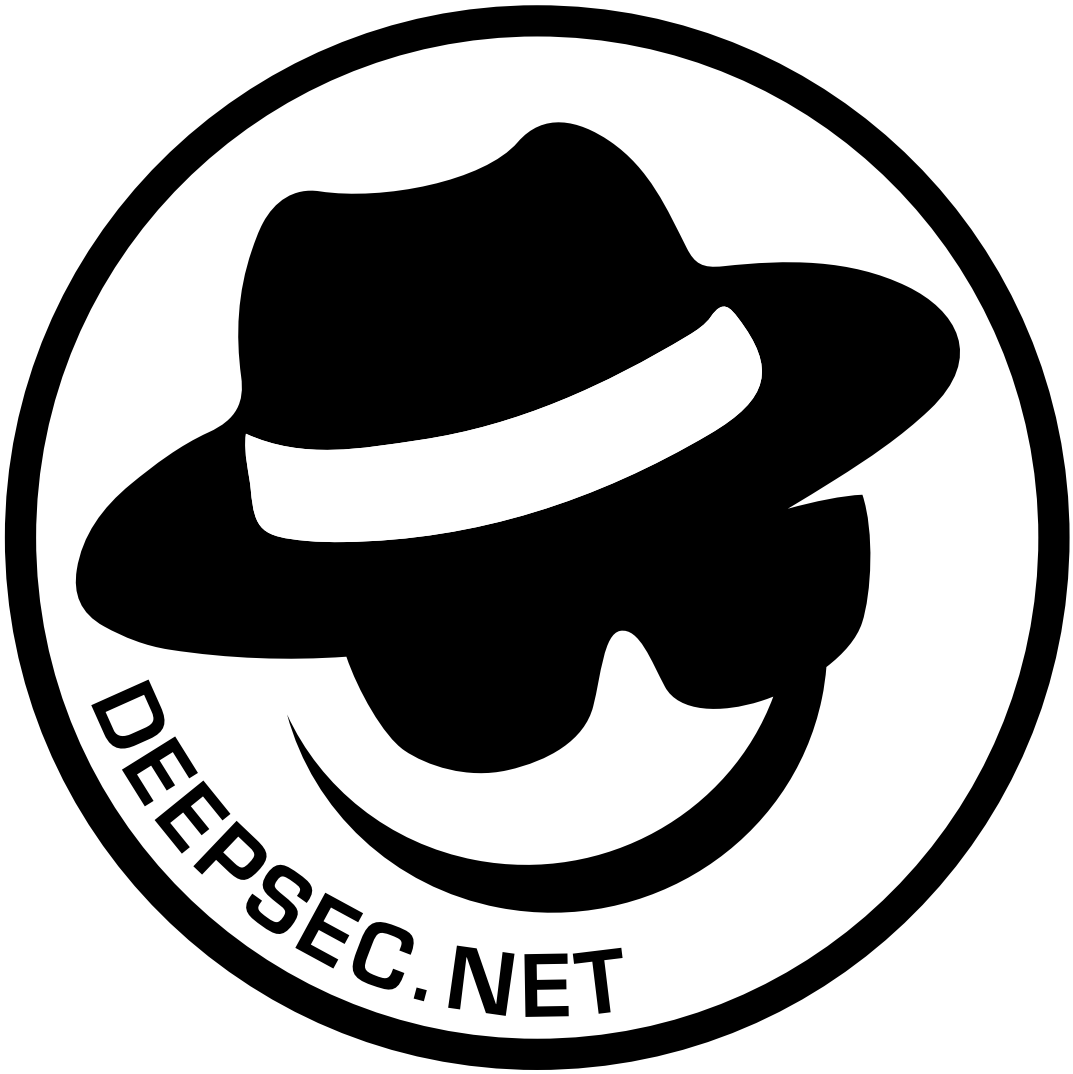


press review 2015

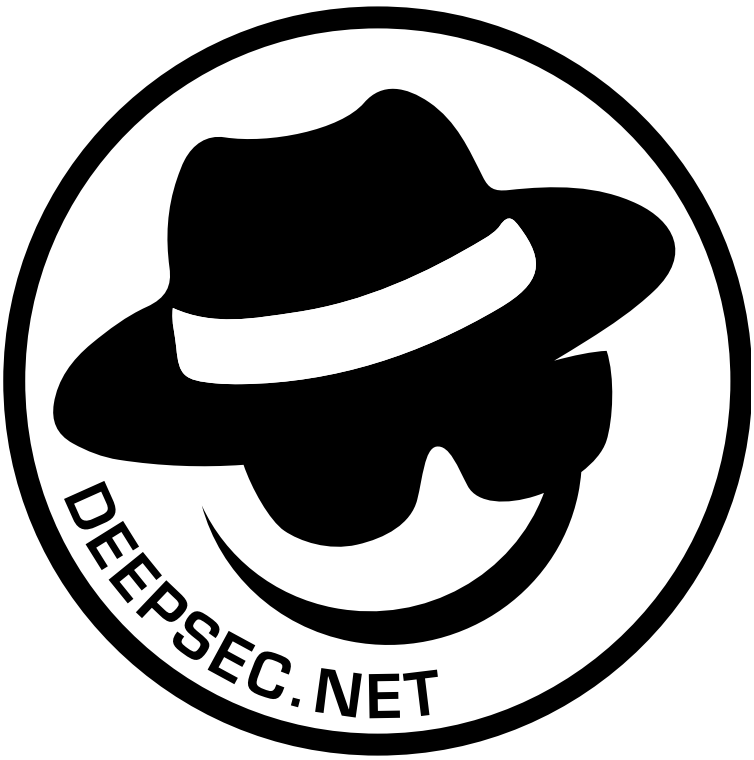
media coverage

2015

contents

press releases
2015

media coverage 2015



http://www.golem.de/news/smart-home-sicherheitsluecken-im-zigbee-protokoll-demonstriert-1511-117657.html

Sicherheitslücken im Zigbee-Protokoll demonstriert

Datum: 26.11.2015

Autor: Hauke Gierow

Deepsec 2015 Sicherheitsforscher haben auf der Sicherheitskonferenz Deepsec in Wien eklatante Mängel in der Sicherheit von Zigbee-Smart-Home-Geräten demonstriert. Es gelang ihnen, ein Türschloss zu übernehmen und zu öffnen.

Smart-Home-Anwendungen sollen den Nutzern das Leben erleichtern. Doch massive Sicherheitslücken könnten das Gegenteil bewirken. Die Sicherheitsforscher Tobias Zillner und Florian Eichelberger haben auf der Sicherheitskonferenz Deepsec in Wien einen praktischen Angriff auf das Smart-Home-Vernetzungsprotokoll vorgestellt. Mit Hilfe eines Software-Defined-Radio, eines Raspberry Pi und einer selbstgeschriebenen Software gelang es ihnen, ein smartes Türschloss zu öffnen und zu schließen. Unter dem Zigbee-Label produzieren zahlreiche Hersteller verschiedene Geräte - nicht alle weisen die im Folgenden beschriebenen Lücken auf.

Eigentlich verfügt das auf dem Funkstandard IEEE 802.15.4 basierende Zigbee-Home-Automation-Protokoll in Version 1.2 über einigermaßen solide Grundlagen - die Geräte kommunizieren auf dem Netzwerk-Layer mit einer 128-Bit-AES-CCM-Verschlüsselung - zumindest theoretisch. Denn wer als Hersteller eine Zigbee-Zertifizierung erhalten will, muss nach Angaben von Zillner einen sogenannten Rückfallmodus einbauen: Es gibt weiterhin eine Verschlüsselung, aber der Schlüsselaustausch wird mit einem öffentlich bekannten Schlüssel abgesichert und kann daher mitgelesen werden.

Zillner und Eichelberger setzen für ihren Angriff ein Software Defined Radio zum Mithören des Funkverkehrs und ein Raspberry Pi mit dem Funkmodul Raspbee ein, um Befehle zu versenden. Außerdem nutzen sie einen handelsüblichen Zigbee-Router. Das im Test verwendete Routermodell geben Zillner und Eichelberger noch nicht bekannt: “Wir haben den Hersteller über die Probleme informiert und wollen ihm die Chance geben, die Probleme zu fixen”, sagte Zillner Golem.de.

Im Test belauschen die Sicherheitsforscher den Netzwerk-Traffic zunächst passiv. Die Geräte senden in regelmäßigen Abständen (im Normalfall alle fünf Sekunden) eine Anfrage an den Zigbee-Router, um Zustandsänderungen abzufragen. Dabei senden die Geräte auch ihre eigene ID mit - die mit Tools wie Wireshark abgefangen werden kann. Eine Verschlüsselung auf Anwendungsebene hatten die von den Sicherheitsforschern

getestete Geräten nicht - auch sicherheitsrelevante Geräte wie Türschlösser hätten eigentlich einen Application Link Key verwenden müssen.

Unsicherer Schlüsselaustausch kann forciert werden

Mit der ID gelang es den Sicherheitsforschern, einen Schlüsselaustausch zu forcieren. Der sogenannte “Insecure Rejoin” ist Teil der Zigbee-Spezifikation - um ihn auszulösen, bedarf es nur der Geräte-ID. Alle von den Sicherheitsforschern getesteten Zigbee-Geräte nutzten nur den bekannten TC-Fallback-Schlüssel und waren somit angreifbar.

Nach Aussage des deutschen Zigbee-Herstellers Ubisys soll das Problem mit der kommenden Version 3 des Standards behoben werden - nachprüfbar ist das bislang nicht, weil die Spezifikationen noch nicht veröffentlicht wurden. Es gäbe einen weiteren Weg, einen unsicheren Schlüsselaustausch zu belauschen.
“Wenn die Funkverbindung lange genug gestört wird, melden die Geräte sich nach einiger Zeit automatisch neu im Netzwerk an”, sagte Zillner. Auch dann kann der Schlüssel ausgelesen werden.

Die Sicherheitsforscher entwickelten für den Angriff die Software Secbee, die bei Github verfügbar ist. Mit Hilfe der Software belauschen sie zunächst den Funkverkehr der Geräte im Netzwerk und lösen dann den unsicheren Schlüsselaustausch aus. Ist das erledigt, kann die Kontrolle über das Türschloss übernommen werden. Pikant: Wird über die Software der Befehl zum Öffnen des Türschlosses gegeben, bekommt die Smartphone-App davon nichts mit. Sie denkt weiterhin, dass die Tür sicher verschlossen ist. Der Angriff soll es auch ermöglichen, die auf dem Türschloss der Marke Yale eingestellte PIN zu ändern, um sich später Zutritt zu verschaffen.

Zigbee wird auch in anderen Bereichen eingesetzt

Zigbee findet nicht nur bei intelligenten Lampen und Türschlössern Verwendung, sondern wird auch genutzt, um Fabriken zu vernetzen. Hier dürften die Sicherheitsimplikationen der gezeigten Lücken noch weitaus gravierender sein als im privaten Umfeld. Auch an Bord von Raumstationen soll das System zum Einsatz kommen.
Die Hersteller sehen in den demonstrierten Angriffen nach Angabe von Zillner kein Problem: Der unverschlüsselt ablaufende Koppelungsprozess würde nur wenig Zeit in Anspruch nehmen, außerdem sei die Reichweite sehr begrenzt. Ein Angriff wäre daher nicht realistisch.

Am Ende ihres Vortrages zeigten die beiden Forscher noch einen weiteren praktischen Angriff. Mittels eines üblichen Lockpicking-Werkzeuges gelang es ihnen, das etwa 300 Euro teure Schloss innerhalb weniger Sekunden zu öffnen - ganz ohne Elektronik.

Gierow/Golem.de)

Smart Home: Sicherheitslücken im Zigbee-Protokoll demonstriert

Deepsec 2015 Sicherheitsforscher haben auf der Sicherheitskonferenz Deepsec in Wien eklatante Mängel in der Sicherheit von Zigbee-Smart-Home-Geräten demonstriert. Es gelang ihnen, ein Türschloss zu übernehmen und zu öffnen.

Smart-Home-Anwendungen sollen den Nutzern das Leben erleichtern. Doch massive Sicherheitslücken könnten das Gegenteil bewirken. Die Sicherheitsforscher Tobias Zillner und Florian Eichelberger haben auf der Sicherheitskonferenz Deepsec in Wien einen praktischen Angriff auf das Smart-Home-Vernetzungsprotokoll vorgestellt. Mit Hilfe eines Software-Defined-Radio, eines Raspberry Pi und einer selbstgeschriebenen Software gelang es ihnen, ein smartes Türschloss zu öffnen und zu schließen. Unter dem Zigbee-Label produzieren zahlreiche Hersteller verschiedene Geräte - nicht alle weisen die im Folgenden beschriebenen Lücken auf.

Eigentlich verfügt das auf dem Funkstandard IEEE 802.15.4 basierende Zigbee-Home-Automation-Protokoll in Version 1.2 über einigermaßen solide Grundlagen - die Geräte kommunizieren auf dem Netzwerk-Layer mit einer 128-Bit-AES-CCM-Verschlüsselung - zumindest theoretisch. Denn wer als Hersteller eine Zigbee-Zertifizierung erhalten will, muss nach Angaben von Zillner einen sogenannten Rückfallmodus einbauen: Es gibt weiterhin eine Verschlüsselung, aber der Schlüsselaustausch wird mit einem öffentlich bekannten Schlüssel abgesichert und kann daher mitgelesen werden.

Video: Smart Home Hack - Bericht (0:45)

Gierow/Golem.de)

Unsicherer Schlüsselaustausch kann forciert werden

Mit der ID gelang es den Sicherheitsforschern, einen Schlüsselaustausch zu forcieren. Der sogenannte "Insecure Rejoin" ist Teil der Zigbee-Spezifikation - um ihn auszulösen, bedarf es nur der Geräte-ID. Alle von den Sicherheitsforschern getesteten Zigbee-Geräte nutzten nur den bekannten TC-Fallback-Schlüssel und waren somit angreifbar.

Nach Aussage des deutschen Zigbee-Herstellers Ubisys soll das Problem mit der kommenden Version 3 des Standards behoben werden - nachprüfbar ist das bislang nicht, weil die Spezifikationen noch nicht veröffentlicht wurden. Es gäbe einen weiteren Weg, einen unsicheren Schlüsselaustausch zu belauschen. *"Wenn die Funkverbindung lange genug gestört wird, melden die Geräte sich nach einiger Zeit automatisch neu im Netzwerk an"*, sagte Zillner. Auch dann kann der Schlüssel ausgelesen werden.

Die Sicherheitsforscher entwickelten für den Angriff die Software Secbee, die bei Github verfügbar ist. Mit Hilfe der Software belauschen sie zunächst den Funkverkehr der Geräte im Netzwerk und lösen dann den unsicheren Schlüsselaustausch aus. Ist das erledigt, kann die Kontrolle über das Türschloss übernommen werden. Pikant: Wird über die Software der Befehl zum Öffnen des Türschlosses gegeben, bekommt die Smartphone-App davon nichts mit. Sie denkt weiterhin, dass die Tür sicher verschlossen ist. Der Angriff soll es auch ermöglichen, die auf dem Türschloss der Marke Yale eingestellte PIN zu ändern, um sich später Zutritt zu verschaffen.

Zigbee wird auch in anderen Bereichen eingesetzt

Zigbee findet nicht nur bei intelligenten Lampen und Türschlössern Verwendung, sondern wird auch genutzt, um Fabriken zu vernetzen. Hier dürften die Sicherheitsimplikationen der gezeigten Lücken noch weitaus gravierender sein als im privaten Umfeld. Auch an Bord von Raumstationen soll das System zum Einsatz kommen.

Die Hersteller sehen in den demonstrierten Angriffen nach Angabe von Zillner kein Problem: Der unverschlüsselt ablaufende Koppelungsprozess würde nur wenig Zeit in Anspruch nehmen, außerdem sei die Reichweite sehr begrenzt. Ein Angriff wäre daher nicht realistisch.

Am Ende ihres Vortrages zeigten die beiden Forscher noch einen weiteren praktischen Angriff. Mittels eines üblichen Lockpicking-Werkzeuges gelang es ihnen, das etwa 300 Euro teure Schloss innerhalb weniger Sekunden zu öffnen - ganz ohne Elektronik. ■

1
2

Smart Home: Sicherheitslücken im Zigbee-Protokoll demonstriert

http://www.csoonline.com/article/3007058/techology-business/notes-from-vienna-deepsec-and-bsides.html

Notes From Vienna: Deepsec & BSides

Datum: 23.11.2015

Autor: Dave Lewis

It was a cold day in Vienna yesterday. It was simply wonderful to wander through the streets of the old city in search of great coffee. Soon I found myself sitting in the Cafe Central with a pot of coffee and my thoughts. This is a coffee shop that was once the hang out of none other than Sigmund Freud. Seemed like as good a place as any to reflect. In the proceeding days leading up to this point I had the privilege of being able to speak at the Deepsec and BSides Vienna conferences.

Both conferences were really well executed and an overall they were very enjoyable experiences. At the speaker's dinner on Thursday night I found myself sitting with people from London, Paris, Rome, Krakow and others all discussing security issues. It was a marvel to me to see all of us sharing ideas with each other. What was even more poignant was that the need for us to do a better job at imparting security ideas with those outside of the sphere that we live in.

The news after the atrocious acts that took place in Paris on November 13, 2015 has devolved into political opportunists trying very hard to capitalize on the tragedy. There has been a seemingly co-orindated disinformation campaign to get the message out that encryption is a large part of the problem as it pertains to terrorism.

Um, whut?

Let us look at the information that is available to us at the time of this writing. We see that the people who launched the attacks in Paris all knew each other, communicated via SMS and discussed issues in person. Encryption, based on the information available, was NOT part of the equation. So, why do we find this conversation spinning up? Just a week ago I wrote about the problem of the demonization of encryption and VPN services. I had even spoken out against this tide of foolishness while I was on stage at Deepsec.

Now, we see talking heads like U.S. Senator Mark Warner complaining that we need to fight against encryption as it helps the terrorists. This is deliberately misleading and frustrating. As we saw with the Paris attackers there was no encryption involved (to the best of our knowledge as of publishing time). Political opportunism on this discussion only penalizes legitimate people who use security tools like VPN. The politicos want to have fundamentally broken

encryption so that they can have unfettered access to internet communications.

It's a good thing that I didn't see James Bond SPECTRE last night. Otherwise I'd be even more paranoid. Oh...wait.

To put a fine point on it, my friend Wim Remes commented on this on the social media platform Twitter when he said, "would you leave a key to your house at the police station? exactly. that's why we can't have cryptography with backdoors."

This goes to the heart of the matter. The ones that control the message can steer the discussion.
Information security practitioners need to get the message beyond the confines of our own echo chamber.
If we fail to do so, we run the very real risk of finding ourselves trying to secure our enterprises from attack with duct tape and bailing wire. That is, until someone decides those are dangerous as well.

BRICK OF ENLIGHTENMENT
By Dave Lewis

About |
Bringing fire to the village.

NEWS

Notes From Vienna: Deepsec & BSides

CSO | Nov 23, 2015 3:00 AM PT

It was a cold day in Vienna yesterday. It was simply wonderful to wander through the streets of the old city in search of great coffee. Soon I found myself sitting in the Cafe Central with a pot of coffee and my thoughts. This is a coffee shop that was once the hang out of none other than Sigmund Freud. Seemed like as good a place as any to reflect. In the proceeding days leading up to this point I had the privilege of being able to speak at the Deepsec and BSides Vienna conferences.

Both conferences were really well executed and an overall they were very enjoyable experiences. At the speaker's dinner on Thursday night I found myself sitting with people from London, Paris, Rome, Krakow and others all discussing security issues. It was a marvel to me to see all of us sharing ideas with each other. What was even more poignant was that the need for us to do a better job at imparting security ideas with those outside of the sphere that we live in.

The news after the atrocious acts that took place in Paris on November 13, 2015 has devolved into political opportunists trying very hard to capitalize on the tragedy. There has been a seemingly co-orindated disinformation campaign to get the message out that encryption is a large part of the problem as it pertains to terrorism.

Um, whut?

Let us look at the information that is available to us at the time of this writing. We see that the people who launched the attacks in Paris all knew each other, communicated via SMS and discussed issues in person. Encryption, based on the information available, was NOT part of the

equation. So, why do we find this conversation spinning up? Just a week ago I wrote about the problem of the demonization of encryption and VPN services. I had even spoken out against this tide of foolishness while I was on stage at Deepsec.

Now, we see talking heads like U.S. Senator Mark Warner complaining that we need to fight against encryption as it helps the terrorists. This is deliberately misleading and frustrating. As we saw with the Paris attackers there was no encryption involved (to the best of our knowledge as of publishing time). Political opportunism on this discussion only penalizes legitimate people who use security tools like VPN. The politicos want to have fundamentally broken encryption so that they can have unfettered access to internet communications.

It's a good thing that I didn't see James Bond SPECTRE last night. Otherwise I'd be even more paranoid. Oh...wait.

To put a fine point on it, my friend Wim Remes commented on this on the social media platform Twitter when he said, “would you leave a key to your house at the police station? exactly. that's why we can't have cryptography with backdoors.”

This goes to the heart of the matter. The ones that control the message can steer the discussion. Information security practitioners need to get the message beyond the confines of our own echo chamber. If we fail to do so, we run the very real risk of finding ourselves trying to secure our enterprises from attack with duct tape and bailing wire. That is, until someone decides those are dangerous as well.

Dave Lewis — *Global Security Advocate*

Dave has over 15 years industry experience. He has extensive experience in IT operations and management. Currently, Dave is a Senior Security Advocate for Akamai Technologies .

Insider: Business continuity and disaster recovery planning: The basics

View Comments

You Might Like

http://www.heise.de/security/meldung/Deepsec-ZigBee-macht-Smart-Home-zum-offenen-Haus-3010287.html

Deepsec: ZigBee macht Smart Home zum offenen Haus

Datum: 21.11.2015

Autor: Daniel AJ Sokolov

ZigBee-Funknetze weisen nach neuen Erkenntnissen von Sicherheitsforschern eklatante Sicherheitsmängel auf. Die Technik wird beispielsweise bei der Steuerung von Türschlössern eingesetzt.

ZigBee bildet energieeffiziente Mesh-Netzwerke, über die sich Geräte drahtlos miteinander verbinden lassen. Das ist zwar praktisch, aber offenbar ist ein Großteil der aktuellen Gerätegeneration anfällig für Attacken. Zumindest die für Smart Homes entwickelte ZigBee-Variante Home Automation 1.2 weist einen grotesken Konstruktionsfehler auf: Angreifer können darüber die Kontrolle über die vernetzten Geräte übernehmen.

Das haben die Security-Forscher Florian Eichelberger und Tobias Zillner von der Firma Cognosec am Freitag auf der Veranstaltung Deepsec in Wien gezeigt. Ihr Demonstrationsobjekt war ein programmierbares Türschloss. Spezielle Hardware brauchten sie nicht: Ein Laptop, ein Software Defined Radio zum Lauschen sowie ein Raspberry Pi mit ZigBee-Modul zum Absetzen von Befehlen reichten aus. Für Angriffe aus größeren Entfernungen wären noch gerichtete Antennen hilfreich. Als Software kommt die von Cognosec auf Github veröffentliche SecBee-Suite zum Einsatz.

Es klingt fast wie ein Witz: Grundsätzlich kommunizieren die Geräte verschlüsselt, die gemäß der ZigBee-Variante Home Automation 1.2 (HA) ausgelegt sind. Jedoch schreibt das ZigBee-Konsortium vor, dass alle Geräte ein und dasselbe Schlüsselpaar (Fallback Key) kennen und akzeptieren müssen – und dieses asymmetrische Schlüsselpaar ist öffentlich bekannt.

Verschlüsselung als Satire

Beim üblichen Betrieb kommt ein anderer, symmetrischer Schlüssel zum Einsatz. Diesen muss man geheim halten, weil ein HA-Netz immer denselben verwendet. Will ein Nutzer oder Administrator ein neues Gerät an einem Netz anmelden, stößt er dazu die Kopplung an. Dabei fordert das neue Gerät den symmetrischen Schlüssel an – weil es ihn ja noch nicht kennt. Den erhält es dann über Funk postwendend.

Diese Übergabe wird zwar auch verschlüsselt, aber lediglich mit dem öffentlich bekannten, asymmetrischen Fallback Key, der ja bekannt ist. Angreifer, die diesen Vorgang belauschen, können die Übergabe mitlesen und

entschlüsseln, erfahren also den symmetrischen Netzschlüssel. “Das ist genau so sicher wie ein Schlüsselaustausch in plain Text”, sagte Zillner. Damit kann der Angreifer nicht nur die gesamte Kommunikation im HA-Netz mitschneiden, sondern auch selbst Befehle übermitteln.

Im Fall des programmierbaren Türschlosses mit PIN-Eingabe sind noch weitere schwerwiegende Mängel aufgefallen. Angreifer können eine Tür aus der Ferne öffnen und schließen und es lassen sich auch PINs löschen oder neue anlegen. Diese kann ein Eindringling zu einem späteren Zeitpunkt für einen ungehinderten Zutritt nutzen. Aber die eigentlich zur Kontrolle vorgesehene App und deren Pendant in der Cloud bekommen von den Umprogrammierungen nichts mit. Und sie halten eine auf diese Weise geöffnete Tür selbst dann noch für verschlossen, wenn sie bereits sperrangelweit offen steht.

Abhilfe: Entsorgen

Bei den meisten ZigBee-Geräten gibt es keine Möglichkeit, Sicherheitseinstellungen vorzunehmen. Selbst einen Reset-Knopf sucht man in der Regel ebenso vergeblich wie eine Möglichkeit für ein Firmwareupdate. Ein einmal kompromittiertes Gerät muss also im übertragenen wie auch im wörtlichen Sinn entsorgt werden. Ein Firmwareupdate würde jedoch auch nur dann helfen, wenn die Entwickler der Spezifikation die gesamte Authentifizierung und Verschlüsselung überarbeiten würden.

Es kommt aber noch schlimmer: “Ich kann immer einen Schlüsselaustausch auslösen, um ihn mitzulesen”, erklärte Zillner. Der Angreifer muss nicht einmal auf die Chance warten, die erstmalige Einrichtung eines neuen Geräts zu belauschen. Er kann dem Netz einfach suggerieren, dass ein Gerät abwesend war und sich erneut verbinden möchte.

Dafür sendet er eine Rejoin-Anfrage im Namen eines Geräts. Dafür reicht die Kenntnis der Systemadresse dieses Geräts und des ZigBee-Routers aus. Diese Adressen lassen sich durch Mitschneiden des echten Netzverkehrs eruieren. “Bei Rejoins gibt es null Sicherheit”, so Zillner.

Jamming-Session

Und wer sich den Aufwand der Rejoin-Anfrage sparen möchte, kann einfach den ZigBee-Funk stören, bis sich die Geräte von selbst neu anmelden müssen. Und Angreifer können sogar ein Wettrennen zwischen dem angreifenden und dem rechtmäßig eingebuchten Gerät umgehen, denn ZigBee-Router versuchen die Kontaktaufnahme zunächst auf den unteren Frequenzbändern. Die meisten Geräte verwenden aber höherfrequente Bänder. Der Angreifer muss also lediglich das niedrigste Frequenzband verwenden, um dem rechtmäßig eingebuchten

zuvorzukommen.

Light Link

Für die Anbindung von Leuchtmitteln gibt es das einfachere ZigBee-Protokoll Light Link 1.0. Entsprechend zertifizierte Geräte verwenden alle denselben Master Key, der jedoch ebenfalls an die Öffentlichkeit gelangt ist. Zwar soll die Anbindung einer Glühbirne eigentlich nur dann gelingen, wenn das Kontrollgerät bis auf wenige Zentimeter herangeführt wird. Mit Richtantennen konnten Eichelberger und Zillner aber auch in größerem Abstand die Kontrolle übernehmen.

Nun klingt das bei Glühbirnen zunächst nicht weiter schlimm. Doch wenn in einem großen Hotel oder Einkaufszentrum plötzlich alle Lichter ausgehen, kann das unangenehme Folgen haben. Und schließlich wird der ZigBee-Infrastruktur auch der Mesh-Ansatz zum Nachteil: Es reicht, in Funkreichweite irgendeines Zipfels des ZigBee-Netzes zu sein. Dank Mesh-Architektur verbreiten sich Befehle selbsttätig im gesamten Netz.

Künftige ZigBee-Profile abwärtskompatibel

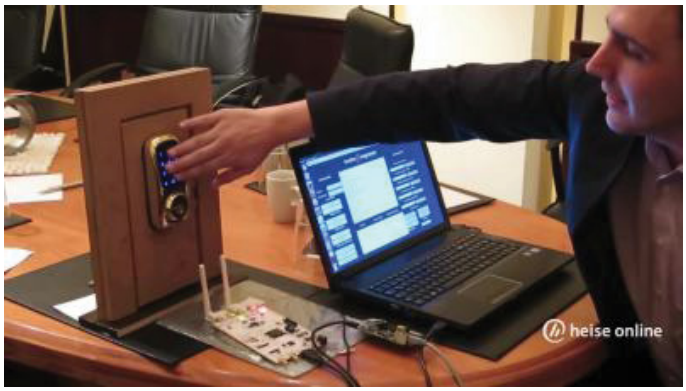
Einfachere Angriffe wie die Replay-Attacken auf ZigBee sind bereits vor fünf Jahren gelungen. Derzeit arbeitet das ZigBee-Konsortium an neuen Versionen der Home-Automation und der Light-Link-Spezifikationen. Damit soll ein Teil der Sicherheitsprobleme behoben werden. Jedoch gibt es keine Updatemöglichkeit für bereits verkaufte Geräte. Und die neuen Profile sollen rückwärtskompatibel werden.

Unter der Marke ZigBee gibt es noch zahlreiche weitere Profile, etwa für den Gesundheitsbereich, Luft- und Raumfahrt oder die Energieversorgung. Diese hat Cognosec bislang nicht getestet. Ihre bisherigen Erkenntnisse hat die Firma in einem Whitepaper zusammengefasst.

21.11.2015 13:01 Uhr – Daniel AJ Sokolov

den symmetrischen Netzschlüssel. "Das ist genau so sicher wie ein Schlüsselaustausch in plain Text", sagte Zillner. Damit kann der Angreifer nicht nur die gesamte Kommunikation im HA-Netz mitschneiden, sondern auch selbst Befehle übermitteln.

Im Fall des programmierbaren Türschlosses mit PIN-Eingabe sind noch weitere schwerwiegende Mängel aufgefallen. Angreifer können eine Tür aus der Ferne öffnen und schließen und es lassen sich auch PINs löschen oder neue anlegen. Diese kann ein Eindringling zu einem späteren Zeitpunkt für einen ungehinderten Zutritt nutzen. Aber die eigentlich zur Kontrolle vorgesehene App und deren Pendant in der Cloud bekommen von den Umprogrammierungen nichts mit. Und sie halten eine auf diese Weise geöffnete Tür selbst dann noch für verschlossen, wenn sie bereits sperrangelweit offen steht.



Abhilfe: Entsorgen

Bei den meisten ZigBee-Geräten gibt es keine Möglichkeit, Sicherheitseinstellungen vorzunehmen. Selbst einen Reset-Knopf sucht man in der Regel ebenso vergeblich wie eine Möglichkeit für ein Firmwareupdate. Ein einmal kompromittiertes Gerät muss also im übertragenen wie auch im wörtlichen Sinn entsorgt werden. Ein Firmwareupdate würde jedoch auch nur dann helfen, wenn die Entwickler der Spezifikation die gesamte Authentifizierung und Verschlüsselung überarbeiten würden.

ZigBee-Modul [http://www.heise.de/security/meldung/Deepsec-ZigBee-macht-Smart-Home-zum-offenen-Haus-3010287.html?view=zoom;zoom=2]
Bild: AutolycusQ **CC-BY-SA 3.0** [https://creativecommons.org/licenses/by-sa/3.0/deed.en]

Es kommt aber noch schlimmer: "Ich kann immer einen Schlüsselaustausch auslösen, um ihn mitzulesen", erklärte Zillner. Der Angreifer muss nicht einmal auf die Chance warten, die erstmalige Einrichtung eines neuen Geräts zu belauschen. Er kann dem Netz einfach suggerieren, dass ein Gerät abwesend war und sich erneut verbinden möchte.

Dafür sendet er eine Rejoin-Anfrage im Namen eines Geräts. Dafür reicht die Kenntnis der Systemadresse dieses Geräts und des ZigBee-Routers aus. Diese Adressen lassen sich durch Mitschneiden des echten Netzverkehrs eruieren. "Bei Rejoins gibt es null Sicherheit", so Zillner.

Jamming-Session

Und wer sich den Aufwand der Rejoin-Anfrage sparen möchte, kann einfach den ZigBee-Funk stören, bis sich die Geräte von selbst neu anmelden müssen. Und Angreifer können sogar ein Wettrennen zwischen dem angreifenden und dem rechtmäßig eingebuchten Gerät umgehen, denn ZigBee-Router versuchen die Kontaktaufnahme zunächst auf den unteren Frequenzbändern. Die meisten Geräte verwenden aber höherfrequente Bänder. Der Angreifer muss also lediglich das niedrigste Frequenzband verwenden, um dem rechtmäßig eingebuchten zuvorzukommen.

Light Link

Für die Anbindung von Leuchtmitteln gibt es das einfachere ZigBee-Protokoll Light Link 1.0. Entsprechend zertifizierte Geräte verwenden alle denselben Master Key, der jedoch ebenfalls an die Öffentlichkeit gelangt ist. Zwar soll die Anbindung einer Glühbirne eigentlich nur dann gelingen, wenn das Kontrollgerät bis auf wenige

Zentimeter herangeführt wird. Mit Richtantennen konnten Eichelberger und Zillner aber auch in größerem Abstand die Kontrolle übernehmen.

Nun klingt das bei Glühbirnen zunächst nicht weiter schlimm. Doch wenn in einem großen Hotel oder Einkaufszentrum plötzlich alle Lichter ausgehen, kann das unangenehme Folgen haben. Und schließlich wird der ZigBee-Infrastruktur auch der Mesh-Ansatz zum Nachteil: Es reicht, in Funkreichweite irgendeines Zipfels des ZigBee-Netzes zu sein. Dank Mesh-Architektur verbreiten sich Befehle selbsttätig im gesamten Netz.

Künftige ZigBee-Profile abwärtskompatibel

Einfachere Angriffe wie die **Replay-Attacken auf ZigBee** [http://www.heise.de/security/meldung/ZigBee-Angriff-der-Killerbiene-948880.html] sind bereits vor fünf Jahren gelungen. Derzeit arbeitet das ZigBee-Konsortium an neuen Versionen der Home-Automation und der Light-Link-Spezifikationen. Damit soll ein Teil der Sicherheitsprobleme behoben werden. Jedoch gibt es keine Updatemöglichkeit für bereits verkaufte Geräte. Und die neuen Profile sollen rückwärtskompatibel werden.

Unter der Marke ZigBee gibt es noch zahlreiche weitere Profile, etwa für den Gesundheitsbereich, Luft- und Raumfahrt oder die Energieversorgung. Diese hat Cognosec bislang nicht getestet. Ihre bisherigen Erkenntnisse hat die Firma in einem **Whitepaper** [http://cognosec.com/zigbee_exploited_8F_Ca9.pdf] zusammengefasst.

[Update (16:15): Video hinzugefügt**]** (**ds** [mailto:ds@heise.de])

Kommentare lesen (196 Beiträge)
[http://www.heise.de/forum/heise-Security/News-Kommentare/Deepsec-ZigBee-macht-Smart-Home-zum-offenen-Haus/forum-249892/comment/]

Forum zum Thema: **Penetration Tests** [http://www.heise.de/forum/heise-Security/Themen-Hilfe/Penetration-Tests/forum-33373/comment/]

http://heise.de/-3010287 [http://heise.de/-3010287]

Drucken [http://www.heise.de/security/meldung/Deepsec-ZigBee-macht-Smart-Home-zum-offenen-Haus-3010287.html?view=print]

Mehr zum Thema **Smart Home** [http://www.heise.de/thema/Smart-Home] **Sicherheitslücken** [http://www.heise.de/thema/Sicherheitsl%C3%BCcken] **Internet der Dinge** [http://www.heise.de/thema/Internet-der-Dinge] **ZigBee** [http://www.heise.de/thema/ZigBee]

http://derstandard.at/2000026060258/Geheimdienstexperten-Paris-zeigt-Versagen-der-Massenueberwachung

Geheimdienstexperten: “Paris zeigt Versagen der Massenüberwachung”

Datum: 20.11.2015

Autor: Andreas Proschofsky

Flächendeckendes Ausspionieren funktioniere nicht: Duncan Campbell und James Bamford zur Deepsec in Wien

Die Diskussion über die Terroranschläge von Paris geht natürlich auch an einer Konferenz zu IT-Sicherheit nicht spurlos vorüber. Zumal die dieser Tage zum mittlerweile neunten Mal in Wien abgehaltene Deepsec dieses Jahr gleich zwei Journalisten eingeladen hat, die sich seit Jahren kritisch mit Geheimdiensten und deren Überwachungspraxis auseinandersetzen. Und sowohl James Bamford als auch Duncan Campbell sind sich einig: Die umgehend angelaufene Diskussion über den Ausbau der Internetüberwachung gehe vollkommen an der Realität vorbei.

Vollkommenes Versagen

Wenn Paris eines eindrücklich gezeigt habe, dann das “vollkommene Versagen der Massenüberwachung”, wie Campbell in der einleitenden Keynote zur Konferenz betonte. Diese funktioniere schlicht nicht, da es in der breiten Masse der Daten unmöglich sei, das Relevante herauszufinden, egal wie mächtig die Rechensysteme der NSA sein mögen. Und diese Erkenntnis sei keineswegs neu, seit Jahrzehnten zeige sich immer wieder das gleiche Bild, wie der seit 1975 zu Geheimdiensten arbeitende Journalist betont.

Falsche Herangehensweise

Es gebe bis dato praktisch keine belegten Beispiel für Erfolge der Massenüberwachung. Dafür zahlreiche Gegenbeispiele: Weder konnte 9/11 verhindert werden noch die Anschläge auf die Londoner U-Bahn im Jahr 2005 oder die Terrorangriffe auf die Redaktion der Satirezeitschrift “Charlie Hebdo” und den Boston-Marathon. Und das, obwohl in all diesen Fällen die Angreifer vorher bereits auf dem Radar der Behörden waren. Das Problem sei eben nicht der Mangel an Daten, sondern deren Analyse. Schlicht zu viel Der NSA sei die Untauglichkeit der Massenüberwachung übrigens durchaus bewusst, wie Campbell betont. Immer wieder gebe es in den Snowden-Dokumenten Hinweise darauf, dass die Behörde mit dem Datenwust kämpfe und künstliche Begrenzungen vornehmen müsse, um überhaupt noch etwas analysieren zu können.

Geschichtsexkurs

Der Umstand, dass die Geheimdienste trotzdem immer mehr Daten wollen, sei schlicht auf die ihnen immanente

Logik zurückzuführen, attestiert Bamford, der sein erstes Buch über die NSA bereits im Jahr 1982 publiziert hat. Man dürfe zudem nicht vergessen, wie die NSA entstanden sei: Sie sollte die Funkübertragung der UdSSR abhören, um eine Art zweites Pearl Harbor zu verhindern. Das sei einst auch tatsächlich relativ einfach umfassend zu bewerkstelligen gewesen, allerdings skaliere dieser Ansatz schlicht nicht, wie Bamford gegenüber dem STANDARD betont. Die NSA störe sich daran aber nicht und sammle immer mehr Daten und Macht um ihrer selbst willen. Realitätscheck Freilich geben sich beide nicht der Illusion hin, dass gerade in der aktuellen Situation eine Trendwende zu erwarten ist. Die Anschläge von Paris werden eine weitere Aushöhlung von Bürgerrechten und eine Ausweitung geheimdienstlicher Befugnisse zur Folge haben und damit auch all jene zarten Verbesserungen, die die Snowden-Enthüllungen ausgelöst haben, wieder zunichtemachen.

Keine Hintertüren

An die Umsetzung einer derzeit vieldiskutierten Maßnahme glaubt Campbell hingegen nicht: Hintertüren für Verschlüsselungssoftware würden nicht kommen, und zwar aus einem ganz einfachen Grund. Diese seien schlicht technischer Nonsens. Befürworter würden sich hier eine Art magische Lösung vorstellen, die in der Realität nicht umsetzbar sei. Eine Crypto-Backdoor für die NSA würde bedeuten, dass umgehend auch jedes andere Land entsprechende eigene Zugänge verlangen würde – von China bis Saudi-Arabien. Und das sei nur eine Hürde von vielen. Aber selbst wenn man es irgendwie schaffen würde, all diese Hürden zu überwinden, was würde Terroristen davon abhalten, eine eigene Software ohne Backdoor einzusetzen? Diese würden all die Verschlüsselungsbeschränkungen also nicht treffen, Unternehmen, die sicher kommunizieren wollen, hingegen sehr wohl.

Mehr Verschlüsselung statt weniger

Auch wenn es zunächst paradox klingen mag, die Lösung für die Krise der Geheimdienste sieht Bamford in einem grundlegenden Kurswechsel, und er verweist dabei auf Edward Snowden, den er vergangenes Jahr für ein ausführliches Interview mit dem US-Magazin “Wired” besucht hat. Dieser sei davon überzeugt, dass in einer Welt, in der alle effektive Ende-zu-Ende-Verschlüsselung benutzen, die Geheimdienste gezwungen würden, wieder auf gezielte Überwachung und klassische Polizeiarbeit zu setzen. Immerhin verhindere auch die beste Verschlüsselung nicht den direkten Zugriff auf den Computer einer Zielperson, sehr wohl aber die Aushöhlung der Privatsphäre der

Gesamtbevölkerung.

Geheimdienstexperten: "Paris zeigt Versagen der Massenüberwachung"

ANDREAS PROSCHOFSKY
20. November 2015, 08:54

foto: andreas proschofsky / standard
Duncan Campbell bei seiner Keynote zur diesjährigen Ausgabe der Sicherheitskonferenz Deepsec.

Flächendeckendes Ausspionieren funktioniere nicht: Duncan Campbell und James Bamford zur Deepsec in Wien

Die Diskussion über die Terroranschläge von Paris geht natürlich auch an einer Konferenz zu IT-Sicherheit nicht spurlos vorüber. Zumal die dieser Tage zum mittlerweile neunten Mal in Wien abgehaltene Deepsec dieses Jahr gleich zwei Journalisten eingeladen hat, die sich seit Jahren kritisch mit Geheimdiensten und deren Überwachungspraxis auseinandersetzen. Und sowohl James Bamford als auch Duncan Campbell sind sich einig: Die umgehend angelaufene Diskussion über den Ausbau der Internetüberwachung gehe vollkommen an der Realität vorbei.

Vollkommenes Versagen

Wenn Paris eines eindrücklich gezeigt habe, dann das "vollkommene Versagen der Massenüberwachung", wie Campbell in der einleitenden Keynote zur Konferenz betonte. Diese funktioniere schlicht nicht, da es in der breiten Masse der Daten unmöglich sei, das Relevante herauszufinden, egal wie mächtig die Rechensysteme der NSA sein mögen. Und diese Erkenntnis sei keineswegs neu, seit Jahrzehnten zeige sich immer wieder das gleiche Bild, wie der seit 1975 zu Geheimdiensten arbeitende Journalist betont.

Falsche Herangehensweise

Es gebe bis dato praktisch keine belegten Beispiel für Erfolge der Massenüberwachung. Dafür zahlreiche Gegenbeispiele: Weder konnte 9/11 verhindert werden noch die Anschläge auf die Londoner U-Bahn im Jahr 2005 oder die Terrorangriffe auf die Redaktion der Satirezeitschrift "Charlie Hebdo" und den Boston-Marathon. Und das, obwohl in all diesen Fällen die Angreifer vorher bereits auf dem Radar der Behörden waren. Das Problem sei eben nicht der Mangel an Daten, sondern deren Analyse.

Schlicht zu viel

Der NSA sei die Untauglichkeit der Massenüberwachung übrigens durchaus bewusst, wie Campbell betont. Immer wieder gebe es in den Snowden-Dokumenten Hinweise darauf, dass die Behörde mit dem Datenwust kämpfe und künstliche Begrenzungen vornehmen müsse, um überhaupt noch etwas analysieren zu können.

Geschichtsexkurs

Der Umstand, dass die Geheimdienste trotzdem immer mehr Daten wollen, sei schlicht auf die ihnen immanente Logik zurückzuführen, attestiert Bamford, der sein erstes Buch über die NSA bereits im Jahr 1982 publiziert hat. Man dürfe zudem

nicht vergessen, wie die NSA entstanden sei: Sie sollte die Funkübertragung der UdSSR abhören, um eine Art zweites Pearl Harbor zu verhindern. Das sei einst auch tatsächlich relativ einfach umfassend zu bewerkstelligen gewesen, allerdings skaliere dieser Ansatz schlicht nicht, wie Bamford gegenüber dem STANDARD betont. Die NSA störe sich daran aber nicht und sammle immer mehr Daten und Macht um ihrer selbst willen.

Realitätscheck

Freilich geben sich beide nicht der Illusion hin, dass gerade in der aktuellen Situation eine Trendwende zu erwarten ist. Die Anschläge von Paris werden eine weitere Aushöhlung von Bürgerrechten und eine Ausweitung geheimdienstlicher Befugnisse zur Folge haben und damit auch all jene zarten Verbesserungen, die die Snowden-Enthüllungen ausgelöst haben, wieder zunichtemachen.

Keine Hintertüren

An die Umsetzung einer derzeit vieldiskutierten Maßnahme glaubt Campbell hingegen nicht: Hintertüren für Verschlüsselungssoftware würden nicht kommen, und zwar aus einem ganz einfachen Grund. Diese seien schlicht technischer Nonsens. Befürworter würden sich hier eine Art magische Lösung vorstellen, die in der Realität nicht umsetzbar sei.

Eine Crypto-Backdoor für die NSA würde bedeuten, dass umgehend auch jedes andere Land entsprechende eigene Zugänge verlangen würde – von China bis Saudi-Arabien. Und das sei nur eine Hürde von vielen. Aber selbst wenn man es irgendwie schaffen würde, all diese Hürden zu überwinden, was würde Terroristen davon abhalten, eine eigene Software ohne Backdoor einzusetzen? Diese würden all die Verschlüsselungsbeschränkungen also nicht treffen, Unternehmen, die sicher kommunizieren wollen, hingegen sehr wohl.

Mehr Verschlüsselung statt weniger

Auch wenn es zunächst paradox klingen mag, die Lösung für die Krise der Geheimdienste sieht Bamford in einem grundlegenden Kurswechsel, und er verweist dabei auf Edward Snowden, den er vergangenes Jahr für ein ausführliches Interview mit dem US-Magazin "Wired" besucht hat. Dieser sei davon überzeugt, dass in einer Welt, in der alle effektive Ende-zu-Ende-Verschlüsselung benutzen, die Geheimdienste gezwungen würden, wieder auf gezielte Überwachung und klassische Polizeiarbeit zu setzen. Immerhin verhindere auch die beste Verschlüsselung nicht den direkten Zugriff auf den Computer einer Zielperson, sehr wohl aber die Aushöhlung der Privatsphäre der Gesamtbevölkerung. (Andreas Proschofsky, 20.11.2015)

Link

Deepsec

http://fm4.orf.at/stories/1764708/

“Geheimdienste versagen gegen Terror immer”

Datum: 19.11.2015

Autor: Erich Möchel

Gründe für Versagen waren nie Verschlüsselung, sondern selbst gemachter Datenoverkill und notorische Defizite bei Fremdsprachen, sagt Geheimdienstexperte James Bamford.

Seit den Massakern in Paris werden von europäischen Politikern und Behörden abwechselnd Edward Snowden, Verschlüsselung, PlayStations und andere Kommunikationsmittel für das Gelingen der Anschläge verantwortlich gemacht. Kaum thematisiert wurde hingegen, dass die für “Gefahrenerkundung” im Vorfeld zuständigen Geheimdienste erneut völlig ahnungslos waren, obwohl enormer Kommunikationsaufwand mit den Anschlägen verbunden war. Und wieder waren die meisten Attentäter den französischen Diensten seit Jahren als notorische Extremisten bekannt.

Für James Bamford, Journalist und Autor mehrerer Standardwerke über die NSA, ist dieses Versagen keine Überraschung. “Die Geheimdienste haben in der jüngeren Geschichte so gut wie nie einen Terroranschlag verhindern können. Die NSA hat von 9/11 aus dem Fernsehen erfahren und auch alle anderen Anschläge in den USA nicht verhindern können”, sagte Bamford am Dienstag in Wien zu ORF.at. Die Gründe dafür seien keineswegs technischer Natur, sondern auf selbst gemachten Datenoverkill, schlechte Koordination sowie Defizite bei Fremdsprachen und Analyse zurückzuführen.

“Forderungen reines Ablenkungsmanöver”

In Frankreich hatten die Behörden bereits Stunden nach den Anschlägen eine Ausweitung der Vorratsdatenspeicherung gefordert. In Großbritannien kündigte Premier David Cameron 1.400 neue Stellen für den Militärdienst GCHQ an, ÖVP-Generalsekretär Reinhold Lopatka gab in Österreich wiederum bekannt, dass “der Kampf gegen den Terror” nun “leider eine Einschränkung der Bürgerrechte” erfordere und twitterte “Staatsschutzgesetz!”.

Auch diese Reaktionen kommen für Bamford wenig überraschend, zumal es die übliche Strategie der Dienste sei, von den eigenen Fehlern mit Forderungen nach noch mehr Daten abzulenken, sagt der Geheimdienstexperte, der am Donnerstag auf der Wiener Sicherheitskonferenz Deepsec einen Vortrag hielt. Zudem haben “die französischen Geheimdienste erst vor den Anschlägen umfassende neue Zugriffsmöglichkeiten erhalten, ihre Kompetenzen über-

steigen mittlerweile sogar die Möglichkeiten der NSA". Diese Maßnahmen des französischen Staats waren nach dem Massaker in der Redaktion von "Charlie Hebdo" erst im Frühsommer 2015 verabschiedet worden.

Methodisches Versagen, Ablenkungsmanöver

Auch im Fall Charlie Hebdo waren die Attentäter den Behörden bereits davor als gewaltbereite Extremisten aufgefallen, die enge Kontakte zur IS-Terrortruppe in Syrien unterhielten. Dass sie in der Folge dennoch völlig ungehindert morden konnten, sei keineswegs ein Ausrutscher gewesen, sagt Bamford. Auch den US-Diensten waren von den Aschlägen auf das World Trade Center 1993, über den "Unterhosenbomber" bis zu den Attentätern auf den Marathon von Boston 2013 zumindest die Masterminds der Terroristen bereits bekannt gewesen. Dass nach jedem dieser Anschläge noch mehr und tiefgreifendere Zugriffe gefordert und auch genehmigt worden seien, habe die Probleme für die Geheimdienste noch verschärft, ist Bamford überzeugt.

Obwohl die russischen Geheimdienste ihre US-Gegenparts schon 2011 davor gewarnt hatten, dass der ältere der beiden Boston-Bomber Kontakte zu Extremisten in Dagestan unterhielt, pendelte der ungeachtet aller Passagierprofile und "No-Fly-Lists" mehrmals unbehelligt zwischen den USA und Dagestan. Der Grund für das Versagen dürfte 2013 auf die unterschiedlichen Transkriptionen des Namens aus dem Kyrillischen gewesen sein. In den englischsprachigen Agenturmeldungen danach wurden die Brüder "Tsarnaev", im deutschen Sprachraum aber als "Zarnajew" bekannt.

Der mit der Vorbereitung der Attentate einhergehende Kommunikationsverkehr war den US-Überwachern ebenso wenig aufgefallen wie nun in Frankreich. "Dabei handelte es sich bei den Attentaten in Paris um eine organisatorisch aufwendige und logistisch komplexe Aktion einer relativ großen Tätergruppe, die über mindestens drei Länder verteilt war. Es ist schon ziemlich merkwürdig, dass die Kommunikationen von bekannten Terrorverdächtigen niemandem in der Geheimdienstwelt aufgefallen sind", sagt Bamford, "ein Mangel an Daten war es nicht, denn die Daten hatten sie."

Bamford über Sprachen und Dienste

"Tatsächlich haben die Dienste nämlich ein Sprachenproblem. Rund um 9/11 gab es in der NSA nur ein paar Analysten, die Pashtu, Dari oder Urdu sprachen. Dieses Sprachenproblem existiert schon seit ewig in der gesamten 'Intelligence Community'. Ich hatte für den Senatsausschuss zur Kontrolle der Geheimdienste ein Jahr vor 9/11 ein Programm zur verbesserten Sprachauswertung für die Geheimdienste vorgeschlagen. Zu meiner Überraschung wurde mein Vorschlag, ein 'Linguist Reserve Corps' aus ehemaligen Militärs und freiwilligen Zivilisten zu bilden, die allesamt Muttersprachler sind, in Folge mehr oder weniger angenommen", erzählt Bamford.

“Weil man nicht einfach fünfzig Muttersprachler in - sagen wir - Lingala anstellen kann, nur für den Fall, dass im Kongo irgendwann eine Krise ausbricht, war die Idee dahinter, ein Corps zu bilden, das ad hoc einberufen werden kann. Dieser Ansatz ist zudem sehr billig, weil die Besoldung für Reservisten ziemlich niedrig ist. Sehr viele Zielpersonen der Geheimdienste stammen aus mehrsprachigen Gebieten, ein abgehörtes Gespräch aus Afghanistan kann von Pashtu schnell einmal zu Urdu oder Dari wechseln. Ein Analyst, der Pashtu an einer Schule in den USA gelernt hat, versteht ab da nur noch Bahnhof, ein Muttersprachler kann derselben Konversation hingegen folgen und auch deren Nuancen in den richtigen Kontext setzen, weil er diese Sprachen nicht zum ersten Mal hört.”

“Auf jeden Fall wurden meine Vorschläge umgesetzt, wie, kann ich leider nicht beurteilen, denn mir fehlt die dafür nötige Sicherheitsüberprüfung durch die Dienste”, sagte Bamford sichtlich amüsiert, deshalb wisse er auch nicht, ob seine Kernforderung nach Muttersprachlern darin verblieben sei. “Sowohl beim CIA-Personal wie in der NSA herrscht enormes Misstrauen gegenüber Muttersprachlern, gerade wenn sie in ihrem Herkunftsland auch aufgewachsen sind, weil es sich ja um Spione handeln könnte. Das ist ziemlicher Schwachsinn, denn auf der Liste der Topspione und Landesverräter waren das von Robert Hansen angefangen allesamt waschechte Amerikaner.”

“Mit Vollgas in die falsche Richtung”

Angesichts der miserablen Erfolgsbilanz der westlichen Geheimdienste wäre es jedoch verfehlt, zu sagen, die Dienste seien “Underachiever”, also Versager, die ihre Ziele nicht erreicht hätten, sagte Bamford: “Die sind mit Vollgas unterwegs, allerdings in die verkehrte Richtung. Statt sie frühzeitig zu erkennen, produzieren sie die Gefahren selbst. Die Invasion im Irak 2003 basierte auf miserabler Nachrichtenaufklärung über angebliche Massenvernichtungswaffen, nichts davon wurde ordnungsgemäß überprüft, weil man sich auf Behauptungen aus unzuverlässigen Quellen verließ.”

“Auf einer so prekären Grundlage wurde das Regime Saddam Husseins gestürzt, von der Zerschlagung der irakischen Armee angefangen hat dann eine blöde Idee die nächste gejagt. In dem daraus resultierenden Machtvakuum entfaltete sich dann der IS, der zuletzt für die Anschläge in Paris verantwortlich war. Was also mit dilettantischer Nachrichtenaufklärung begonnen und Krieg zur Folge hatte, resultiert seitdem in Terroranschlägen gegen Zivilisten. Anstatt diese Bedrohungen abzuwehren, hat die NSA sie in diesem Fall selber mitproduziert.”

SMS statt Verschlüsselung

Nach all den von Politikern, Polizei und Diensten in die Welt gesetzten Gerüchten hatte sich spätestens am

Mittwoch herausgestellt, dass die Täter vor dem Anschlag via SMS kommuniziert hatten. SMS ist ein nicht verschlüsselbarer Dienst, der zusammen mit allen Metadaten der Kommunikation in ein und demselben SS7-Datenstrom transportiert wird. Diese Inhaltsdaten werden im Regime der Vorratsdatenspeicherung, das in Frankreich seit mehr als zehn Jahren gültig ist, von den Telekoms aus technischen Gründen im Volltext mitgespeichert, weil das Gesamtvolumen dieser Daten unerheblich ist.

Wie methodisch die Propaganda gegen Verschlüsselung von den Geheimdiensten eingesetzt wird, zeigt eine von der “Washington Post” im September veröffentlichte E-Mail des Chefjuristen beim obersten Geheimdienstdirektor. Obwohl die gesetzgeberische Umgebung derzeit sehr feindlich sei, solle man alle Optionen offen lassen, schrieb General Counsel Bob Litt an seine Kollegen: “Das könnte sich im Fall eines Terroranschlags sehr schnell ändern, wenn sichere Verschlüsselung für eine Verhinderung der Aufklärung verantwortlich gemacht werden kann.”

Erstellt am: 19. 11. 2015 - 14:43 Uhr

"Geheimdienste versagen gegen Terror immer"

Gründe für Versagen waren nie Verschlüsselung, sondern selbst gemachter Datenoverkill und notorische Defizite bei Fremdsprachen, sagt Geheimdienstexperte James Bamford.

Seit den Massakern in Paris werden von europäischen Politikern und Behörden abwechselnd Edward Snowden, Verschlüsselung, PlayStations und andere Kommunikationsmittel für das Gelingen der Anschläge verantwortlich gemacht. Kaum thematisiert wurde hingegen, dass die für "Gefahrenerkundung" im Vorfeld zuständigen Geheimdienste erneut völlig ahnungslos waren, obwohl enormer Kommunikationsaufwand mit den Anschlägen verbunden war. Und wieder waren die meisten Attentäter den französischen Diensten seit Jahren als notorische Extremisten bekannt.

Aktuell dazu in ORF.at
Am Donnerstag fanden neue Razzien im Brüsseler Stadtteil Molenbeek statt, aus dem mehrere der Attentäter in Paris stammen

Für James Bamford, Journalist und Autor mehrerer Standardwerke über die NSA, ist dieses Versagen keine Überraschung. "Die Geheimdienste haben in der jüngeren Geschichte so gut wie nie einen Terroranschlag verhindern können. Die NSA hat von 9/11 aus dem Fernsehen erfahren und auch alle anderen Anschläge in den USA nicht verhindern können", sagte Bamford am Dienstag in Wien zu ORF.at. Die Gründe dafür seien keineswegs technischer Natur, sondern auf selbst gemachten Datenoverkill, schlechte Koordination sowie Defizite bei Fremdsprachen und Analyse zurückzuführen.

CC BY SA 3.0 Fm4/Erich Moechel

James Bamford vor dem Tagungsort der DeepSec Konferenz (https://deepsec.net) im Botschaftsviertel des dritten Wiener Gemeindebezirks.

"Forderungen reines Ablenkungsmanöver"

Das neue französische Staatsschutzgesetz "Projet de loi relatif au renseignement" ähnelt dem österreichischen insofern, als in beiden polizeiliche und geheimdienstliche Befugnisse vermischt werden.

In Frankreich hatten die Behörden bereits Stunden nach den Anschlägen eine Ausweitung der Vorratsdatenspeicherung gefordert. In Großbritannien kündigte Premier David Cameron 1.400 neue Stellen für den Militärdienst GCHQ an, ÖVP-Generalsekretär Reinhold Lopatka gab in Österreich wiederum bekannt, dass "der Kampf gegen den Terror" nun "leider eine Einschränkung der Bürgerrechte" erfordere und twitterte "Staatsschutzgesetz!".

Auch diese Reaktionen kommen für Bamford wenig überraschend, zumal es die übliche Strategie der Dienste sei, von den eigenen Fehlern mit Forderungen nach noch mehr Daten abzulenken, sagt der Geheimdienstexperte, der am Donnerstag auf der Wiener Sicherheitskonferenz Deepsec einen Vortrag hielt. Zudem haben "die französischen Geheimdienste erst vor den Anschlägen umfassende neue Zugriffsmöglichkeiten erhalten, ihre Kompetenzen übersteigen mittlerweile sogar die Möglichkeiten der NSA". Diese Maßnahmen des französischen Staats waren nach dem Massaker in der Redaktion von "Charlie Hebdo" erst im Frühsommer 2015 verabschiedet worden.

Methodisches Versagen, Ablenkungsmanöver

Nach den Attentaten auf die Redaktion von Charlie Hebdo kam die Speicherung von Vorratsdaten aus dem Flugverkehr wieder auf die Agenda des EU-Parlaments.

Auch im Fall Charlie Hebdo waren die Attentäter den Behörden bereits davor als gewaltbereite Extremisten aufgefallen, die enge Kontakte zur IS-Terrortruppe in Syrien unterhielten. Dass sie in der Folge dennoch völlig ungehindert morden konnten, sei keineswegs ein Ausrutscher gewesen, sagt Bamford. Auch den US-Diensten waren von den Aschlägen auf das World Trade Center 1993, über

den "Unterhosenbomber" bis zu den Attentätern auf den Marathon von Boston 2013 zumindest die Masterminds der Terroristen bereits bekannt gewesen. Dass nach jedem dieser Anschläge noch mehr und tiefgreifendere Zugriffe gefordert und auch genehmigt worden seien, habe die Probleme für die Geheimdienste noch verschärft, ist Bamford überzeugt.

CC BY SA 3.0 Fm4/Erich Moechel

Die Misserfolge der Fahndung nach den Boston-Bombern in den USA hatten auch maßgeblich dazu beigetragen, dass die geplante Vorratsspeicherung von Fluggastdaten im EU-Parlament 2013 noch keine Mehrheit fand.

Obwohl die russischen Geheimdienste ihre US-Gegenparts schon 2011 davor gewarnt hatten, dass der ältere der beiden Boston-Bomber Kontakte zu Extremisten in Dagestan unterhielt, pendelte der ungeachtet aller Passagierprofile und "No-Fly-Lists" mehrmals unbehelligt zwischen den USA und Dagestan. Der Grund für das Versagen dürfte 2013 auf die unterschiedlichen Transkriptionen des Namens aus dem Kyrillischen gewesen sein. In den englischsprachigen Agenturmeldungen danach wurden die Brüder "Tsarnaev", im deutschen Sprachraum aber als "Zarnajew" bekannt.

Der mit der Vorbereitung der Attentate einhergehende Kommunikationsverkehr war den US-Überwachern ebenso wenig aufgefallen wie nun in Frankreich. "Dabei handelte es sich bei den Attentaten in Paris um eine organisatorisch aufwendige und logistisch komplexe Aktion einer relativ großen Tätergruppe, die über mindestens drei Länder verteilt war. Es ist schon ziemlich merkwürdig, dass die Kommunikationen von bekannten Terrorverdächtigen niemandem in der Geheimdienstwelt aufgefallen sind", sagt Bamford, "ein Mangel an Daten war es nicht, denn die Daten hatten sie."

Nachdem der "Unterhosenbomber", dessen eigener Vater die US-Botschaft vor seinem Sohn gewarnt hatte, an seinem eigenen Unvermögen gescheitert war, wurde nach einem solchen Täterprofil gefahndet.

Bamford über Sprachen und Dienste

"Tatsächlich haben die Dienste nämlich ein Sprachenproblem. Rund um 9/11 gab es in der NSA nur ein paar Analysten, die Pashtu, Dari oder Urdu sprachen. Dieses Sprachenproblem existiert schon seit

ewig in der gesamten 'Intelligence Community'. Ich hatte für den Senatsausschuss zur Kontrolle der Geheimdienste ein Jahr vor 9/11 ein Programm zur verbesserten Sprachauswertung für die Geheimdienste vorgeschlagen. Zu meiner Überraschung wurde mein Vorschlag, ein 'Linguist Reserve Corps' aus ehemaligen Militärs und freiwilligen Zivilisten zu bilden, die allesamt Muttersprachler sind, in Folge mehr oder weniger angenommen", erzählt Bamford.

Der Hinweis, dass die NSA einen "Durchbruch in der Verschlüsselung" erzielt haben musste, war 2012 ebenfalls von Bamford gekommen (http://www.wired.com/2012/03/ff_nsadatacenter/) . Erst vor einem Monat hatte eine Gruppe namhafter Kryptologen die Natur dieses "Durchbruchs" mit einiger Sicherheit identifizieren können.

"Weil man nicht einfach fünfzig Muttersprachler in - sagen wir - Lingala anstellen kann, nur für den Fall, dass im Kongo irgendwann eine Krise ausbricht, war die Idee dahinter, ein Corps zu bilden, das ad hoc einberufen werden kann. Dieser Ansatz ist zudem sehr billig, weil die Besoldung für Reservisten ziemlich niedrig ist. Sehr viele Zielpersonen der Geheimdienste stammen aus mehrsprachigen Gebieten, ein abgehörtes Gespräch aus Afghanistan kann von Pashtu schnell einmal zu Urdu oder Dari wechseln. Ein Analyst, der Pashtu an einer Schule in den USA gelernt hat, versteht ab da nur noch Bahnhof, ein Muttersprachler kann derselben Konversation hingegen folgen und auch deren Nuancen in den richtigen Kontext setzen, weil er diese Sprachen nicht zum ersten Mal hört."

United States Civilian Linguist Reserve Corps
Feasibility Study

Prepared by:

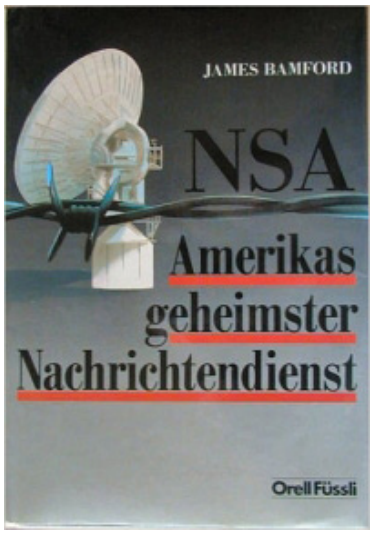
National Security Education Program
National Defense University
Department of Defense

As Requested by the United States Congress
Per Section 325 of Public Law 107-306
(Intelligence Authorization Act for Fiscal Year 2003)

Public Domain

"Auf jeden Fall wurden meine Vorschläge umgesetzt, wie, kann ich leider nicht beurteilen, denn mir fehlt die dafür nötige Sicherheitsüberprüfung durch die Dienste", sagte Bamford sichtlich amüsiert, deshalb wisse er auch nicht, ob seine Kernforderung nach Muttersprachlern darin verblieben sei. "Sowohl beim CIA-Personal wie in der NSA herrscht enormes Misstrauen gegenüber Muttersprachlern, gerade wenn sie in ihrem Herkunftsland auch aufgewachsen sind, weil es sich ja um Spione handeln könnte. Das ist ziemlicher Schwachsinn, denn auf der Liste der Topspione und Landesverräter waren das von Robert Hansen angefangen allesamt waschechte Amerikaner."

"Mit Vollgas in die falsche Richtung"



Orrell Füssli

James Bamford hat schon in den 1980ern über die NSA geschrieben

Bamfords erstes Buch über die davor so gut wie unbekannte NSA hatte 1982 wie eine Bombe eingeschlagen, wie alle folgenden Bücher landete auch "The Puzzle Palace" auf der Beststellerliste der New York Times. Mehr über Bamford in der Wikipedia (https://en.wikipedia.org/wiki/James_Bamford)

Angesichts der miserablen Erfolgsbilanz der westlichen Geheimdienste wäre es jedoch verfehlt, zu sagen, die Dienste seien "Underachiever", also Versager, die ihre Ziele nicht erreicht hätten, sagte Bamford: "Die sind mit Vollgas unterwegs, allerdings in die verkehrte Richtung. Statt sie frühzeitig zu erkennen, produzieren sie die Gefahren selbst. Die Invasion im Irak 2003 basierte auf miserabler Nachrichtenaufklärung über angebliche Massenvernichtungswaffen, nichts davon wurde ordnungsgemäß überprüft, weil man sich auf Behauptungen aus unzuverlässigen Quellen verließ."

"Auf einer so prekären Grundlage wurde das Regime Saddam Husseins gestürzt, von der Zerschlagung der irakischen Armee angefangen hat dann eine blöde Idee die nächste gejagt. In dem daraus resultierenden Machtvakuum entfaltete sich dann der IS, der zuletzt für die Anschläge in Paris verantwortlich war. Was also mit dilettantischer Nachrichtenaufklärung begonnen und Krieg zur Folge hatte, resultiert seitdem in Terroranschlägen gegen Zivilisten. Anstatt diese Bedrohungen abzuwehren, hat die NSA sie in diesem Fall selber mitproduziert."

William Binney, Mathematiker, Kryptologe und nach mehr als 30 Dienstjahren seit 2001 NSA-Dissident, sagt überhaupt, dass NSA und Co gar keine Nachrichtenaufklärung mehr, sondern Forensik im Nachhinein betreiben

SMS statt Verschlüsselung

Nach all den von Politikern, Polizei und Diensten in die Welt gesetzten Gerüchten hatte sich spätestens am Mittwoch herausgestellt, dass die Täter vor dem Anschlag via SMS kommuniziert hatten. SMS ist ein nicht verschlüsselbarer Dienst, der zusammen mit allen Metadaten der Kommunikation in ein und demselben SS7-Datenstrom transportiert wird. Diese Inhaltsdaten werden im Regime der Vorratsdatenspeicherung, das in Frankreich seit mehr als zehn Jahren gültig ist, von den Telekoms aus technischen Gründen im Volltext mitgespeichert, weil das Gesamtvolumen dieser Daten unerheblich ist.

Wie methodisch die Propaganda gegen Verschlüsselung von den Geheimdiensten eingesetzt wird, zeigt eine von der "Washington Post" im September veröffentlichte E-Mail des Chefjuristen beim obersten Geheimdienstdirektor. Obwohl die gesetzgeberische Umgebung derzeit sehr feindlich sei, solle man alle Optionen offen lassen, schrieb General Counsel Bob Litt an seine Kollegen: "Das könnte sich im Fall eines Terroranschlags sehr schnell ändern, wenn sichere Verschlüsselung für eine Verhinderung der Aufklärung verantwortlich gemacht werden kann."

http://blog.c22.cc/2015/11/19/deepsec-201550-shades-of-waf/

[DeepSec 2015] 50 Shades of WAF

Datum: 19.11.2015

Autor: Chris John Riley

50 Shades of WAF – Exemplified at Barracuda & Sucuri

Ashar Javed (Hyundai AutoEver Europe GmbH)

This talk will present 50 (25*2) bypasses of Barracuda and Sucuri's WAF default signatures that deal with Cross-Site Scripting (XSS). 150,000 organizations worldwide including Fortune 1000 companies are using Barracuda while around 10,000 web applications are behind Sucuri's cloud-based WAF. The XSS bypasses we will present in this talk are also applicable to other WAFs. All bypasses were responsibly reported to the vendors and most of them were fixed. Further, we will show XSS in Barracuda's admin interface and in their web application. Finally, we will present one unfixed bypass of Barracuda and Sucuri and will see how quickly vendors will react to fix it, given it will make thousands of sites vulnerable.

Barracuda

150,000 organizations use Barracuda Networks technology.

Over 10 months during 2014/2015 Barracuda had 7 updates of their ruleset, none of which included XSS. 6 months after that, they released 5 updates and 1 firmware patch that included fixes for XSS issues. Updating is hard, meaning there are a lot of WAFs out there that are letting XSS attacks through.

How to detect Barracuda… if you see this message, then you're looking at Barracuda:

The specified URL cannot be found

After testing the regular expressions used to detect XSS, their was a number of XSS discovered.

Event Handlers

4 separate regexes handling event handlers.

Large number of event handlers missing, and the ones in the regex are hard-coded (for logging and tracking purposes).

ontoggle

onsearch

onlaungaugechange

oncuechange

ondragexit

…

Moving to a more generic event handler detection e.g. on(.*) would catch these.

However, even if the event handler was detected it was bypassable. However the logic didn't allow for backtick (`) which is supported in some browsers. It was also possible to bypass by injecting a newline between the equals and quotes (onclick=%0A"stuff"). This was due to the use of "." in the regex, which matches anything except a newline.

meta tags where also treated differently, resulting in a number of ways of bypassing the filters. The same issues existed in a number of html tags.

Some other issues that cause bypasses:

Tags < 10 chars

Tags alphanumeric

Tags are closed properly

Data URI JS injection (resulted in multiple issues)

expression

All these Regexes work together to detect issues. However these are not always turned on. They need to activated, and whitelisting specific checks may have a knock-on effect in other areas where mutliple regexes are needed for detection.

Constant tweaks to the payload and complexity of the regexes results in false positives. The knock-on effect of this is disabling of protections, which lowers overall the level of security.

Some of the bypasses effected the BarracudaNetworks.com login page and stored XSS in their main admin interface.

Takeaway: Updated to 1.102 version and apply the firmware patch 8.0.1

Sucuri

Cloud-based WAF… priced cheaper than a takeaway pizza.

Sucuri offers a bug bounty (through HackerOne) on bypasses.

A large number of bypasses using encoding, backticks, unclosed tags, VBscript…

Blocked all onmouse*, onkey*, and many many more. Blacklists are a zero sum game.

Blocking of script tags appeared work well, however <script%2fsrc was a workable bypass technique. There's always new bypasses, and almost an endless way to bypass the protections given enough time.

Conclusion

WAFs are not the only protection layer. It can be an extra layer, but not the only defense.

[DeepSec 2015]50 Shades of WAF

50 Shades of WAF – Exemplified at Barracuda & Sucuri
Ashar Javed (Hyundai AutoEver Europe GmbH)

DEEPSEC

> *This talk will present 50 (25*2) bypasses of Barracuda and Sucuri's WAF default signatures that deal with Cross-Site Scripting (XSS). 150,000 organizations worldwide including Fortune 1000 companies are using Barracuda while around 10,000 web applications are behind Sucuri's cloud-based WAF. The XSS bypasses we will present in this talk are also applicable to other WAFs. All bypasses were responsibly reported to the vendors and most of them were fixed. Further, we will show XSS in Barracuda's admin interface and in their web application. Finally, we will present one unfixed bypass of Barracuda and Sucuri and will see how quickly vendors will react to fix it, given it will make thousands of sites vulnerable.*

Barracuda

150,000 organizations use Barracuda Networks technology.

Over 10 months during 2014/2015 Barracuda had 7 updates of their ruleset, none of which included XSS. 6 months after that, they released 5 updates and 1 firmware patch that included fixes for XSS issues. Updating is hard, meaning there are a lot of WAFs out there that are letting XSS attacks through.

How to detect Barracuda… if you see this message, then you're looking at Barracuda:

> *The specified URL cannot be found*

After testing the regular expressions used to detect XSS, their was a number of XSS discovered.

Event Handlers

4 separate regexes handling event handlers.

Large number of event handlers missing, and the ones in the regex are hard-coded (for logging and tracking purposes).

- ontoggle
- onsearch
- onlaungaugechange
- oncuechange
- ondragexit
- …

Moving to a more generic event handler detection e.g. on(.*) would catch these.

However, even if the event handler was detected it was bypassable. However the logic didn't allow for backtick (`) which is supported in some browsers. It was also possible to bypass by injecting a newline between the equals and quotes (onclick=%0A"stuff"). This was due to the use of "." in the regex, which matches anything except a newline.

meta tags where also treated differently, resulting in a number of ways of bypassing the filters. The same issues existed in a number of html tags.

Some other issues that cause bypasses:

- Tags < 10 chars
- Tags alphanumeric
- Tags are closed properly

- Data URI JS injection (resulted in multiple issues)
- expression

All these Regexes work together to detect issues. However these are not always turned on. They need to activated, and whitelisting specific checks may have a knock-on effect in other areas where mutliple regexes are needed for detection.

Constant tweaks to the payload and complexity of the regexes results in false positives. The knock-on effect of this is disabling of protections, which lowers overall the level of security.

Some of the bypasses effected the BarracudaNetworks.com login page and stored XSS in their main admin interface.

Takeaway: Updated to 1.102 version and apply the firmware patch 8.0.1

Sucuri

Cloud-based WAF… priced cheaper than a takeaway pizza.

Sucuri offers a bug bounty (through HackerOne) on bypasses.

A large number of bypasses using encoding, backticks, unclosed tags, VBscript…

Blocked all onmouse*, onkey*, and many many more. Blacklists are a zero sum game.

Blocking of script tags appeared work well, however <script%2fsrc was a workable bypass technique. There's always new bypasses, and almost an endless way to bypass the protections given enough time.

Conclusion

WAFs are not the only protection layer. It can be an ex

Links:

- Presentation Abstract
- Ashar Javed Twitter

Related

[Defcon] You Spent All That Money And You Still Got Owned...
In "Conference"

[SecTorCA] Reverse Engineering a Web Application - for fun, behavior & WAF Detection
In "Conference"

The more things change, the more they stay the same!
In "Security"

Conference, Security deepsec

http://blog.c22.cc/2015/11/19/deepsec-2015-file-format-fuzzing-in-android-giving-a-stagefright-to-the-android-installer/

[DeepSec 2015] File Format Fuzzing in Android – Giving a Stagefright to the Android Installer

File Format Fuzzing in Android – Giving a Stagefright to the Android Installer
Alexandru Blanda (Intel Corporation)

Datum: 19.11.2015

Autor: Chris John Riley

The presentation focuses on revealing a fuzzing approach that can be used to uncover different types of vulnerabilities inside multiple core system components of the Android OS. The session will be targeted on exposing the general idea behind this approach and how it applies to several real-life targets from the Android OS, with examples of actual discovered vulnerabilities. These vulnerabilities affect critical components of the Android OS and the audience will have the opportunity to learn about the way they were discovered and possible exploit scenarios. The most important targets that will be included in the talk: the Android APK installer and the Stagefright media framework.

An approach that can be used for file-format fuzzing on Android

File Format Fuzzing

First steps in file format fuzzing:

Data Generation
Log process (Execute Tests)
Triage mechanism
Analyze and Debug crashes
If the fuzzing is successful, triage and categorization of the issues is an important step to avoid being overwhelmed by responses.

Data Generation

Mutational vs. generational Fuzzing

Maintain the structural validity of the file being processed. The target needs to accept that the file is valid otherwise it won't run.

Tools use for test-case generation:

Basic Fuzzing Framework (BFF)

FuzzBox

Radamsa

American Fuzzy Lop (AFL)

Log Process

To find out what's happening with the test-cases we send to the Android device, we need to check the logs. This can be read out using the logcat on the device. This can be done by looking for Fatal messages and seeding the logcat before and after the run to identify the test case details and information required to reproduce.

adb shell logcat -v time *:F

Triage Mechanism

Each time a crash occurs a tombstone file is created under /data/tombstones and /data/system/dropbox. This data is important to have for triaging the issues and tracking the various crashes.
By looking at the value where the crash occurs you can collect a unique list of crashes without duplicates.

Parse logcat for input that causes crashes

Execute input to cause the crash again

Grab the Tombstone data to check against existing know issues

Analyze and Debug Crashes

After triage maybe you have 2 or 3 interesting crashes to investigate. Using the Tombstone data can give a good indication of the severity and location of where the crash occurs. Dmesg also gives a good source of information.
Using gdbserver you can debug crashes on the device. gdb can then be used to start a remote debugging session (make sure you set the Android debugging symbols).
addr2line can be useful in getting the information on where the call took place (example: where libstagefright called libc.so)

Fuzzing the Stagefright Media Framework

Media files are interesting attack vectors as the contain complex data and result in a large attack surface (audio, video, images, etc…). Media files are also seen as innocuous to users, and can be played through various sources without the users consent (MMS etc..).
Easiest way to test was the build the stagefright CLI tool (frameworks/av/cmds/stagefright) and calling it from the Android command line for testing.
Initially started fuzzing in early 2014… thousands of crashes (needed a triage mechanism to cope). First severe issues reported to Google in September 2014.

Fuzzing the Android application installer

The application installer is an attractive target (runs with high system privileges). If an attacker can exploit this, the impact will be high. The installer also allows for unprivileged users to send input to system components.
The process of application installation differs between ART and Dalvik (Lollipop and KitKat respectively).
Extract the APK, fuzz the components to be tested, repack
ART is easier as alterations can be made without extraction.
Modifications to the APK will result in an application signature mismatch. This means that the APK will need to be re-signed before testing.

Fuzzing with AFL in Android

Android port of the tool developed by Adrian Denkiewicz of Intel
Using alongside MFFA to discover issues. In some cases, AFL reported crashes that could not be confirmed when running the test case singularly.
This method of testing showed some results that were not seen in other tests (1 high RCE issue, and several low severity issues).

[DeepSec 2015] File Format Fuzzing in Android – Giving a Stagefright to the Android Installer

File Format Fuzzing in Android – Giving a Stagefright to the Android Installer
Alexandru Blanda (Intel Corporation)

DEEPSEC

> *The presentation focuses on revealing a fuzzing approach that can be used to uncover different types of vulnerabilities inside multiple core system components of the Android OS. The session will be targeted on exposing the general idea behind this approach and how it applies to several real-life targets from the Android OS, with examples of actual discovered vulnerabilities. These vulnerabilities affect critical components of the Android OS and the audience will have the opportunity to learn about the way they were discovered and possible exploit scenarios. The most important targets that will be included in the talk: the Android APK installer and the Stagefright media framework.*

An approach that can be used for file-format fuzzing on Android

File Format Fuzzing

First steps in file format fuzzing:

- Data Generation
- Log process (Execute Tests)
- Triage mechanism
- Analyze and Debug crashes

If the fuzzing is successful, triage and categorization of the issues is an important step to avoid being overwhelmed by responses.

Data Generation

Mutational vs. generational Fuzzing

Maintain the structural validity of the file being processed. The target needs to accept that the file is valid otherwise it won't run.

Tools use for test-case generation:

- Basic Fuzzing Framework (BFF)
- FuzzBox
- Radamsa
- American Fuzzy Lop (AFL)

Log Process

To find out what's happening with the test-cases we se k the logs. This can be read out using the logcat on the device. This can be done by looking for Fatal messages and seeding the logcat b case details and information required to reproduce.

```
adb shell logcat -v time *:F
```

Triage Mechanism

Each time a crash occurs a tombstone file is created under /data/tombstones and /data/system/dropbox. This data is important to have for triaging the issues and tracking the various crashes.

By looking at the value where the crash occurs you can collect a unique list of crashes without duplicates.

1. Parse logcat for input that causes crashes

2. Execute input to cause the crash again
3. Grab the Tombstone data to check against existing know issues

Analyze and Debug Crashes

After triage maybe you have 2 or 3 interesting crashes to investigate. Using the Tombstone data can give a good indication of the severity and location of where the crash occurs. Dmesg also gives a good source of information.

Using gdbserver you can debug crashes on the device. gdb can then be used to start a remote debugging session (make sure you set the Android debugging symbols).

addr2line can be useful in getting the information on where the call took place (example: where libstagefright called libc.so)

Fuzzing the Stagefright Media Framework

Media files are interesting attack vectors as the contain complex data and result in a large attack surface (audio, video, images, etc…). Media files are also seen as innocuous to users, and can be played through various sources without the users consent (MMS etc..).

Easiest way to test was the build the stagefright CLI tool (frameworks/av/cmds/stagefright) and calling it from the Android command line for testing.

Initially started fuzzing in early 2014… thousands of crashes (needed a triage mechanism to cope). First severe issues reported to Google in September 2014.

Fuzzing the Android application installer

The application installer is an attractive target (runs with high system privileges). If an attacker can exploit this, the impact will be high. The installer also allows for unprivileged users to send input to system components.

The process of application installation differs between ART and Dalvik (Lollipop and KitKat respectively).

Extract the APK, fuzz the components to be tested, repack

ART is easier as alterations can be made without extraction.

Modifications to the APK will result in an application signature mismatch. This means that the APK will need to be re-signed before testing.

Fuzzing with AFL in Android

Android port of the tool developed by Adrian Denkiewicz of Intel

Using alongside MFFA to discover issues. In some cases, AFL reported crashes that could not be confirmed when running the test case singularly.

This method of testing showed some results that were not seen in other tests (1 high RCE issue, and several low severity issues).

Links:

- Presentation Abstract
- Presentation Paper
- Alexandru Blanda Twitter

Rate this:

Rate This

http://blog.c22.cc/2015/11/19/deepsec-2015how-to-break-xml-encryption-automatically/

[DeepSec 2015]How to Break XML Encryption – Automatically

Datum: 19.11.2015

Autor: Chris John Riley

How to Break XML Encryption – Automatically

Juraj Somorovsky (Ruhr University Bochum)

In recent years, XML Encryption became a target of several new attacks. These attacks belong to the family of adaptive chosen-ciphertext attacks, and allow an adversary to decrypt symmetric and asymmetric XML cipher-texts, without knowing the secret keys. In order toprotect XML Encryption implementations, the World Wide Web Consortium (W3C) published an updated version of the standard.

Unfortunately, most of the current XML Encryption implementations do not support the newest standard and offer different XML Security configurations to protect confidentiality of the exchanged messages. Resulting from the at-tack and specification complexity, evaluation of the security configuration correctness becomes tedious and error prone.
In this talk, we will first give an overview on Web Service specific attacks. Afterwards, we present attacks on XML Encryption and how to evaluate security of XML Encryption interfaces automatically. Our algorithm can detect a vulnerability and exploit it to retrieve a plaintext from an encrypted message. To assess practicability of our ap-proach, we implemented an open source attack plugin for Web Service attacking tool called WS-Attacker. With the plugin, we discovered new security problems in four out of five analyzed Web Service implementations, including IBM Datapower or Apache CXF.

What is a WebService and XML Security

SOAP WebService are a standard that allows you to execute a function on the server and receive a response (re-mote procedure calls). This range from simple to very complex requests.

There are many ways to secure this communication. SSL/TLS can be used to secure the tunnel between the client and server (transport communication). The broker however (the server in this case) can see the data. To stops this from happening, you need to encrypt the data within the SOAP request using something like XML Security.

XML Security consists of 2 standards (XML Signature and XML Encryption). This can be used to protect to the entire document, or sections individually.

XML Signature Wrapping

One of the problems of XML Security is XML Signature wrapping. As the XML signature should protect against alteration to the document, by allowing validation of specific elements.

An attacker can however relocate the signed element, maintaining the valid signature. Then an attacker can add additional data to the request that are understood by the application layer. As the verification and application logic are separate, the verification will pass due to the presence of a valid signature. The application will then accept the attackers data as validated when it hasn't been confirmed at the validation layer.

This problem was seen in 2011 in Amazon Web Services by bypassing signed SOAP requests. This resulted in the ability for an active attacker to alter the SOAP data and start instances without permission.

Further attacks against SAML were performed, where <10 out of 22 systems tested were vulnerable to signature wrapping attacks.

Attacks on XML encryption

In most cases XML Encryption uses a hybrid encryption scheme (Asymmetric and symmetric keys). Published attacks (2011/2012) exist for both portions of the encryption (adapted chosen-ciphertext attacks) using the server as an oracle.

XML is a text-based data format. Therefore it must be parsed to be understood (usually ASCII encoded). Certain ASCII characters are not parseable or can be excluded. This reduces the understood character set and makes the attack easier.

Validity oracle

Content Decryption

XML parsing

XML Evaluation

Be using this oracle and checking the error type returned, it's possible to see if the failure occurs at the decryption of parsing phase.

This attack is made possible as an attacker can flip bits in the request. Cipher Block Chaining Mode has been dis-

cussed previously in several padding oracle attacks.

Performance (against Symmetric encryption): 14 queries / pain-text byte

How to analyze WebServices Automatically

WS-Attacker tool – https://github.com/RUB-NDS/WS-Attacker

Automated tool to validate attacks against WebServices, implementing XML Signature wrapping and sending requests to the oracle to validate if the system is vulnerable.

If the oracle can be identified, the attack is performed.

Examples of vulnerable systems discovered in testing:

Apache Axis2

Apache CXF

Axway Gateway

IBM DataPower

Microsoft WCF

Countermeasures that were in place for Apache CXF were found to be incorrectly implemented, resulting it being vulnerable to attack.

Conclusion

XML is very complicated, so application of XML Encryption should be validated using tools like WS-Attacker to ensure that it’s not vulnerable.

This attack is also applies to other scenarios like SAML, JSON, Web Crypto

Prefer authentication encryption (AES-GCM instead of AES-CBC)

[DeepSec 2015]How to Break XML Encryption – Automatically

How to Break XML Encryption – Automatically
Juraj Somorovsky (Ruhr University Bochum)

DEEPSEC

In recent years, XML Encryption became a target of several new attacks. These attacks belong to the family of adaptive chosen-ciphertext attacks, and allow an adversary to decrypt symmetric and asymmetric XML ciphertexts, without knowing the secret keys. In order toprotect XML Encryption implementations, the World Wide Web Consortium (W3C) published an updated version of the standard.

Unfortunately, most of the current XML Encryption implementations do not support the newest standard and offer different XML Security configurations to protect confidentiality of the exchanged messages. Resulting from the attack and specification complexity, evaluation of the security configuration correctness becomes tedious and error prone.
In this talk, we will first give an overview on Web Service specific attacks. Afterwards, we present attacks on XML Encryption and how to evaluate security of XML Encryption interfaces automatically. Our algorithm can detect a vulnerability and exploit it to retrieve a plaintext from an encrypted message. To assess practicability of our approach, we implemented an open source attack plugin for Web Service attacking tool called WS-Attacker. With the plugin, we discovered new security problems in four out of five analyzed Web Service implementations, including IBM Datapower or Apache CXF.

What is a WebService and XML Security

SOAP WebService are a standard that allows you to execute a function on the server and receive a response (remote procedure calls). This range from simple to very complex requests.

There are many ways to secure this communication. SSL/TLS can be used to secure the tunnel between the client and server (transport communication). The broker however (the server in this case) can see the data. To stops this from happening, you need to encrypt the data within the SOAP request using something like XML Security.

XML Security consists of 2 standards (XML Signature and XML Encryption). This can be used to protect to the entire document, or sections individually.

XML Signature Wrapping

One of the problems of XML Security is XML Signature wrapping. As the XML signa tect against alteration to the document, by allowing validation of specific elements.

An attacker can however relocate the signed element, tacker can add additional data to the request that are understood by the application layer. As the verification and application log e to the presence of a valid signature. The application will then accept the attackers data as validated when it hasn't been confirm

This problem was seen in 2011 in Amazon Web Service resulted in the ability for an active attacker to alter the SOAP data and start instances without permission.

Further attacks against SAML were performed, where ble to signature wrapping attacks.

Attacks on XML encryption

In most cases XML Encryption uses a hybrid encryption . Published attacks (2011/2012) exist for both portions of the encryption (adapted chosen-ciphertext attacks) using the server as an oracle.

XML is a text-based data format. Therefore it must be parsed to be understood (usually ASCII encoded). Certain ASCII characters are not parseable or can be excluded. This reduces the understood character set and makes the attack easier.

Validity oracle

1. Content Decryption
2. XML parsing
3. XML Evaluation

Be using this oracle and checking the error type returned, it's possible to see if the failure occurs at the decryption of parsing phase.

This attack is made possible as an attacker can flip bits in the request. Cipher Block Chaining Mode has been discussed previously in several padding oracle attacks.

Performance (against Symmetric encryption): 14 queries / pain-text byte

How to analyze WebServices Automatically

WS-Attacker tool – https://github.com/RUB-NDS/WS-Attacker

Automated tool to validate attacks against WebServices, implementing XML Signature wrapping and sending requests to the oracle to validate if the system is vulnerable.

If the oracle can be identified, the attack is performed.

Examples of vulnerable systems discovered in testing:

- Apache Axis2
- Apache CXF
- Axway Gateway
- IBM DataPower
- Microsoft WCF

Countermeasures that were in place for Apache CXF were found to be incorrectly implemented, resulting it being vulnerable to attack.

Conclusion

XML is very complicated, so application of XML Encryption should be validated using tools like WS-Attacker to ensure that it's not vulnerable.

This attack is also applies to other scenarios like SAML, JSON, Web Crypto

Prefer authentication encryption (AES-GCM instead of AES-CBC)

Links:

- Presentation Abstract
- Juraj Somorovsky Twitter
- WS-Attacker – Github – Blogpost
- How to Break XML Encryption – Automatically Paper

http://blog.c22.cc/2015/11/19/deepsec-2015-hacking-cookies-in-modern-web-applications-and-browsers/

Datum: 19.11.2015

Autor: Chris John Riley

Hacking Cookies in Modern Web Applications and Browsers

Dawid Czagan (Silesia Security Lab)

Since cookies store sensitive data (session ID, CSRF token, etc.) they are interesting from an attacker's point of view. As it turns out, quite many web applications (including sensitive ones like bitcoin platforms) have cookie related vulnerabilities, that lead, for example, to user impersonation, remote cookie tampering, XSS and more.

Developers tend to forget that multi-factor authentication does not help if cookies are insecurely processed. Security evaluators underestimate cookie related problems. Moreover, there are problems with the secure processing of cookies in modern browsers. And browser dependent exploitation can be used to launch more powerful attacks. That's why secure cookie processing (from the perspective of web application and browser) is a subject worth discussing. The following topics will be presented:

– cookie related vulnerabilities in web applications
– insecure processing of secure flag in modern browsers
– bypassing HttpOnly flag in Safari
– problems with Domain attribute in Internet Explorer
– cookie tampering in Safari
– underestimated XSS via cookie
– HTTP Strict Transport Security (HSTS)
– importance of regeneration
– and more

Why are we interested in Cookies…
Even when an application enforced 2 Factor Authentication, an attacker can gain access by getting the cookies. Security is always measured at the least protected part. If Cookies aren't correctly protected, then even a 2FA system can be bypassed.Many testers underestimate the security issues caused by mis-configured Cookie protections. Exploitation of Cookie related issues is not limited to local attacks.
Browsers also have issues dealing with secure Cookie processing. These kind of issues can be combined with application issues to make attacks on cookies more impactful.

What are the consequences of insecure Cookie processing?

SQL injection

XSS

User impersonation

…

Web Application

Secure flag and HSTS

Setting “Secure” on Cookies protects the confidentiality of the cookies by making sure that they are only send over secure connections.

RFC6265 prevents this cookie being sent over unencrypted HTTP, however it specifically allows an attacker to overwrite a cookie in the browser. This allows an attacker to inject a cookie (new or overwriting an existing cookie) that will be used in the HTTPS protected sessions.

HSTS to the rescue… even if a Cookie is not marked as “Secure” an HSTS header will tell the browser to only communicate over HTTPS. Therefore it’s not required to set “Secure” right… wrong!

Although HSTS works fine, as long as it’s supported by all major browsers. This is not the case with HSTS, as Internet Explorer 10 doesn’t support it.

Setting both “Secure” and HSTS is the safest mechanism here… to ensure maximum security.

Importance of regeneration

If session IDs are regenerated after a session change (logon, logout, etc…) then this may allow an attacker access (session fixation).

An attacker who can learn the value of the Cookie prior to the user authenticating, can re-use this knowledge once the Cookie is authenticated.

All Cookies with sensitive data or used within the application should be regenerated on a state change (include CSRF tokens etc…)

Server-side invalidation

Just because the session cookie is deleted by the users browser, doesn’t mean that it’s invalidated on the server. This can lead to issues where the session remains open, however the server still has a valid session.

HttpOnly Flag

Assigning this flag prevents a non-HTTP API (e.g JavaScript) from reading out the session Cookie… the theory being, that it can be used to protect against XSS attacks stealing the session Cookies.

Problems here are that RFC6265 talks about “reading” the cookie. However non-HTTP API can still write or overwrite depending on how the RFC is understood and implemented.

Specific browsers (e.g. Safari 9) will allow you to overwrite the cookie. This means that an XSS vulnerability can overwrite the Cookie and switch the user into an attacker controlled account. If the user can then be prompted to enter private data into this session, it is exposed to the attacker.

Combining this with the previously seen session fixation issue (Cookie value not changed after state change). This would allow an attacker to set a known Cookie and use it to gain access to a user’s session once they authenticate.

Domain Attribute

RFC6265 says – When a domain attribute is not specified, then it should only be sent to the domain where it originated.

However Internet Explorer 11 sends this Cookie to all subdomains of this domain.

This can be a real issue where a cookie is set on example.com where a sensitive application lives under example.com/wallet. The cookie is set without the domain attribute, according to the RFC. In Internet Explorer 11 this means that the user will also send this Cookie to sub-domains that are less sensitive, meaning an XSS in test.example.com can read out the Cookie value.

This kind of leakage can happen to externally hosted domains. As the rules only take effect on the Domain name, the fact that the site is hosted externally is incidental, however may expose sensitive data to a 3rd party vendor.

Cookie Tampering

Safari 9 allows comma-separated lists of Cookies (taken from the obsoleted RFC2109)

Example:

/index.php?lang=de,%20PHPSESSID=abc

As this is taken from the request and put into the Set-Cookie header, it allows an attacker fully remotely to tamper with the Cookie jar of the user. This allows changing the users account, as discussed previously.

It’s also possible to perform XSS via Cookie without locally setting a Cookie.

Underestimated XS via Cookie

Commonly this issue has a low assigned risk as the Cookie value has to be set locally. However if you can gain

access to a low sensitive website on a subdomain like x.example.com, you can set a Cookie for y.example.com in order to exploit the user without local access to the browser.

Response splitting also allows exploitation of this issue, by allowing an attacker to set a Cookie by injecting a Set-Cookie header to place the XSS into the browser's Cookie Jar.

Conclusions

Educate development teams about the risks of Cookies

Discuss/improve RFC 6265

Cooperate with Browser vendors

[DeepSec 2015] Hacking Cookies in Modern Web Applications and Browsers

Hacking Cookies in Modern Web Applications and Browsers
Dawid Czagan (Silesia Security Lab)

DEEPSEC

> *Since cookies store sensitive data (session ID, CSRF token, etc.) they are interesting from an attacker's point of view. As it turns out, quite many web applications (including sensitive ones like bitcoin platforms) have cookie related vulnerabilities, that lead, for example, to user impersonation, remote cookie tampering, XSS and more.*
>
> *Developers tend to forget that multi-factor authentication does not help if cookies are insecurely processed. Security evaluators underestimate cookie related problems. Moreover, there are problems with the secure processing of cookies in modern browsers. And browser dependent exploitation can be used to launch more powerful attacks.*
>
> *That's why secure cookie processing (from the perspective of web application and browser) is a subject worth discussing. The following topics will be presented:*
>
> *– cookie related vulnerabilities in web applications*
> *– insecure processing of secure flag in modern browsers*
> *– bypassing HttpOnly flag in Safari*
> *– problems with Domain attribute in Internet Explorer*
> *– cookie tampering in Safari*
> *– underestimated XSS via cookie*
> *– HTTP Strict Transport Security (HSTS)*
> *– importance of regeneration*
> *– and more*

Why are we interested in Cookies…

Even when an application enforced 2 Factor Authentication, an attacker can gain access by getting the cookies. Security is always measured at the least protected part. If Cookies aren't correctly protected, then even a 2FA system can be bypassed.

Many testers underestimate the security issues caused by mis-configured Cookie p oitation of Cookie related issues is not limited to local attacks.

Browsers also have issues dealing with secure Cookie p bined with application issues to make attacks on cookies more impactful.

What are the consequences of insecure Cookie process

- SQL injection
- XSS
- User impersonation
- …

Web Application

Secure flag and HSTS

Setting "Secure" on Cookies protects the confidentiality e only send over secure connections.

RFC6265 prevents this cookie being sent over unencrypted HTTP, however it specifically allows an attacker to overwrite a cookie in the browser. This allows an attacker to inject a cookie (new or overwriting an existing cookie) that will be used in the HTTPS protected sessions.

HSTS to the rescue… even if a Cookie is not marked as "Secure" an HSTS header will tell the browser to only communicate over HTTPS. Therefore it's not required to set "Secure" right… wrong!

Although HSTS works fine, as long as it's supported by all major browsers. This is not the case with HSTS, as Internet Explorer 10 doesn't support it.

Setting both "Secure" and HSTS is the safest mechanism here… to ensure maximum security.

Importance of regeneration

If session IDs are regenerated after a session change (logon, logout, etc…) then this may allow an attacker access (session fixation).

An attacker who can learn the value of the Cookie prior to the user authenticating, can re-use this knowledge once the Cookie is authenticated.

All Cookies with sensitive data or used within the application should be regenerated on a state change (include CSRF tokens etc…)

Server-side invalidation

Just because the session cookie is deleted by the users browser, doesn't mean that it's invalidated on the server. This can lead to issues where the session remains open, however the server still has a valid session.

HttpOnly Flag

Assigning this flag prevents a non-HTTP API (e.g JavaScript) from reading out the session Cookie… the theory being, that it can be used to protect against XSS attacks stealing the session Cookies.

Problems here are that RFC6265 talks about "reading" the cookie. However non-HTTP API can still write or overwrite depending on how the RFC is understood and implemented.

Specific browsers (e.g. Safari 9) will allow you to overwrite the cookie. This means that an XSS vulnerability can overwrite the Cookie and switch the user into an attacker controlled account. If the user can then be prompted to enter private data into this session, it is exposed to the attacker.

Combining this with the previously seen session fixation issue (Cookie value not changed after state change). This would allow an attacker to set a known Cookie and use it to gain access to a user's session once they authenticate.

Domain Attribute

RFC6265 says – When a domain attribute is not specified, then it should only be sent to the domain where it originated.

However Internet Explorer 11 sends this Cookie to all subdomains of this domain.

This can be a real issue where a cookie is set on example.com where a sensitive application lives under example.com/wallet. The cookie is set without the domain attribute, according to the RFC. In Internet Explorer 11 this means that the user will also send this Cookie to sub-domains that are less sensitive, meaning an XSS in test.example.com can read out the Cookie value.

This kind of leakage can happen to externally hosted domains. As the rules only take effect on the Domain name, the fact that the site is hosted externally is incidental, however may expose sensitive data to a 3rd party vendor.

Cookie Tampering

Safari 9 allows comma-separated lists of Cookies (taken from the obsoleted RFC2109)

Example:

```
/index.php?lang=de,%20PHPSESSID=abc
```

As this is taken from the request and put into the Set-Cookie header, it allows an attacker fully remotely to tamper with the Cookie jar of the user. This allows changing the users account, as discussed previously.

It's also possible to perform XSS via Cookie without locally setting a Cookie.

Underestimated XS via Cookie

Commonly this issue has a low assigned risk as the Cookie value has to be set locally. However if you can gain access to a low sensitive website on a subdomain like x.example.com, you can set a Cookie for y.example.com in order to exploit the user without local access to the browser.

Response splitting also allows exploitation of this issue, by allowing an attacker to set a Cookie by injecting a Set-Cookie header to place the XSS into the browser's Cookie Jar.

Conclusions

- Educate development teams about the risks of Cookies
- Discuss/improve RFC 6265
- Cooperate with Browser vendors

http://blog.c22.cc/2015/11/19/deepsec-2015-can-societies-manage-the-sigint-monster/

[DeepSec 2015] Can societies manage the SIGINT monster?

Datum: 19.11.2015

Autor: Chris John Riley

Can societies manage the SIGINT monster?

Duncan Campbell (IPTV Ltd)

Behind closed doors, ubiquitous surveillance systems have evolved in parallel to and hidden within the global communications infrastructure. Developments in signals intelligence (Sigint) technology and tradecraft have shadowed all new telecommunications developments. Sigint agencies have covertly sought to lead, change, and subvert arrangements that IT practitioners make for security and privacy.

Everybody with an open data connection is being monitored and recorded at all time.
We can do privacy and security. The fallacy that we can't have both needs to be disproven.
Even though there's no wall of sheep here, there is an embassy only meters from the hotel were this conference takes place. On the rooftop of the British embassy there is massive surveillance and recording equipment. Phased arrays trying to scan and record anything within range.
This kind of system was exposed in the Snowden document leaks, and boasts a range of collection types (WiFi, CDMA, GSM, Satellite, WiMAX, Microwave, …).
To the other side of the Danube, sitting atop the United Nations tower is an almost identical tower (part of a project called STATEROOM). These are covert special collection sites.
Other collection points exist at the US embassy in Vienna… and are listed in the Snowden leaks.
Outside of Vienna, there are obviously other monitoring stations, including the famous event in Athens were GSM networks were monitored resulting in the death of a telecom employee.
Austria has a history of being central to monitoring within europe dating back many years. These capabilities have only expanded under the RAMPART program, accessing international communications from around the world.
These 3rd party relationships are key to the US monitoring plans.
Access to communications data and monitoring is traded for access to advanced techniques and technologies.
Austria is only one part of the process… with data flowing through Germany and back to Washington for further analysis.
Without knowing the language used to describe things, the Snowden documents (and others) are hard to decipher.
The word hacking isn't used, instead being replaced with words such as "touch" and "implant" to describe mal-

ware.

A brief history of sessionizers:

1998 First optical fibre rate sessionizers

2000 Grandmaster

2002 WEALTHCLUSTER (known publicly as DPI)

2006 TURMOIL (also known as TULLURIAN)

2010 Increased to 10 Gbps

2013 100 Gbps (post Snowden information)

This data is all then fed into projects like XKeystore… however this is a broken system as the recent attacks in Paris show.Extraordinary mis-purposing of systems designed for one use, but resulting in the large-scale collection of data from civilians.

Massive amounts of information, incompetent tools, coupled with wide reaching monitoring.

XKeystore runs on MySQL, relies on Crontab, and uses CADENCE, an ancient and inefficiently designed system (scaled up from the days of telegraphy).

Little intelligence value… You give them big data, and they screw up badly

Anything that they can't get is their biggest target. Access to mobile communications, leading to attacks on Belgacom to get insight into their network and communications.
Even with all that access however, they still don't do their job. Stealing data, but not stopping the attacks that they are meant to detect by invading this privacy.
Recent Wikeleaks data shows that US monitoring stations in the EU are targeting politicians and business talks… and not attempting to try and find the bad guys.
Going for data at scale, exposes their overreach and inability to gain meaningful insight from the data.

Privacy and Security do not trade-off against each other… it's not a zero sum game!

[DeepSec 2015] Can societies manage the SIGINT monster?

Can societies manage the SIGINT monster?
Duncan Campbell (IPTV Ltd)

DEEPSEC

> *Behind closed doors, ubiquitous surveillance systems have evolved in parallel to and hidden within the global communications infrastructure. Developments in signals intelligence (Sigint) technology and tradecraft have shadowed all new telecommunications developments. Sigint agencies have covertly sought to lead, change, and subvert arrangements that IT practitioners make for security and privacy.*

Everybody with an open data connection is being monitored and recorded at all time.

We **can** do privacy and security. The fallacy that we can't have both needs to be disproven.

Even though there's no wall of sheep here, there is an embassy only meters from the hotel were this conference takes place. On the rooftop of the British embassy there is massive surveillance and recording equipment. Phased arrays trying to scan and record anything within range.

This kind of system was exposed in the Snowden document leaks, and boasts a range of collection types (WiFi, CDMA, GSM, Satellite, WiMAX, Microwave, …).

To the other side of the Danube, sitting atop the United Nations tower is an almost identical tower (part of a project called STATEROOM). These are covert special collection sites.

Other collection points exist at the US embassy in Vienna… and are listed in the Snowden leaks.

Outside of Vienna, there are obviously other monitoring stations, including the famous event in Athens were GSM networks were monitored resulting in the death of a telecom employee.

Austria has a history of being central to monitoring within europe dating back many years. These capabilities have only expanded under the RAMPART program, accessing international communications from around the world. These 3rd party relationships are key to the US monitoring plans.

Access to communications data and monitoring is traded for access to advanced techniques and technologies.

Austria is only one part of the process… with data flowing through Germany and [illegible]ton for further analysis.

Without knowing the language used to describe things [illegible] hard to decipher. The word hacking isn't used, instead being replaced with words such as "touch" and "implant" to describe malw[illegible]

A brief history of sessionizers

- 1998 First optical fibre rate sessionizers
- 2000 Grandmaster
- 2002 WEALTHCLUSTER (known publicly as DPI)
- 2006 TURMOIL (also known as TULLURIAN)
- 2010 Increased to 10 Gbps
- 2013 100 Gbps (post Snowden information)

This data is all then fed into projects like XKeystore… h[illegible]nt attacks in Paris show.

Extraordinary mis-purposing of systems designed for one use, but resulting in the large-scale collection of data from civilians.

> *Massive amounts of information, incompetent tools, coupled with wide reaching monitoring.*

XKeystore runs on MySQL, relies on Crontab, and uses CADENCE, an ancient and inefficiently designed system (scaled up from the days of telegraphy).

> *Little intelligence value…*
>
> *You give them big data, and they screw up badly"*

Anything that they can't get is their biggest target. Access to mobile communications, leading to attacks on Belgacom to get insight into their network and communications.

Even with all that access however, they still don't do their job. Stealing data, but not stopping the attacks that they are meant to detect by invading this privacy.

Recent Wikeleaks data shows that US monitoring stations in the EU are targeting politicians and business talks… and not attempting to try and find the bad guys.

Going for data at scale, exposes their overreach and inability to gain meaningful insight from the data.

> *Privacy and Security do not trade-off against each other… it's not a zero sum game!*

Links:

- Presentation Abstract
- Presentation Blogpost
- Duncan Campbell Bio

Related

#FIRST2011 - Security Challenges For Future Systems
In "Conference"

[Plumbercon/Ninjacon] Security in a changing world
In "Conference"

[BruCON] The Belgian beer lovers guide to Cloud Security
In "Conference"

Conference, Security deepsec

← [LHS Microcast] DeepSec 2015

[DeepSec 2015] Hacking Cookies in Modern Web Applications and Browsers →

http://www.monitorpro.si/170797/novice/na-deepsec-2015-tudi-nasi-predavatelji/

Na DeepSec 2015 tudi naši predavatelji

Datum: 16.11.2015

Autor: Stanka Salamun

Na DeepSec 2015, najpomembnejšem varnostno informacijskem dogodku zime v širšem sosedstvu, igramo zadnja leta pomembno vlogo tudi Slovenci – letos s kar dvema našima prispevkoma. To je dober kazalnik, da se domača varnostno informacijska srenja lahko kosa s svetom in da so tudi pri nas strokovnjaki, ki pomembno vplivajo na varnostno stanje globalne informacijske družbe.

Prvi dan konference bo Mitja Kolšek iz družbe ACROS prvič javno predstavil projekt 0patch, inovativni pristop, ki je v celoti plod slovenske pameti. Govoril bo o povsem novih pristopih izdelave varnostnih popravkov, ki bodo omogočili bistveno preprostejši in cenejši način izdelave ter uporabe le-teh, tako za proizvajalce programske opreme kot tudi za uporabnike. Mitja bo obiskovalce konference naučil, kako lahko sami napišejo svoj varnostni popravek za ranljivost v izdelku, za katerega nimajo izvorne kode.
Dan kasneje bodo udeleženci lahko prisluhnili Milanu Gaboru iz podjetja Viris, ki bo predstavil, kako na enostaven način in brez programiranja dobiti hiter vpogled v čudoviti svet paketov Wi-Fi. Iz teh je namreč mogoče pridobiti kopico informacij in do določene mere analizirati celo obnašanje lastnikov telefonov. Vsi ti podatki večinoma »letijo« prosto po zraku in večina uporabnikov se sploh ne zaveda, kako zelo pomembne podatke nosijo s sabo, zato so lahko v nepravih rokah še kako močno orožje napadalcev.


www.monitorpro.si/170797/novice/na-deepsec-2015-tudi-nasi-predavatelji/
Monitor PRO
ZADNJA ŠTEVILKA ARHIV NAROČANJE KJE KUPITI ISKANJE
Prijava
Registracija
Pod Lupo (Whitepaper) Primeri iz prakse
MONITORJEV PANEL
TRENDI IN TEHNOLOGIJE
IT IN POSLOVNA STRATEGIJA
POSLOVNE APLIKACIJE
UPRAVLJANJE IT
PRAVO IN IT
VARNOST IN ZASEBNOST
KARIERE
Izbor uredništva
Fiasko prenove informacijskega sistema davčne uprave z desetmilijonsko škodo
Nov začetek
Lev na kavču
Novi MonitorPro že v trafikah!
Na DeepSec 2015 tudi naši predavatelji
Na DeepSec 2015, najpomembnejšem varnostno informacijskem dogodku zime v širšem sosedstvu, igramo zadnja leta pomembno vlogo tudi Slovenci – letos s kar dvema našima prispevkoma. To je dober kazalnik, da se domača varnostno informacijska srenja lahko kosa s svetom in da so tudi pri nas strokovnjaki, ki pomembno vplivajo na varnostno stanje globalne informacijske družbe. 16.11.2015
Prvi dan konference bo Mitja Kolšek iz družbe ACROS prvič javno predstavil projekt 0patch, inovativni pristop, ki je v celoti plod slovenske pameti. Govoril bo o povsem novih pristopih izdelave varnostnih popravkov, ki bodo omogočili bistveno preprostejši in cenejši način izdelave ter uporabe le-teh, tako za proizvajalce programske opreme kot tudi za uporabnike. Mitja bo obiskovalce konference naučil, kako lahko sami napišejo svoj varnostni popravek za ranljivost v izdelku, za katerega nimajo izvorne kode.
Dan kasneje bodo udeleženci lahko prisluhnili Milanu Gaboru iz podjetja Viris, ki bo predstavil, kako na enostaven način in brez programiranja dobiti hiter vpogled v čudoviti svet paketov Wi-Fi. Iz teh je namreč mogoče pridobiti kopico informacij in do določene mere analizirati celo obnašanje lastnikov telefonov. Vsi ti podatki večinoma »letijo« prosto po zraku in večina uporabnikov se sploh ne zaveda, kako zelo pomembne podatke nosijo s sabo, zato so lahko v napravih rokah še kako močno orožje napadalcev.
nazaj
Komentarji
Novice
Nove grožnje bo vse težje zaznati Družba Kaspersky Lab je organizirala dogodek Cyber...
Microsoft bo ohranil brezplačnih 15 GB Microsoft je zaradi ostrih kritik uporabnikov...
Agilizacija Slovenije Številna slovenska podjetja, tudi največja, so v...
Mariborski EqualEyes zmagal na TechCrunch Disrupt 2015 Ekipa slovensko-angleškega startupa Drugi vid oziroma...
Za nami je prvi finančno-tehnološki Hackathon Gre za prireditev, na kateri je kakih šestdeset...
Arhiv novic ›
Komentarji
Davčne blagajne
Spletno mesto uporablja piškotke z namenom zagotavljanja spletne storitve, oglasnih sistemov in funkcionalnosti, ki jih brez piškotkov ne bi mogli nuditi. Z obiskom in uporabo spletnega mesta soglašate s piškotki.
Strinjam se
Več o piškotkih in nastavitve piškotkov

http://www.golem.de/news/geschaeftsgeheimnisse-sicherheitsforscher-warnt-vor-ttip-1511-117419.html

GESCHÄFTSGEHEIMNISSE: Sicherheitsforscher warnt vor TTIP

Datum: 12.11.2015

Autor: Hauke Gierow

Deepsec 2015 Das Freihandelsabkommmen TTIP hat eine weitere Gegnergruppe: IT-Sicherheitsforscher. Das jedenfalls sagt René Pfeiffer, Organisator der Deepsec in Wien. Er fürchtet, dass Informationen über Sicherheitsrisiken damit noch stärker unterbunden werden.

Der Sicherheitsforscher René Pfeiffer - Organisator der Sicherheitskonferenz Deepsec in Wien - warnt vor dem transatlantischen Freihandelsabkommen TTIP - weil es neue Regelungen zum Schutz von Geschäftsgeheimnissen mitbringt, die auch die IT-Sicherheitsforschung betreffen könnten. Bereits heute werden Sicherheitsforscher häufig von Unternehmen mit Klagen bedroht, wenn sie Informationen über Sicherheitslücken veröffentlichen wollen. Tatsächlich enthalten die aktuellen Entwürfe für TTIP bedenkliche Klauseln, die den Schutz von Geschäftsgeheimnissen deutlich ausweiten sollen. So soll sich, wenn es nach dem aktuellen Entwurf des Abkommens geht, strafbar machen, wer “unautorisierten, willentlichen Zugang zu einem Geschäftsgeheimnis hat, das sich in einem Computersystem befindet”. Davon betroffen wären heute praktisch alle denkbaren Geschäftsgeheimnisse. Ein Problem für Sicherheitsforscher, aber auch Menschen, die illegale Geschäftsgeheimnisse einer Firma an die Öffentlichkeit bringen wollen.

Die IT-Sicherheit wird nicht mit Geschäftsgeheimnissen geschützt

“Wenn Sicherheitsforscher den Quellcode von Produkten nicht untersuchen dürfen, wird die IT-Sicherheit langfristig leiden”, sagte Pfeiffer Golem.de “Sicherheitslücken zu ignorieren oder Untersuchungsergebnisse von Gerichten wegsperren zu lassen, hilft niemandem.” Denn Informationen über Sicherheitslücken zu veröffentlichen, gehört nicht nur zum täglichen Brot der Hacker - sondern ist oft auch das einzige Druckmittel, damit Lücken von den Unternehmen tatsächlich geschlossen werden.Schon heute gibt es zahlreiche Beispiele für Auseinandersetzungen zwischen Forschern und Unternehmen. Hacker, die die Sicherheit moderner Autos testen, machen sich unter Umständen strafbar, wenn sie für ihre Analyse den Quellcode der Software untersuchen. Denn dieser ist oft mit technischen Mitteln wie Verschlüsselung vor einem Zugriff Dritter geschützt und gilt als Geschäftsgeheimnis. Eine Umgehung dieser technischen Sicherungsmaßnahmen ist durch Gesetze wie den Digital Millennium Copyright Act verboten.

Urheberrecht und Geschäftsgeheimnisse gegen Autohacker

Ein Gericht in Großbritannien untersagte bereits im Jahr 2012 die Veröffentlichung eines wissenschaftlichen Artikels, in dem der Sicherheitsforscher Flavio Garcia und andere beschrieben, wie sich der elektronische Startvorgang zahlreicher Autos über Sicherheitslücken in verbauter Mifare-Technologie manipulieren lässt. Der umstrittene Artikel wurde nach zahlreichen Gerichtsverfahren erst in diesem Jahr veröffentlicht.In den USA soll die Rechtslage im kommenden Jahr an die neuen Sicherheitsbedürfnisse angepasst werden - dann treten Ausnahmeregelungen für den Digital Millennium Copyright Act in Kraft, die die Suche nach Sicherheitslücken unter bestimmten Voraussetzungen legalisieren sollen.

Zahlreiche weitere Drohungen, Klagen und abgesagte Vorträge

Die Webseite Attrition.org sammelt in einer fortlaufenden Liste Drohungen von Unternehmen gegen Sicherheitsforscher. Erst im September 2015 erwirkte die Sicherheitsfirma Fireeye eine einstweilige Verfügung gegen die Forscher von ERNW, einem Sicherheitsunternehmen aus Hamburg, das Schwachstellen in Fireeye-Appliances nachgewiesen hatte. Der Vortrag wurde zwar gehalten - musste aber um zahlreiche technische Details beschnitten werden.Ein namentlich nicht genanntes Unternehmen verhinderte der Website zufolge im Jahr 2012 einen Vortrag zu Schwachstellen in Scada-Systemen auf der Konferenz ICS Cyber Security Conference, die innerhalb von Atomkraftwerken eingesetzt werden. Bei derselben Konferenz wurde ein weiterer Vortrag zum selben Thema aus ähnlichen Gründen kurzfristig abgesetzt.

Ein bisschen Entwarnung bei TPP

Zwischenzeitlich hatten in der Open-Source-Szene Berichte über den neuen Entwurf für das Transpazifische Freihandelsabkommen TPP Aufregung entfacht - der Text sei eine Bedrohung für freie Software, weil er unter Umständen die Einhaltung der GPL und ähnlicher Lizenzen unmöglich machen würde. Dieser Deutung hat die Software Freedom Conservancy jetzt jedoch widersprochen. Man lehne das Abkommen zwar nach wie vor ab, für Privatanwender und Programmierer habe der Text jedoch nicht die befürchteten Auswirkungen.Neuer Ärger für Sicherheitsforscher könnte aber im Vereinigten Königreich drohen. Das vor kurzem verabschiedete Überwachungsgesetz - meist nur Snoopers Charter genannt - verbietet es, Details über gefundene Abhörschnittstellen der Regierung zu veröffentlichen. Würde also ein Hacker bei einem von einem Telekommunikationsunternehmen beauftragten Sicherheitsaudit Schwachstellen finden, dann könnten diese von der Regierung stammen. Eine Veröffentlichung der Informationen wäre zumindest solange riskant, wie nicht zweifelsfrei geklärt ist, ob diese Sicherheitslücke absichtlich durch die Regierung eingebaut wurde.Die Deepsec findet am 19. und 20. November in Wien statt. Nach Angaben der Veranstalter steht in diesem Jahr das Thema Industriespionage auf dem Programm - und was Unternehmen dagegen tun können. Golem.de wird von dort berichten.

Original-URL des Artikels: http://www.golem.de/news/geschaeftsgeheimnisse-sicherheitsforscher-warnt-vor-ttip-1511-117419.html **Veröffentlicht:** 12.11.2015 12:00

Geschäftsgeheimnisse

Sicherheitsforscher warnt vor TTIP

Deepsec 2015 Das Freihandelsabkommmen TTIP hat eine weitere Gegnergruppe: IT-Sicherheitsforscher. Das jedenfalls sagt René Pfeiffer, Organisator der Deepsec in Wien. Er fürchtet, dass Informationen über Sicherheitsrisiken damit noch stärker unterbunden werden.

Der Sicherheitsforscher René Pfeiffer - Organisator der Sicherheitskonferenz Deepsec in Wien - warnt vor dem transatlantischen Freihandelsabkommen TTIP - weil es neue Regelungen zum Schutz von Geschäftsgeheimnissen mitbringt, die auch die IT-Sicherheitsforschung betreffen könnten. Bereits heute werden Sicherheitsforscher häufig von Unternehmen mit Klagen bedroht, wenn sie Informationen über Sicherheitslücken veröffentlichen wollen.

Tatsächlich enthalten die aktuellen Entwürfe für TTIP bedenkliche Klauseln, die den Schutz von Geschäftsgeheimnissen deutlich ausweiten sollen. So soll sich, wenn es nach dem aktuellen Entwurf des Abkommens geht, strafbar machen, wer "*unautorisierten, willentlichen Zugang zu einem Geschäftsgeheimnis hat, das sich in einem Computersystem befindet*". Davon betroffen wären heute praktisch alle denkbaren Geschäftsgeheimnisse. Ein Problem für Sicherheitsforscher, aber auch Menschen, die illegale Geschäftsgeheimnisse einer Firma an die Öffentlichkeit bringen wollen.

Die IT-Sicherheit wird nicht mit Geschäftsgeheimnissen geschützt

"*Wenn Sicherheitsforscher den Quellcode von Produkten nicht untersuchen dürfen, wird die IT-Sicherheit langfristig leiden*", sagte Pfeiffer Golem.de "*Sicherheitslücken zu ignorieren oder Untersuchungsergebnisse von Gerichten wegsperren zu lassen, hilft niemandem*." Denn Informationen über Sicherheitslücken zu veröffentlichen, gehört nicht nur zum täglichen Brot der Hacker - sondern ist oft auch das einzige Druckmittel, damit Lücken von den Unternehmen tatsächlich geschlossen werden.

Schon heute gibt es zahlreiche Beispiele für Auseinandersetzungen zwischen Forschern und Unternehmen. Hacker, die die Sicherheit moderner Autos testen, machen sich unter Umständen strafbar, wenn sie für ihre Analyse den Quellcode der Software untersuchen. Denn dieser ist oft mit technischen Mitteln wie Verschlüsselung vor einem Zugriff Dritter geschützt und gilt als Geschäftsgeheimnis. Eine Umgehung dieser technischen Sicherungsmaßnahmen ist durch Gesetze wie den Digital Millennium Copyright Act verboten.

Urheberrecht und Geschäftsgeheimnisse gegen Autohacker

Ein Gericht in Großbritannien untersagte bereits im Jahr 2012 die Veröffentlichung eines wissenschaftlichen Artikels, in dem der Sicherheitsforscher Flavio Garcia und andere beschrieben, wie sich der elektronische Startvorgang zahlreicher Autos über Sicherheitslücken in verbauter Mifare-Technologie manipulieren lässt. Der umstrittene Artikel wurde nach zahlreichen Gerichtsverfahren erst in diesem Jahr veröffentlicht.

In den USA soll die Rechtslage im kommenden Jahr an die neuen Sicherheitsbedürfnisse angepasst werden - dann treten Ausnahmeregelungen für den Digital Millennium Copyright Act in Kraft, die die Suche nach Sicherheitslücken unter bestimmten Voraussetzungen legalisieren sollen.

Zahlreiche weitere Drohungen, Klagen und abgesagte Vorträge

Die Webseite Attrition.org sammelt in einer fortlaufenden Liste Drohungen von Unternehmen gegen Sicherheitsforscher. Erst im September 2015 erwirkte die Sicherheitsfirma Fireeye eine einstweilige Verfügung gegen die Forscher von ERNW, einem Sicherheitsunternehmen aus Hamburg, das Schwachstellen in Fireeye-Appliances nachgewiesen hatte. Der Vortrag wurde zwar gehalten - musste aber um zahlreiche technische Details beschnitten werden.

Ein namentlich nicht genanntes Unternehmen verhinderte der Website zufolge im Jahr 2012 einen Vortrag zu Schwachstellen in Scada-Systemen auf der Konferenz ICS Cyber Security Conference, die innerhalb von Atomkraftwerken eingesetzt werden. Bei derselben Konferenz wurde ein weiterer Vortrag zum selben Thema aus ähnlichen Gründen kurzfristig abgesetzt.

Ein bisschen Entwarnung bei TPP

Zwischenzeitlich hatten in der Open-Source-Szene Berichte über den neuen Entwurf für das Transpazifische Freihandelsabkommen TPP Aufregung entfacht - der Text sei eine Bedrohung für freie Software, weil er unter Umständen die Einhaltung der GPL und ähnlicher Lizenzen unmöglich machen würde. Dieser Deutung hat die Software Freedom Conservancy jetzt jedoch widersprochen. Man lehne das Abkommen zwar nach wie vor ab, für Privatanwender und Programmierer habe der Text jedoch nicht die befürchteten Auswirkungen.

Neuer Ärger für Sicherheitsforscher könnte aber im Vereinigten Königreich drohen. Das vor kurzem verabschiedete Überwachungsgesetz - meist nur Snoopers Charter genannt - verbietet es, Details über gefundene Abhörschnittstellen der Regierung zu veröffentlichen. Würde also ein Hacker bei einem von einem Telekommunikationsunternehmen beauftragten Sicherheitsaudit Schwachstellen finden, dann könnten diese von der Regierung stammen. Eine Veröffentlichung der Informationen wäre zumindest solange riskant, wie nicht zweifelsfrei geklärt ist, ob diese Sicherheitslücke absichtlich durch die Regierung eingebaut wurde.

Die Deepsec findet am 19. und 20. November in Wien statt. Nach Angaben der Veranstalter steht in diesem Jahr das Thema Industriespionage auf dem Programm - und was Unternehmen dagegen tun können. Golem.de wird von dort berichten. (hg)

Verwandte Artikel:
Troopers: Ruhe bewahren im Cyberkriegsgetümmel
(15.03.2013 14:31, http://www.golem.de/news/it-sicherheitskonferenz-troopers-ruhe-bewahren-im-cyberkriegsgetuemmel-1303-98202.html)
IT-Sicherheit: Zero-Day-Lücke in Java 1.8 entdeckt
(14.07.2015 09:40, http://www.golem.de/news/it-sicherheit-zero-day-luecke-in-java-1-8-entdeckt-1507-115202.html)
Android-Sicherheit: Google kann nicht ohne weiteres geschützte Geräte entsperren
(25.11.2015 11:41, http://www.golem.de/news/android-sicherheit-google-kann-nicht-ohne-weiteres-geschuetzte-geraete-entsperren-1511-117629.html)
Security: Amazon.com setzt Passwörter von Kunden zurück
(25.11.2015 13:18, http://www.golem.de/news/security-amazon-com-setzt-passwoerter-von-kunden-zurueck-1511-117634.html)
Allgemeine Relativitätstheorie: Knapp vier Seiten verändern die Welt
(25.11.2015 17:40, http://www.golem.de/news/allgemeine-relativitaetstheorie-knapp-vier-seiten-veraendern-die-welt-1511-117641.html)

---

http://fm4.orf.at/stories/1763953/

Kryptologen schlagen gegen die NSA zurück

Datum: 22.10.2015

Autor: Erich Möchel

Freie “https”-Zertifikate zur Website-Verschlüsselung vor dem Start. Seit einer Woche ist auch klar, wie die NSA serienweise Virtual Private Networks von Firmen knackt.

Zwei Jahre nach dem Beginn der Enthüllungen Edward Snowdens werden die technischen Folgen dieser Leaks für die NSA nun schlagend. Seit Dienstag werden die freien Zertifikate der Sicherheitsinitiative “Let’s encrypt” von allen Browsern anerkannt, damit ist sichere und kostenlose Verschlüsselung für alle Betreiber von Websites in Kürze möglich. “Let’s encrypt”, hinter der die Mozilla Stiftung (Firefox) steht, war als Reaktion auf das Bekanntwerden des NSA-Massenabgriffs von Daten an den Glasfasern Ende 2014 gegründet worden.

Eine Studie von namhaften Kryptologen sorgt seit einer Woche für Aufregung in der Industrie. Das Forscherteam um Professor Alex Halderman (University of Michigan) hat nämlich eines der größten Rätsel in den Snowden-Leaks geklärt: Wie die NSA eine so enorme Zahl an verschlüsselten Verbindungen - vor allem von Firmen - automatisiert abgreifen konnte, obwohl die Schlüssel selbst bis heute nicht geknackt werden können.

Handlungsbedarf für die Wirtschaft

Besonders für Unternehmen besteht nun einigermaßen dringender Handlungsbedarf, weil der weltweite de-facto-Industriestandard zur Erzeugung von 1024-Bit starker Verschlüsselung großteils gebrochen ist. Diese Studie mit dem Titel “Imperfect Forward Secrecy” wirft nämlich zwei technische Paradigmen über den Haufen. Die bis jetzt gültige Annahme, dass 1024-bit Algorithmen vor solchen Massenzugriffen sicher sind, wurde damit außer Kraft gesetzt. Zudem kam heraus, dass die nach ihren Erfindern “Diffie-Hellman” benannte Methode zum Aufbau der Verschlüsselung ihre Tücken hat, obwohl sie prinzipiell auch weiterhin als sicher gilt. “2048-Bit und stärkere Versionen gelten noch als sicher und werden von allen modernen Implementierungen unterstützt”, sagte der Wiener Sicherheitsexperte Michael Kafka zu ORF.at.

Vorgegebene Primzahlen

Der Haken an dieser ältesten Methode zum sicheren Austausch geheimer Schlüssel in einem unsicheren Umfeld wie dem Internet habe vor allem historische Gründe, so Kafka zu ORF.at. Da die Rechner zur Zeit der ersten Imple-

mentationen von Diffie-Hellman während der 80er Jahre noch sehr langsam waren, wurden die für die Berechnung der jeweiligen Sitzungsschlüssel benötigten, extralangen Primzahlen nicht jeweils aktuell berechnet.

Man griff vielmehr auf vorgegebene Primzahlen zurück, allein für 512-Bit-Schlüssel, die schon länger als unsicher galten, hat diese Primzahl 232 Stellen. Damit greifen die meisten der Abermillionen Anwendungen der Methode Diffie-Hellman auf höchstens ein oder zwei Dutzend verschiedener solcher Primzahlen zu, die alle öffentlich bekannt sind. So greift eine große Mehrheit der verbreiteten Apache-Webserver auf ein- und dieselbe Primzahl zurück.

“Pre-Computing” bekannter Primzahlen

“Das galt lange nicht als problematisch, weil die Kenntnis dieser Primzahlen bei ‘brute force’-Angriffen direkt auf die Schlüssel keinen Nutzen hat”, sagte Kafka, “die technische Entwicklung hat allerdings dafür gesorgt, dass nun andersartige Angriffe möglich sind.” Anstatt den Schlüssel selbst frontal anzugreifen, wird “Pre-Computing” auf diese Primzahl angewendet, um den Schlüssel auf diesem Weg aufzukriegen. “Diese Methode ähnelt sehr den ‘Rainbow Tables’, die etwa zum Cracken von Passwörtern und Angriffen auf die GSM-Verschlüsselung zum Einsatz kommen. Dabei werden die für einen solchen Angriff wichtigen Zwischenschritte vorausberechnet und in großen Tabellen gespeichert”, sagte Kafka, “das sorgt für eine massive Kürzung der Berechnungszeit.”

Diese Vorabberechnungen einer oder mehrerer dieser Primzahlen erklären den “Durchbruch in der Verschlüsselungstechnologie” der NSA, über den der weltweit wohl beste Kenner dieser Spionageorganisatioon, James Bamford, 2012 erstmals berichtet hat. Laut Bamford, der Mitte November einen Vortrag bei der Sicherheitskonferenz Deepsec in Wien halten wird, machte dieser nicht näher bekannte “Durchbruch” den Bau des monströsen Datencenters im US-Bundesstaat Utah nötig.

Des Rätsels Lösung

Auch die Snowden-Dokumente über das TURMOIL-Programm geben keinen Aufschluss über diese neuen Methoden der NSA beim Schlüsselknacken, wohl aber zeigen sie, dass der Geheimdienst massive Datensätze aus verschlüsselten Firmennetzen (VPNs) routinemäßig abzieht und bis zu einem gewissen Ausmaß auch auf SSL/TLS-verschlüsselten Datenverkehr zugreifen kann. Man wußte bloß nicht, wie.

Dieses Rätsel haben Professor Halderman und die anderen Kryptographen gelöst und auch gleich eine Kostenschätzung angestellt. Zwar ist der Aufwand für alle zum “Pre-Computing” nötigen Rechenschritte mit 45 Millionen Prozessorjahren absurd hoch, jeder moderne Rechencluster aus dem Top-Segment verfügt allerdings über zigtausende solcher Prozessoren. Zudem sind die dort verbauten Allzweck-CPUs nur bedingt für die Schlüsselknack-

erei geeignet, im Design für diese Aufgabe optimierte ASIC-Chips würden die Kosten - und damit die Zeitdauer der Berechnung - um das Achtzigfache verringern. Letztendlich kommen die Kryptographen auf eine Kostenschätzung von mehreren 100 Millionen Dollar für eine solche Installation, mit deren Hilfe eine 1024-bit entsprechende Primzahl binnen eines Jahres so vorberechnet werden könnte, dass die Schlüsselknackerei dann nahe an Echtzeit möglich ist.

Das schwarze Budget für Kryptoanalyse

Angesichts von 600 Millionen allein für zwei Programme der NSA zum Thema Kryptoanalyse - also Schüsselknacken - im “schwarzen Budget” des Jahres 2012, sind die Thesen von Halderman und Co ausgesprochen plausibel. Und: Sie korrelieren mit den Informationen aus den Snowden-Leaks, aus denen klar hervorgeht, dass die NSA einen Routineweg zum Eindringen in Virtual Private Networks gefunden hat, die von allen Firmen rund um die Welt zur Vernetzung ihrer Filialen benutzt werden. Die Kryptographen haben hochgerechnet, dass die Aufbereitung einer einzigen 1024-bit Primzahl den Verkehr von 18 Prozent aller mit “https” verschlüsselten Websites öffnet, über eine zusätzliche zweite käme man dann bereits auf 66 Prozent aller VPNS mit dem IPSec-Protokoll und 26 % jener Firmennetze die SSH benutzen.

Deshalb ist gerade jetzt für Firmen Handlungsbedarf, die verhindern wollen, dass die Geschäftsgeheimnisse aus ihren Firmennetzen Tag für Tag im US-Bundesstaat Utah landen. Das wird nicht in Kürze zu bewerkstelligen sein, denn das nötige Upgrade aller unsicheren Anwendungen auf 2048-bit ist zeitaufwändig und wird in vielen Fällen neue Hardware nötig machen. Ebensowenig wird es durch “Let’s encrypt” sofort messbare Änderungen geben, denn bis die nötige Infrastruktur mit Zertifikations-Servern operativ ist, wird noch etwas Zeit vergehen. Wie komplex dieses Vorhaben nämlich ist, zeigt schon die Beschreibung der Zertifikatspolitik, die mehr als 80 Seiten in Anspruch nimmt.

Fazit und Ausblick

Von der neuen Zertifikatsstelle “Let’s encrypt” ist an technischen wie operativen Sicherheitsmaßnahmen Einiges zu erwarten, zumal auch der Hauptautor der Studie über den NSA-Angriff auf die Standardprimzahlen, nämlich Professor Alex Halderman im Vorstand dieser Initiative sitzt. In der NSA laufen gerade die Vorbereitungen auf die für 29. November geplante Abschaltung mehrerer Programme, mit denen sie bis jetzt sämtlichen Datenverkehr aus den Telefonienetzen der USA abgezapft hat. Die Folgen der Studie von Halderman und Co. aber wird der mächtigste Geheimdienstapparat erst im Anschluss zu spüren bekommen.

Es ist völlig klar, dass die überkommenen Methoden für Schlüsseltausch nach der Methode Diffie-Hellman mit

vordefinierten Primzahlen relativ schnell zugunsten neuer und sicherer Methoden fallengelassen werden. Die NSA verfügt zwar über den größten Apparat und das weitaus größte Budget aller weltweiten Geheimdienste und wird von der US-Regierung, wo es nur geht, bis jetzt gedeckt. Doch neben den großen Internetkonzernen, die obendrein alle US-Unternehmen sind, hat die Agency noch einen weitaus mächtigeren Gegner: Sie hat die Mathematik gegen sich.

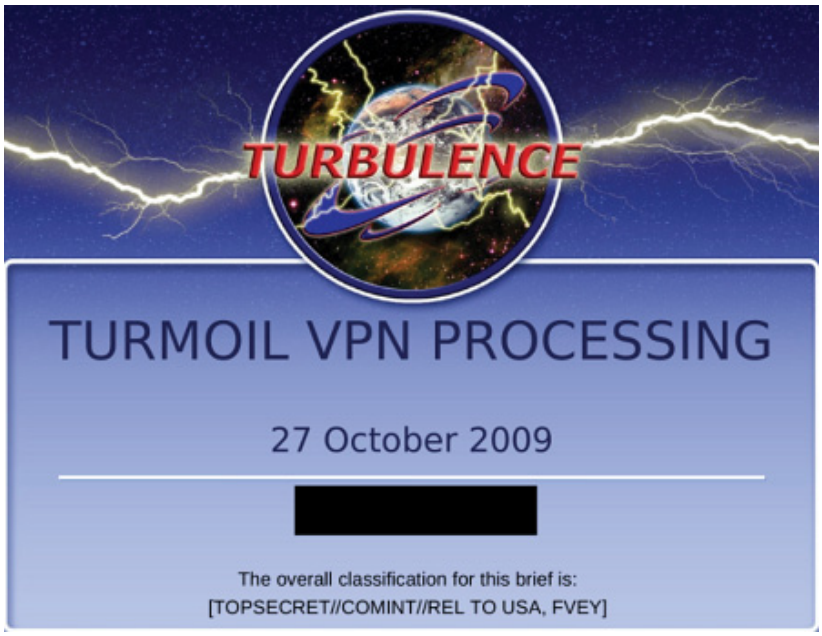
Erstellt am: 22. 10. 2015 - 19:00 Uhr

Kryptologen schlagen gegen die NSA zurück

Freie "https"-Zertifikate zur Website-Verschlüsselung vor dem Start. Seit einer Woche ist auch klar, wie die NSA serienweise Virtual Private Networks von Firmen knackt.

Zwei Jahre nach dem Beginn der Enthüllungen Edward Snowdens werden die technischen Folgen dieser Leaks für die NSA nun schlagend. Seit Dienstag werden die freien Zertifikate der Sicherheitsinitiative "Let's encrypt" von allen Browsern anerkannt, damit ist sichere und kostenlose Verschlüsselung für alle Betreiber von Websites in Kürze möglich. "Let's encrypt", hinter der die Mozilla Stiftung (Firefox) steht, war als Reaktion auf das Bekanntwerden des NSA-Massenabgriffs von Daten an den Glasfasern Ende 2014 gegründet worden.

Eine Studie von namhaften Kryptologen sorgt seit einer Woche für Aufregung in der Industrie. Das Forscherteam um Professor Alex Halderman (University of Michigan) hat nämlich eines der größten Rätsel in den Snowden-Leaks geklärt: Wie die NSA eine so enorme Zahl an verschlüsselten Verbindungen - vor allem von Firmen - automatisiert abgreifen konnte, obwohl die Schlüssel selbst bis heute nicht geknackt werden können.



Public Domain

Neben der Sicherheitsstufe "Top Secret" haben diese Folien noch die höhere Klassifikation COMINT wegen ihres direkten Bezugs auf operative Nachrichtenaufklärung

Handlungsbedarf für die Wirtschaft

Die Sammlung von "Betriebsgeheimnissen und anderen Daten ausländischer Firmen" der NSA diene "ausschließlich dem Schutz der nationalen Sicherheit der USA und ihrer Alliierten", heißt es dazu offiziell

Besonders für Unternehmen besteht nun einigermaßen dringender Handlungsbedarf, weil der weltweite de-facto-Industriestandard zur Erzeugung von 1024-Bit starker Verschlüsselung großteils gebrochen ist. Diese Studie mit dem Titel "Imperfect Forward Secrecy" wirft nämlich zwei technische Paradigmen über den Haufen. Die bis jetzt gültige Annahme, dass 1024-bit Algorithmen vor solchen Massenzugriffen sicher sind, wurde damit außer Kraft gesetzt. Zudem kam heraus, dass die nach ihren Erfindern "Diffie-Hellman" benannte Methode zum Aufbau der Verschlüsselung ihre Tücken hat, obwohl sie prinzipiell auch weiterhin als sicher gilt. "2048-Bit und stärkere Versionen gelten noch als sicher und werden von allen modernen Implementierungen unterstützt", sagte der Wiener Sicherheitsexperte Michael Kafka zu ORF.at.

Vorgegebene Primzahlen

Die "Let's Encrypt"- Initiative geht von der gemeinnützigen "Internet Research Group aus", die von Mozilla, Cisco, Akamai und der Electronic Frontier Foundation getragen wird (https://letsencrypt.org/documents/ISRG-CP-May-5-2015.pdf)

Der Haken an dieser ältesten Methode zum sicheren Austausch geheimer Schlüssel in einem unsicheren Umfeld wie dem Internet habe vor allem historische Gründe, so Kafka zu ORF.at. Da die Rechner zur Zeit der ersten Implementationen von Diffie-Hellman während der 80er Jahre noch sehr langsam waren, wurden die für die Berechnung der jeweiligen Sitzungsschlüssel benötigten, extralangen Primzahlen nicht jeweils aktuell berechnet.

```
6.2 Second Oakley Group

   IKE implementations SHOULD support a MODP group with the following
   prime and generator. This group is assigned id 2 (two).

   The prime is 2^1024 - 2^960 - 1 + 2^64 * { [2^894 pi] + 129093 }.
   Its hexadecimal value is

         FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1
         29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD
         EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245
         E485B576 625E7EC6 F44C42E9 A637ED6B 0BFF5CB6 F406B7ED
         EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE65381
         FFFFFFFF FFFFFFFF

   The generator is 2 (decimal)
```

IETF

Das ist die Primzahl für 1024 -bit starke Verschlüsselung die bereits aus dem Internetstandard RFC 2409 von 1998 stammt (https://www.rfc-editor.org/rfc/rfc2409.txt) . Anstatt in einer Zahl mit 309 Stellen werden so hohe Werte entweder als Gleichung oder hexadezimal dargestellt.

"Imperfect Forward Secrecy" - kryptolgische Studie des NSA-Angriffs auf die Primzahlen, die bei der Methode Diffie-Hellman zum Einsatz kommen (https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf)

Man griff vielmehr auf vorgegebene Primzahlen zurück, allein für 512-Bit-Schlüssel, die schon länger als unsicher galten, hat diese Primzahl 232 Stellen. Damit greifen die meisten der Abermillionen Anwendungen der Methode Diffie-Hellman auf höchstens ein oder zwei Dutzend verschiedener solcher Primzahlen zu, die alle öffentlich bekannt sind. So greift eine große Mehrheit der verbreiteten Apache-Webserver auf ein- und dieselbe Primzahl zurück.

"Pre-Computing" bekannter Primzahlen

Der im European Telecom Standards Institute geplante Standard für "lawful interception" von mobilen Datenverkehr sah eine ähnliche Methode des Angriffs während des initialen Schlüsseltausches vor. Statt auf vorberechnete Primzahlen griff man auf nicht-zufällige Zahlen eines manipulierten Generators für Pseudo-Zufallszahlern zurück

"Das galt lange nicht als problematisch, weil die Kenntnis dieser Primzahlen bei 'brute force'-Angriffen direkt auf die Schlüssel keinen Nutzen hat", sagte Kafka, "die technische Entwicklung hat allerdings dafür gesorgt, dass nun andersartige Angriffe möglich sind." Anstatt den Schlüssel selbst frontal anzugreifen, wird "Pre-Computing" auf diese Primzahl angewendet, um den Schlüssel auf diesem Weg aufzukriegen. "Diese Methode ähnelt sehr den 'Rainbow Tables', die etwa zum Cracken von Passwörtern und Angriffen auf die GSM-Verschlüsselung zum Einsatz kommen. Dabei werden die für einen solchen Angriff wichtigen Zwischenschritte vorausberechnet und in großen Tabellen gespeichert", sagte Kafka, "das sorgt für eine massive Kürzung der Berechnungszeit."

James Bamford

James Bamford ist Autor mehrerer Standardwerke über die NSA, deren erstes bereits 1982 erschienen ist (https://en.wikipedia.org/wiki/James_Bamford) .

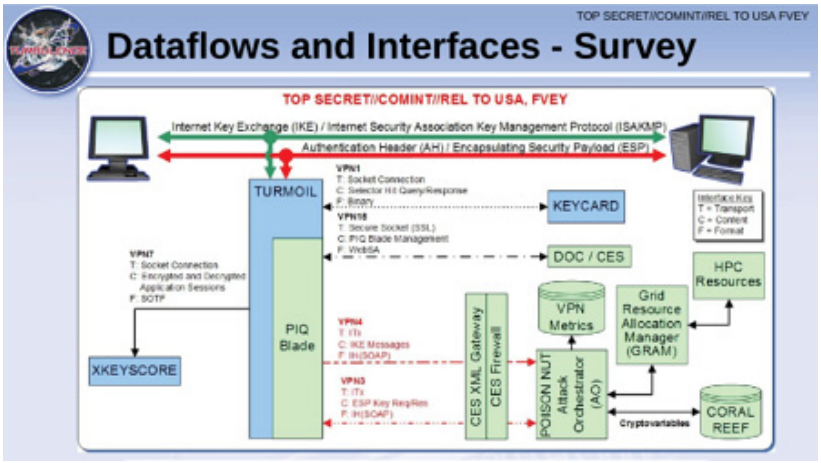
Diese Vorabberechnungen einer oder mehrerer dieser Primzahlen erklären den "Durchbruch in der Verschlüsselungstechnologie" der NSA, über den der weltweit wohl beste Kenner dieser Spionageorganisatioon, James Bamford, 2012 erstmals berichtet hat. Laut Bamford, der Mitte November einen Vortrag bei der Sicherheitskonferenz Deepsec in Wien halten wird, machte dieser nicht näher bekannte "Durchbruch" den Bau des monströsen Datencenters im US-Bundesstaat Utah nötig.

Des Rätsels Lösung

Auch die Snowden-Dokumente über das TURMOIL-Programm geben keinen Aufschluss über diese neuen Methoden der NSA beim Schlüsselknacken, wohl aber zeigen sie, dass der Geheimdienst massive Datensätze aus verschlüsselten Firmennetzen (VPNs) routinemäßig abzieht und bis zu einem gewissen Ausmaß auch auf SSL/TLS-verschlüsselten Datenverkehr zugreifen kann. Man wußte bloß nicht, wie.

James Bamford wird einen der ersten Vorträge auf der Wiener Sicherheitskonferenz DeepSec halten, die am 19. November in Wien beginnt (http://deepsec.net/schedule.html) . Anders als vergleichbare Konferenzen ist die DeepSec "community driven", sie wird von Hackern aus dem Umkreis des Metalabs organisiert.

Dieses Rätsel haben Professor Halderman und die anderen Kryptographen gelöst und auch gleich eine Kostenschätzung angestellt. Zwar ist der Aufwand für alle zum "Pre-Computing" nötigen Rechenschritte mit 45 Millionen Prozessorjahren absurd hoch, jeder moderne Rechencluster aus dem Top-Segment verfügt allerdings über zigtausende solcher Prozessoren. Zudem sind die dort verbauten Allzweck-CPUs nur bedingt für die Schlüsselknackerei geeignet, im Design für diese Aufgabe optimierte ASIC-Chips würden die Kosten - und damit die Zeitdauer der Berechnung - um das Achtzigfache verringern. Letztendlich kommen die Kryptographen auf eine Kostenschätzung von mehreren 100 Millionen Dollar für eine solche Installation, mit deren Hilfe eine 1024-bit entsprechende Primzahl binnen eines Jahres so vorberechnet werden könnte, dass die Schlüsselknackerei dann nahe an Echtzeit möglich ist.



Public Domain

Die Datenflüsse beim Knacken von 1024-bit starken Schlüsseln in einer Folie der NSA. Ganz links ist zu sehen, dass die Ergebnisse auch direkt an die Metasuchmaschine XKEYSCORE der NSA-Analysten gehen.

Die NSA-Folien zum TURMOIL-Programm wurden vom "Spiegel" 2013 veröffentlicht (`http://www.spiegel.de/media/media-35526.pdf`)

Das schwarze Budget für Kryptoanalyse

Angesichts von 600 Millionen allein für zwei Programme der NSA zum Thema Kryptoanalyse - also Schüsselknacken - im "schwarzen Budget" des Jahres 2012, sind die Thesen von Halderman und Co ausgesprochen plausibel. Und: Sie korrelieren mit den Informationen aus den Snowden-Leaks, aus denen klar hervorgeht, dass die NSA einen Routineweg zum Eindringen in Virtual Private Networks gefunden hat, die von allen Firmen rund um die Welt zur Vernetzung ihrer Filialen benutzt werden. Die Kryptographen haben hochgerechnet, dass die Aufbereitung einer einzigen 1024-bit Primzahl den Verkehr von 18 Prozent aller mit "https" verschlüsselten Websites öffnet, über eine zusätzliche zweite käme man dann bereits auf 66 Prozent aller VPNS mit dem IPSec-Protokoll und 26 % jener Firmennetze die SSH benutzen.

Metalab

Der Sicherheitsexperte Michael Kafka ist einer der sieben Mitgründer des Wiener Hackerspace Metalab und Miterfinder der DeepSec-Konferenz.

Deshalb ist gerade jetzt für Firmen Handlungsbedarf, die verhindern wollen, dass die Geschäftsgeheimnisse aus ihren Firmennetzen Tag für Tag im US-Bundesstaat Utah landen. Das wird nicht in Kürze zu bewerkstelligen sein, denn das nötige Upgrade aller unsicheren Anwendungen auf 2048-bit ist zeitaufwändig und wird in vielen Fällen neue Hardware nötig machen. Ebensowenig wird es durch "Let's encrypt" sofort messbare Änderungen geben, denn bis die nötige Infrastruktur mit Zertifikations-Servern operativ ist, wird noch etwas Zeit vergehen. Wie komplex dieses Vorhaben nämlich ist, zeigt schon die Beschreibung der Zertifikatspolitik, die mehr als 80 Seiten in Anspruch nimmt.

Fazit und Ausblick

Von der neuen Zertifikatsstelle "Let's encrypt" ist an technischen wie operativen Sicherheitsmaßnahmen Einiges zu erwarten, zumal auch der Hauptautor der Studie über den NSA-Angriff auf die Standardprimzahlen, nämlich Professor Alex Halderman im Vorstand dieser Initiative sitzt. In der NSA laufen gerade die Vorbereitungen auf die für 29. November geplante Abschaltung mehrerer Programme, mit denen sie bis jetzt sämtlichen Datenverkehr aus den Telefonienetzen der USA abgezapft hat. Die Folgen der Studie von Halderman und Co. aber wird der mächtigste Geheimdienstapparat erst im Anschluss zu spüren bekommen.

Es ist völlig klar, dass die überkommenen Methoden für Schlüsseltausch nach der Methode Diffie-Hellman mit vordefinierten Primzahlen relativ schnell zugunsten neuer und sicherer Methoden fallengelassen werden. Die NSA verfügt zwar über den größten Apparat und das weitaus größte Budget aller weltweiten Geheimdienste und wird von der US-Regierung, wo es nur geht, bis jetzt gedeckt. Doch neben den großen Internetkonzernen, die obendrein alle US-Unternehmen sind, hat die Agency noch einen weitaus mächtigeren Gegner: Sie hat die Mathematik gegen sich.

http://www.finanzen.at/nachrichten/aktien/DeepSec-Workshops-Digitale-Verteidigung-Wissen-ist-Macht-IT-Security-Workshops-fuer-moderne-Unternehmen-1000866401

DeepSec-Workshops: Digitale Verteidigung - Wissen ist Macht - IT-Security-Workshops für moderne Unternehmen

Datum: 20.10.12015

Autor: René Pfeiffer

-1 of 2- 20 Oct 2015 06:30:00 UTC DJ DeepSec-Workshops: Digitale Verteidigung - Wissen ist Macht - IT-Security-Workshops für moderne Unternehmen

Wien (pts008/20.10.2015/08:30) - Wann haben Sie Ihren letzten Geschäftsbrief geschrieben? Und wann haben Sie das letzte Mal Stift und Papier dazu benutzt? Es macht nichts, wenn Sie sich nicht daran erinnern können: Digitale Kommunikation ist Teil unseres Alltagslebens, nicht nur in der Geschäftswelt. Wir haben uns so sehr daran gewöhnt, ständig online zu kommunizieren, dass offline sein sich schon fast unnatürlich anfühlt. Das heißt natürlich auch, dass wir ständig irgendwelchen Netzwerken ausgeliefert sind, vor allem dem Internet. Unsere Tür steht Tag und Nacht offen. Wir können sie nicht mehr schließen und laden somit offen auch ungebetene Gäste ein, die dieselben Netzwerke nutzen wie wir. Es ist Zeit, ernsthaft darüber nachzudenken. Was für Bedrohungen gibt es da draußen? Und wie können wir uns vor ihnen schützen?

Cyber-Kriminalität und Datenschutz

Alles ist "Cyber" heutzutage. Kriminalität genauso wie Sicherheitsbestrebungen. Das Militär verwendet das chice Wort, um ihre Strategien und Taktiken zu beschreiben. Die Politik hat das Wort entdeckt, genauso wie Journalisten und PR-Strategen. Doch der Gebrauch dieses Worts birgt Risiken, es verbirgt, wie die digitale Welt wirklich funktioniert im Nebel einer leicht mystischen Aura. Aber wenn es um die Verteidigung Ihrer Daten geht, ist Nebel das Letzte, was Sie brauchen. Sie brauchen Wissen und harte Fakten, klare Sicht. Ablenkung und Missverständnisse sind Ihre Feinde, genauso wie bedeutungslose Trendwörter.

Hive Mind Technology

Informationssicherheit ist ein weites Feld. Vor Jahrzehnten ging es nur um Systeme mit lokal gespeicherten Daten und ein junges Internet, das seine zarten Fühler ausstreckte. Natürlich gab es auch schon damals Stör- und Zwischenfälle, aber die Auswirkungen waren nicht auf der ganzen Welt zu spüren. Heute ist das anders. Wachstum hat seine Nebenwirkungen. Lang ist es her, dass Sicherheitsprobleme allein von IT- Technikern behoben werden konnten. Heute braucht man ein Team aus (internationalen) Rechtsexperten, Entwicklern, Technikern, Sicherheitsforschern, Mathematikern (wenn es um Algorithmen geht), Psychologen, Geschäftsführern, Produzenten und Regierungsbeamten. Und das ist nur die Spitze des Eisbergs.

Als Sicherheitsexperten im Juli 2015 Konstruktionsfehler in Chrysler-Jeeps offenlegten, musste der Automobilhersteller eine Rückholaktion starten, die 1,4 Millionen Autos betraf. Die Auswirkungen sind riesig. Hat ein solcher Jeep noch das Recht auf Zulassung? Wie bekommt man 1,4 Millionen Autobesitzer dazu, sich rechtzeitig um dieses Problem zu kümmern und den Konstruktionsfehler beheben zu lassen? Wer entscheidet über eine Strafe und wer bezahlt sie? Können Versicherungen höhere Preise veranschlagen für Autos, die mit einem Netzwerk verbunden sind? Große Probleme werfen große Fragen auf.

Auch wenn Sie vielleicht kein Auto haben, haben sie wahrscheinlich Haushaltsgeräte. Noch schlimmer, denn das "Internet der Dinge" dräut am Horizont. Eigentlich ist es schon da. Alles vom Toaster über die Kaffeemaschine, verbreitetem Wasserkocher, Personenwaage im Badezimmer, Glühbirne, Waschmaschine, Fernseher, Kamera, Heizstrahler, Schalter, Stecker, Mikrowelle bis zu Schuhen, Zahnbürsten, Uhren, Drohnen (eh klar) und dem Würstelgrill (komplett mit eigener Forschungabteilung), Bett, Golfschläger und vielem vielem mehr - alles ist bereits vernetzt. Sekündlich kommen neue Geräte hinzu. Werden manche dieser Geräte Fehler in sich tragen, die Ihre Sicherheit gefährden? Mit Sicherheit.

Zurück zum Geschäft

Was bedeutet das nun alles für Sie als Unternehmer? Wie sichern Sie die Daten Ihrer Organisation und Ihrer Kunden? Leider gibt es keine Lösung, die alle Gefahren, die auf sie lauern, auf einmal beseitigt. Wir haben es hier nicht mit einer Erkältung zu tun, wo Ruhe und warmer Tee reichen, um die Krankheit zu kurieren. Unternehmen benutzen eine Unmenge an verschiedenen Geräten und Software, die wiederum alle mit unterschiedlichster Software untereinander verbunden sind. Nicht einmal Sicherheitsforscher können mit der rasanten Entwicklung Schritt halten. Smartphones sind dafür das beste Beispiel. Neue Modelle, neue Apps und Operationssysteme tauchen schneller am Markt auf, als sie auf Konstruktionsfehler und Sicherheitslücken getestet werden können. Das wiederum heißt natürlich, dass es Ihnen schwer fallen wird Ihr Smartphone zu regulieren.

Und es kommt noch schlimmer. Tausende europäische Unternehmen vertrauen mittlerweile auf undurchsichtige cloud services. "cloud" ist genau so ein nebulöser Begriff wie "cyber".

Wussten Sie beispielsweise, dass ein Großteil der cloud-Anbieter in der USA beheimatet sind und sich ihre Dienste somit nicht an das europäische Datenschutzrecht halten müssen? Die EU-Kommission hat versucht, dieses Problem zu lösen, indem sie mit den USA ein "Safe Harbour"-Abkommen getroffen hat, bei dem amerikanische Unternehmen sich freiwillig bereit erklären den europäischen Datenschutzprinzipien zu folgen. Der NSA-Skandal hat das Vertrauen in dieses Abkommen erschüttert und der Europäische Gerichtshof hat die Vereinbarung diesen Oktober widerrufen.

All dies verdeutlicht, dass Sie eine Menge darüber wissen müssen, was sich hinter der Bühne abspielt. Sie können sich nicht auf Gerüchte oder nette Anekdoten verlassen. Sie brauchen Fakten, um zu entscheiden, welche Technologie sie nutzen wollen, welche sie vermeiden sollten und wo Verbesserungsbedarf besteht. Vor allem

müssen Sie sich und Ihre Entscheidungen konstant hinterfragen. Die Geschäftswelt muss dringend lernen, Fehler zuzugeben und die Umstände zu analysieren, die zu Störfällen geführt haben. Und sie muss lernen, Experten aus den verschiedendsten Forschungs- und Entwicklungsfeldern in ihre Entscheidungen miteinzubeziehen. Geben wir es zu, nicht einmal Wonder Woman oder Superman könnten die digitale Welt auf eigene Faust retten. Machen Sie nicht den Fehler zu glauben, Sie könnten es, denn der Weg zum Datenleck ist mit Selbstüberschätzung gepflastert.

Wachen Sie auf!

Die jährliche DeepSec In-Depth Security-Konferenz versucht, jeden Aspekt der Informationssicherheit in ihr Programm zu integrieren. Sie versammelt Experten aus Wissenschaft, Regierung und Wirtschaft, Anwender und Entwickler genauso wie Mitglieder der Hacking Community. Informationssicherheit ist eine Herausforderung, der man nur gemeinsam entgegentreten kann. Und auf der DeepSec geht es nicht nur um Theorie. In einem 50-minütigen Talk kann man viele Themen vielleicht nicht im Detail behandeln oder das Publikum bitten, vorgestellte Lösungen gleich selbst auszuprobieren - dafür gibt es die Workshops! Die DeepSec bietet praktische Workshops an, in denen jeder Teilnehmer selbst Hand anlegen kann und im Programm findet sich alles, was Sie wirklich brauchen: Lösungen, die wirklich funktionieren, nicht nur im Labor, sondern in Ihrem realen Umfeld und die Sie auch gleich ausprobieren können; praktische Erfahrung mit Angriffs-und Verteidigungswerkzeug, um für den nächsten Angriff gewappnet zu sein.

Die Workshops dauern zwei Tage; das bedeutet genug Zeit, um sich wirklich gründlich mit einem Thema auseinanderzusetzen und Wissen zu gewinnen. Thematisch richten sie sich an jeden, der sich gegen moderne Angriffe verteidigen will. Hier ein kurzer Überblick über die Workshops:

Cryptographic Attacks: Lernen Sie alles über Attacken auf Kryptographie, die in ihren Software-Applikationen verwendet wird. Vieles hat sich in den letzten zwei Jahren verändert, und auch, wenn Sie sich mathematisch nicht weiterbilden müssen, wollen Sie Ihre Kunden sicher nicht gefährden, indem Sie veraltete Verschlüsselung verwenden.

Hacking Web Applications: Nahezu jedes Unternehmen präsentiert sich heute im World Wide Web. Ihre Website ist sozusagen Ihre Vordertüre. Und diese sollte so sicher wie möglich sein, vor allem, weil sie jeder sieht. Leider denken Entwickler oft nicht außerhalb gängiger Konventionen und verlassen sich auf Annahmen, auf die man sich nicht verlassen kann: Vertrauen Sie nicht auf ihren Browser und lernen Sie, auf was sie sich bei diversen Internet Clients gefasst machen müssen. Denn Kriminelle kommen nicht immer durch die Hintertüre.

Exploiting Devices being used in the Internet of Things: Eine bestimmte Art von Hardware-Prozessoren wird viel

für Kontroll- und Messzwecke benutzt. Dieses Training erklärt, wie ein Prozessor funktioniert und was ein Angreifer versuchen wird, um zu erreichen, dass der Prozessor seinen Code statt Ihrem verwendet.

Testing the Security of the Next-Generation Internet Protocols (IPv6): Auch wenn Sie vielleicht keine Ahnung haben, wie die nächste Generation des Internet aussieht, benutzen Sie es schon. Jedes moderne Betriebssystem unterstützt die neuen Protokolle und sie sind standardmäßig aktiviert. Aber dass etwas funktioniert, ohne dass man etwas davon bemerkt, heißt noch lange nicht, dass man sich nicht damit beschäftigen soll. Vergessen Sie nicht, Sie müssen wissen was vor sich geht, sowohl in ihrem Betrieb wie in Ihrem Betriebssystem. Dieses Training wird ihnen zeigen, auf was Sie achten müssen, wenn Sie eine Internetverbindung herstellen.

Windows PowerShell for Penetration Testers: Seine eigene Abwehr zu testen, ist immer eine gute Idee. Tun Sie es, bevor es Ihre Gegner für Sie tun. Die Methode dafür heißt "Penetration Testing". Dieser Workshop befasst sich mit der Microsoft Windows-Plattform und ihren Werkzeugen und wie Sie diese zu Ihrem Vorteil einsetzen können.

Social Engineering and Security Awareness: Das gefährlichste Gerät in Ihrem Betrieb ist das Telefon. Ein einfacher Anruf genügt oft, um die ausgeklügeltste Verteidigung Schachmatt zu setzen. Der menschliche Faktor ist nicht zu unterschätzen. Lässt nur ein Mitarbeiter sich dazu überreden, die Zugbrücke runterzulassen, nimmt das Unglück seinen Lauf. Um sich zu schützen, sollten Sie lernen, wie menschliche Interaktion funktioniert und wie Angreifer versuchen, Sie und ihre Mitarbeiter zu manipulieren. Ein ausgebildeter Psychologe wird Ihnen zeigen, wogegen Sie sich wappnen müssen und wie Sie sich am besten verteidigen.

Developing and Using Threat Intelligence: Wissen Sie, wer Ihre Gegner sind und was Sie wollen? Wenn nicht, ist es Zeit, das herauszufinden. Die Technik hierfür heißt "Threat Intelligence". In diesem Workshop lernen Sie, wie Sie Gefahren richtig einschätzen können, basierend auf den Daten die Sie selbst zur Verfügung haben.

Secure Web Development: Entwickler haben einen schlechten Ruf, wenn es um Informationssicherheit geht. Dafür gibt es viele Gründe, aber Ignoranz fällt sicher nicht darunter. Sie müssen sich an bestimmte Arten der Kodierung anpassen und die richtigen Werkzeuge verwenden, um Ihren Code zu testen. Sobald Sie das getan haben, wird Ihre Software viel besser funktionieren. Dieses Training ist für jeden, der es mit Code zu tun hat, von großem Vorteil.

Practical Incident Handling: Früher oder später passiert etwas. Was machen Sie dann? Haben Sie sich jemals vorgestellt, wie ein Tag in ihrer Firma aussieht, wenn der Hauptserver kompromittiert ist? Jede Organisation unterwirft sich den Brandschutzbestimmungen. Sie müssen vielleicht sogar einmal im Jahr eine Brandschutzübung ab-

solvieren. Sie sollten auch einen digitale Brandschutzübung machen. Simulieren Sie einen Störfall und spielen Sie durch, was getan werden muss, um ihn gut zu überstehen. Solche Übungen sind sehr wichtig und Gold wert, wenn wirklich ein Schaden entsteht und sie die Behörden informieren müssen. Denn diese werden vielleicht schnelle Antworten und klare Informationen von Ihnen brauchen, bevor Sie ihnen helfen können.

Die Themen der Workshops sind vielfältig. Sie geben Ihnen eine Vorstellung davon, wo sie ansetzen müssen, wenn es um die Verteidigung Ihrer eigenen Sicherheit geht. Egal, ob Sie sich tiefergehend mit eingesetzter Technologie befassen oder sich einen strategischen Überblick verschaffen wollen. Als Unternehmer müssen Sie wissen, wie die IT in ihrer Organisation arbeitet, was ihre Schwachstellen und Stärken sind. Die Übungen in unserem Workshops werden sie vor unangenehmen Überraschungen am stressigsten Tag im Büro retten.
Melden Sie sich daher noch heute zu unseren Workshops an.
Sie finden am 17./18. November statt, gefolgt von der DeepSec-Konferenz am 19./20. November.

Veranstaltungsort:
The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.
Konferenzwebseite: https://deepsec.net/
Registrierung: https://deepsec.net/register.html
Blog: http://blog.deepsec.net/
(Ende)
Aussender: DeepSec GmbH Ansprechpartner: René Pfeiffer Tel.: +43-676-5626390 E-Mail: deepsec@deepsec.net
Website: www.deepsec.net
Quelle: http://www.pressetext.com/news/20151020008
(END) Dow Jones Newswires

October 20, 2015 02:30 ET (06:30 GMT)- - 02 30 AM EDT 10-20-15

DeepSec-Workshops: Digitale Verteidigung - Wissen ist Macht - IT-Security-Workshops für moderne Unternehmen

-1 of 2- 20 Oct 2015 06:30:00 UTC DJ DeepSec-Workshops: Digitale Verteidigung - Wissen ist Macht - IT-Security-Workshops für moderne Unternehmen

Wien (pts008/20.10.2015/08:30) - Wann haben Sie Ihren letzten Geschäftsbrief geschrieben? Und wann haben Sie das letzte Mal Stift und Papier dazu benutzt? Es macht nichts, wenn Sie sich nicht daran erinnern können: Digitale Kommunikation ist Teil unseres Alltagslebens, nicht nur in der Geschäftswelt. Wir haben uns so sehr daran gewöhnt, ständig online zu kommunizieren, dass offline sein sich schon fast unnatürlich anfühlt. Das heißt natürlich auch, dass wir ständig irgendwelchen Netzwerken ausgeliefert sind, vor allem dem Internet. Unsere Tür steht Tag und Nacht offen. Wir können sie nicht mehr schließen und laden somit offen auch ungebetene Gäste ein, die dieselben Netzwerke nutzen wie wir. Es ist Zeit, ernsthaft darüber nachzudenken. Was für Bedrohungen gibt es da draußen? Und wie können wir uns vor ihnen schützen?

Cyber-Kriminalität und Datenschutz

Alles ist "Cyber" heutzutage. Kriminalität genauso wie Sicherheitsbestrebungen. Das Militär verwendet das chice Wort, um ihre Strategien und Taktiken zu beschreiben. Die Politik hat das Wort entdeckt, genauso wie Journalisten und PR-Strategen. Doch der Gebrauch dieses Worts birgt Risiken, es verbirgt, wie die digitale Welt wirklich funktioniert im Nebel einer leicht mystischen Aura. Aber wenn es um die Verteidigung Ihrer Daten geht, ist Nebel das Letzte, was Sie brauchen. Sie brauchen Wissen und harte Fakten, klare Sicht. Ablenkung und Missverständnisse sind Ihre Feinde, genauso wie bedeutungslose Trendwörter.

Hive Mind Technology

Informationssicherheit ist ein weites Feld. Vor Jahrzehnten ging es nur um Systeme mit lokal gespeicherten Daten und ein junges Internet, das seine zarten Fühler ausstreckte. Natürlich gab es auch schon damals Stör- und Zwischenfälle, aber die Auswirkungen waren nicht auf der ganzen Welt zu spüren. Heute ist das anders. Wachstum hat seine Nebenwirkungen. Lang ist es her, dass Sicherheitsprobleme allein von IT-Technikern behoben werden konnten. Heute braucht man ein Team aus (internationalen) Rechtsexperten, Entwicklern, Technikern, Sicherheitsforschern, Mathematikern (wenn es um Algorithmen geht), Psychologen, Geschäftsführern, Produzenten und Regierungsbeamten. Und das ist nur die Spitze des Eisbergs.

Als Sicherheitsexperten im Juli 2015 Konstruktionsfehler in Chrysler-Jeeps offenlegten, musste der Automobilhersteller eine Rückholaktion starten, die 1,4 Millionen Autos betraf. Die Auswirkungen sind riesig. Hat ein solcher Jeep noch das Recht auf Zulassung? Wie bekommt man 1,4 Millionen Autobesitzer dazu, sich rechtzeitig um dieses Problem zu kümmern und den Konstruktionsfehler beheben zu lassen? Wer entscheidet über eine Strafe und wer bezahlt sie? Können Versicherungen höhere Preise veranschlagen für Autos, die mit einem Netzwerk verbunden sind? Große Probleme werfen große Fragen auf.

Auch wenn Sie vielleicht kein Auto haben, haben sie wahrscheinlich Haushaltsgeräte. Noch schlimmer, denn das "Internet der Dinge" dräut am Horizont. Eigentlich ist es schon da. Alles vom Toaster über die Kaffeemaschine, verbreitetem Wasserkocher, Personenwaage im Badezimmer, Glühbirne, Waschmaschine, Fernseher, Kamera, Heizstrahler, Schalter, Stecker, Mikrowelle bis zu Schuhen, Zahnbürsten, Uhren, Drohnen (eh klar) und dem Würstelgrill (komplett mit eigener Forschungabteilung), Bett, Golfschläger und vielem vielem mehr - alles ist bereits vernetzt. Sekündlich kommen neue Geräte hinzu. Werden manche dieser Geräte Fehler in sich tragen, die Ihre Sicherheit gefährden? Mit Sicherheit.

Zurück zum Geschäft

Was bedeutet das nun alles für Sie als Unternehmer? Wie sichern Sie die Daten Ihrer Organisation und Ihrer Kunden? Leider gibt es keine Lösung, die alle Gefahren, die auf sie lauern, auf einmal beseitigt. Wir haben es hier nicht mit einer Erkältung zu tun, wo Ruhe und warmer Tee reichen, um die Krankheit zu kurieren. Unternehmen benutzen eine Unmenge an verschiedenen Geräten und Software, die wiederum alle mit unterschiedlichster Software untereinander verbunden sind. Nicht einmal Sicherheitsforscher können mit der rasanten Entwicklung Schritt halten. Smartphones sind dafür das beste Beispiel. Neue Modelle, neue Apps und Operationssysteme tauchen schneller am Markt auf, als sie auf Konstruktionsfehler und Sicherheitslücken getestet werden können. Das wiederum heißt natürlich, dass es Ihnen schwer fallen wird Ihr Smartphone zu regulieren.

Und es kommt noch schlimmer. Tausende europäische Unternehmen vertrauen mittlerweile auf undurchsichtige cloud services. "cloud" ist genau so ein nebulöser Begriff wie "cyber".

Wussten Sie beispielsweise, dass ein Großteil der cloud-Anbieter in der USA beheimatet sind und sich ihre Dienste somit nicht an das europäische Datenschutzrecht halten müssen? Die EU-Kommission hat versucht, dieses Problem zu lösen, indem sie mit den USA ein "Safe Harbour"-Abkommen getroffen hat, bei dem amerikanische Unternehmen sich freiwillig bereit erklären den europäischen Datenschutzprinzipien zu folgen. Der NSA-Skandal hat das Vertrauen in dieses Abkommen erschüttert und der Europäische Gerichtshof hat die Vereinbarung diesen Oktober widerrufen.

All dies verdeutlicht, dass Sie eine Menge darüber wissen müssen, was sich hinter der Bühne abspielt. Sie können sich nicht auf Gerüchte oder nette Anekdoten verlassen. Sie brauchen Fakten, um zu entscheiden, welche Technologie sie nutzen wollen, welche sie vermeiden sollten und wo Verbesserungsbedarf besteht. Vor allem müssen Sie sich und Ihre Entscheidungen konstant hinterfragen. Die Geschäftswelt muss dringend lernen, Fehler zuzugeben und die Umstände zu analysieren, die zu Störfällen geführt haben. Und sie muss lernen, Experten aus den verschiedendsten Forschungs- und Entwicklungsfeldern in ihre Entscheidungen miteinzubeziehen. Geben wir es zu, nicht einmal Wonder Woman oder Superman könnten die digitale Welt auf eigene Faust retten. Machen Sie nicht den Fehler zu glauben, Sie könnten es, denn der Weg zum Datenleck ist mit Selbstüberschätzung gepflastert.

Wachen Sie auf!

Die jährliche DeepSec In-Depth Security-Konferenz versucht, jeden Aspekt der Informationssicherheit in ihr Programm zu integrieren. Sie versammelt Experten aus Wissenschaft, Regierung und Wirtschaft, Anwender und Entwickler genauso wie Mitglieder der Hacking Community. Informationssicherheit ist eine Herausforderung, der man nur gemeinsam entgegentreten kann. Und auf der DeepSec geht es nicht nur um Theorie. In einem 50-minütigen Talk kann man viele Themen vielleicht nicht im Detail behandeln oder das Publikum bitten, vorgestellte Lösungen gleich selbst auszuprobieren - dafür gibt es die Workshops! Die DeepSec bietet praktische Workshops an, in denen jeder Teilnehmer selbst Hand anlegen kann und im Programm findet sich alles, was Sie wirklich brauchen: Lösungen, die wirklich funktionieren, nicht nur im Labor, sondern in Ihrem realen Umfeld und die Sie auch gleich ausprobieren können; praktische Erfahrung mit Angriffs-und Verteidigungswerkzeug, um für den nächsten Angriff gewappnet zu sein.

Die Workshops dauern zwei Tage; das bedeutet genug Zeit, um sich wirklich gründlich mit einem Thema auseinanderzusetzen und Wissen zu gewinnen. Thematisch richten sie sich an jeden, der sich gegen moderne Angriffe verteidigen will. Hier ein kurzer Überblick über die Workshops:

Cryptographic Attacks Lernen Sie alles über Attacken auf Kryptographie, die in ihren Software-Applikationen verwendet wird. Vieles hat sich in den letzten zwei Jahren verändert, und auch, wenn Sie sich mathematisch nicht weiterbilden müssen, wollen Sie Ihre Kunden sicher nicht gefährden, indem Sie veraltete Verschlüsselung verwenden.

Hacking Web Applications Nahezu jedes Unternehmen präsentiert sich heute im World Wide Web. Ihre Website ist sozusagen Ihre Vordertüre. Und diese sollte so sicher wie möglich sein, vor allem, weil sie jeder sieht. Leider denken Entwickler oft nicht außerhalb gängiger Konventionen und verlassen sich auf Annahmen, auf die man sich nicht verlassen kann: Vertrauen Sie nicht auf ihren Browser und lernen Sie, auf was sie sich bei diversen Internet Clients gefasst machen müssen. Denn Kriminelle kommen nicht immer durch die Hintertüre.

Exploiting Devices being used in the Internet of Things Eine bestimmte Art von Hardware-Prozessoren wird viel für Kontroll- und Messzwecke benutzt. Dieses Training erklärt, wie ein Prozessor funktioniert und was ein Angreifer versuchen wird, um zu erreichen, dass der Prozessor seinen Code statt Ihrem verwendet.

Testing the Security of the Next-Generation Internet Protocols (IPv6) Auch wenn Sie vielleicht keine Ahnung haben, wie die nächste Generation des Internet aussieht, benutzen Sie es schon. Jedes moderne Betriebssystem unterstützt die neuen Protokolle und sie sind standardmäßig aktiviert. Aber dass etwas funktioniert, ohne dass man etwas davon bemerkt, heißt noch lange nicht, dass man sich nicht damit beschäftigen soll. Vergessen Sie nicht, Sie müssen wissen was vor sich geht, sowohl in ihrem Betrieb wie in Ihrem Betriebssystem. Dieses Training wird ihnen zeigen, auf was Sie achten müssen, wenn Sie eine Internetverbindung herstellen.

Windows PowerShell for Penetration Testers Seine eigene Abwehr zu testen, ist immer eine gute Idee. Tun Sie es, bevor es Ihre Gegner für Sie tun. Die Methode dafür heißt "Penetration Testing". Dieser Workshop befasst sich mit der Microsoft Windows-Plattform und ihren Werkzeugen (MORE TO FOLLOW) Dow Jones Newswires

October 20, 2015 02:30 ET (06:30 GMT)- - 02 30 AM EDT 10-20-15

-2 of 2- 20 Oct 2015 06:30:00 UTC DJ DeepSec-Workshops: Digitale Verteidigung - Wissen -2-
und wie Sie diese zu Ihrem Vorteil einsetzen können.

Social Engineering and Security Awareness Das gefährlichste Gerät in Ihrem Betrieb ist das Telefon. Ein einfacher Anruf genügt oft, um die ausgeklügeltste Verteidigung Schachmatt zu setzen. Der menschliche Faktor ist nicht zu unterschätzen. Lässt nur ein Mitarbeiter sich dazu überreden, die Zugbrücke runterzulassen, nimmt das Unglück seinen Lauf. Um sich zu schützen, sollten Sie lernen, wie menschliche Interaktion funktioniert und wie Angreifer versuchen, Sie und ihre Mitarbeiter zu manipulieren. Ein ausgebildeter Psychologe wird Ihnen zeigen, wogegen Sie sich wappnen müssen und wie Sie sich am besten verteidigen.

Developing and Using Threat Intelligence Wissen Sie, wer Ihre Gegner sind und was Sie wollen? Wenn nicht, ist es Zeit, das herauszufinden. Die Technik hierfür heißt "Threat Intelligence". In diesem Workshop lernen Sie, wie Sie Gefahren richtig einschätzen können, basierend auf den Daten die Sie selbst zur Verfügung haben.

Secure Web Development Entwickler haben einen schlechten Ruf, wenn es um Informationssicherheit geht. Dafür gibt es viele Gründe, aber Ignoranz fällt sicher nicht darunter. Sie müssen sich an bestimmte Arten der Kodierung anpassen und die richtigen Werkzeuge verwenden, um Ihren Code zu testen. Sobald Sie das getan haben, wird Ihre Software viel besser funktionieren. Dieses Training ist für jeden, der es mit Code zu tun hat, von großem Vorteil.

Practical Incident Handling Früher oder später passiert etwas. Was machen Sie dann? Haben Sie sich jemals vorgestellt, wie ein Tag in ihrer Firma aussieht, wenn der Hauptserver kompromittiert ist? Jede Organisation unterwirft sich den Brandschutzbestimmungen. Sie müssen vielleicht sogar einmal im Jahr eine Brandschutzübung absolvieren. Sie sollten auch einen digitale Brandschutzübung machen. Simulieren Sie einen Störfall und spielen Sie durch, was getan werden muss, um ihn gut zu überstehen. Solche Übungen sind sehr wichtig und Gold wert, wenn wirklich ein Schaden entsteht und sie die Behörden informieren müssen. Denn diese werden vielleicht schnelle Antworten und klare Informationen von Ihnen brauchen, bevor Sie ihnen helfen können.

Die Themen der Workshops sind vielfältig. Sie geben Ihnen eine Vorstellung davon, wo sie ansetzen müssen, wenn es um die Verteidigung Ihrer eigenen Sicherheit geht. Egal, ob Sie sich tiefergehend mit eingesetzter Technologie befassen oder sich einen strategischen Überblick verschaffen wollen. Als Unternehmer müssen Sie wissen, wie die IT in ihrer Organisation arbeitet, was ihre Schwachstellen und Stärken sind. Die Übungen in unserem Workshops werden sie vor unangenehmen Überraschungen am stressigsten Tag im Büro retten.

Melden Sie sich daher noch heute zu unseren Workshops an. Sie finden am 17./18. November statt, gefolgt von der DeepSec-Konferenz am 19./20. November. Veranstaltungsort ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien. Konferenzwebseite: https://deepsec.net/ Registrierung: https://deepsec.net/register.html Blog: http://blog.deepsec.net/

(Ende)

Aussender: DeepSec GmbH Ansprechpartner: René Pfeiffer Tel.: +43-676-5626390 E-Mail: deepsec@deepsec.net Website: www.deepsec.net

Quelle: http://www.pressetext.com/news/20151020008

(END) Dow Jones Newswires

October 20, 2015 02:30 ET (06:30 GMT)- - 02 30 AM EDT 10-20-15

http://lasthackerstanding.com/2015/10/19/lhs-microcast-deepsec-2015/

Last Hacker Standing

LHS MICROCAST – DEEPSEC 2015

Datum: 19.10.2015

Autor: Chris John Riley

Chris sits down with Mika and René from the DeepSec conference to talk a little bit about what the upcoming conference and how embedded dependencies are causing such headaches in security.

Last Hacker Standing

LHS MICROCAST – DEEPSEC 2015

AUDIO | OCTOBER 19, 2015 | ADMINISTRATOR | LEAVE A COMMENT

00:00 00:00

Podcast: Play in new window | Download (Duration: 14:21 — 13.1MB)

Chris sits down with Mika and René from the DeepSec conference to talk a little bit about what the upcoming conference and how embedded dependencies are causing such headaches in security.

DEEPSEC

http://blog.c22.cc/2015/10/19/lhs-microcase-deepsec-2015/

[LHS Microcast] DeepSec 2015

Datum: 19.10.2015

Autor: Chris John Riley

Chris sits down with Mika and René from the DeepSec conference to talk a little bit about what the upcoming conference and how embedded dependencies are causing such headaches in security.

[LHS Microcast] DeepSec 2015

Chris sits down with Mika and René from the DeepSec conference to talk a little bit about what the upcoming conference and how embedded dependencies are causing such headaches in security.

00:00 00:00

Rate this:

Rate This

Share this:

Twitter Facebook 1 LinkedIn Tumblr Reddit Google

Conference, podcast, Security deepsec, podcast

← [LHS Microcast] Interview w/ Jen Ellis [DeepSec 2015] Can societies manage the SIGINT monster? →

http://www.monitorpro.si/170248/novice/deepsec-2015-defence---beating-the-odds-with-knowledge/

DeepSec 2015: Defence – Beating the Odds with Knowledge

Datum: 16.10.2015

Autor: Stanka Salamun

Konferenca DeepSec 2015, ki se bo odvila med 17. in 20. novembrom na Dunaju, že devetič odpira svoja popularna vrata. 16.10.2015

Ni ga pravega varnostnega strokovnjaka, ki ne bi poznal mednarodne varnostno-informacijske konference DeepSec v naši najbližji soseščini, na Dunaju. Tudi letos na konferenci naslavljajo vse vidike informacijske varnosti z izbiro predavateljev z različnih področij: iz stroke, akademskega in vladnega sektorja, iz vrst uporabnikov, razvijalcev in pripadnikov podtalne hekerske srenje. Informacijska varnost je pač izziv, ki se ga je treba lotiti s skupnimi močmi. In na konferenci DeepSec ne gre le za teorijo, ampak za rešitve, ki so učinkovite v realnih okoljih, ter za praktične izkušnje z orodji za obrambo in napad.

Kraljestvo informacijske varnosti danes pokriva veliko področij. Pred desetletji smo morali varovati le sistem z lokalno hrambo podatkov, nato se je zgodil mladoletni internet, ki je eksplodiral v globalno »superomrežje« in omogočil vdore v informacijske sisteme. Čeprav je tudi v preteklosti že prišlo do varnostnih incidentov, ti niso imeli takega globalnega in finančnega vpliva. Danes je drugače, rast ima stranske učinke. Če so nekoč varnostne probleme večinoma reševali inženirji, je zdaj za to potrebna ekipa, sestavljena iz pravnih strokovnjakov, razvijalcev, inženirjev, varnostnih raziskovalcev, matematikov, psihologov, izvršnih direktorjev, proizvajalcev in vladnih uradnikov.

Za vse te skupine je na letošnjem DeepSecu na razpolago nekaj poglobljenih strokovnih delavnic, na katerih se je mogoče poučiti o vdiranju v spletne aplikacije, kripto napadih, izrabi naprav IoT, preverjanju varnosti protokola IPv6, orodju Windows PowerShell, družbenem inženiringu, praktičnem upravljanju incidentov in še o čem. Delavnicam bodo sledila zanimiva predavanja, ki jih še posebej cenijo poznavalci. Tudi letos imamo med predavatelji Slovenci častna predstavnika – Mitja Kolška (ACROS) in Milana Gabora (Viris).

DeepSec 2015: Defence – Beating the Odds with Knowledge

Konferenca DeepSec 2015, ki se bo odvila med 17. in 20. novembrom na Dunaju, že devetič odpira svoja popularna vrata. 16.10.2015

Ni ga pravega varnostnega strokovnjaka, ki ne bi poznal mednarodne varnostno-informacijske konference DeepSec v naši najbližji soseščini, na Dunaju. Tudi letos na konferenci naslavljajo vse vidike informacijske varnosti z izbiro predavateljev z različnih področij: iz stroke, akademskega in vladnega sektorja, iz vrst uporabnikov, razvijalcev in pripadnikov podtalne hekerske srenje. Informacijska varnost je pač izziv, ki se ga je treba lotiti s skupnimi močmi. In na konferenci DeepSec ne gre le za teorijo, ampak za rešitve, ki so učinkovite v realnih okoljih, ter za praktične izkušnje z orodji za obrambo in napad.

Kraljestvo informacijske varnosti danes pokriva veliko področij. Pred desetletji smo morali varovati le sistem z lokalno hrambo podatkov, nato se je zgodil mladoletni internet, ki je eksplodiral v globalno »superomrežje« in omogočil vdore v informacijske sisteme. Čeprav je tudi v preteklosti že prišlo do varnostnih incidentov, ti niso imeli takega globalnega in finančnega vpliva. Danes je drugače, rast ima stranske učinke. Če so nekoč varnostne probleme večinoma reševali inženirji, je zdaj za to potrebna ekipa, sestavljena iz pravnih strokovnjakov, razvijalcev, inženirjev, varnostnih raziskovalcev, matematikov, psihologov, izvršnih direktorjev, proizvajalcev in vladnih uradnikov.

Za vse te skupine je na letošnjem DeepSecu na razpolago nekaj poglobljenih strokovnih delavnic, na katerih se je mogoče poučiti o vdiranju v spletne aplikacije, kripto napadih, izrabi naprav IoT, preverjanju varnosti protokola IPv6, orodju Windows PowerShell, družbenem inženiringu, praktičnem upravljanju incidentov in še o čem. Delavnicam bodo sledila zanimiva predavanja, ki jih še posebej cenijo poznavalci. Tudi letos imamo med predavatelji Slovenci častna predstavnika – Mitja Kolška (ACROS) in Milana Gabora (Viris).

‹ nazaj

Novice RSS FEED

Gartner IT potrošnja bo presegla 3,5 bilijona dolarjev Tako v svojem globalnem poročilu za letos napoveduje...

Azure Marketplace tudi za naše ponudnike V trgovini Azure Marketplace lahko zdaj svoje rešitve...

Yahoo podpri razvoj strojnega učenja Podjetje je v raziskovalne namene podarilo13,5 TB...

Citrix odkupil Comtradovo rešitev Iz družbe Comtrade System Software & Tools,...

Na voljo je Amazonov WorkMail Končano je poskusno obdobje za potencialnega rivala...

Arhiv novic ›

Komentarji

- Davčne blagajne
- Cio leta je Jurij Bertok
- RapidMiner v partnerstvo s CRMT
- Strici v ozadju

http://www.finanzen.net/nachricht/aktien/Der-Feind-in-meinem-Netz-Sicherheitskonferenz-DeepSec-Wie-schuetzt-man-sich-vor-Wirtschaftsspionage-4492447@print

Der Feind in meinem Netz - Sicherheitskonferenz DeepSec: Wie schützt man sich vor Wirtschaftsspionage?

Datum: 28.08.2015

Autor: René Pfeiffer

Wien (pts013/27.08.2015/08:30) - Vernetzung ist in der Geschäftswelt unabdingbar für die Gewinnung von Aufträgen, Leitung von Projekten und Entwicklung von Produkten. Wo anfangs das World Wide Web war, sorgen nun auch diverse Clouds und Social Media Plattformen für Interaktion. Daten werden an Fremde ausgelagert, und Geschäftsbriefe werden mittlerweile munter per Instant Messenger verschickt. Gedankenlose Umarmung von Netzwerken lädt Bedrohungen ein, die man bislang nur aus dem Kino kennt - Spione.
Die DeepSec möchte Unternehmen mit dieser Problemstellung nicht alleine im Regen stehen lassen. Die internationale IT Security-Konferenz findet vom 17.11 bis 20.11 im Wiener Imperial Riding School Renaissance Hotel statt.

In der digitalen Welt reicht es leider nicht mehr aus einfach nur die Tür zu schließen. Es gibt viel mehr zu beachten. Genau dabei werden Ihnen unsere Experten in Vorträgen und Trainings zur Seite stehen.
Auf der DeepSec erfahren Sie in Vorträgen wie gefährlich das World Wide Web ist: Denn jede aufgerufene Webseite erlaubt die Wechselwirkung mit Ihren internen Systemen. Ein falscher Klick kann verheerende Folgen haben, da schützt auch das verwendete System nicht. Attacken durch scheinbar harmlose Dokumente sind an der Tagesordnung, selbst das bloße Anzeigen von Daten kann schon gefährlich sein. Die Stagefright Sicherheitslücke für Multimedia Nachrichten (MMS) auf Android Smartphones, der Fehler im PDF Viewer von Mozilla Firefox, die Lücke im Microsoft OpenType Font Format oder die Nachricht, die Apple iPhones einfrieren läßt, zeigen wie herstellerübergreifend Attacken funktionieren. Wir zeigen Ihnen worauf es zu achten gilt.

Sie lernen Ihre Gegner kennen: Zu einer guten Verteidigung gehören ebenso Übungen und Sicherheitstests aus der Sicht des Spions. Unsere Trainer zeigen wie man diese richtig durchführt und wie weit man durch kontrollierte Einbrüche kommt. Es geht dabei um das Ausnutzen aller Mittel wie Drohnen, eingeschmuggelte Smartphones, Vortäuschen von Identitäten oder kopierten Authentisierungsdaten. "Man darf sich bei solchen Tests nicht von Beginn an einschränken. Moderne Attacken gehen ungewöhnliche Wege, die man nur mit Out of the Box - Denken erfassen kann", berichtet Michael Kafka, Organisator der DeepSec.

Und Sie lernen, sich richtig zu schützen: Zum Beispiel im IPv6 Workshop. IPv6 ist mittlerweile automatisch Teil

jedes Unternehmensnetzwerks, egal ob man will oder nicht. Es ist also höchste Zeit es korrekt zu konfigurieren und sicher zu verwalten. Darüber hinaus bieten wir ein Web Application Security Training an, welches an prominenten Beispielen von Google, Yahoo! oder Mozilla Web Apps zeigt was alles schiefgehen kann. Ein weiterer Kurs behandelt Attacken auf Kryptographie und gibt Ihnen einen Überblick wie man Verschlüsselung richtig einsetzt. Allen, die in der Softwareentwicklung arbeiten, legen wir dieses Training besonders ans Herz. Spione bedienen sich aber oft auch ganz alltäglicher Methoden: Sie benutzen das Telefon, Social Media oder täuschen Menschen in dem sie sich einfach in passender Kleidung präsentieren, um Ihnen den Zugang zu firmeninternen Geheimnissen zu entlocken. Tarnen & Täuschen - Ausnutzen von alltäglicher Kommunikation durch Social Engineering ist an der Tagesordnung. Auch dort müssen Sie Maßnahmen zur Verteidigung treffen. Wir bieten mit dem Social Engineering Workshop Abhilfe.

Jedes Unternehmen hat Geheimnisse. Sie gehören zur Basis jedes Geschäfts. In Zeiten wo Unternehmer von Regierungen keine Hilfe mehr zu erwarten haben, wenn es um ihren digitalen Schutz geht, sollte man sich den Problemen selbst stellen. Bringen Sie Ihre eigene IT-Mannschaft auf den neuesten Stand - besuchen Sie die diesjährige DeepSec 2015-Konferenz.
DeepSec 2015 17.11 - 20.11.2015 Imperial Riding School Renaissance Vienna Hotel Ungargasse 60 1030 Wien
(Ende)

Aussender: DeepSec GmbH Ansprechpartner: René Pfeiffer Tel.: +436765626390 E-Mail: deepsec@deepsec.net
Website: deepsec.net
Quelle: http://www.pressetext.com/news/20150827013

August 27, 2015 02:30 ET (06:30 GMT)- - 02 30 AM EDT 08-27-15

27.08.2015 09:00

Der Feind in meinem Netz - Sicherheitskonferenz DeepSec: Wie schützt man sich vor Wirtschaftsspionage?

Wien (pts013/27.08.2015/08:30) - Vernetzung ist in der Geschäftswelt unabdingbar für die Gewinnung von Aufträgen, Leitung von Projekten und Entwicklung von Produkten. Wo anfangs das World Wide Web war, sorgen nun auch diverse Clouds und Social Media Plattformen für Interaktion. Daten werden an Fremde ausgelagert, und Geschäftsbriefe werden mittlerweile munter per Instant Messenger verschickt. Gedankenlose Umarmung von Netzwerken lädt Bedrohungen ein, die man bislang nur aus dem Kino kennt - Spione.

Die DeepSec möchte Unternehmen mit dieser Problemstellung nicht alleine im Regen stehen lassen. Die internationale IT Security-Konferenz findet vom 17.11 bis 20.11 im Wiener Imperial Riding School Renaissance Hotel statt.

In der digitalen Welt reicht es leider nicht mehr aus einfach nur die Tür zu schließen. Es gibt viel mehr zu beachten. Genau dabei werden Ihnen unsere Experten in Vorträgen und Trainings zur Seite stehen.

Auf der DeepSec erfahren Sie in Vorträgen wie gefährlich das World Wide Web ist: Denn jede aufgerufene Webseite erlaubt die Wechselwirkung mit Ihren internen Systemen. Ein falscher Klick kann verheerende Folgen haben, da schützt auch das verwendete System nicht. Attacken durch scheinbar harmlose Dokumente sind an der Tagesordnung, selbst das bloße Anzeigen von Daten kann schon gefährlich sein. Die Stagefright Sicherheitslücke für Multimedia Nachrichten (MMS) auf Android Smartphones, der Fehler im PDF Viewer von Mozilla Firefox, die Lücke im Microsoft OpenType Font Format oder die Nachricht, die Apple iPhones einfrieren läßt, zeigen wie herstellerübergreifend Attacken funktionieren. Wir zeigen Ihnen worauf es zu achten gilt.

Sie lernen Ihre Gegner kennen: Zu einer guten Verteidigung gehören ebenso Übungen und Sicherheitstests aus der Sicht des Spions. Unsere Trainer zeigen wie man diese richtig durchführt und wie weit man durch kontrollierte Einbrüche kommt. Es geht dabei um das Ausnutzen aller Mittel wie Drohnen, eingeschmuggelte Smartphones, Vortäuschen von Identitäten oder kopierten Authentisierungsdaten. "Man darf sich bei solchen Tests nicht von Beginn an einschränken. Moderne Attacken gehen ungewöhnliche Wege, die man nur mit Out of the Box - Denken erfassen kann", berichtet Michael Kafka, Organisator der DeepSec.

Und Sie lernen, sich richtig zu schützen: Zum Beispiel im IPv6 Workshop. IPv6 ist mittlerweile automatisch Teil jedes Unternehmensnetzwerks, egal ob man will oder nicht. Es ist also höchste Zeit es korrekt zu konfigurieren und sicher zu verwalten. Darüber hinaus bieten wir ein Web Application Security Training an, welches an prominenten Beispielen von Google, Yahoo! oder Mozilla Web Apps zeigt was alles schiefgehen kann. Ein weiterer Kurs

behandelt Attacken auf Kryptographie und gibt Ihnen einen Überblick wie man Verschlüsselung richtig einsetzt. Allen, die in der Softwareentwicklung arbeiten, legen wir dieses Training besonders ans Herz. Spione bedienen sich aber oft auch ganz alltäglicher Methoden: Sie benutzen das Telefon, Social Media oder täuschen Menschen in dem sie sich einfach in passender Kleidung präsentieren, um Ihnen den Zugang zu firmeninternen Geheimnissen zu entlocken. Tarnen & Täuschen - Ausnutzen von alltäglicher Kommunikation durch Social Engineering ist an der Tagesordnung. Auch dort müssen Sie Maßnahmen zur Verteidigung treffen. Wir bieten mit dem Social Engineering Workshop Abhilfe.

Jedes Unternehmen hat Geheimnisse. Sie gehören zur Basis jedes Geschäfts. In Zeiten wo Unternehmer von Regierungen keine Hilfe mehr zu erwarten haben, wenn es um ihren digitalen Schutz geht, sollte man sich den Problemen selbst stellen. Bringen Sie Ihre eigene IT-Mannschaft auf den neuesten Stand - besuchen Sie die diesjährige DeepSec 2015-Konferenz.

DeepSec 2015 17.11 - 20.11.2015 Imperial Riding School Renaissance Vienna Hotel Ungargasse 60 1030 Wien

(Ende)

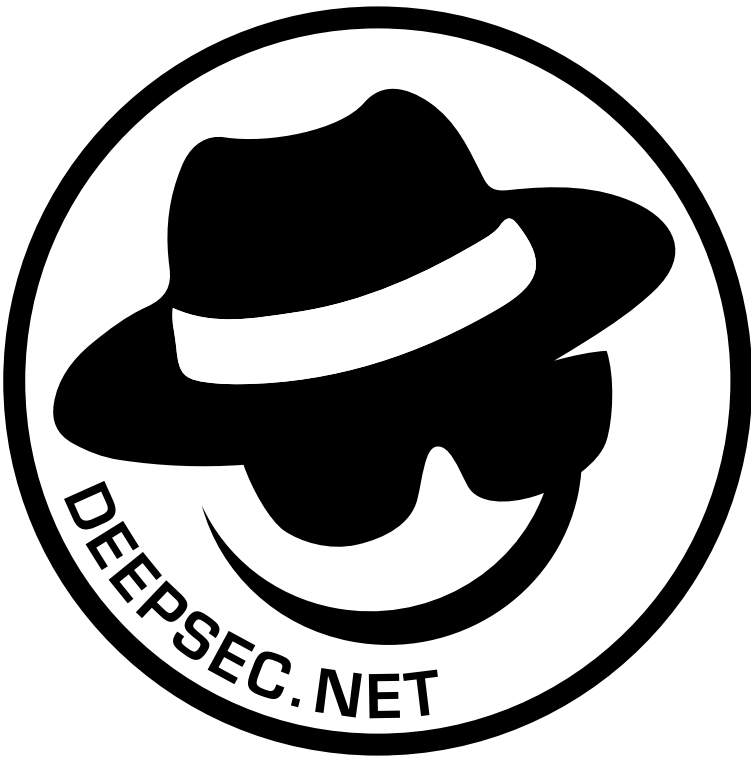
Aussender: DeepSec GmbH Ansprechpartner: René Pfeiffer Tel.: +436765626390 E-Mail: deepsec@deepsec.net Website: deepsec.net

Quelle: http://www.pressetext.com/news/20150827013

(END) Dow Jones Newswires

August 27, 2015 02:30 ET (06:30 GMT)- - 02 30 AM EDT 08-27-15

.
.


DEEPSEC.NET

http://www.pressetext.com/news/20151116006

Hätte Whistleblower Bill Binney 9/11 verhindern können? DeepSec 2015 proudly presents den Dokumentarfilm “A Good American”

Datum: 16.11.2015

Autor: René Pfeiffer

Wien (pts006/16.11.2015/08:00) - Edward Snowden ist wohl der berühmteste Whistleblower, aber der Einzige ist er nicht. Hätte Bill Binney 9/11 verhindern können? DeepSec 2015 proudly presents: “A Good American”. Die Spezialvorführung des Dokumentarfilms im Wiener Burg Kino am 20.11. ist eines der Highlights der diesjährigen DeepSec In-Depth Security Konferenz. Direkt im Anschluß nach dem Film gibt es eine Live-Diskussion mit Regisseur Friedrich Moser, dem NSA-Experten James Bamford, Investigativ-Journalist Duncan Campbell und dem Star der Doku, Bill Binnley. Achtung: Die Teilnehmerzahl ist begrenzt. RSVP!

Teilnehmer der DeepSec In-Depth Security Konferenz erwartet dieses Jahr ein cineastischer Leckerbissen. Friedrich Moser hat zugestimmt, seinen Dokumentarfilm “A Good American” exklusiv im Rahmen der DeepSec zu zeigen.

Die Privatvorführung findet am 20. November 2015 um 21 Uhr im Wiener Burg Kino statt, das vor allem dadurch bekannt ist dass es “The Third Man” seit über 15 Jahren regelmäßig dreimal in der Woche in englischer Originalfassung zeigt. Der passende Ort für “A Good American”.

Bill Binney und die NSA

Ein Codebreaker Genie, ein revolutionäres Überwachungsprogramm und die Korruption in allen Bereichen der NSA. Vor diesem Hintergrund entfaltet sich der Dokumentarfilm “A good American”. Der Film erzählt die Geschichte von Bill Binney und seinem Programm ThinThread. William Binney, Bill für seine Freunde, ist ein Krypto-Mathematiker und ehemaliger NSA-Analyst und vielleicht der beste Code-Breaker, den die USA je hatte.

Nach Ende des Kalten Krieges nimmt Bill die Herausforderungen des digitalen Zeitalters an und entwickelt ein Überwachungstool, das jedes elektronische Signal auf der ganzen Welt erfassen, es nach Zielobjekten filtern und Ergebnisse in Echtzeit liefern kann und dabei auch noch die Privatsphäre der BürgerInnen schützt, so wie von der US-Verfassung verlangt. Das Tool ist perfekt. Doch die NSA-Tätigkeiten werden an die Privatindustrie ausgelagert. Das Programm wird von einer Gruppe mächtiger Männer mit massiven Eigeninteressen abgeschossen und begraben - im August 2001, nur wenige Wochen vor den Terroranschlägen des 11.September.

Hätte ThinThread 9/11 verhindern können?

Live in Talk: Ein Regisseur, ein Whistleblower, ein NSA-Experte und ein Investigativ-Journalist

Nach dem Film werden Friedrich Moser und Bill Binney Ihre Fragen direkt im Burg Kino beantworten. Auch die Eröffnungsvortragenden der diesjährigen DeepSec IT Security Konferenz, der britische Investigativ-Journalist und Forensik-Experte Duncan Campbell, sowie der amerikanische Autor und NSA-Spezialist James Bamford, werden an der Veranstaltung und anschließenden Diskussion teilnehmen. Verpassen Sie diesen einmaligen Abend nicht. Achtung: Sitzplätze sind begrenzt! Um Voranmeldung wird gebeten. Reservierung ausschließlich per Mail unter deepsec@deepsec.net.

“A Good American”
20.11. 2015, 21 Uhr
Burg Kino
Opernring 19
1010 Vienna

pts20151116006 Medien/Kommunikation, Computer/Telekommunikation

Hätte Whistleblower Bill Binney 9/11 verhindern können?

DeepSec 2015 proudly presents den Dokumentarfilm "A Good American"

Wien (pts006/16.11.2015/08:00) - **Edward Snowden ist wohl der berühmteste Whistleblower, aber der Einzige ist er nicht. Hätte Bill Binney 9/11 verhindern können? DeepSec 2015 proudly presents: "A Good American". Die Spezialvorführung des Dokumentarfilms im Wiener Burg Kino am 20.11. ist eines der Highlights der diesjährigen DeepSec In-Depth Security Konferenz. Direkt im Anschluß nach dem Film gibt es eine Live-Diskussion mit Regisseur Friedrich Moser, dem NSA-Experten James Bamford, Investigativ-Journalist Duncan Campbell und dem Star der Doku, Bill Binnley. Achtung: Die Teilnehmerzahl ist begrenzt. RSVP!**

Teilnehmer der DeepSec In-Depth Security Konferenz erwartet dieses Jahr ein cineastischer Leckerbissen. Friedrich Moser hat zugestimmt, seinen Dokumentarfilm "A Good American" exklusiv im Rahmen der DeepSec zu zeigen.

Die Privatvorführung findet am 20. November 2015 um 21 Uhr im Wiener Burg Kino statt, das vor allem dadurch bekannt ist dass es "The Third Man" seit über 15 Jahren regelmäßig dreimal in der Woche in englischer Originalfassung zeigt. Der passende Ort für "A Good American".

Bill Binney und die NSA

Ein Codebreaker Genie, ein revolutionäres Überwachungsprogramm und die Korruption in allen Bereichen der NSA. Vor diesem Hintergrund entfaltet sich der Dokumentarfilm "A good American". Der Film erzählt die Geschichte von Bill Binney und seinem Programm ThinThread. William Binney, Bill für seine Freunde, ist ein Krypto-Mathematiker und ehemaliger NSA-Analyst und vielleicht der beste Code-Breaker, den die USA je hatte.

Nach Ende des Kalten Krieges nimmt Bill die Herausforderungen des digitalen Zeitalters an und entwickelt ein Überwachungstool, das jedes elektronische Signal auf der ganzen Welt erfassen, es nach Zielobjekten filtern und Ergebnisse in Echtzeit liefern kann und dabei auch noch die Privatsphäre der BürgerInnen schützt, so wie von der US-Verfassung verlangt. Das Tool ist perfekt. Doch die NSA-Tätigkeiten werden an die Privatindustrie ausgelagert. Das Programm wird von einer Gruppe mächtiger Männer mit massiven Eigeninteressen abgeschossen und begraben - im August 2001, nur wenige Wochen vor den Terroranschlägen des 11.September.

Hätte ThinThread 9/11 verhindern können?

Live in Talk: Ein Regisseur, ein Whistleblower, ein NSA-Experte und ein Investigativ-Journalist

Nach dem Film werden Friedrich Moser und Bill Binney Ihre Fragen direkt im Burg Kino beantworten. Auch die Eröffnungsvortragenden der diesjährigen DeepSec IT Security Konferenz, der britische Investigativ-Journalist und Forensik-Experte Duncan Campbell, sowie der amerikanische Autor und NSA-Spezialist James Bamford, werden an der Veranstaltung und anschließenden Diskussion teilnehmen. Verpassen Sie diesen einmaligen Abend nicht. Achtung: Sitzplätze sind begrenzt! Um Voranmeldung wird gebeten. Reservierung ausschließlich per Mail unter deepsec@deepsec.net.

"A Good American"
20.11. 2015, 21 Uhr
Burg Kino
Opernring 19
1010 Vienna

(Ende)

Aussender: DeepSec GmbH
Ansprechpartner: René Pfeiffer
Tel.: +43-676-5626390
E-Mail: deepsec@deepsec.net
Website: deepsec.net

http://www.pressetext.com/news/20151105008

Leeres Versprechen namens Datensicherung
DeepSec: Mit richtigem Rat muss Datenhaltung nicht zum Datengrab werden

Datum: 05.11.2015

Autor: René Pfeiffer

Wien (pts008/05.11.2015/09:15) - Daten bestimmen unseren Alltag. Wir haben täglich mit ihnen zu tun, seien es E-Mails, Kurznachrichten, Dokumente oder Datenbanken. Im Privatleben ist es nicht anders. Wo speichern Sie Ihre wichtigen Daten, die sie täglich benötigen? Früher kaufte man Disketten. Heutzutage sind es Festplatten, USB-Sticks und Speicherkarten. Sind diese gut verwahrt und bewacht? Wie stellen Sie sicher diese Daten auch morgen noch verwenden zu können? Ihre Antworten werden sehr wahrscheinlich nicht ausreichen, um kritische Unternehmensdaten zu sichern - wir erklären Ihnen warum.

Verschlüsselte Daten

Einige Hersteller bieten verschlüsselte Festplatten an, die Ihre Daten auch nach einem Diebstahl noch schützen. Die Idee ist gut. Die Umsetzung oft leider mangelhaft. Der Glaube an die Sicherheit von Hardwareverschlüsselung trügt, denn eine Publikation des Cryptology ePrint Archivs vom 28. September 2015 bescheinigt Festplatten einer sehr beliebten USB-Festplatten-Serie Schwachstellen, die zum Auslesen der Daten führen können. Die Geräte erlauben teilweise den Zugriff auf den internen Speicher, erleichtern das Erraten von Schlüsseln und besitzen Hintertüren zur Entschlüsselung.

Gerade bei Lösungen, die Kryptographie einsetzen, muß man viele Fragen stellen. Lösungen ohne Standardverfahren und mit eigener Implementation sind besonders gefährlich. Verschlüsselungsmethoden lassen sich mit dem richtigen Wissen effizient angreifen, wenn die Implementation Fehler aufweist. Bloße Verschleierungen der Entwickler fallen zuerst, dann wird es brenzlig. Unbedachte Umsetzung im Produkt führt dann zu Datendiebstahl. Wenn man sich schon für eine Lösung zum Schutz von Data at Rest entscheidet, dann muss es die Richtige sein.

“Wenn es um Verschlüsselung geht, dann muss man Fachwissen mitbringen. Leider fehlt es diesbezüglich bei Entwicklern von vielen Firmen an der nötigen Ausbildung. Wir haben bei der Analyse von Schwachstellen Code gesehen, der vor 70 Jahren bereits überholt gewesen wäre. Kombiniert man diese Wissenslücken mit Schlampigkeit, mangelnden Tests durch Experten und kurzen Produktzyklen, so ist das Rezept für einbruchsanfällige Infrastruktur perfekt”, hat René Pfeiffer, Geschäftsführer der in Wien beheimateten DeepSec IT Security Konferenz, zu berichten. Er fügt ergänzend hinzu: “Wir organisieren jedes Jahr Workshops mit hochqualifizierten Trainern, um Firmen zu

helfen ihre Mitarbeiter auf den neuesten Stand zu bringen."

Wolkig, kalte Schauer mit Datenverlust

Viele vertrauen blind auf die Cloud, in der man alles ewig und problemlos speichern kann. Aber gepaart mit Virtualisierungtechnologien können dort Sollbruchstellen entstehen, die elegant das ganze Unternehmen lahmlegen. Selbst die beste Storage-Lösung kann versagen. Hat man dann die Architektur nicht auf Redundanz mit Backups oder Echtzeitkopien ausgelegt, so verliert man den Boden unter den Füßen. Dasselbe gilt für die Virtualisierungsplattformen, die oft einsam und ohne Standby-Maschine auf die unvermeidliche Katastrophe warten. Bei moderner Infrastruktur ist es mit der Konfiguration eines RAID-Verbunds leider nicht getan.

Da viele davon ausgehen, dass ihre Speicherlösungen immer funktionieren, wird nichts hinterfragt. In der Realität werden dauernd defekte Datenträger ausgetauscht, sprich die Chance für Datenverlust ist immer gegeben. Sie ist auch von der Wahl der Produkte kaum abhängig.

Über einen komplexen Fall von drohendem Datenverlust im virtuellen Umfeld kann Nicolas Ehrschwendner, Geschäftsführer der Attingo Datenrettung GmbH, berichten: "Eine Hosting-Firma, die für Kunden aus der Versicherungsbranche als auch für eine Verwaltung aus dem öffentlichen Bereich den Betrieb von virtuellen Servern hostete, hatte im Zuge einer Serverumstellung kurzfristig kein Backup für das eingesetzte NAS. In dessen RAID5 sind binnen weniger Stunden zwei Festplatten ausgefallen, so dass ein Rebuild nicht mehr durchgeführt werden konnte und der Storage offline ging. Im Zuge unseres Rund-um-die-Uhr-Services konnten wir die zwölf virtuellen Maschinen auf dem 6 TB Volume rekonstruieren. Als besondere Herausforderungen waren die Daten im NTFS-Dateisystem der NAS als iSCSI Container gespeichert, der anschließend erst den virtuellen Host darstellte. Als wäre das noch nicht genug, war auch noch ein Teil der Server über mehrere virtuelle RAW Devices verteilt, die erst per LVM zusammengespannt waren."

Folgen Sie den Angreifern!

Natürlich sind Sie auf der Suche nach Lösungen von Speicherproblemen nicht alleine. Kaum eine IT-Abteilung verfügt über die detaillierten Kenntnisse um kryptografische Implementationen oder ausfallsichere Virtualisierungsumgebungen auf alle möglichen Schwachstellen zu untersuchen. Aber Sie benötigen dennoch dieses Wissen, um Ihren Alltag gegen Katastrophen zu schützen. Wir schlagen daher vor, den Rat von Experten einzuholen, die die Thematik der Datenkatastrophen zu ihrem Alltag gemacht haben.

Achten Sie darauf, dass Vorfälle Ihre Datensicherheit nicht gefährden. Im Notfall kann eine Panikreaktion noch

größeren Schaden anrichten. Im Normalbetrieb sollte man daher die eingesetzten Speicherlösungen und Sicherheitsmaßnahmen überprüfen. Das Wichtigste daran: Sie müssen all dies tun, bevor die Katastrophe eintritt.

Mit dem Fall des Safe Harbor-Abkommens müssen Sie ohnehin Ihre firmeninterne Strategie zur Datenhaltung und -verarbeitung hinterfragen. Bei der Gelegenheit denken Sie an Ihre Dienstleister für den Katastrophenschutz. Viele Sicherheitsfirmen und Datenretter behaupten zwar, dass sie Ihre Daten sicher nach europäischem Datenschutzrecht speichern und verarbeiten. Die Frage ist, ob das für alle wirklich zutrifft.

pts20151105008 Unternehmen/Finanzen, Computer/Telekommunikation

Leeres Versprechen namens Datensicherung

DeepSec: Mit richtigem Rat muss Datenhaltung nicht zum Datengrab werden

Wien (pts008/05.11.2015/09:15) - **Daten bestimmen unseren Alltag. Wir haben täglich mit ihnen zu tun, seien es E-Mails, Kurznachrichten, Dokumente oder Datenbanken. Im Privatleben ist es nicht anders. Wo speichern Sie Ihre wichtigen Daten, die sie täglich benötigen? Früher kaufte man Disketten. Heutzutage sind es Festplatten, USB-Sticks und Speicherkarten. Sind diese gut verwahrt und bewacht? Wie stellen Sie sicher diese Daten auch morgen noch verwenden zu können? Ihre Antworten werden sehr wahrscheinlich nicht ausreichen, um kritische Unternehmensdaten zu sichern - wir erklären Ihnen warum.**

Verschlüsselte Daten

Einige Hersteller bieten verschlüsselte Festplatten an, die Ihre Daten auch nach einem Diebstahl noch schützen. Die Idee ist gut. Die Umsetzung oft leider mangelhaft. Der Glaube an die Sicherheit von Hardwareverschlüsselung trügt, denn eine Publikation des Cryptology ePrint Archivs vom 28. September 2015 bescheinigt Festplatten einer sehr beliebten USB-Festplatten-Serie Schwachstellen, die zum Auslesen der Daten führen können. Die Geräte erlauben teilweise den Zugriff auf den internen Speicher, erleichtern das Erraten von Schlüsseln und besitzen Hintertüren zur Entschlüsselung.

Gerade bei Lösungen, die Kryptographie einsetzen, muß man viele Fragen stellen. Lösungen ohne Standardverfahren und mit eigener Implementation sind besonders gefährlich. Verschlüsselungsmethoden lassen sich mit dem richtigen Wissen effizient angreifen, wenn die Implementation Fehler aufweist. Bloße Verschleierungen der Entwickler fallen zuerst, dann wird es brenzlig. Unbedachte Umsetzung im Produkt führt dann zu Datendiebstahl. Wenn man sich schon für eine Lösung zum Schutz von Data at Rest entscheidet, dann muss es die Richtige sein.

"Wenn es um Verschlüsselung geht, dann muss man Fachwissen mitbringen. Leider fehlt es diesbezüglich bei Entwicklern von vielen Firmen an der nötigen Ausbildung. Wir haben bei der Analyse von Schwachstellen Code gesehen, der vor 70 Jahren bereits überholt gewesen wäre. Kombiniert man diese Wissenslücken mit Schlampigkeit, mangelnden Tests durch Experten und kurzen Produktzyklen, so ist das Rezept für einbruchsanfällige Infrastruktur perfekt", hat René Pfeiffer, Geschäftsführer der in Wien beheimateten DeepSec IT Security Konferenz, zu berichten. Er fügt ergänzend hinzu: "Wir organisieren jedes Jahr Workshops mit hochqualifizierten Trainern, um Firmen zu helfen ihre Mitarbeiter auf den neuesten Stand zu bringen."

Wolkig, kalte Schauer mit Datenverlust

Viele vertrauen blind auf die Cloud, in der man alles ewig und problemlos speichern kann. Aber gepaart mit Virtualisierungtechnologien können dort Sollbruchstellen entstehen, die elegant das ganze Unternehmen lahmlegen. Selbst die beste Storage-Lösung kann versagen. Hat man dann die Architektur nicht auf Redundanz mit Backups oder Echtzeitkopien ausgelegt, so verliert man den Boden unter den Füßen. Dasselbe gilt für die Virtualisierungsplattformen, die oft einsam und ohne Standby-Maschine auf die unvermeidliche Katastrophe warten. Bei moderner Infrastruktur ist es mit der Konfiguration eines RAID-Verbunds leider nicht getan.

Da viele davon ausgehen, dass ihre Speicherlösungen immer funktionieren, wird nichts hinterfragt. In der Realität werden dauernd defekte Datenträger ausgetauscht, sprich die Chance für Datenverlust ist immer gegeben. Sie ist auch von der Wahl der Produkte kaum abhängig.

Über einen komplexen Fall von drohendem Datenverlust im virtuellen Umfeld kann Nicolas Ehrschwendner, Geschäftsführer der Attingo Datenrettung GmbH, berichten: "Eine Hosting-Firma, die für Kunden aus der Versicherungsbranche als auch für eine Verwaltung aus dem öffentlichen Bereich den Betrieb von virtuellen Servern hostete, hatte im Zuge einer Serverumstellung kurzfristig kein Backup für das eingesetzte NAS. In dessen RAID5 sind binnen weniger Stunden zwei Festplatten ausgefallen, so dass ein Rebuild nicht mehr durchgeführt werden konnte und der Storage offline ging. Im Zuge unseres Rund-um-die-Uhr-Services konnten wir die zwölf virtuellen Maschinen auf dem 6 TB Volume rekonstruieren. Als besondere Herausforderungen waren die Daten im NTFS-Dateisystem der NAS als iSCSI Container gespeichert, der anschließend erst den virtuellen Host darstellte. Als wäre das noch nicht genug, war auch noch ein Teil der Server über mehrere virtuelle RAW-Devices verteilt, die erst per LVM zusammengespannt waren."

Folgen Sie den Angreifern!

Natürlich sind Sie auf der Suche nach Lösungen von Speicherproblemen nicht alleine. Kaum eine IT-Abteilung verfügt über die detaillierten Kenntnisse um kryptografische Implementationen oder ausfallsichere Virtualisierungsumgebungen auf alle möglichen Schwachstellen zu untersuchen. Aber Sie benötigen dennoch dieses Wissen, um Ihren Alltag gegen Katastrophen zu schützen. Wir schlagen daher vor, den Rat von Experten einzuholen, die die Thematik der Datenkatastrophen zu ihrem Alltag gemacht haben.

Achten Sie darauf, dass Vorfälle Ihre Datensicherheit nicht gefährden. Im Notfall kann eine Panikreaktion noch größeren Schaden anrichten. Im Normalbetrieb sollte man daher die eingesetzten Speicherlösungen und Sicherheitsmaßnahmen überprüfen. Das Wichtigste daran: Sie müssen all dies tun, bevor die Katastrophe eintritt.

Mit dem Fall des Safe Harbor-Abkommens müssen Sie ohnehin Ihre firmeninterne Strategie zur Datenhaltung und -verarbeitung hinterfragen. Bei der Gelegenheit denken Sie an Ihre Dienstleister für den Katastrophenschutz. Viele Sicherheitsfirmen und Datenretter behaupten zwar, dass sie Ihre Daten sicher nach europäischem Datenschutzrecht speichern und verarbeiten. Die Frage ist, ob das für alle wirklich zutrifft.

(Ende)

Aussender:	DeepSec GmbH
Ansprechpartner:	René Pfeiffer
Tel.:	+43-676-5626390
E-Mail:	deepsec@deepsec.net
Website:	deepsec.net

http://www.pressetext.com/news/20151023006

Informationssicherheit abgehört: Selbstverteidigung für Unternehmer
Duncan Campbell und James Bamford eröffnen DeepSec IT Security Konferenz am 19.11. in Wien

Datum: 23.10.2015

Autor: René Pfeiffer

Wien (pts006/23.10.2015/08:05) - Datenlecks sind ein ständiger Begleiter der Wirtschaft. Dieser Eindruck drängt sich auf, wenn man die Nachrichten verfolgt. Kundenportale, Webshops, digitale Kommunikation, Baupläne von Produkten, Personaldaten und vieles mehr lässt sich in den Kaufhäusern der ganz dunklen Schattenwirtschaft finden. Das blinde Vertrauen in weltweite Netzwerke hat zwar in den letzten Jahre gelitten, aber Unternehmen und Privatpersonen haben immer noch einen teilweise unbeschwerten Zugang zum drohenden Risiko für ihre Daten. “Wer interessiert sich schon für unsere Daten?”, heißt es oft. Die diesjährige DeepSec IT Security Konferenz bietet sehr konkrete Antworten auf diese Frage. Zwei prominente Journalisten eröffnen die Konferenz.

Duncan Campbell ist ein freier britischer Journalist, Autor und TV-Produzent. Seit 1975 hat er sich auf Nachrichten- und Sicherheitsdienste, Verteidigung, Polizeiarbeit und bürgerliche Freiheit spezialisiert. Er wird in seinem Eröffnungsvortrag illustrieren wie selbst Produzenten harmloser Produkte, wie beispielsweise von Gummienten für die Badewanne, zum Ziel von kriminellen oder organisierten Angreifern werden können. Es geht längst nicht mehr nur alleine um einzelne Betriebe. Die stetige Vernetzung führt zu Ereignissen, denen man nur mit einer professionellen Risikoanalyse begegnen kann. Nichts im Internet ist bedeutungslos. Alles kann für Angriffe verwendet werden. Bei der Verteidigung müssen die IT-Veranwortlichen mindestens genauso viel Kreativität aufbringen wie die Gegenspieler.

James Bamford wird ebenso über die Auswirkungen technologischer Möglichkeiten auf den Alltag von Unternehmen referieren. Er referiert über den weltbekannten Abhörskandal aus dem Jahre 2005 bei Vodafone Griechenland. Damals hatten Eindringlinge gesetzlich vorgeschriebene Systeme zur Telekommunikationsüberwachung kompromittiert, um die Mobiltelefone griechischer Politiker und Sicherheitskräfte zu belauschen. Die Ermittlungen gestalteten sich als schwierig, und erst im Februar 2015 wurde ein Haftbefehl gegen einen Verdächtigen erlassen. James Bamford wird den Fall nochmals erklären und in den Kontext von Wirtschaftsspionage stellen.

Selbst wenn man nicht ständig gegen die Allmacht von Diensten steht, so hat doch Big Data auch bei Angreifern Einzug gefunden und ist sowohl selbst Ziel als auch Mittel zum Zweck Konkurrenten auszuspähen und letztlich elegant auszuschalten.

Unternehmer müssen mit der Zeit gehen

IT Security-Konferenzen sind längst nicht nur für Techniker. Spätestens seit der Entdeckung des Stuxnet Computerwurms hat Schadsoftware Einzug in die Politik gehalten. Ganz analog zählen heute Netzwerke, allen voran das Internet, zur Infrastruktur aller Firmen; ganz egal ob Einzelunternehmer oder Großkonzerne. Das Internet der alltäglichen Dinge schwächt die Verteidigung obendrein, weil man jetzt Sicherheitslücken günstig mit Haushaltsgeräten und Unterhaltungselektronik einschleppen kann. Informationssicherheit ist somit Mainstream geworden. Die DeepSec Konferenz ist daher stets bemüht alle Beteiligten und Betroffenen an einen Tisch zu bringen um Probleme aus verschiedensten Blickwinkeln zu betrachten, Lösungen zu diskutieren und den Betroffenen zugänglich zu machen.

Schließen Sie sich daher unserem Austausch an und besuchen Sie die 9. DeepSec Konferenz. Sie findet am 19./20. November 2015 in Wien statt. Vor der Konferenz am 17./18. November werden Workshops zu Themen der IT Security abgehalten, die wir Ihnen sehr ans Herz legen. Details finden Sie unter https://deepsec.net und in unserem Blog http://blog.deepsec.net .

Über die Eröffnungsvortragenden

James Bamford ist ein amerikanischer Bestseller-Autor und Journalist, der für seine Schriften über USA-Geheimdienste, insbesondere die National Security Agency (NSA) bekannt wurde. Bamford hat u.a. für renommierte Zeitungen wie The Washington Post, the Los Angeles Times, das New York Times Magazine, The Atlantic, Harpers geschrieben. Zudem war Bamford als Produzent der ABC World News tätig und mehrere Jahre Gastdozent an der University of California, Berkeley. Im Jahr 2006 gewann er den National Magazine Award für seinen Artikel “The Man Who Sold The War”, der im Rolling Stone Magazin veröffentlicht wurde.

Seit über drei Jahrzehnten, recherchiert und produziert Duncan Campbell detaillierte Berichte für das Fernsehen, Print- und Online-Medien. Seine Beiträge zu Themen wie Staatsgeheimnisse, Wirtschaftskriminalität und medizinische Betrug haben im nicht nur Preise und Beifall der Kritiker eingetragen sondern in auch vor rechtliche Herausforderungen gestellt. Seine bekanntesten Untersuchungen führten zu großen rechtlichen Auseinandersetzungen mit der britischen Regierung.Er wurde unter dem Official Secrets Act im “ABC Verfahren” im Jahr 1978 strafrechtlichverfolgt, 1987 gestaltete er die umstrittene Serie “Secret Society” für die BBC (siehe Zircon-Affäre). Im Jahr 1988 enthüllte er die Existenz des ECHELON-Überwachungsprogramms. Zudem hat Campbell sich als Forensik Experte auf dem Gebiet der Computern und Kommunikationsdaten einen Namen gemacht.

pts20151023006 Unternehmen/Finanzen, Computer/Telekommunikation

Informationssicherheit abgehört: Selbstverteidigung für Unternehmer

Duncan Campbell und James Bamford eröffnen DeepSec IT Security Konferenz am 19.11. in Wien

Wien (pts006/23.10.2015/08:05) - **Datenlecks sind ein ständiger Begleiter der Wirtschaft. Dieser Eindruck drängt sich auf, wenn man die Nachrichten verfolgt. Kundenportale, Webshops, digitale Kommunikation, Baupläne von Produkten, Personaldaten und vieles mehr lässt sich in den Kaufhäusern der ganz dunklen Schattenwirtschaft finden. Das blinde Vertrauen in weltweite Netzwerke hat zwar in den letzten Jahre gelitten, aber Unternehmen und Privatpersonen haben immer noch einen teilweise unbeschwerten Zugang zum drohenden Risiko für ihre Daten. "Wer interessiert sich schon für unsere Daten?", heißt es oft. Die diesjährige DeepSec IT Security Konferenz bietet sehr konkrete Antworten auf diese Frage. Zwei prominente Journalisten eröffnen die Konferenz.**

Duncan Campbell ist ein freier britischer Journalist, Autor und TV-Produzent. Seit 1975 hat er sich auf Nachrichten- und Sicherheitsdienste, Verteidigung, Polizeiarbeit und bürgerliche Freiheit spezialisiert. Er wird in seinem Eröffnungsvortrag illustrieren wie selbst Produzenten harmloser Produkte, wie beispielsweise von Gummienten für die Badewanne, zum Ziel von kriminellen oder organisierten Angreifern werden können. Es geht längst nicht mehr nur alleine um einzelne Betriebe. Die stetige Vernetzung führt zu Ereignissen, denen man nur mit einer professionellen Risikoanalyse begegnen kann. Nichts im Internet ist bedeutungslos. Alles kann für Angriffe verwendet werden. Bei der Verteidigung müssen die IT-Veranwortlichen mindestens genauso viel Kreativität aufbringen wie die Gegenspieler.

James Bamford wird ebenso über die Auswirkungen technologischer Möglichkeiten auf den Alltag von Unternehmen referieren. Er referiert über den weltbekannten Abhörskandal aus dem Jahre 2005 bei Vodafone Griechenland. Damals hatten Eindringlinge gesetzlich vorgeschriebene Systeme zur Telekommunikationsüberwachung kompromittiert, um die Mobiltelefone griechischer Politiker und Sicherheitskräfte zu belauschen. Die Ermittlungen gestalteten sich als schwierig, und erst im Februar 2015 wurde ein Haftbefehl gegen einen Verdächtigen erlassen. James Bamford wird den Fall nochmals erklären und in den Kontext von Wirtschaftsspionage stellen.

Selbst wenn man nicht ständig gegen die Allmacht von Diensten steht, so hat doch Big Data auch bei Angreifern Einzug gefunden und ist sowohl selbst Ziel als auch Mittel zum Zweck Konkurrenten auszuspähen und letztlich elegant auszuschalten.

Unternehmer müssen mit der Zeit gehen

IT Security-Konferenzen sind längst nicht nur für Techniker. Spätestens seit der Entdeckung des Stuxnet Computerwurms hat Schadsoftware Einzug in die Politik gehalten. Ganz analog zählen heute Netzwerke, allen voran das Internet, zur Infrastruktur aller Firmen; ganz egal ob Einzelunternehmer oder Großkonzerne. Das Internet der alltäglichen Dinge schwächt die Verteidigung obendrein, weil man jetzt Sicherheitslücken günstig mit Haushaltsgeräten und Unterhaltungselektronik einschleppen kann. Informationssicherheit ist somit Mainstream geworden. Die DeepSec Konferenz ist daher stets bemüht alle Beteiligten und Betroffenen an einen Tisch zu bringen um Probleme aus verschiedensten Blickwinkeln zu betrachten, Lösungen zu diskutieren und den Betroffenen zugänglich zu machen.

Schließen Sie sich daher unserem Austausch an und besuchen Sie die 9. DeepSec Konferenz. Sie findet am 19./20. November 2015 in Wien statt. Vor der Konferenz am 17./18. November werden Workshops zu Themen der IT Security abgehalten, die wir Ihnen sehr ans Herz legen. Details finden Sie unter https://deepsec.net und in unserem Blog http://blog.deepsec.net .

Über die Eröffnungsvortragenden

James Bamford ist ein amerikanischer Bestseller-Autor und Journalist, der für seine Schriften über USA-Geheimdienste, insbesondere die National Security Agency (NSA) bekannt wurde. Bamford hat u.a. für renommierte Zeitungen wie The Washington Post, the Los Angeles Times, das New York Times Magazine, The Atlantic, Harpers geschrieben. Zudem war Bamford als Produzent der ABC World News tätig und mehrere Jahre Gastdozent an der University of California, Berkeley. Im Jahr 2006 gewann er den National Magazine Award für seinen Artikel "The Man Who Sold The War", der im Rolling Stone Magazin veröffentlicht wurde.

Seit über drei Jahrzehnten, recherchiert und produziert Duncan Campbell detaillierte Berichte für das Fernsehen, Print- und Online-Medien. Seine Beiträge zu Themen wie Staatsgeheimnisse, Wirtschaftskriminalität und medizinische Betrug haben im nicht nur Preise und Beifall der Kritiker eingetragen sondern in auch vor rechtliche Herausforderungen gestellt. Seine bekanntesten Untersuchungen führten zu großen rechtlichen Auseinandersetzungen mit der britischen Regierung.Er wurde unter dem Official Secrets Act im "ABC Verfahren" im Jahr 1978 strafrechtlichverfolgt, 1987 gestaltete er die umstrittene Serie "Secret Society" für die BBC (siehe Zircon-Affäre). Im Jahr 1988 enthüllte er die Existenz des ECHELON-Überwachungsprogramms. Zudem hat Campbell sich als Forensik Experte auf dem Gebiet der Computern und Kommunikationsdaten einen Namen gemacht.

(Ende)

Aussender:	DeepSec GmbH
Ansprechpartner:	René Pfeiffer
Tel.:	+43-676-5626390
E-Mail:	deepsec@deepsec.net
Website:	deepsec.net

http://www.pressetext.com/news/20151020008

DeepSec-Workshops: Digitale Verteidigung - Wissen ist Macht
IT-Security-Workshops für moderne Unternehmen

Datum: 20.10.2015

Autor: René Pfeiffer

Wien (pts008/20.10.2015/08:30) - Wann haben Sie Ihren letzten Geschäftsbrief geschrieben? Und wann haben Sie das letzte Mal Stift und Papier dazu benutzt? Es macht nichts, wenn Sie sich nicht daran erinnern können: Digitale Kommunikation ist Teil unseres Alltagslebens, nicht nur in der Geschäftswelt. Wir haben uns so sehr daran gewöhnt, ständig online zu kommunizieren, dass offline sein sich schon fast unnatürlich anfühlt. Das heißt natürlich auch, dass wir ständig irgendwelchen Netzwerken ausgeliefert sind, vor allem dem Internet. Unsere Tür steht Tag und Nacht offen. Wir können sie nicht mehr schließen und laden somit offen auch ungebetene Gäste ein, die dieselben Netzwerke nutzen wie wir. Es ist Zeit, ernsthaft darüber nachzudenken. Was für Bedrohungen gibt es da draußen? Und wie können wir uns vor ihnen schützen?

Cyber-Kriminalität und Datenschutz

Alles ist “Cyber” heutzutage. Kriminalität genauso wie Sicherheitsbestrebungen. Das Militär verwendet das chice Wort, um ihre Strategien und Taktiken zu beschreiben. Die Politik hat das Wort entdeckt, genauso wie Journalisten und PR-Strategen. Doch der Gebrauch dieses Worts birgt Risiken, es verbirgt, wie die digitale Welt wirklich funktioniert im Nebel einer leicht mystischen Aura. Aber wenn es um die Verteidigung Ihrer Daten geht, ist Nebel das Letzte, was Sie brauchen. Sie brauchen Wissen und harte Fakten, klare Sicht. Ablenkung und Missverständnisse sind Ihre Feinde, genauso wie bedeutungslose Trendwörter.

Hive Mind Technology

Informationssicherheit ist ein weites Feld. Vor Jahrzehnten ging es nur um Systeme mit lokal gespeicherten Daten und ein junges Internet, das seine zarten Fühler ausstreckte. Natürlich gab es auch schon damals Stör- und Zwischenfälle, aber die Auswirkungen waren nicht auf der ganzen Welt zu spüren. Heute ist das anders. Wachstum hat seine Nebenwirkungen. Lang ist es her, dass Sicherheitsprobleme allein von IT- Technikern behoben werden konnten. Heute braucht man ein Team aus (internationalen) Rechtsexperten, Entwicklern, Technikern, Sicherheitsforschern, Mathematikern (wenn es um Algorithmen geht), Psychologen, Geschäftsführern, Produzenten und Regierungsbeamten. Und das ist nur die Spitze des Eisbergs.

Als Sicherheitsexperten im Juli 2015 Konstruktionsfehler in Chrysler-Jeeps offenlegten, musste der Automobilher-

steller eine Rückholaktion starten, die 1,4 Millionen Autos betraf. Die Auswirkungen sind riesig. Hat ein solcher Jeep noch das Recht auf Zulassung? Wie bekommt man 1,4 Millionen Autobesitzer dazu, sich rechtzeitig um dieses Problem zu kümmern und den Konstruktionsfehler beheben zu lassen? Wer entscheidet über eine Strafe und wer bezahlt sie? Können Versicherungen höhere Preise veranschlagen für Autos, die mit einem Netzwerk verbunden sind? Große Probleme werfen große Fragen auf.

Auch wenn Sie vielleicht kein Auto haben, haben sie wahrscheinlich Haushaltsgeräte. Noch schlimmer, denn das "Internet der Dinge" dräut am Horizont. Eigentlich ist es schon da. Alles vom Toaster über die Kaffeemaschine, verbreitetem Wasserkocher, Personenwaage im Badezimmer, Glühbirne, Waschmaschine, Fernseher, Kamera, Heizstrahler, Schalter, Stecker, Mikrowelle bis zu Schuhen, Zahnbürsten, Uhren, Drohnen (eh klar) und dem Würstelgrill (komplett mit eigener Forschungabteilung), Bett, Golfschläger und vielem vielem mehr - alles ist bereits vernetzt. Sekündlich kommen neue Geräte hinzu. Werden manche dieser Geräte Fehler in sich tragen, die Ihre Sicherheit gefährden? Mit Sicherheit.

Zurück zum Geschäft

Was bedeutet das nun alles für Sie als Unternehmer? Wie sichern Sie die Daten Ihrer Organisation und Ihrer Kunden? Leider gibt es keine Lösung, die alle Gefahren, die auf sie lauern, auf einmal beseitigt. Wir haben es hier nicht mit einer Erkältung zu tun, wo Ruhe und warmer Tee reichen, um die Krankheit zu kurieren. Unternehmen benutzen eine Unmenge an verschiedenen Geräten und Software, die wiederum alle mit unterschiedlichster Software untereinander verbunden sind. Nicht einmal Sicherheitsforscher können mit der rasanten Entwicklung Schritt halten. Smartphones sind dafür das beste Beispiel. Neue Modelle, neue Apps und Operationssysteme tauchen schneller am Markt auf, als sie auf Konstruktionsfehler und Sicherheitslücken getestet werden können. Das wiederum heißt natürlich, dass es Ihnen schwer fallen wird Ihr Smartphone zu regulieren.

Und es kommt noch schlimmer. Tausende europäische Unternehmen vertrauen mittlerweile auf undurchsichtige cloud services. "cloud" ist genau so ein nebulöser Begriff wie "cyber".

Wussten Sie beispielsweise, dass ein Großteil der cloud-Anbieter in der USA beheimatet sind und sich ihre Dienste somit nicht an das europäische Datenschutzrecht halten müssen? Die EU-Kommission hat versucht, dieses Problem zu lösen, indem sie mit den USA ein "Safe Harbour"-Abkommen getroffen hat, bei dem amerikanische Unternehmen sich freiwillig bereit erklären den europäischen Datenschutzprinzipien zu folgen. Der NSA-Skandal hat das Vertrauen in dieses Abkommen erschüttert und der Europäische Gerichtshof hat die Vereinbarung diesen Oktober widerrufen.

All dies verdeutlicht, dass Sie eine Menge darüber wissen müssen, was sich hinter der Bühne abspielt. Sie können sich nicht auf Gerüchte oder nette Anekdoten verlassen. Sie brauchen Fakten, um zu entscheiden, welche Technologie sie nutzen wollen, welche sie vermeiden sollten und wo Verbesserungsbedarf besteht. Vor allem müssen Sie sich und Ihre Entscheidungen konstant hinterfragen. Die Geschäftswelt muss dringend lernen, Fehler zuzugeben und die Umstände zu analysieren, die zu Störfällen geführt haben. Und sie muss lernen, Experten aus den verschiedendsten Forschungs- und Entwicklungsfeldern in ihre Entscheidungen miteinzubeziehen. Geben wir es zu, nicht einmal Wonder Woman oder Superman könnten die digitale Welt auf eigene Faust retten. Machen Sie nicht den Fehler zu glauben, Sie könnten es, denn der Weg zum Datenleck ist mit Selbstüberschätzung gepflastert.

Wachen Sie auf!

Die jährliche DeepSec In-Depth Security-Konferenz versucht, jeden Aspekt der Informationssicherheit in ihr Programm zu integrieren. Sie versammelt Experten aus Wissenschaft, Regierung und Wirtschaft, Anwender und Entwickler genauso wie Mitglieder der Hacking Community. Informationssicherheit ist eine Herausforderung, der man nur gemeinsam entgegentreten kann. Und auf der DeepSec geht es nicht nur um Theorie. In einem 50-minütigen Talk kann man viele Themen vielleicht nicht im Detail behandeln oder das Publikum bitten, vorgestellte Lösungen gleich selbst auszuprobieren - dafür gibt es die Workshops! Die DeepSec bietet praktische Workshops an, in denen jeder Teilnehmer selbst Hand anlegen kann und im Programm findet sich alles, was Sie wirklich brauchen: Lösungen, die wirklich funktionieren, nicht nur im Labor, sondern in Ihrem realen Umfeld und die Sie auch gleich ausprobieren können; praktische Erfahrung mit Angriffs-und Verteidigungswerkzeug, um für den nächsten Angriff gewappnet zu sein.

Die Workshops dauern zwei Tage; das bedeutet genug Zeit, um sich wirklich gründlich mit einem Thema auseinanderzusetzen und Wissen zu gewinnen. Thematisch richten sie sich an jeden, der sich gegen moderne Angriffe verteidigen will. Hier ein kurzer Überblick über die Workshops:

Cryptographic Attacks

Lernen Sie alles über Attacken auf Kryptographie, die in ihren Software-Applikationen verwendet wird. Vieles hat sich in den letzten zwei Jahren verändert, und auch, wenn Sie sich mathematisch nicht weiterbilden müssen, wollen Sie Ihre Kunden sicher nicht gefährden, indem Sie veraltete Verschlüsselung verwenden.

Hacking Web Applications

Nahezu jedes Unternehmen präsentiert sich heute im World Wide Web. Ihre Website ist sozusagen Ihre Vordertüre.

Und diese sollte so sicher wie möglich sein, vor allem, weil sie jeder sieht. Leider denken Entwickler oft nicht außerhalb gängiger Konventionen und verlassen sich auf Annahmen, auf die man sich nicht verlassen kann: Vertrauen Sie nicht auf ihren Browser und lernen Sie, auf was sie sich bei diversen Internet Clients gefasst machen müssen. Denn Kriminelle kommen nicht immer durch die Hintertüre.

Exploiting Devices being used in the Internet of Things

Eine bestimmte Art von Hardware-Prozessoren wird viel für Kontroll- und Messzwecke benutzt. Dieses Training erklärt, wie ein Prozessor funktioniert und was ein Angreifer versuchen wird, um zu erreichen, dass der Prozessor seinen Code statt Ihrem verwendet.

Testing the Security of the Next-Generation Internet Protocols (IPv6)

Auch wenn Sie vielleicht keine Ahnung haben, wie die nächste Generation des Internet aussieht, benutzen Sie es schon. Jedes moderne Betriebssystem unterstützt die neuen Protokolle und sie sind standardmäßig aktiviert. Aber dass etwas funktioniert, ohne dass man etwas davon bemerkt, heißt noch lange nicht, dass man sich nicht damit beschäftigen soll. Vergessen Sie nicht, Sie müssen wissen was vor sich geht, sowohl in ihrem Betrieb wie in Ihrem Betriebssystem. Dieses Training wird ihnen zeigen, auf was Sie achten müssen, wenn Sie eine Internetverbindung herstellen.

Windows PowerShell for Penetration Testers

Seine eigene Abwehr zu testen, ist immer eine gute Idee. Tun Sie es, bevor es Ihre Gegner für Sie tun. Die Methode dafür heißt “Penetration Testing”. Dieser Workshop befasst sich mit der Microsoft Windows-Plattform und ihren Werkzeugen und wie Sie diese zu Ihrem Vorteil einsetzen können.

Social Engineering and Security Awareness

Das gefährlichste Gerät in Ihrem Betrieb ist das Telefon. Ein einfacher Anruf genügt oft, um die ausgeklügeltste Verteidigung Schachmatt zu setzen. Der menschliche Faktor ist nicht zu unterschätzen. Lässt nur ein Mitarbeiter sich dazu überreden, die Zugbrücke runterzulassen, nimmt das Unglück seinen Lauf. Um sich zu schützen, sollten Sie lernen, wie menschliche Interaktion funktioniert und wie Angreifer versuchen, Sie und ihre Mitarbeiter zu manipulieren. Ein ausgebildeter Psychologe wird Ihnen zeigen, wogegen Sie sich wappnen müssen und wie Sie sich am besten verteidigen.

Developing and Using Threat Intelligence

Wissen Sie, wer Ihre Gegner sind und was Sie wollen? Wenn nicht, ist es Zeit, das herauszufinden. Die Technik

hierfür heißt “Threat Intelligence”. In diesem Workshop lernen Sie, wie Sie Gefahren richtig einschätzen können, basierend auf den Daten die Sie selbst zur Verfügung haben.

Secure Web Development

Entwickler haben einen schlechten Ruf, wenn es um Informationssicherheit geht. Dafür gibt es viele Gründe, aber Ignoranz fällt sicher nicht darunter. Sie müssen sich an bestimmte Arten der Kodierung anpassen und die richtigen Werkzeuge verwenden, um Ihren Code zu testen. Sobald Sie das getan haben, wird Ihre Software viel besser funktionieren. Dieses Training ist für jeden, der es mit Code zu tun hat, von großem Vorteil.

Practical Incident Handling

Früher oder später passiert etwas. Was machen Sie dann? Haben Sie sich jemals vorgestellt, wie ein Tag in ihrer Firma aussieht, wenn der Hauptserver kompromittiert ist? Jede Organisation unterwirft sich den Brandschutzbestimmungen. Sie müssen vielleicht sogar einmal im Jahr eine Brandschutzübung absolvieren. Sie sollten auch einen digitale Brandschutzübung machen. Simulieren Sie einen Störfall und spielen Sie durch, was getan werden muss, um ihn gut zu überstehen. Solche Übungen sind sehr wichtig und Gold wert, wenn wirklich ein Schaden entsteht und sie die Behörden informieren müssen. Denn diese werden vielleicht schnelle Antworten und klare Informationen von Ihnen brauchen, bevor Sie ihnen helfen können.

Die Themen der Workshops sind vielfältig. Sie geben Ihnen eine Vorstellung davon, wo sie ansetzen müssen, wenn es um die Verteidigung Ihrer eigenen Sicherheit geht. Egal, ob Sie sich tiefergehend mit eingesetzter Technologie befassen oder sich einen strategischen Überblick verschaffen wollen. Als Unternehmer müssen Sie wissen, wie die IT in ihrer Organisation arbeitet, was ihre Schwachstellen und Stärken sind. Die Übungen in unserem Workshops werden sie vor unangenehmen Überraschungen am stressigsten Tag im Büro retten.

Melden Sie sich daher noch heute zu unseren Workshops an. Sie finden am 17./18. November statt, gefolgt von der DeepSec-Konferenz am 19./20. November. Veranstaltungsort ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.
Konferenzwebseite: https://deepsec.net/
Registrierung: https://deepsec.net/register.html
Blog: http://blog.deepsec.net/

pts20151020008 Computer/Telekommunikation, Unternehmen/Finanzen

DeepSec-Workshops: Digitale Verteidigung - Wissen ist Macht

IT-Security-Workshops für moderne Unternehmen

Wien (pts008/20.10.2015/08:30) - **Wann haben Sie Ihren letzten Geschäftsbrief geschrieben? Und wann haben Sie das letzte Mal Stift und Papier dazu benutzt? Es macht nichts, wenn Sie sich nicht daran erinnern können: Digitale Kommunikation ist Teil unseres Alltagslebens, nicht nur in der Geschäftswelt. Wir haben uns so sehr daran gewöhnt, ständig online zu kommunizieren, dass offline sein sich schon fast unnatürlich anfühlt. Das heißt natürlich auch, dass wir ständig irgendwelchen Netzwerken ausgeliefert sind, vor allem dem Internet. Unsere Tür steht Tag und Nacht offen. Wir können sie nicht mehr schließen und laden somit offen auch ungebetene Gäste ein, die dieselben Netzwerke nutzen wie wir. Es ist Zeit, ernsthaft darüber nachzudenken. Was für Bedrohungen gibt es da draußen? Und wie können wir uns vor ihnen schützen?**

Cyber-Kriminalität und Datenschutz

Alles ist "Cyber" heutzutage. Kriminalität genauso wie Sicherheitsbestrebungen. Das Militär verwendet das chice Wort, um ihre Strategien und Taktiken zu beschreiben. Die Politik hat das Wort entdeckt, genauso wie Journalisten und PR-Strategen. Doch der Gebrauch dieses Worts birgt Risiken, es verbirgt, wie die digitale Welt wirklich funktioniert im Nebel einer leicht mystischen Aura. Aber wenn es um die Verteidigung Ihrer Daten geht, ist Nebel das Letzte, was Sie brauchen. Sie brauchen Wissen und harte Fakten, klare Sicht. Ablenkung und Missverständnisse sind Ihre Feinde, genauso wie bedeutungslose Trendwörter.

Hive Mind Technology

Informationssicherheit ist ein weites Feld. Vor Jahrzehnten ging es nur um Systeme mit lokal gespeicherten Daten und ein junges Internet, das seine zarten Fühler ausstreckte. Natürlich gab es auch schon damals Stör- und Zwischenfälle, aber die Auswirkungen waren nicht auf der ganzen Welt zu spüren. Heute ist das anders. Wachstum hat seine Nebenwirkungen. Lang ist es her, dass Sicherheitsprobleme allein von IT- Technikern behoben werden konnten. Heute braucht man ein Team aus (internationalen) Rechtsexperten, Entwicklern, Technikern, Sicherheitsforschern, Mathematikern (wenn es um Algorithmen geht), Psychologen, Geschäftsführern, Produzenten und Regierungsbeamten. Und das ist nur die Spitze des Eisbergs.

Als Sicherheitsexperten im Juli 2015 Konstruktionsfehler in Chrysler-Jeeps offenlegten, musste der Automobilhersteller eine Rückholaktion starten, die 1,4 Millionen Autos betraf. Die Auswirkungen sind riesig. Hat ein solcher Jeep noch das Recht auf Zulassung? Wie bekommt man 1,4 Millionen Autobesitzer dazu, sich rechtzeitig um dieses Problem zu kümmern und den Konstruktionsfehler beheben zu lassen? Wer entscheidet über eine Strafe und wer bezahlt sie? Können Versicherungen höhere Preise veranschlagen für Autos, die mit einem Netzwerk verbunden sind? Große Probleme werfen große Fragen auf.

Auch wenn Sie vielleicht kein Auto haben, haben sie wahrscheinlich Haushaltsgeräte. Noch schlimmer, denn das "Internet der Dinge" dräut am Horizont. Eigentlich ist es schon da. Alles vom Toaster über die Kaffeemaschine, verbreitetem Wasserkocher, Personenwaage im Badezimmer, Glühbirne, Waschmaschine, Fernseher, Kamera, Heizstrahler, Schalter, Stecker, Mikrowelle bis zu Schuhen, Zahnbürsten, Uhren, Drohnen (eh klar) und dem Würstelgrill (komplett mit eigener Forschungabteilung), Bett, Golfschläger und vielem vielem mehr - alles ist bereits vernetzt. Sekündlich kommen neue Geräte hinzu. Werden manche dieser Geräte Fehler in sich tragen, die Ihre Sicherheit gefährden? Mit Sicherheit.

Zurück zum Geschäft

Was bedeutet das nun alles für Sie als Unternehmer? Wie sichern Sie die Daten Ihrer Organisation und Ihrer Kunden? Leider gibt es keine Lösung, die alle Gefahren, die auf sie lauern, auf einmal beseitigt. Wir haben es hier nicht mit einer Erkältung zu tun, wo Ruhe und warmer Tee reichen, um die Krankheit zu kurieren. Unternehmen benutzen eine Unmenge an verschiedenen Geräten und Software, die wiederum alle mit unterschiedlichster Software untereinander verbunden sind. Nicht einmal Sicherheitsforscher können mit der rasanten Entwicklung Schritt halten. Smartphones sind dafür das beste Beispiel. Neue Modelle, neue Apps und Operationssysteme tauchen schneller am Markt auf, als sie auf Konstruktionsfehler und Sicherheitslücken getestet werden können. Das wiederum heißt natürlich, dass es Ihnen schwer fallen wird Ihr Smartphone zu regulieren.

Und es kommt noch schlimmer. Tausende europäische Unternehmen vertrauen mittlerweile auf undurchsichtige cloud services. "cloud" ist genau so ein nebulöser Begriff wie "cyber".

Wussten Sie beispielsweise, dass ein Großteil der cloud-Anbieter in der USA beheimatet sind und sich ihre Dienste somit nicht an das europäische Datenschutzrecht halten müssen? Die EU-Kommission hat versucht, dieses Problem zu lösen, indem sie mit den USA ein "Safe Harbour"-Abkommen getroffen hat, bei dem amerikanische Unternehmen sich freiwillig bereit erklären den europäischen Datenschutzprinzipien zu folgen. Der NSA-Skandal hat das Vertrauen in dieses Abkommen erschüttert und der Europäische Gerichtshof hat die Vereinbarung diesen Oktober widerrufen.

All dies verdeutlicht, dass Sie eine Menge darüber wissen müssen, was sich hinter der Bühne abspielt. Sie können sich nicht auf Gerüchte oder nette Anekdoten verlassen. Sie brauchen Fakten, um zu entscheiden, welche Technologie sie nutzen wollen, welche sie vermeiden sollten und wo Verbesserungsbedarf besteht. Vor allem müssen Sie sich und Ihre Entscheidungen konstant hinterfragen. Die Geschäftswelt muss dringend lernen, Fehler zuzugeben und die Umstände zu analysieren, die zu Störfällen geführt haben. Und sie muss lernen, Experten aus den verschiedendsten Forschungs- und Entwicklungsfeldern in ihre Entscheidungen miteinzubeziehen. Geben wir es zu, nicht einmal Wonder Woman oder Superman könnten die digitale Welt auf eigene Faust retten. Machen Sie nicht den Fehler zu glauben, Sie könnten es, denn der Weg zum Datenleck ist mit Selbstüberschätzung gepflastert.

Wachen Sie auf!

Die jährliche DeepSec In-Depth Security-Konferenz versucht, jeden Aspekt der Informationssicherheit in ihr Programm zu integrieren. Sie versammelt Experten aus Wissenschaft, Regierung und Wirtschaft, Anwender und Entwickler genauso wie Mitglieder der Hacking Community. Informationssicherheit ist eine Herausforderung, der man nur gemeinsam entgegentreten kann. Und auf der DeepSec geht es nicht nur um Theorie. In einem 50-minütigen Talk kann man viele Themen vielleicht nicht im Detail behandeln oder das Publikum bitten, vorgestellte Lösungen gleich selbst auszuprobieren - dafür gibt es die Workshops! Die DeepSec bietet praktische Workshops an, in denen jeder Teilnehmer selbst Hand anlegen kann und im Programm findet sich alles, was Sie wirklich brauchen: Lösungen, die wirklich funktionieren, nicht nur im Labor, sondern in Ihrem realen Umfeld und die Sie auch gleich ausprobieren können; praktische Erfahrung mit Angriffs-und Verteidigungswerkzeug, um für den nächsten Angriff gewappnet zu sein.

Die Workshops dauern zwei Tage; das bedeutet genug Zeit, um sich wirklich gründlich mit einem Thema auseinanderzusetzen und Wissen zu gewinnen. Thematisch richten sie sich an jeden, der sich gegen moderne Angriffe verteidigen will. Hier ein kurzer Überblick über die Workshops:

Cryptographic Attacks
Lernen Sie alles über Attacken auf Kryptographie, die in ihren Software-Applikationen verwendet wird. Vieles hat sich in den letzten zwei Jahren verändert, und auch, wenn Sie sich mathematisch nicht weiterbilden müssen, wollen Sie Ihre Kunden sicher nicht gefährden, indem Sie veraltete Verschlüsselung verwenden.

Hacking Web Applications
Nahezu jedes Unternehmen präsentiert sich heute im World Wide Web. Ihre Website ist sozusagen Ihre Vordertüre. Und diese sollte so sicher wie möglich sein, vor allem, weil sie jeder sieht. Leider denken Entwickler oft nicht außerhalb gängiger Konventionen und verlassen sich auf Annahmen, auf die man sich nicht verlassen kann: Vertrauen Sie nicht auf ihren Browser und lernen Sie, auf was sie sich bei diversen Internet Clients gefasst machen müssen. Denn Kriminelle kommen nicht immer durch die Hintertüre.

Exploiting Devices being used in the Internet of Things
Eine bestimmte Art von Hardware-Prozessoren wird viel für Kontroll- und Messzwecke benutzt. Dieses Training erklärt, wie ein Prozessor funktioniert und was ein Angreifer versuchen wird, um zu erreichen, dass der Prozessor seinen Code statt Ihrem verwendet.

Testing the Security of the Next-Generation Internet Protocols (IPv6)
Auch wenn Sie vielleicht keine Ahnung haben, wie die nächste Generation des Internet aussieht, benutzen Sie es schon. Jedes moderne Betriebssystem unterstützt die neuen Protokolle und sie sind standardmäßig aktiviert. Aber dass etwas funktioniert, ohne dass man etwas davon bemerkt, heißt noch lange nicht, dass man sich nicht damit beschäftigen soll. Vergessen Sie nicht, Sie müssen wissen was vor sich geht, sowohl in ihrem Betrieb wie in Ihrem Betriebssystem. Dieses Training wird ihnen zeigen, auf was Sie achten müssen, wenn Sie eine Internetverbindung herstellen.

Windows PowerShell for Penetration Testers
Seine eigene Abwehr zu testen, ist immer eine gute Idee. Tun Sie es, bevor es Ihre Gegner für Sie tun. Die

Methode dafür heißt "Penetration Testing". Dieser Workshop befasst sich mit der Microsoft Windows-Plattform und ihren Werkzeugen und wie Sie diese zu Ihrem Vorteil einsetzen können.

Social Engineering and Security Awareness
Das gefährlichste Gerät in Ihrem Betrieb ist das Telefon. Ein einfacher Anruf genügt oft, um die ausgeklügeltste Verteidigung Schachmatt zu setzen. Der menschliche Faktor ist nicht zu unterschätzen. Lässt nur ein Mitarbeiter sich dazu überreden, die Zugbrücke runterzulassen, nimmt das Unglück seinen Lauf. Um sich zu schützen, sollten Sie lernen, wie menschliche Interaktion funktioniert und wie Angreifer versuchen, Sie und ihre Mitarbeiter zu manipulieren. Ein ausgebildeter Psychologe wird Ihnen zeigen, wogegen Sie sich wappnen müssen und wie Sie sich am besten verteidigen.

Developing and Using Threat Intelligence
Wissen Sie, wer Ihre Gegner sind und was Sie wollen? Wenn nicht, ist es Zeit, das herauszufinden. Die Technik hierfür heißt "Threat Intelligence". In diesem Workshop lernen Sie, wie Sie Gefahren richtig einschätzen können, basierend auf den Daten die Sie selbst zur Verfügung haben.

Secure Web Development
Entwickler haben einen schlechten Ruf, wenn es um Informationssicherheit geht. Dafür gibt es viele Gründe, aber Ignoranz fällt sicher nicht darunter. Sie müssen sich an bestimmte Arten der Kodierung anpassen und die richtigen Werkzeuge verwenden, um Ihren Code zu testen. Sobald Sie das getan haben, wird Ihre Software viel besser funktionieren. Dieses Training ist für jeden, der es mit Code zu tun hat, von großem Vorteil.

Practical Incident Handling
Früher oder später passiert etwas. Was machen Sie dann? Haben Sie sich jemals vorgestellt, wie ein Tag in ihrer Firma aussieht, wenn der Hauptserver kompromittiert ist? Jede Organisation unterwirft sich den Brandschutzbestimmungen. Sie müssen vielleicht sogar einmal im Jahr eine Brandschutzübung absolvieren. Sie sollten auch einen digitale Brandschutzübung machen. Simulieren Sie einen Störfall und spielen Sie durch, was getan werden muss, um ihn gut zu überstehen. Solche Übungen sind sehr wichtig und Gold wert, wenn wirklich ein Schaden entsteht und sie die Behörden informieren müssen. Denn diese werden vielleicht schnelle Antworten und klare Informationen von Ihnen brauchen, bevor Sie ihnen helfen können.

Die Themen der Workshops sind vielfältig. Sie geben Ihnen eine Vorstellung davon, wo sie ansetzen müssen, wenn es um die Verteidigung Ihrer eigenen Sicherheit geht. Egal, ob Sie sich tiefergehend mit eingesetzter Technologie befassen oder sich einen strategischen Überblick verschaffen wollen. Als Unternehmer müssen Sie wissen, wie die IT in ihrer Organisation arbeitet, was ihre Schwachstellen und Stärken sind. Die Übungen in unserem Workshops werden sie vor unangenehmen Überraschungen am stressigsten Tag im Büro retten.

Melden Sie sich daher noch heute zu unseren Workshops an. Sie finden am 17./18. November statt, gefolgt von der DeepSec-Konferenz am 19./20. November. Veranstaltungsort ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.
Konferenzwebseite: https://deepsec.net/
Registrierung: https://deepsec.net/register.html
Blog: http://blog.deepsec.net/

(Ende)

Aussender:	DeepSec GmbH
Ansprechpartner:	René Pfeiffer
Tel.:	+43-676-5626390
E-Mail:	deepsec@deepsec.net
Website:	www.deepsec.net

http://www.pressetext.com/news/20150827013

Der Feind in meinem Netz
Sicherheitskonferenz DeepSec: Wie schützt man sich vor Wirtschaftsspionage?

Datum: 27.08.2015

Autor: René Pfeiffer

Wien (pts013/27.08.2015/08:30) - Vernetzung ist in der Geschäftswelt unabdingbar für die Gewinnung von Aufträgen, Leitung von Projekten und Entwicklung von Produkten. Wo anfangs das World Wide Web war, sorgen nun auch diverse Clouds und Social Media Plattformen für Interaktion. Daten werden an Fremde ausgelagert, und Geschäftsbriefe werden mittlerweile munter per Instant Messenger verschickt. Gedankenlose Umarmung von Netzwerken lädt Bedrohungen ein, die man bislang nur aus dem Kino kennt - Spione.

Die DeepSec möchte Unternehmen mit dieser Problemstellung nicht alleine im Regen stehen lassen. Die internationale IT Security-Konferenz findet vom 17.11 bis 20.11 im Wiener Imperial Riding School Renaissance Hotel statt.

In der digitalen Welt reicht es leider nicht mehr aus einfach nur die Tür zu schließen. Es gibt viel mehr zu beachten. Genau dabei werden Ihnen unsere Experten in Vorträgen und Trainings zur Seite stehen.

Auf der DeepSec erfahren Sie in Vorträgen wie gefährlich das World Wide Web ist:
Denn jede aufgerufene Webseite erlaubt die Wechselwirkung mit Ihren internen Systemen. Ein falscher Klick kann verheerende Folgen haben, da schützt auch das verwendete System nicht. Attacken durch scheinbar harmlose Dokumente sind an der Tagesordnung, selbst das bloße Anzeigen von Daten kann schon gefährlich sein. Die Stagefright Sicherheitslücke für Multimedia Nachrichten (MMS) auf Android Smartphones, der Fehler im PDF Viewer von Mozilla Firefox, die Lücke im Microsoft OpenType Font Format oder die Nachricht, die Apple iPhones einfrieren läßt, zeigen wie herstellerübergreifend Attacken funktionieren. Wir zeigen Ihnen worauf es zu achten gilt.

Sie lernen Ihre Gegner kennen:
Zu einer guten Verteidigung gehören ebenso Übungen und Sicherheitstests aus der Sicht des Spions. Unsere

Trainer zeigen wie man diese richtig durchführt und wie weit man durch kontrollierte Einbrüche kommt. Es geht dabei um das Ausnutzen aller Mittel wie Drohnen, eingeschmuggelte Smartphones, Vortäuschen von Identitäten oder kopierten Authentisierungsdaten. “Man darf sich bei solchen Tests nicht von Beginn an einschränken. Moderne Attacken gehen ungewöhnliche Wege, die man nur mit Out of the Box - Denken erfassen kann”, berichtet Michael

Kafka, Organisator der DeepSec.

Und Sie lernen, sich richtig zu schützen:
Zum Beispiel im IPv6 Workshop. IPv6 ist mittlerweile automatisch Teil jedes Unternehmensnetzwerks, egal ob man will oder nicht. Es ist also höchste Zeit es korrekt zu konfigurieren und sicher zu verwalten. Darüber hinaus bieten wir ein Web Application Security Training an, welches an prominenten Beispielen von Google, Yahoo! oder Mozilla Web Apps zeigt was alles schiefgehen kann. Ein weiterer Kurs behandelt Attacken auf Kryptographie und gibt Ihnen einen Überblick wie man Verschlüsselung richtig einsetzt. Allen, die in der Softwareentwicklung arbeiten, legen wir dieses Training besonders ans Herz. Spione bedienen sich aber oft auch ganz alltäglicher Methoden: Sie benutzen das Telefon, Social Media oder täuschen Menschen in dem sie sich einfach in passender Kleidung präsentieren, um Ihnen den Zugang zu firmeninternen Geheimnissen zu entlocken. Tarnen & Täuschen - Ausnutzen von alltäglicher Kommunikation durch Social Engineering ist an der Tagesordnung. Auch dort müssen Sie Maßnahmen zur Verteidigung treffen. Wir bieten mit dem Social Engineering Workshop Abhilfe.

Jedes Unternehmen hat Geheimnisse. Sie gehören zur Basis jedes Geschäfts. In Zeiten wo Unternehmer von Regierungen keine Hilfe mehr zu erwarten haben, wenn es um ihren digitalen Schutz geht, sollte man sich den Problemen selbst stellen. Bringen Sie Ihre eigene IT-Mannschaft auf den neuesten Stand - besuchen Sie die diesjährige DeepSec 2015-Konferenz.

DeepSec 2015
17.11 - 20.11.2015
Imperial Riding School Renaissance Vienna Hotel
Ungargasse 60
1030 Wien

E-Mail: deepsec@deepsec.net
Website: deepsec.net

pts20150827013 Computer/Telekommunikation, Unternehmen/Finanzen

Der Feind in meinem Netz

Sicherheitskonferenz DeepSec: Wie schützt man sich vor Wirtschaftsspionage?

Wien (pts013/27.08.2015/08:30) - **Vernetzung ist in der Geschäftswelt unabdingbar für die Gewinnung von Aufträgen, Leitung von Projekten und Entwicklung von Produkten. Wo anfangs das World Wide Web war, sorgen nun auch diverse Clouds und Social Media Plattformen für Interaktion. Daten werden an Fremde ausgelagert, und Geschäftsbriefe werden mittlerweile munter per Instant Messenger verschickt. Gedankenlose Umarmung von Netzwerken lädt Bedrohungen ein, die man bislang nur aus dem Kino kennt - Spione.**

Die DeepSec möchte Unternehmen mit dieser Problemstellung nicht alleine im Regen stehen lassen. Die internationale IT Security-Konferenz findet vom 17.11 bis 20.11 im Wiener Imperial Riding School Renaissance Hotel statt.

In der digitalen Welt reicht es leider nicht mehr aus einfach nur die Tür zu schließen. Es gibt viel mehr zu beachten. Genau dabei werden Ihnen unsere Experten in Vorträgen und Trainings zur Seite stehen.

Logo DeepSec 2015 (Design: Florian Stocker)

Auf der DeepSec erfahren Sie in Vorträgen wie gefährlich das World Wide Web ist:
Denn jede aufgerufene Webseite erlaubt die Wechselwirkung mit Ihren internen Systemen. Ein falscher Klick kann verheerende Folgen haben, da schützt auch das verwendete System nicht. Attacken durch scheinbar harmlose Dokumente sind an der Tagesordnung, selbst das bloße Anzeigen von Daten kann schon gefährlich sein. Die Stagefright Sicherheitslücke für Multimedia Nachrichten (MMS) auf Android Smartphones, der Fehler im PDF Viewer von Mozilla Firefox, die Lücke im Microsoft OpenType Font Format oder die Nachricht, die Apple iPhones einfrieren läßt, zeigen wie herstellerübergreifend Attacken funktionieren. Wir zeigen Ihnen worauf es zu achten gilt.

Sie lernen Ihre Gegner kennen:
Zu einer guten Verteidigung gehören ebenso Übungen und Sicherheitstests aus der Sicht des Spions. Unsere Trainer zeigen wie man diese richtig durchführt und wie weit man durch kontrollierte Einbrüche kommt. Es geht dabei um das Ausnutzen aller Mittel wie Drohnen, eingeschmuggelte Smartphones, Vortäuschen von Identitäten oder kopierten Authentisierungsdaten. "Man darf sich bei solchen Tests nicht von Beginn an einschränken. Moderne Attacken gehen ungewöhnliche Wege, die man nur mit Out of the Box - Denken erfassen kann", berichtet Michael Kafka, Organisator der DeepSec.

Und Sie lernen, sich richtig zu schützen:
Zum Beispiel im IPv6 Workshop. IPv6 ist mittlerweile automatisch Teil jedes Unternehmensnetzwerks, egal ob man will oder nicht. Es ist also höchste Zeit es korrekt zu konfigurieren und sicher zu verwalten. Darüber hinaus bieten wir ein Web Application Security Training an, welches an prominenten Beispielen von Google, Yahoo! oder Mozilla Web Apps zeigt was alles schiefgehen kann. Ein weiterer Kurs behandelt Attacken auf Kryptographie und gibt Ihnen einen Überblick wie man Verschlüsselung richtig einsetzt. Allen, die in der Softwareentwicklung arbeiten, legen wir dieses Training besonders ans Herz. Spione bedienen sich aber oft auch ganz alltäglicher Methoden: Sie benutzen das Telefon, Social Media oder täuschen Menschen in dem sie sich einfach in passender Kleidung präsentieren, um Ihnen den Zugang zu firmeninternen Geheimnissen zu entlocken. Tarnen & Täuschen - Ausnutzen von alltäglicher Kommunikation durch Social Engineering ist an der Tagesordnung. Auch dort müssen Sie Maßnahmen zur Verteidigung treffen. Wir bieten mit dem Social Engineering Workshop Abhilfe.

Jedes Unternehmen hat Geheimnisse. Sie gehören zur Basis jedes Geschäfts. In Zeiten wo Unternehmer von Regierungen keine Hilfe mehr zu erwarten haben, wenn es um ihren digitalen Schutz geht, sollte man sich den Problemen selbst stellen. Bringen Sie Ihre eigene IT-Mannschaft auf den neuesten Stand - besuchen Sie die diesjährige DeepSec 2015-Konferenz.

DeepSec 2015
17.11 - 20.11.2015

Imperial Riding School Renaissance Vienna Hotel
Ungargasse 60
1030 Wien

(Ende)

Aussender:	DeepSec GmbH
Ansprechpartner:	René Pfeiffer
Tel.:	+436765626390
E-Mail:	deepsec@deepsec.net
Website:	deepsec.net

PRESS RELEASE 01
DEEPSEC 2015

Datum: 25.06.2015

Autor: René Pfeiffer, Susanne Firzinger

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 informa-

tion 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

Contact

René Pfeiffer

rpfeiffer@deepsec.net

+43/676/5626390

DeepSec GmbH

c/o Mr. René Pfeiffer

Bräuhausgasse 32

1050 Vienna, Austria

VAT ID: ATU63522646

Business registration number: FN 294621 t

Customs EORI code: ATEOS1000025635