datenretter erforderlich wird. "Bei kritischen Systemausfällen werden oft plötzlich zentrale Security-Regeln außer Acht gelassen und in Windeseile Server, RAID-Systeme oder Festplatten mit hochsensiblen Informationen an externe Dienstleister übergeben - ohne dass diese im Vorfeld auf Sicherheit geprüft wurden", berichtet René Pfeiffer, Geschäftsführer der Wiener Sicherheitskonferenz DeepSec.

Datendiebe zapfen Dritte an

Die Gefahr dabei: Einige Datenrettungsanbieter schicken defekte Medien an Recovery-Labore im benachbarten Ausland, ohne ihre Kunden explizit davon zu informieren. "Organisierte Datendiebe zapfen aber nicht selten Quellen über Dritte in Insider-Branchen an. Wenn auf diesem Weg Daten verloren gehen oder entwendet werden, hat das Unternehmen den doppelten Schaden", warnt Pfeiffer. Denn es kommt auch noch das Haftungsrisiko hinzu. "Laut Datenschutzgesetz haftet der Eigentümer dann voll für seine Informationen, wenn er es verabsäumt, die 'sichere Datenverarbeitung' durch seinen Dienstleister vorab zu prüfen", erklärt Nicolas Ehrschwendner, Geschäftsführer des heimischen Datenrettungsunternehmens Attingo. De facto fordert das DSG damit die Durchführung von Dienstleister-Audits.

Notfallplan für Datenrettung

Nach dem Motto: "Prüfe deinen Datenretter, so lange die IT-Welt noch in Ordnung ist", bietet Attingo seinen Kunden die gemeinsame Erarbeitung von Notfallplänen schon im Vorfeld an. Der Recovery-Spezialist betreibt sein Reinraumlabor in Wien, so dass ein Versand ins Ausland kein Thema ist. Aber mit seiner Strategie begegnet Attingo einer weiteren Gefahrenquelle: Bei Ausfall von Datenträgern liegt das größte technische Risiko in unsachgemäßen Wiederherstellungsversuchen. "In mehr als 80 Prozent aller Fälle, bei denen selbstständig Rettungsversuche unternommen werden, vergrößert sich der Schaden dadurch letztendlich", berichtet Ehrschwendner aus der täglichen Praxis.

Typische Fehler

"Bei Ausfall von Servern oder RAID-Systemen werden in der Hektik oft hausintern Schritte unternommen, die zwar logisch erscheinen, aber aufgrund der Komplexität gerade diesmal nicht funktionieren", führt er aus. Typische Fehler sind etwa: unkontrolliertes Tauschen defekter Festplatten, Löschen und neu-Anlegen von RAID-Konfigurationen, das Erzwingen des Online-Status von RAIDs oder Ausprobieren von unbekannten Funktionen. Generell sind die Daten auf einem defekten Speichermedium im Reinraumlabor bis zu 100 Prozent rekonstruierbar, solange die betreffenden Sektoren nicht durch falsch veranlasste Vorgänge im Betriebssystem überschrieben wurden. Ein schädigender Vorgang kann aber schon ein simpler Systemstart sein.

Recovery-Partner in die Policy

Vor allem Banken, Health-Care- und Forschungsunternehmen mit sensiblen Daten nutzen verstärkt die Möglichkeit, gemeinsam mit den Recovery-Spezialisten von Attingo eigene Notfallpläne für die Datenrettung auszuarbeiten. Ein wesentlicher Punkt dabei ist, dass der Datenrettungspartner schon auditiert wird, lange bevor eine Katastrophe eintritt. Auch DeepSec Geschäftsführer René Pfeiffer empfiehlt: "Die Auswahl des Datenrettungspartners gehört konsequenterweise in die Security-Policy integriert."

Über DeepSec

PRESSEFACH interactiv

Pressemeldungen als RSS-Feed

E-Mail Abo der Pressemeldungen

Digitale Pressemappe jetzt erstellen (pdf)

Meldungen in Ihre Webseite einbinden

Die DeepSec bringt als neutrale Plattform Sicherheitsexperten aus allen Bereichen zum Gedanken- und Erfahrungsaustausch zusammen. Die Konferenz will aber auch dem verbreiteten Vorurteil entgegenwirken, dass Hacker zwangsläufig Kriminelle sind. "Ganz im Gegenteil. Vielen sogenannten Hackern geht es eher darum, Sicherheitslücken aufzuzeigen und bekannt zu machen. Man kann nur Gefahren beseitigen, die man kennt und die erforscht sind, ganz so wie in anderen Bereichen", so Pfeiffer.
Weitere Informationen zur DeepSec finden Sie hier: https://deepsec.net/

Über Attingo Datenrettung
Attingo Datenrettung ist ein führender, europäischer Anbieter von Datenrettungen. Die Datenrettung befasst sich mit der Rekonstruktion von Daten, die durch Löschung, Formatierung, technische Defekte, Manipulation, Sabotage oder äußere Einflüsse wie Wasser oder Feuer beeinträchtigt wurden. Attingo rettet diese Daten. Das Unternehmen betreibt dazu modernste Reinraumlaboratorien in Wien, Hamburg und Amsterdam und verfügt über Experten mit jahrelanger Erfahrung. Attingo ist in Notfällen für seine Klienten 24/7 erreichbar.
Weitere Informationen: http://www.attingo.com/

Rückfragehinweis: DI Nicolas Ehrschwendner: +43(1)2360101, +49(40)5488756-0, presse@attingo.com
Aussender: Attingo Datenrettung GmbH

(Ende)

Aussender:	Attingo Datenrettung GmbH
Ansprechpartner:	Dipl. Ing. Nicolas Ehrschwendner
Tel.:	+43 / 1 / 236 01 01
E-Mail:	ne@attingo.com
Website:	www.attingo.com

Contact

Michael Kafka

mkafka@deepsec.net

+43/664/4145905

René Pfeiffer

rpfeiffer@deepsec.net

+43/676/5626390

DeepSec GmbH

c/o Mr. Michael Kafka & Mr. René Pfeiffer

Weyringergasse 30a/10

1040 Wien, Austria

VAT ID: ATU63522646

Business registration number: FN 294621 t

Customs EORI code: ATEOS1000025635