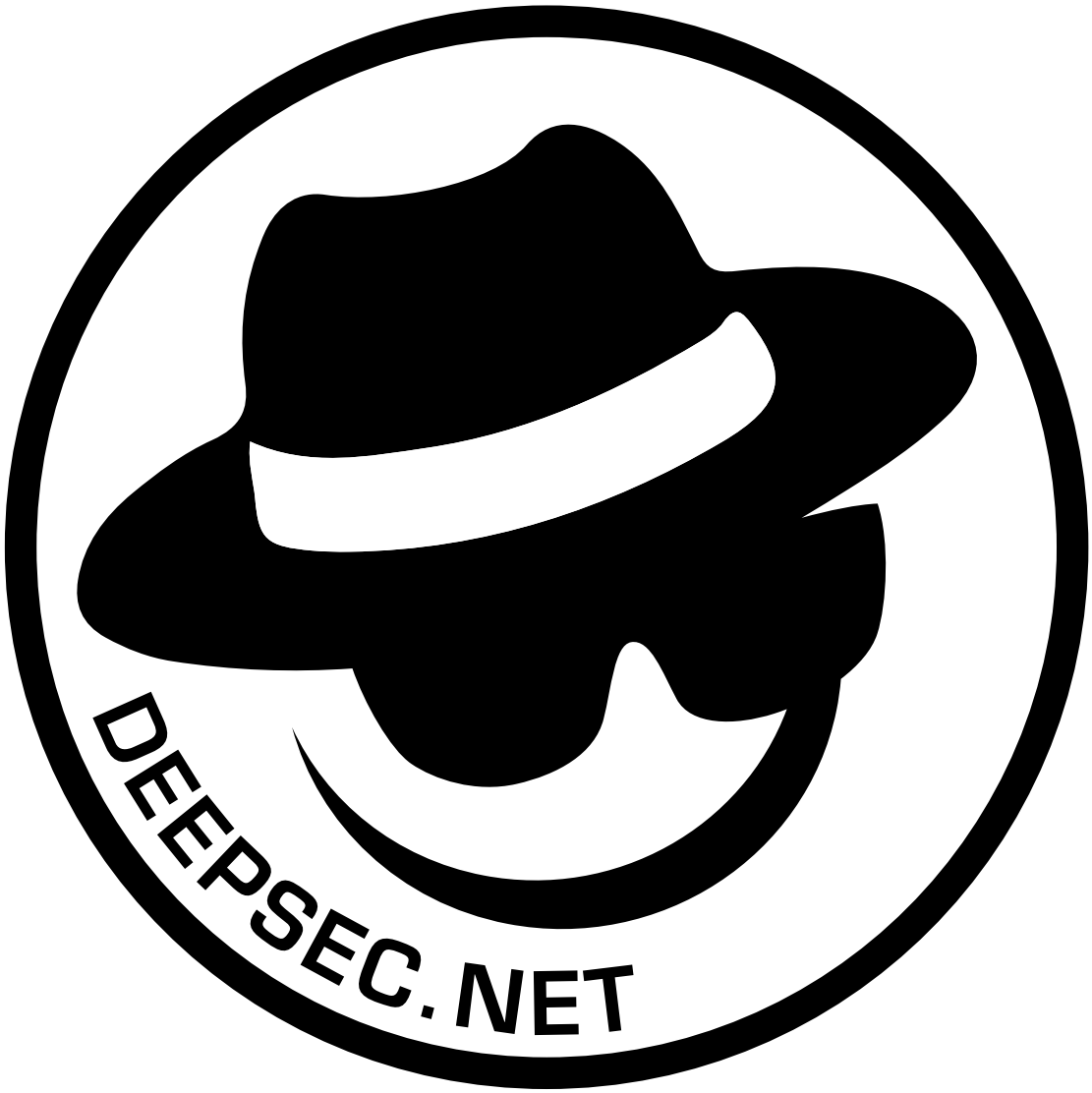


press review 2013

media coverage

2013

DeepSec 2013 5

(securityninja.co.uk 17.12.2013)

Der hackbare Patient 9

(golem.de 16.12.2013)

DeepSec 2013 16

(insinuator.net 09.12.2013)

Geheimnisse, Pleiten und Visionen - Die DeepSec 2013 21

(ö1 01.12.2013)

Verfolgungsjagd per Bluetooth.....23

(golem.de 29.11.2013)

Forscher zeigt: So leicht lassen sich Medizingeräte hacken 28

(futurezone.at 25.11.2013)

Forscher zeigt: So leicht lassen sich Medizingeräte hacken 37

(kurier.at 25.11.2013)

Konferenz DeepSec hinterfragt den Cyberwar 47

(deutschlandfunk.de 23.11.2013)

“Europäische Netze sind reine Augenauswischerei”.....51

(standard.at 22.11.2013)

DeepSec: Falsches Vertrauen in Facebook-Freunde 59

(futurezone.at 21.11.2013)

DeepSec: Vom Herzschrittmacher-Hack bis zum Profiling 63

(futurezone 24.10.2013)

DeepSEC - Effective IDS/IPS Auditing And Testing With Finux 66

(alba13.com 24.10.2013)

Datenschutz hilft Cyberspionage abzuwehren 69

(fm4.orf.at 03.06.2013)

contents

press releases

2013

press release 04 81

(19.11.2013)

press release 03 83

(31.10.2013)

press release 02 89

(24.10.2013)

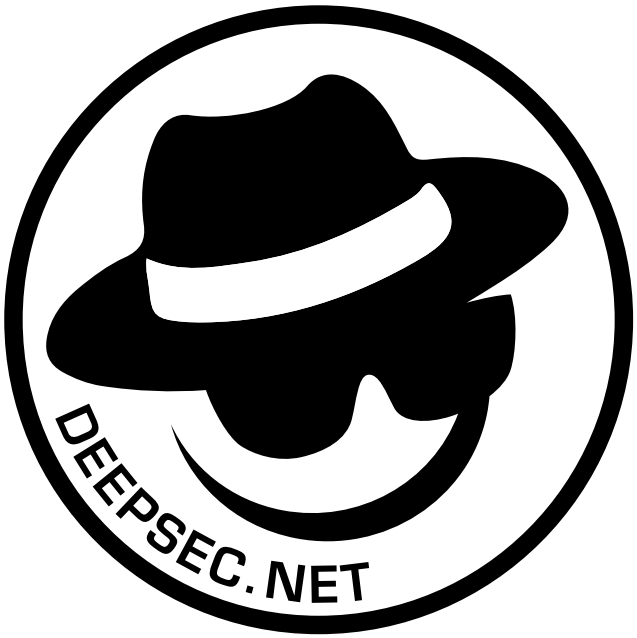
press release 01 95

(09.10.2013)

contact / impressum

.....101

media coverage 2013



https://www.securityninja.co.uk/hacking/deepsec-2013/

DeepSec 2013

Datum: 17.12.2013

Autor: Security Ninja

Hi everyone,

DeepSec is a security conference lauded by its fans as having the most interesting talks and inviting atmosphere. In its seventh year, it runs in Vienna, Austria, chosen for its central EU location, and not just because it's a beautiful city, with Christmas markets on at the same time as the conference – another good reason to visit. This was my first year going to DeepSec, thanks to the organizers offering a trip as the BSides London Rookie Track prize last April.

NSA Device

The morning after checking into the hotel and exploring Vienna on Wednesday night, the first thing I got my hands on was the magnetic badges. It was nice that I didn't have to put holes in my clothes to get in and made a nice difference to lanyards, and there was an added risk factor of wiping the hotels room cards magnetic strip (which happened to at least one of the speakers I chatted to).

The talks were all very interesting, and I was torn at times between which track to choose. I don't have the space to mention each talk I found impressive, but the best takeaway was an explanation of Session Puzzling by Shay Chen of Hacktics, who demonstrated how to use an applications functionality to populate server-side session variables in a way to bypass authorization checks, as one example. There were some great live demos, especially the root exploit on Cray supercomputers demonstrated by two researchers from MWR Infosecurity – exploited by hot patching a return statement using gdb.

Unlike other conferences where there was time to have quick breakout sessions in the hallways, I found myself hopping from room to room unable to take a break because of the quality of the talks.

The conference was rounded off with a meal at the aptly named "Hakka Cun":before rushing to MetaLab for the after party. The main classroom had been set up with decks, a couple of people mixing while "cyber cyber cyber" – the theme of DeepSec this year – scrolled across the projector screens over visualisations that would have made WinAmp envious.

DeepSec is a very welcoming conference, with great technical talks, located in a beautiful city. It's definitely a con-

ference I want to revisit, and one I'd recommend to anyone who's involved in building or breaking security.

Diarmaid

DeepSec 2013

DECEMBER 17, 2013 | WRITTEN BY SECURITY NINJA | APPLICATION SECURITY, HACKING, NINJA NEWS AND UPDATES | LEAVE A COMMENT

Hi everyone,

DeepSec is a security conference lauded by its fans as having the most interesting talks and inviting atmosphere. In its seventh year, it runs in Vienna, Austria, chosen for its central EU location, and not just because it's a beautiful city, with Christmas markets on at the same time as the conference – another good reason to visit. This was my first year going to DeepSec, thanks to the organizers offering a trip as the BSides London Rookie Track prize last April.

The morning after checking into the hotel and exploring Vienna on Wednesday night, the first thing I got my hands on was the magnetic badges. It was nice that I didn't have to put holes in my clothes to get in and made a nice difference to lanyards, and there was an added risk factor of wiping the hotels room cards magnetic strip (which happened to at least one of the speakers I chatted to).

The talks were all very interesting, and I was torn at times between which track to choose. I don't have the space to mention each talk I found impressive, but the best takeaway was an explanation of Session Puzzling by Shay Chen of Hacktics, who demonstrated how to use an applications functionality to populate server-side session variables in a way to bypass authorization checks, as one example. There were some great live demos, especially the root exploit on Cray supercomputers demonstrated by two researchers from MWR Infosecurity – exploited by hot patching a return statement using gdb.

Unlike other conferences where there was time to have quick breakout sessions in the hallways, I found myself hopping from room to room unable to take a break because of the quality of the talks.

The conference was rounded off with a meal at the aptly named "Hakka Can":

before rushing to MetaLab for the after party. The main classroom had been set up with decks, a couple of people mixing while "cyber cyber cyber" – the theme of DeepSec this year – scrolled across the projector screens over visualisations that would have made WinAmp envious.

DeepSec is a very welcoming conference, with great technical talks, located in a beautiful city. It's definitely a conference I want to revisit, and one I'd recommend to anyone who's involved in building or breaking security.

Diarmaid

This entry was posted on December 17, 2013 at 1:30 pm and is filed under Application Security, Hacking, Ninja News and Updates . You can follow any responses to this entry through the RSS 2.0 feed. You can leave a response, or trackback from your own site.

Like 0 Tweet 2

Leave a comment

Name *

Mail (will not be published) *

Website

Your Comment*

Submit

VIDEOS & SLIDESHARES
Look at our latest security Videos & SlideShares

EVENTS & SEMINARS
Upcoming Security Events & Seminars

PODCASTS & DOWNLOADS
Check out our Podcasts & White Papers

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

MEDIZINISCHE GERÄTE

Der hackbare Patient

Datum: 16.12.2013

Autor:Jörg Thoma

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

Das Szenario klingt nach einem Agentenfilm: Ein Vitaldatenmonitor wird so gehackt, dass er keinen Alarm mehr auslöst, wenn die Vitalfunktionen eines Patienten außerhalb der normalen Parameter erfasst werden. Über eine Man-in-the-Middle-Attacke werden dann falsche Daten an die Überwachungszentrale geschickt. Der Patient kann so getötet werden, ohne dass es jemand im Krankenhaus bemerkt. Reine Fiktion ist das aber nicht.
Solche Szenarien würden im Gegenteil immer wahrscheinlicher, sagte Sicherheitsexperte Florian Grunow von der Sicherheitsfirma ERNW auf der Sicherheitskonferenz Deepsec 2013 in Wien. Der Hacker Barnaby Jack manipulierte beispielsweise eine Insulinpumpe so, dass sie die gesamte Dosis auf einmal abgab. Für einen Patienten wäre das tödlich. Jack nutzte dafür die Funkschnittstelle des Geräts - aus bis zu 300 Meter Entfernung ist das möglich.
Der Sicherheitsexperte Kevin Fu experimentierte mit einem Defibrilator, dessen abgehörte Funksignale genutzt werden können, um ihn ein- und auszuschalten. Auch das kann für einen Patienten tödlich sein. Mit zunehmender Konnektivität der diversen medizinischen Geräte erweitere sich auch die Angriffsfläche, sagte Grunow Golem.de. Gleichzeitig werde die Gefahr von den Herstellern aber immer weiter unterschätzt.

Unsichere Systeme können tödlich sein

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

meln und sie über das Netzwerk an Ärzte und Krankenhäuser versenden.

Gefährdete Patientendaten

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

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

Veraltete Software und gefährliche Funktionen

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

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

Viel, zu viel Netzwerk

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

also eine verantwortungsvolle Veröffentlichung von Sicherheitslücken, um Patienten nicht zu gefährden.

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

Warnungen vom FDA

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

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

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

MEDIZINISCHE GERÄTE

Der hackbare Patient

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

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

Artikel: MEDIZINISCHE GERÄTE
Der hackbare Patient

Inhalt: Veraltete Software und gefährliche Funktionen

Datum: 16.12.2013, 17:00

Autor: Jörg Thoma

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

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

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

Unsichere Systeme können tödlich sein

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

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

Gefährdete Patientendaten

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

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

1 2 ›

Veraltete Software und gefährliche Funktionen ›

Veraltete Software und gefährliche Funktionen

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

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

Viel, zu viel Netzwerk

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

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

Warnungen vom FDA

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

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

Artikel: MEDIZINISCHE GERÄTE
Der hackbare Patient

Inhalt: Veraltete Software und gefährliche Funktionen

Datum: 16.12.2013, 17:00

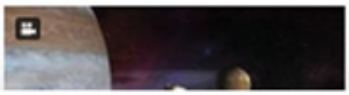
Autor: Jörg Thoma

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

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

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

‹ 1 2



https://www.insinuator.net/2013/12/deepsec-2013/#more-2678

DeepSec 2013

Datum: 09.12.2013

Autor: Niklaus Schiess

Last week Florian and I participated at this year's DeepSec in Vienna. We had a really good time, thanks again to the DeepSec staff for a nice conference. Although it might be a bit late, I want to share some impressions about various talks I enjoyed.

spin: Static Instrumentation For Binary Reverse-Engineering

This talk primarily covered a technique called binary instrumentation, which is used e.g. for performance evaluation, CPU emulation, tracing and profiling but also for malware- and threat-analysis. David Guillen Fandos proposed the application of this technique in the field of reverse engineering. Binary instrumentation is a technique which allows to modify and rewrite binaries during their execution by injecting instructions into the original code (pretty much like virtual machines do too). Therefore one could easily wrap instructions with logging/tracing functions, to observe the execution status before and after easy instruction step (and/or dump the output into a file). For the purpose of reversing, one could also create complex conditional breakpoints (retaining status across executions), which makes it possible to characterize functions.

David developed a tool called "spin" (a somehow static version of Intel's Pin tool) which is able to characterize and identify security-critical functions by applying conditions. Additionally, it can automatically hook functions by injecting DLL's during runtime. He demonstrated this in a little demo by hooking Winzip's serial verify function so it would accept any serial. Spin is still in early development but it's aid to the automation of reverse engineering seems really promising. Hopefully David will add support for API-Hooking, which isn't yet supported due to the lack of 2Byte-Opcode hooking.

Trusted Friend Attack: Guardian Angels Strike

Ashar Javed from the Ruhr University Bochum presented how an attacker can exploit social networks in order to gain access to user accounts. Especially functions where trusted third parties are involved, like Facebook's password recovery, are mostly vulnerable to those attacks. Ashar demonstrated that it's not the implementation of these functions that is vulnerable, but the logic behind. As those trusted third parties are just accounts that are in a users friend list, becoming one of them is a rather easy task, because most people confirm arbitrary friendship requests anyway. The slides are available here.

The Boomerang Effect – Using Session Puzzling To Attack Apps From The Backend

Shay Chen presented a pretty interesting technique for web application hacking called session puzzling. Instead of directly sending payloads to a web application's front end, this technique aims at attacking the application from the back end by polluting session related memory in order to prepare payloads across multiple requests. Shay also demonstrated a few ways to attack an application via session puzzling (e.g. authentication bypass) at a self developed training platform called PuzzleMall. For further information, read the blog post as well as Shay's whitepaper.

Mutually Assured Pwange

This was the first anti cyber war talk I've every heard and I really liked it. Karin Kosina did a great job explaining why this so called "cyberwar" cannot be compared with the cold war. Those of you who are really interested in this topic should take a look at her master's thesis, which covers this topic as well. The slides are also available.

Applied Crypto Hardening

Aaron Kaplan and three others presented a project called Applied Crypto Hardening, which was initiated by CERT.at and Adi Kriegisch (VRVis). It aims at providing a paper for (mainly) system administrators with copy&paste-ready configuration examples for common applications like webservers (Apache, Nginx, …), mail transfer agents (like Postfix and Sendmail), SSHD and many others. So far those configuration examples only cover security related recommendations, mostly about choosing strong cipher suites for various tasks. It would be nice to see some performance related information for those configurations in the future (like suggested by an attendee after the talk) to further improve the quality of this paper. In my opinion this is a really important project but there is still a lot of work to do. I'm a little bit disappointed that there won't be a SSTP section. Instead they prefer to stick to PPTP. Furthermore I seriously doubt that a paper in PDF format is the right choice for content that's supposed to be copy&paste'd.

Hopefully the recordings won't take that long, so we can enjoy the other talks we missed during the conference.

Regards,

Niklaus

Recent Comments

- Florian Grunow on RedStar OS Watermarking
- Jean-Christophe Manciot on Evasion of Cisco ACLs by (Ab)Using IPv6 – Part 2
- Isaias on Is IPv6 more Secure than IPv4? Or Less?
- witness digital on How to Get a BaseStation
- James Small on OS IPv6 Behavior in Conflicting Environments

Dec/13

9

DeepSec 2013

0 Comments | Posted by *Niklaus Schiess*

Last week Florian and I participated at this year's DeepSec in Vienna. We had a really good time, thanks again to the DeepSec staff for a nice conference. Although it might be a bit late, I want to share some impressions about various talks I enjoyed.

spin: Static Instrumentation For Binary Reverse-Engineering

This talk primarily covered a technique called *binary instrumentation*, which is used e.g. for performance evaluation, CPU emulation, tracing and profiling but also for malware- and threat-analysis. David Guillen Fandos proposed the application of this technique in the field of reverse engineering. Binary instrumentation is a technique which allows to modify and rewrite binaries during their execution by injecting instructions into the original code (pretty much like virtual machines do too). Therefore one could easily wrap instructions with logging/tracing functions, to observe the execution status before and after easy instruction step (and/or dump the output into a file). For the purpose of reversing, one could also create complex conditional breakpoints (retaining status across executions), which makes it possible to characterize functions.

David developed a tool called "spin" (a somehow static version of Intel's Pin tool) which is able to characterize and identify security-critical functions by applying conditions. Additionally, it can automatically hook functions by injecting DLL's during runtime. He demonstrated this in a little demo by hooking Winzip's serial verify function so it would accept any serial. Spin is still in early development but it's aid to the automation of reverse engineering seems really promising. Hopefully David will add support for API-Hooking, which isn't yet supported due to the lack of 2Byte-Opcode hooking.

Trusted Friend Attack: Guardian Angels Strike

Ashar Javed from the Ruhr University Bochum presented how an attacker can exploit social networks in order to gain access to user accounts. Especially functions where trusted third parties are involved, like Facebook's password recovery, are mostly vulnerable to those attacks. Ashar demonstrated that it's not the implementation of these functions that is vulnerable, but the logic behind. As those trusted

third parties are just accounts that are in a users friend list, becoming one of them is a rather easy task, because most people confirm arbitrary friendship requests anyway. The slides are available here.

The Boomerang Effect – Using Session Puzzling To Attack Apps From The Backend

Shay Chen presented a pretty interesting technique for web application hacking called session puzzling. Instead of directly sending payloads to a web application's front end, this technique aims at attacking the application from the back end by polluting session related memory in order to prepare payloads across multiple requests. Shay also demonstrated a few ways to attack an application via session puzzling (e.g. authentication bypass) at a self developed training platform called PuzzleMall. For further information, read the blog post as well as Shay's whitepaper.

Mutually Assured Pwange

This was the first anti cyber war talk I've every heard and I really liked it. Karin Kosina did a great job explaining why this so called "cyberwar" cannot be compared with the cold war. Those of you who are really interested in this topic should take a look at her master's thesis, which covers this topic as well. The slides are also available.

Applied Crypto Hardening

Aaron Kaplan and three others presented a project called Applied Crypto Hardening, which was initiated by CERT.at and Adi Kriegisch (VRVis). It aims at providing a paper for (mainly) system administrators with copy&paste-ready configuration examples for common applications like webservers (Apache, Nginx, …), mail transfer agents (like Postfix and Sendmail), SSHD and many others. So far those configuration examples only cover security related recommendations, mostly about choosing strong cipher suites for various tasks. It would be nice to see some performance related information for those configurations in the future (like suggested by an attendee after the talk) to further improve the quality of this paper. In my opinion this is a really important project but there is still a lot of work to do. I'm a little bit disappointed that there won't be a SSTP section. Instead they prefer to stick to PPTP. Furthermore I seriously doubt that a paper in PDF format is the right choice for content that's supposed to be copy&paste'd.

Hopefully the recordings won't take that long, so we can enjoy the other talks we missed during the conference.

Regards,
Niklaus

No tags

No comments yet.

Leave a comment!

Name* Mail* (will not be published) Website
Spam protection*: Sum of 3 + 7 ? Comment

Insinuator

Some outright rants from a bunch of infosec practitioners.

Search this Blog

Search... Go

Tag Cloud

3G 4G Android attacks Cisco cloud conferences DHCPv6 ERNW Extension Headers Fragmentation fuzzing gsm gtp hacking Hardening HITB iOS IPv6 IPv6 Security Summit Loki LTE MitM MLD mobile newsletter pcap pentest python risk SAP slides TelcoSecDay tool TR14 TROOPERS TROOPERS12 TROOPERS13 TROOPERS15 video Virtualization vmdk vmware VoIP web application

Stay up-to-date

Twitter
Posts
Comments

NEW DATE: TROOPERS16 Conference March 14-18, 2016

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

matrix - computer & neue medien

Datum: 01.11. 2013

Autor: Sarah Kriesche

Geheimnisse, Pleiten und Visionen
Die DeepSec 2013

Gestaltung: Sarah Kriesche

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

zur Sendereihe

Standort: oe1.ORF.at

OE1 ORF.at

Navigation

matrix - computer & neue medien

Sonntag
01. Dezember 2013
22:30

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

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

zurück

zur Sendereihe

Kategorie: Wissen

Programm

Mo	Di	Mi	Do	Fr	Sa	So
						1

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

SECURITY

Verfolgungsjagd per Bluetooth

Datum:29.11.2013

Autor:Jörg Thoma

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

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

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

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

Bluetooth überall

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

name.

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

Bis zu 100 Meter

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

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

Mit Python Bluetooth-Daten sammeln

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

Mit ihrem Experiment wollten Valeros und García die Aufmerksamkeit auf eine mögliche Schwachstelle lenken, die viele Menschen unbemerkt mit sich herumtragen, sagten sie zu Golem.de. Es gebe aber auch Hersteller, die es dem Nutzer gar nicht ermöglichen, Bluetooth auszuschalten, etwa Audiogeräte in einigen Autos und sogar auf Laptops. Bluetooth biete als Schnittstelle zahlreiche Möglichkeiten, könne aber auch sehr einfach dazu missbraucht

werden, die Privatsphäre zu verletzen. Vor allem mit der zunehmenden Verbreitung von Bluetooth in medizinischen Geräten steige auch die Gefahr für die Anwender nochmals deutlich.

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

SECURITY

Verfolgungsjagd per Bluetooth

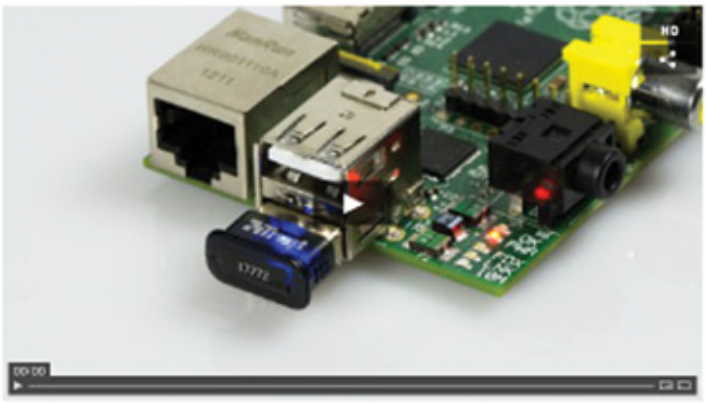
Ausgestattet mit einem Raspberry Pi samt Bluetooth-Dongle haben sich Sicherheitsexperten auf die Suche nach Geräten mit aktivierter Bluetooth-Schnittstelle gemacht. Es waren erstaunlich viele, die zudem viele Informationen über ihren Besitzer verraten.

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

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

Tools: Drucken

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



Video: Bluedriving (0:50)

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

Bluetooth überall

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

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

Bis zu 100 Meter

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

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

Mit Python Bluetooth-Daten sammeln

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

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

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

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

DEEPSEC

Forscher zeigt: So leicht lassen sich Medizingeräte hacken

Datum: 25.11.13

Autor: Barbara Wimmer

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

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

Futurezone: Herr Grunow, Sie erforschen die Sicherheit von Medizingeräten. War es einfach, an die entsprechenden Geräte heranzukommen?
Florian Grunow: Nein, es ist nicht ganz einfach, an die Geräte zu kommen. Entweder man braucht dafür Lizenzen z.B. wenn man sich ein Röntgengerät anschauen möchte. Das darf man auch nicht ohne spezielle Ausbildung und Berechtigungsscheine betreiben. Da wir das als IT-Security-Unternehmen nicht aufweisen können, haben wir beim Patientenmonitoring angefangen. Die Daten, die man aus dem Patientenmonitor gewinnt, sind für den Arzt auch Grundlage, um Entscheidungen über seine nächsten Schritte zu treffen.
Was genau haben Sie bei Ihren Forschungen rausgefunden und auf der DeepSec demonstriert?
Die Idee ist, den Überwachungsbildschirm, der die Vitalzeichen des Patienten anzeigt, so zu manipulieren, dass es halt einen lebenden Patienten anzeigt, obwohl der Patient gerade Probleme hat oder möglicherweise schon verstorben ist. Der Monitor ist dabei mit einem Netzwerkkabel am internen Netzwerk angeschlossen und sendet seine Daten an die Zentralstation. Wir haben getestet, ob man diese Zentralstation so angreifen kann, dass ich ihr vorgauklen kann, dass es dem Patienten wunderbar geht, obwohl er gerade Probleme hat. Das haben wir bei den Modellen von Monitoren, die wir uns bisher angesehen haben, geschafft.

Wie haben Sie das bewerkstelligt?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Kann man Herstellerversäumnisse in einem Krankenhausnetzwerk überhaupt ausbügeln?

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

Was für Medizingeräte sind noch gefährdet, außer Patientenmonitore?

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

noch lange nicht, dass das auch stimmt.

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

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

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

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

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

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

Wie lange ist Ihr Forschungsprojekt bei ERNW angelegt?

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

(FUTUREZONE) ERSTELLT AM 25.11.2013, 00:00

DEEPSEC

Forscher zeigt: So leicht lassen sich Medizingeräte hacken

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

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

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

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

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

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

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

FEATURED

VERKEHR
Hier-Box holt bei Autounfällen automatisch Hilfe

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

AKTION

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

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

Foto: Joanna Pianka

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

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

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

Facebook-Video zeigt waghalsige Aktion im AKW Zwentendorf

Foto: Joanna Pianka

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

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

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

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

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

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

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

Foto: Joanna Pianka

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

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

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

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

jedem raten.

Foto: Barbara Wimmer

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

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

(FUTUREZONE) ERSTELLT AM 25.11.2013, 00:00

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

Kommentare (8)

Ihr Kommentar
Bitte loggen Sie sich ein

Einloggen / Registrieren

ABSENDEN

rasierklingenritterin vor einem jahrpermalink | melden 0 0

Dank an die Autorin für den Themenfokus.

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

DEEPSEC

Forscher zeigt: So leicht lassen sich Medizingeräte hacken

Autor: Barbara Wimmer

Datum: 25.11.2013

FUTUREZONE

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

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

Futurezone: Herr Grunow, Sie erforschen die Sicherheit von Medizingeräten. War es einfach, an die entsprechenden Geräte heranzukommen?
Florian Grunow: Nein, es ist nicht ganz einfach, an die Geräte zu kommen. Entweder man braucht dafür Lizenzen z.B. wenn man sich ein Röntgengerät anschauen möchte. Das darf man auch nicht ohne spezielle Ausbildung und Berechtigungsscheine betreiben. Da wir das als IT-Security-Unternehmen nicht aufweisen können, haben wir beim Patientenmonitoring angefangen. Die Daten, die man aus dem Patientenmonitor gewinnt, sind für den Arzt auch Grundlage, um Entscheidungen über seine nächsten Schritte zu treffen.
Was genau haben Sie bei Ihren Forschungen rausgefunden und auf der DeepSec demonstriert?
Die Idee ist, den Überwachungsbildschirm, der die Vitalzeichen des Patienten anzeigt, so zu manipulieren, dass es halt einen lebenden Patienten anzeigt, obwohl der Patient gerade Probleme hat oder möglicherweise schon verstorben ist. Der Monitor ist dabei mit einem Netzwerkkabel am internen Netzwerk angeschlossen und sendet seine Daten an die Zentralstation. Wir haben getestet, ob man diese Zentralstation so angreifen kann, dass ich ihr vorgauklen kann, dass es dem Patienten wunderbar geht, obwohl er gerade Probleme hat. Das haben wir bei den Modellen von Monitoren, die wir uns bisher angesehen haben, geschafft.

Wie haben Sie das bewerkstelligt?

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

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

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

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

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

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

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

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

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

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

kein Problem mehr. Doch so etwas kostet etwas, ist aufwendig und deswegen bleibt es oft auf der Strecke.

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

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

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

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

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

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

Kann man Herstellerversäumnisse in einem Krankenhausnetzwerk überhaupt ausbügeln?

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

Was für Medizingeräte sind noch gefährdet, außer Patientenmonitore?

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

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

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

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

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

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

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

Wie lange ist Ihr Forschungsprojekt bei ERNW angelegt?

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

Erstellt am 25.11.2013 00:00 Uhr

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

DEEPSEC

Forscher zeigt: So leicht lassen sich Medizingeräte hacken

Letztes Update am 25.11.2013, 00:00

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

Barbara Wimmer
FUTUREZONE

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

…geräten. War

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

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

Foto: Joanna Pianka

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

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

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

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

Foto: Joanna Pianka

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

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

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

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

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

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

Foto: Joanna Pianka

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

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

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

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

Foto: Barbara Wimmer

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

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

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

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

Erstellt am 25.11.2013 00:00 Uhr

DISKUSSION

IHRE MEINUNG ZUM THEMA

EINLOGGEN / REGISTRIEREN

SENDEN

ALEX SORGHI | VOR EINEM JAHR PERMALINK | MELDEN 0 0

Dank an die Autorin für den Themenfokus.

ANTWORTEN

MICHAEL SABRANSKY | VOR EINEM JAHR PERMALINK | MELDEN 0 0

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

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

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

IT-Sicherheit

Konferenz Deep Sec hinterfragt den Cyberwar

Datum: 23.11.2013

Autor: Mariann Unterluggauer

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

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

Rund 160 internationale Sicherheitsexperten trafen sich auf der "Deep Sec", um darüber zu reden, wie Computersysteme sicherer gemacht werden können. Um dies zu erreichen, brauche es vor allem eine offene Diskussion über Fehlschläge, sagt René Pfeiffer, Sicherheitsberater und einer der Veranstalter.
"Fehlschläge sind ein Teil von IT-Security, weil man es nicht immer schafft. Es gibt Einbrüche, es gibt Kompromittierungen. Wir wollten einfach nur klarmachen, dass dies völlig in Ordnung ist, dass man über alles offen reden kann. Das hat nichts mit Preisgabe zu tun, sondern ist ein Zugeben: Ja, ich habe welche. Ja, es gelingt mir nicht immer und wie können wir das in Zukunft besser machen."
Ein Credo der Sicherheitsbranche lautet: Fehler lassen sich vermeiden, indem man sie oft genug begeht.
"Wir haben das in unserem Motto drinnen, ja. Dieser Spruch: 'If you want to fail less, fail often' heißt letztendlich: Hier muss man die geeignete Portion lernen, damit man etwas verbessern kann. Das Problem, das in der IT-Security oft stattfindet, ist: Wenn nicht passiert, glaubt man, dass alles in Ordnung ist. Erst dann, wenn etwas passiert, fängt man an, die Konfigurationen zu hinterfragen und zu verbessern. Übersetzt heißt das einfach: Wenn ich weniger Fehlschläge haben will, muss ich oft etwas verbessern. Denn die Fehlschläge sind der Anlass, wo man was macht, denn normalerweise macht man ohne Anlass nichts."
Ein altbekanntes Problem: Sicherungen werden meist erst dann erstellt, wenn Daten bereits verloren gegangen sind. Und auch die Auslagerung der Daten in eine Cloud ist keine Lösung - auch nicht für die NASA. In einem Vortrag wurde darauf hingewiesen, dass es der NASA keineswegs billiger kommt, wenn sie ihre Daten in entfernte Rechenzentren auslagert. Ein Grund dafür ist, dass nicht nur ein Cloud-Service genutzt werden kann, sondern

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

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

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

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

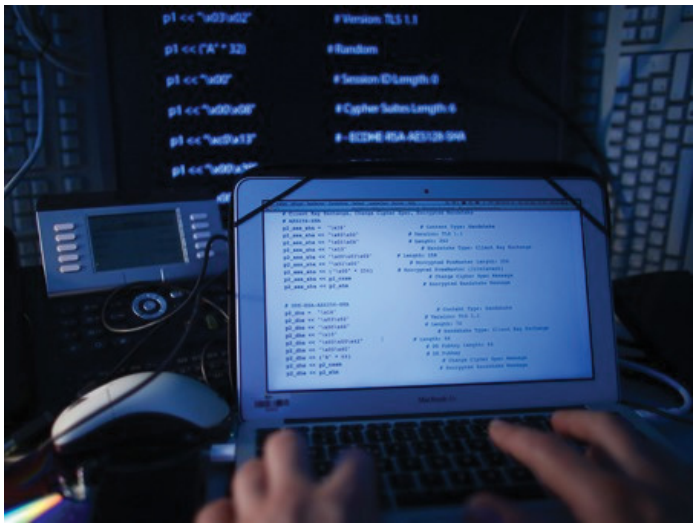
René Pfeiffer: "Also das große Problem da ist, dass oft mithilfe von Analogien diskutiert wird. Das heißt, man verwendet Metaphern, man verwendet 'Cyberwar'. Wenn ich 'Krieg' sage, dann habe ich plötzlich Waffen, und dann hat der eine mehr und der andere weniger. Das sind alles Analogien. Die klingen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

IT-Sicherheit

Konferenz Deep Sec hinterfragt den Cyberwar

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

Von Mariann Unterluggauer



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

E-Mail
Teilen
Tweet
Drucken

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

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

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

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

MEHR ZUM THEMA

Zum Themenportal "Risiko Internet"

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

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

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

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

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

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

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

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

"Europäische Netze sind reine Augenauswischerei"

Datum: 22.11. 2013

Autor: Andreas Proschofsky

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

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

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

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

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

René Pfeiffer: Die Konsequenzen wären eine Verbesserung der Sicherheit, und da schlägt bei vielen eine einfache Risikoanalyse verbunden mit Resignation zu: Kaum eine Firma und keine Privatperson kann das Budget der Geheimdienste schlagen. Selbst große Firmen wurden kompromittiert, teilweise ohne ihr Wissen, und das ist die psychologische Kehrseite der Spionageaffäre. Es schleicht sich trotz Empörung eine Machtlosigkeit ein, da man

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

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

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

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

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

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

René Pfeiffer: Ja, das können sie. Weder Privatpersonen noch kleine Firmen sind zur Gänze machtlos. Man kann mit der Geldbörse abstimmen und nicht vertrauenswürdige Dienstleistungen (ob Cloud oder andere) gegen andere austauschen. Man kann Lieferanten unbequeme Fragen stellen, und man kann versuchen seine eigenen Daten

nicht einem Einzelnen anzuvertrauen. Darüber hinaus kann man das Verhalten hinterfragen, wie mit Daten umgegangen wird. Das ist der schwerste Schritt, denn oft muss man Gewohnheiten umstellen. Es ist eine Vielzahl von Möglichkeiten, die zur Verfügung stehen. Leider ist der "NSA off" Schalter oder die "Anti-NSA-App" nicht dabei.

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

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

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

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

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

René Pfeiffer: Das ist eine Kombination aus "never change a running system" und dem "Black Box Problem". Gerade bei Internetanbietern mit sehr vielen Anschlüssen können missglückte Upgrades zu vermehrten Supportanfragen führen, die dann Geld kosten. Dazu kommt, dass Hersteller verschieden gut im Beheben von Schwachstellen sind und gerne "Black Boxes" ausliefern, in die man nicht reinschauen sollte. Das Problem wird in Deutschland gerade diskutiert, wo man den Routerzwang des Anbieters abschaffen möchte. Das halten wir für eine gute Idee, weil dann die Router-/Modemlandschaft weniger eine Monokultur darstellt und man den Herstellern, die gute Qualität liefern, den Vorzug geben kann.

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

René Pfeiffer: Das "Internet der Dinge" ist definitiv eine Herausforderung an die Sicherheit und wird uns in der Zukunft noch sehr viele Überraschungen bescheren. Man findet auch jetzt schon sehr seltsame Geräte im Internet

(sei es IPv4 oder IPv6). Es sollte nicht verwundern, wenn die IT-Sicherheit auf der Strecke bleibt, weil die Sicherheitstests für die IPv6-fähige Glühbirne bestimmt nicht ganz so streng ausfallen wie solche für die neueste Firewall. Solchen Umgebungen kann man nur mit Risikoanalyse und Abschottung begegnen – wenn etwas passiert, dann sollte nicht die Kompromittierung der Beleuchtung oder des Kühlschranks ausreichen, um das ganze Netzwerk zu übernehmen.

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

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

(Andreas Proschofsky, derStandard.at, 22.11.13)

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

"Europäische Netze sind reine Augenauswischerei"

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

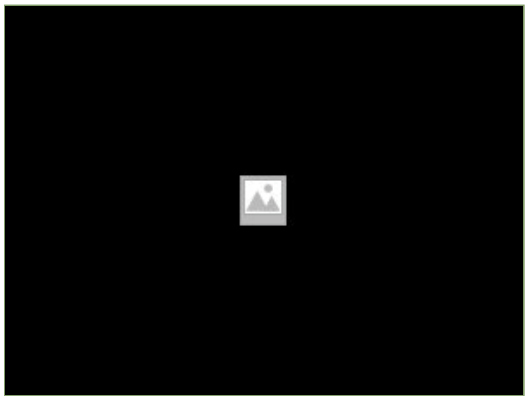


foto: joanna pianka / ap
DeepSec-Co-Organisator René Pfeiffer.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Link

DeepSec

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

SICHERHEITSKONFERENZ

DeepSec: Falsches Vertrauen in Facebook-Freunde

Datum: 21.11.2013

Autor: Barbara Wimmer

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

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

"Passwort verloren"

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

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

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

"Trusted Friends" manipulierbar

Doch auch das „Trusted Friends“-Prinzip von Facebook lässt sich laut Javed überlisten. Auf Facebook geht es vielen Nutzern nämlich darum, möglichst viele Freunde zu sammeln. Viele Nutzer akzeptieren daher auch Personen als Freunde, die sie gar nicht persönlich aus dem „echten Leben“ kennen. Javed legte drei Facebook-Profile an,

befreundete sich mit seinen 250 „echten“ Freunden, um die Attacke zu erproben. Das Ergebnis: Er konnte elf Accounts übernehmen.

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

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

SICHERHEITSKONFERENZ

DeepSec: Falsches Vertrauen in Facebook-Freunde

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

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

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

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

FACEBOOK, IT, SECURITY

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

"Passwort verloren"

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

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

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

"Trusted Friends" manipulierbar

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

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

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

(FUTUREZONE) ERSTELLT AM 21.11.2013, 16:12

FACEBOOK, IT, SECURITY

Kommentare (1)

Ihr Kommentar
Bitte loggen Sie sich ein

Einloggen / Registrieren

ABSENDEN

wolfgangh.wã¶gerer vor einem jahr

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

permalink | melden 0 0

antworten

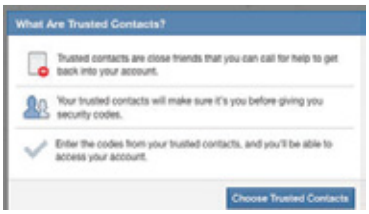
Mehr zum Thema

KAMPF GEGEN FACEBOOK

Schlag ins Gesicht für Aktivisten

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

von Barbara Wimmer



SICHERHEIT

Facebook bringt Notfall-Schlüssel für Freunde

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

SICHERHEIT

Facebook: Freunde sollen Account entsperren

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

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

SICHERHEITSKONFERENZ

DeepSec: Vom Herzschrittmacher-Hack bis zum Profiling

Datum: 24.10.2013

Autor: Barbara Wimmer

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

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

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

Vorträge über Online-Betrug und Profiling

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

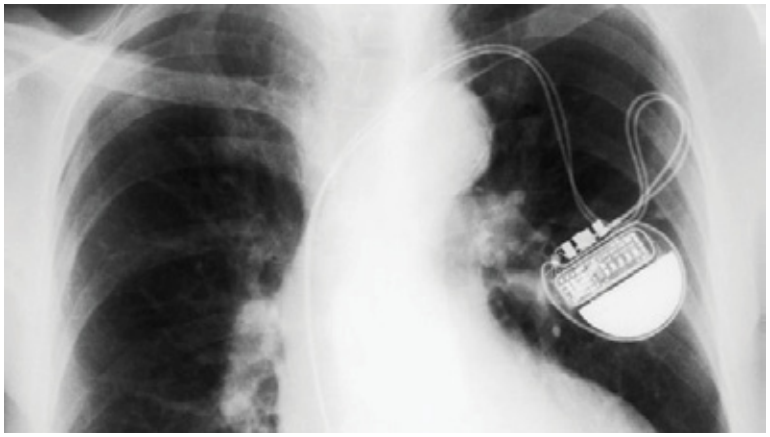
Der Forscher und Security-Analyst Florian Grunow aus Heidelberg beschäftigt sich unter anderem damit, wie sich die Wireless-Funktionen von Herzschrittmachern ausschalten lassen. Insulinpumpen oder Herzschrittmacher sind schon lang mit Wireless-Zugangsfunktionen ausgestattet, doch genau über diese Funktion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

Das detailliierte Programm zu allen Sessions findet sich hier.

SICHERHEITSKONFERENZ

DeepSec: Vom Herzschrittmacher-Hack bis zum Profiling

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



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

SICHERHEITSKONFERENZ

DeepSec: Vom Herzschrittmacher-Hack bis zum Profiling

KOMMENTARE ()

MEHR ZUM THEMA

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

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

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

Vorträge über Online-Betrug und Profiling

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

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

FEATURED

VERKEHR
Hier-Box holt bei Autounfällen automatisch Hilfe

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

AKTION
Facebook-Video zeigt waghalsige Aktion im AKW Zwentendorf

Das detailliierte Programm zu allen Sessions findet sich hier.

(FUTUREZONE) ERSTELLT AM 24.10.2013, 14:35

1 2

Kommentare ()

Ihr Kommentar
Bitte loggen Sie sich ein

Einloggen / Registrieren

ABSENDEN

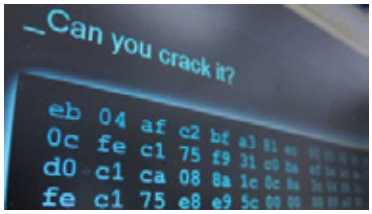
Mehr zum Thema

DEEPSEC

Forscher zeigt: So leicht lassen sich Medizingeräte hacken

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

von Barbara Wimmer



DEEPSEC

"White Hat Hacking ist nicht lukrativ genug"

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

von Florian Christof

SICHERHEITSKONFERENZ

DeepSec: Falsches Vertrauen in Facebook-Freunde

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

von Barbara Wimmer

Digital-Life

15.07.2015 13:30 Uhr

REPORTAGE

Chinas mobile Medienrevolution hinter der virtuellen Mauer

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

PLÄNE

EU überlegt neue Energie-Kennzeichnung für Elektrogeräte

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

DER NEUE JOKER

Erster Trailer zu Suicide Squad veröffentlicht

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

DATENSCHUTZ 3

Google Fotos lädt Bilder auch nach Löschen der App hoch

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

Featured

VERKEHR

Hier-Box holt bei Autounfällen automatisch Hilfe

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

von David Kotrba

http://www.alba13.com/2013/10/deepsec-effective-idsips-auditing-and.html

DeepSEC - Effective IDS/IPS Auditing And Testing With Finux – Arron 'f1nux' Finnon

Datum: 24.10. 2013

Autor: Arron “Finux” Finnon

There comes a time in your life when you have to walk the walk! As a public speaker, I’ve done my share of talking the talk, and those that know me, know I have recently been conducting a lot of small training courses and work-shops on effective NIDS/NIPS auditing and testing.

Truth be told, I’ve been doing this for two reasons. The first reason, is no matter how much I talk about this issue, nothing is going to help people more than sitting down and working with them. The second reason I’ve been on the road so much is getting myself in shape for DeepSEC training. Now, if you have to ask why getting myself fighting fit for DeepSEC is so important to me then you've either not been to the conference, or frankly you have no idea what on earth you're talking about.

I've always had a great love and respect for the crew of DeepSEC, and I have never hid that. I've been to a lot of conferences and frankly a lot of conferences like to boast about being the best in Europe, DeepSEC doesn't need to boast! I believe DeepSEC to be the best full-stop! The lack of egotistical babel; the beautiful city of Vienna; the amazing speakers and trainers; the warm and friendly family feeling you get there; and most importantly the crew that manages it, shows that bigging yourself up doesn't count for anything, doing it does!

So that being said, time to big up our training offering. So yes, of course ours is the best training offering ever! Of course you should hurry right now and purchase a ticket before they sell-out, in fact buy two or three, I mean every geek has at least one friend! Yeah, it will be biblical and we'll shove so much information into your brains that you'll be crying pcap files till new years day, blar, blar, blar. Seriously though, we have put together something special. Hand on my heart as I swear to God himself, we have taken everything we've learned about NIDS/NIPS testing and put together a course that will actually help. No silver bullets to be found here (we're based in Scotland, we sold the silver a very long time ago!), just what's needed to actually make a test of a NIDS/NIPS worthwhile. We cover everything in the Open Source Network Intrusion Framework (OSNIF) Top5, so NIDS/NIPS Evasion Techniques, False-Positive Issues, Protocol Ambiguities, Detection Rates, and Misconfiguration and Invisible Traffic Issues. We cover why sacrificial host testing with NIDS/NIPS has some serious flaws, and how to produce clean sample attack traffic to test attacks. However, we do have something very special indeed planned for the second day of training.

Now this part is where I get to be mean, I'm not actually going to tell you the actual details of the second day. All I'm going to say is we're going to take an issue that faces enterprise networks everyday, and we're going to analyse and build an effective defence against it. Now the details are interesting, and without doubt everyone there will learn a lot. However, more importantly we'll show attendees how easy it is to take a threat, no matter how big the hype is, and actually defend against it.

This training course will be of benefit to testers as well as defenders. Whilst I'm here, I'm going to put this out there too. This is the début of our OSNIF Top5 training in Europe, it hasn't been done here, it has never been done, EVER, with a two day practical defence module. We will be dropping a new open source project on the second day too. So buy your tickets now for DeepSEC, come do the training, and come see me and Gavin's talk whilst you're there too.

Visit DeepSEC training pages for more information. http://deepsec.net/speaker.html#WSLOT96

alba 13 research labs

Thursday, 24 October 2013

DeepSEC - Effective IDS/IPS Auditing And Testing With Finux

DeepSEC - Effective IDS/IPS Auditing And Testing With Finux - Arron 'f1nux' Finnon

There comes a time in your life when you have to walk the walk! As a public speaker, I've done my share of talking the talk, and those that know me, know I have recently been conducting a lot of small training courses and workshops on effective NIDS/NIPS auditing and testing.

Truth be told, I've been doing this for two reasons. The first reason, is no matter how much I talk about this issue, nothing is going to help people more than sitting down and working with them. The second reason I've been on the road so much is getting myself in shape for DeepSEC training. Now, if you have to ask why getting myself fighting fit for DeepSEC is so important to me then you've either not been to the conference, or frankly you have no idea what on earth you're talking about.

I've always had a great love and respect for the crew of DeepSEC, and I have never hid that. I've been to a lot of conferences and frankly a lot of conferences like to boast about being the best in Europe, DeepSEC doesn't need to boast! I believe DeepSEC to be the best full-stop! The lack of egotistical babel; the beautiful city of Vienna; the amazing speakers and trainers; the warm and friendly family feeling you get there; and most importantly the crew that manages it, shows that bigging yourself up doesn't count for anything, doing it does!

So that being said, time to big up our training offering. So yes, of course ours is the best training offering ever! Of course you should hurry right now and purchase a ticket before they sell-out, in fact buy two or three, I mean every geek has at least one friend! Yeah, it will be biblical and we'll shove so much information into your brains that you'll be crying pcap files till new years day, blar, blar, blar. Seriously though, we have put together something special. Hand on my heart as I swear to God himself, we have taken everything we've learned about NIDS/NIPS testing and put together a course that will actually help. No silver bullets to be found here (we're based in Scotland, we sold the silver a very long time ago!), just what's needed to actually make a test of a NIDS/NIPS worthwhile. We cover everything in the Open Source Network Intrusion Framework (OSNIF) Top5, so NIDS/NIPS Evasion Techniques, False-Positive Issues, Protocol Ambiguities, Detection Rates, and Misconfiguration and Invisible Traffic Issues. We cover why sacrificial host testing with NIDS/NIPS has some serious flaws, and how to produce clean sample attack traffic to test attacks. However, we do have something very special indeed planned for the second day of training.

Now this part is where I get to be mean, I'm not actually going to tell you the actual details of the second day. All I'm going to say is we're going to take an issue that faces enterprise networks everyday, and we're going to analyse and build an effective defence against it. Now the details are interesting, and without doubt everyone there will learn a lot. However, more importantly we'll show attendees how easy it is to take a threat, no matter how big the hype is, and actually defend against it.

This training course will be of benefit to testers as well as defenders. Whilst I'm here, I'm going to put this out there too. This is the début of our OSNIF Top5 training in Europe, it hasn't been done here, it has never been done, EVER, with a two day practical defence module. We will be dropping a new open source project on the second day too. So buy your tickets now for DeepSEC, come do the training, and come see me and Gavin's talk whilst you're there too.

Visit DeepSEC training pages for more information.
http://deepsec.net/speaker.html#WSLOT96

Posted by Arron 'finux' Finnon at 09:18

Blog Archive

- ► 2014 (6)
- ▼ 2013 (6)
  - ▼ October (4)
    - DeepSEC - Effective IDS/IPS Auditing And Testing W...
    - Alba13 going deep with janet
    - Historical Tour Of IDS Evasion
    - The Economics of False Positives
  - ► July (2)

There was an error in this gadget

Contact Form

Name

Email *

Message *

Send

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

Datenschutz hilft, Cyberspionage abzuwehren

Datum: 03.06.2013

Autor: Erich Möchel

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

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

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

Datenschutz, Informationssicherheit

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

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

HNA, Hacker, Wirtschaft

Der nunmehrige Sicherheitsberater Polli war mehr als zwei Jahrzehnte für das Heeresnachrichtenamt (HNA) tätig und wurde 2002 Direktor des damals neu gegründeten Bundesamts für Verfassungsschutz und Terrorismus-

bekämpfung (BVT) im Innenministerium. Dass ein gelernter Geheimdienstmann derselben Ansicht zu diesem Thema ist, wie ein gelernter Hacker und der Geschäftsführer einer mittelständischen Anti-Virusfirma klingt nur für Außenstehende befremdlich.

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

Ein Bärendienst

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

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

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

"Geistiges Eigentum der KMUs"

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

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

"Authentizität, Integrität und Vertraulichkeit"

Solche "Targeted Attacks" oder "Spear Phishing" genannten Angriffsformen zielen auf einen definierten Personenkreis. Im Fall von Cyberspionage zum wirtschaftlichen Vorteil werden etwa die Mitarbeiter einer Firma in Sozialen

Netzen beobachtet und dann kontaktiert. Sobald eine gewisse Vertraulichkeit gegegeben ist, kommen die Angriffsmails, deren Anhänge eine bis dahin nicht bekannte Sicherheitslücke angreifen. Damit ist man im Firmennetzwerk.

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

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

Das Prinzip in der Praxis

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

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

Historische Datenskandale

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

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

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

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

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

Die Crux mit dem Verwendungszweck

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

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

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

Die Position der EVP

Während vor allem deutsche EU-Parlamentarier von CDU/CSU und FDP in ihren Änderungsvorschlägen einander an solcher "Wirtschaftsfreundlichkeit" zu überbieten suchen, bezieht die EVP hier eine deutlich ausgewogenere

Position. Auf Anfrage von ORF.at wurde der derzeitige Stand der Meinungsbildung zum EU-Datenschutzpaket vom für das Thema zuständigen EVP-Abgeordneten Hubert Pirker so zusammengefasst:

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

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

Meinungsbildung im EU-Parlament

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

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

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

Österreich und Irland im Vergleich

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

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

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

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

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

Datenschutz hilft, Cyberspionage abzuwehren

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

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

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

Datenschutz, Informationssicherheit

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

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

HNA, Hacker, Wirtschaft

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

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

Ein Bärendienst

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

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

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

"Geistiges Eigentum der KMUs"

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

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

"Authentizität, Integrität und Vertraulichkeit"

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

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

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

Das Prinzip in der Praxis

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

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

Historische Datenskandale

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

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

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

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

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

Die Crux mit dem Verwendungszweck

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

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

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

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

Die Position der EVP

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

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

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

Meinungsbildung im EU-Parlament

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

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

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

Österreich und Irland im Vergleich

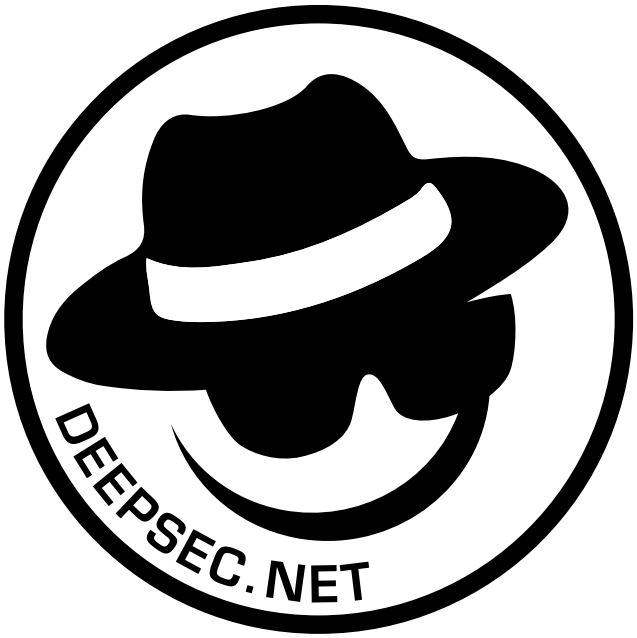
Was die Kette der Datenskandale im österreichischen Innenministerium betrifft, so rissen diese abrupt ab, nachdem eine einfache Maßnahme gesetzt wurde, die wiederum auf den drei Säulen der Informationssicherheit beruht. Es wurde schlicht und einfach protokolliert, wer wann intern auf welche Datensätze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

Plausibilitätsprüfung unterzogen.

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

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

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


DEEPSEC.NET

Press Release

Datum: 19.11.2013

Autor: René Pfeiffer

Hackers sending out a message to managers: “Watch your risks!”

Vienna. On the occasion of the DeepSec Conference taking place in Vienna, the Scottish IT research company Alba 13 Research Labs reveals a new risk assessment system that is relevant to the business side of cyber crime. While Alba 13 Research Labs developed the “Open Source Network Intrusion Framework” (OSNIF) and successfully implements the technological rule set already in various cooperations with international companies, the enlargement of the project now will support the risk assessment referring to the algorithms of the technical threats. This will help companies in their decision making whether an investigation or courntermeasures of all kind would be more cost effective than tolerating the level of risks.
The technical detection system with its proven alert system is therefore a component to the overall commercial controlling that is necessary for each corporation of significant value to mitigate cyber risks and protect their assets. “A technical rule set cannot 'make that decision', but a cost based one can! “, states Gavin Ewan, Chief Management Researcher at Alba 13 Research Labs.

Alba 13 Research Labs is founded in 2012 in Dundee/United Kingdom by Arron M. Finnon (Chief Technology Researcher) and Gavin Ewan (Chief Management Researcher). The foundation of the company was a result of successful research, presentation and training at various international Cyber Security Conferences in years. Focusing on the broader perspective involving IT Technology research as well as their impact for commercial risk assessment and decision making, Alba 13 Reserch Labs is unique in building bridges between managers and technical experts.

The DeepSec IDSC is an annual European two-day in-depth conference on computer, network, and application security. It is a non-product, non-vendor-biased conference event. The aim is to present the best research and experience from the fields' leading experts, bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community.

More information on: www.alba13.co.uk and www.deepsec.net

V.i.s.d.P. René Pfeiffer

Press Release

Vienna/Austria, November 19th, 2013

Hackers sending out a message to managers: “Watch your risks!”

Vienna. On the occasion of the DeepSec Conference taking place in Vienna, the Scottish IT research company Alba 13 Research Labs reveals a new risk assessment system that is relevant to the business side of cyber crime.

While Alba 13 Research Labs developed the “Open Source Network Intrusion Framework” (OSNIF) and successfully implements the technological rule set already in various cooperations with international companies, the enlargement of the project now will support the risk assessment referring to the algorithms of the technical threats. This will help companies in their decision making whether an investigation or courntermeasures of all kind would be more cost effective than tolerating the level of risks.

The technical detection system with its proven alert system is therefore a component to the overall commercial controlling that is necessary for each corporation of significant value to mitigate cyber risks and protect their assets. “A technical rule set cannot 'make that decision', but a cost based one can! “, states Gavin Ewan, Chief Management Researcher at Alba 13 Research Labs.

Alba 13 Research Labs is founded in 2012 in Dundee/United Kingdom by Arron M. Finnon (Chief Technology Researcher) and Gavin Ewan (Chief Management Researcher). The foundation of the company was a result of successful research, presentation and training at various international Cyber Security Conferences in years. Focusing on the broader perspective involving IT Technology research as well as their impact for commercial risk assessment and decision making, Alba 13 Reserch Labs is unique in building bridges between managers and technical experts.

The DeepSec IDSC is an annual European two-day in-depth conference on computer, network, and application security. It is a *non-product*, *non-vendor-biased* conference event. The aim is to present the best research and experience from the fields' leading experts, bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community.

More information on: www.alba13.co.uk and www.deepsec.net
V.i.s.d.P. René Pfeiffer

P R E S S E I N F O R M A T I O N

Datum:31.10.2013

Autor: René Pfeiffer, Birgit E. Astl-Kurz

Dicke Luft in Apples iCloud (oder: Dicke Luft in Daten Clouds)

Heitere Wölkchen versprechen Komfort – doch wer schützt meine Daten darin?
Bluetooth wurde massentauglich – aber deshalb auch sicherer?
Falschen Freunden vertraut - Social Media Dienste zeigen es vor

Wien, 31. Oktober 2013 – Diesmal Profis aus Russland, Argentinien und Deutschland zu Wort: Vladimir Katalov, Gründer von Elcomsoft, Veronica Valeros und Garcia Sebastian, und Ashar Javed, Ruhr Universität Bochum, sprechen auf der DeepSec - Depth Security Conference im Imperial Riding School Renaissance Vienna Hotel vom 19. bis 22.11.2013 über die globale Web-Wetterlage.

Cracking And Analyzing Apple iCloud von Vladimir Katalov, Begründer von Elcomsoft

Apples iCloud ist ein Dienst, mit dem Benutzer Daten speichern können. Gedacht war Apple iCloud dafür, Komfort und Flexibilität von iDevices Kunden zu erhöhen. Nicht bedacht wird oft, welche Möglichkeiten die Wolke bietet, Informationen über den Nutzer selbst herauszufinden.

Elcomsoft „rettet“ Passwörter durch ausprobieren bzw knacken. Das Unternehmen prüfte bereits unzählige Produkte auf Herz und Nieren. Bei Apples iCloud wurde aufgrund der nicht offengelegten Dokumentation des Protokolls die Interaktion zwischen der iCloud und den angeschlossenen Geräten ausgeforscht. Katalov nennt das „reverse engineering“.
Reverse Engineering bietet die Möglichkeit zu beliebig vielen Wechselwirkungen zwischen Applikationen der iCloud und des Nutzers. Vladimir Katalovs Arbeit leistet Grundlagenforschung, um die Funktionsweise und Sicherheit von Clouddiensten testen zu können. Katalov ist Russe, studierter Mathematiker und schrieb das erste Programm zur Passwortwiederherstellung. 1190 gründete er www.elcomsoft.com

Um Bluetooth Devices geht es im Vortrag der beiden Security Spezialisten Verónica Valeros & Sebastian Garcia: Privacy Issues of Bluetooth Devices

Bluetooth ist Teil unserer täglichen Welt. Drucker, Handys, Computer und viele andere Geräte haben eine Bluetooth-Schnittstelle. Ende der 90er Jahre, als die Technologie neu war, fanden Sicherheitsforscher rasch Schwächen in Implementierung und Protokoll. Es wurde erfolgreich am Bluetooth Standard nachgebessert.

Von „Sicher“ sind wir weit entfernt: Bluetooth bietet reichhaltige Möglichkeiten für Angreifer und birgt große Angriffsflächen für die Privatsphäre. Verónica Valeros & Garcia Sebastian stellen die Risikopotentiale der derzeitigen Bluetooth Implementierungen vor.

Veronica Valeros und Sebastian Garcia sind MatesLab Co-Gründer, des ersten Hackerspace in Mar del Plata, Argentina. Beide leben und arbeitet derzeit in Tschechien.

Traue niemanden....?
Ashar Javed probiert es aus: Trusted Friend Attack (Ashar Javed)
Wir alle haben schon mal Passwörter vergessen. Social Media Webseiten und andere Dienste bieten hierfür einfache Mechanismen, um den Zugang zu einem Konto auf alternativem Weg
wiederherzustellen. Ashar Javed hat sich 50 populäre Social Media Webseiten angesehen und dabei Erschreckendes festgestellt: Sechs Konten – das sind mehr als 10% - ließen sich kompromittieren, eines sogar blocken – und zwar nicht vom Inhaber.
Ein Angreifer kann dazu einfach das gute „trusted Friend“ Vertrauensverhältnis ausnutzen.
Klingt beunruhigend? Muss es nicht sein, wenn man einfache aber wirkungsvolle Ratschläge befolgt.

Ashar forscht als “Chair of Network & Data Security” an der Ruhr Universität in Bochum (D) und bereitet sich auf sein Doktorat vor. Sein Name wurde neun Mal in Google Security Hall of Fame genannt.

Bitte melden Sie Interview Anfragen bei uns an – wir organisieren gern vorab Gespräche.

Akkreditierungen für die Konferenz und die Workshops nehmen wir ab sofort entgegen:

Aufgrund limitierter Plätze bitten wir um rasche Anmeldungen:

info@deepsec.net oder René Pfeiffer: 043 676 /562 63 90

Das laufend aktualisierte Programm finden Sie auf http://deepsec.net/schedule.html

Übersicht aller Sprecher & Themen: http://deepsec.net/speaker.html

Kurzprofil DeepSec:

Die DeepSEC bildet die neutrale Plattform für ein unabhängiges Zusammentreffen von weltweit renommierten Sicherheitsexperten von Universitäten, Regierungen, der Industrie, sowie unabhängigen Wissenschaftlern, Autoren und der zumeist im Untergrund tätigen Hacker Community und interessierten Gäste aus der ganzen Welt, die sich im engeren oder weiteren Sinn mit Sicherheitsbelangen auseinandersetzen.

Die vielzitierte Vision „Leben im global vernetzten Dorf“ ist für die meisten von uns real und oft sogar Existenz bestimmend. Im selben Ausmaß wachsen auch die Bedeutung und somit die Teilnehmerbreite der DeepSec, die 2007 zum ersten Mal stattfand. Mittlerweile hat die Wiener Konferenz 200 Teilnehmer. Längst zählen nicht mehr nur Entwickler, Netzwerktechniker und Administratoren zum Besucherkreis.

DeepSec führt Interessierte aus unterschiedlichsten Bereichen wie Bildungseinrichtungen, Finanzinstitute oder Gesundheits- und Versicherungsorganisationen mit IT-Security Experten zusammen.

Kontakt / Pressekontakt

DeepSec GmbH

René Pfeiffer & Michael Kafka

Weyringergasse 30a/10

1040 Wien, Austria

rpfeiffer@deepsec.net

Mobiltelefon: +43/676/5626390

Bürotelefon: +43/720/349387

DEEPSEC

P R E S S E I N F O R M A T I O N

Dicke Luft in Apples iCloud *(oder: Dicke Luft in Daten Clouds)*

Heitere Wölkchen versprechen Komfort – doch wer schützt meine Daten darin?
Bluetooth wurde massentauglich – aber deshalb auch sicherer?
Falschen Freunden vertraut - Social Media Dienste zeigen es vor

Wien, 31. Oktober 2013 – Diesmal Profis aus Russland, Argentinien und Deutschland zu Wort: Vladimir Katalov, Gründer von Elcomsoft, Veronica Valeros und Garcia Sebastian, und Ashar Javed, Ruhr Universität Bochum, sprechen auf der DeepSec - Depth Security Conference im Imperial Riding School Renaissance Vienna Hotel vom 19. bis 22.11.2013 über die globale Web-Wetterlage.

Cracking And Analyzing Apple iCloud von Vladimir Katalov, Begründer von Elcomsoft

Apples iCloud ist ein Dienst, mit dem Benutzer Daten speichern können. Gedacht war Apple iCloud dafür, Komfort und Flexibilität von iDevices Kunden zu erhöhen. Nicht bedacht wird oft, welche Möglichkeiten die Wolke bietet, Informationen über den Nutzer selbst herauszufinden.

Elcomsoft „rettet“ Passwörter durch ausprobieren bzw knacken. Das Unternehmen prüfte bereits unzählige Produkte auf Herz und Nieren. Bei **Apples iCloud** wurde aufgrund der nicht offengelegten Dokumentation des Protokolls die Interaktion zwischen der iCloud und den angeschlossenen Geräten ausgeforscht. Katalov nennt das „reverse engineering“.
Reverse Engineering bietet die Möglichkeit zu beliebig vielen Wechselwirkungen zwischen Applikationen der iCloud und des Nutzers. Vladimir Katalovs Arbeit leistet Grundlagenforschung, um die Funktionsweise und Sicherheit von Clouddiensten testen zu können. Katalov ist Russe, studierter Mathematiker und schrieb das erste Programm zur Passwortwiederherstellung. 1190 gründete er www.elcomsoft.com

Um Bluetooth Devices geht es im Vortrag der beiden Security Spezialisten Verónica Valeros & Sebastian Garcia: **Privacy Issues of Bluetooth Devices**

Bluetooth ist Teil unserer täglichen Welt. Drucker, Handys, Computer und viele andere Geräte haben eine Bluetooth-Schnittstelle. Ende der 90er Jahre, als die Technologie neu war, fanden Sicherheitsforscher rasch Schwächen in Implementierung und Protokoll. Es wurde erfolgreich am Bluetooth Standard nachgebessert.

Von „Sicher" sind wir weit entfernt: Bluetooth bietet reichhaltige Möglichkeiten für Angreifer und birgt große Angriffsflächen für die Privatsphäre. Verónica Valeros & Garcia Sebastian stellen die Risikopotentiale der derzeitigen Bluetooth Implementierungen vor.

Veronica Valeros und Sebastian Garcia sind MatesLab Co-Gründer, des ersten Hackerspace in Mar del Plata, Argentina. Beide leben und arbeitet derzeit in Tschechien.

Traue niemanden....?
Ashar Javed probiert es aus: Trusted Friend Attack (Ashar Javed)
Wir alle haben schon mal Passwörter vergessen. Social Media Webseiten und andere Dienste bieten hierfür einfache Mechanismen, um den Zugang zu einem Konto auf alternativem Weg wiederherzustellen. Ashar Javed hat sich 50 populäre Social Media Webseiten angesehen und dabei Erschreckendes festgestellt: Sechs Konten – das sind mehr als 10% - ließen sich kompromittieren, eines sogar blocken – und zwar nicht vom Inhaber.
Ein Angreifer kann dazu einfach das gute „trusted Friend" Vertrauensverhältnis ausnutzen.
Klingt beunruhigend? Muss es nicht sein, wenn man einfache aber wirkungsvolle Ratschläge befolgt.

Ashar forscht als "Chair of Network & Data Security" an der Ruhr Universität in Bochum (D) und bereitet sich auf sein Doktorat vor. Sein Name wurde neun Mal in Google Security Hall of Fame genannt.

Bitte melden Sie **Interview Anfragen** bei uns an – wir organisieren gern vorab Gespräche.
Akkreditierungen für die Konferenz und die Workshops nehmen wir ab sofort entgegen:
Aufgrund limitierter Plätze bitten wir um rasche Anmeldungen:
info@deepsec.net oder René Pfeiffer: 043 676 /562 63 90

Das laufend aktualisierte Programm finden Sie auf http://deepsec.net/schedule.html

Übersicht aller Sprecher & Themen: http://deepsec.net/speaker.html

Kurzprofil DeepSec:
Die DeepSEC bildet die neutrale Plattform für ein unabhängiges Zusammentreffen von weltweit renommierten Sicherheitsexperten von Universitäten, Regierungen, der Industrie, sowie unabhängigen Wissenschaftlern, Autoren und der zumeist im Untergrund tätigen Hacker Community und interessierten Gäste aus der ganzen Welt, die sich im engeren oder weiteren Sinn mit Sicherheitsbelangen auseinandersetzen.
Die vielzitierte Vision „Leben im global vernetzten Dorf“ ist für die meisten von uns real und oft sogar Existenz bestimmend. Im selben Ausmaß wachsen auch die Bedeutung und somit die Teilnehmerbreite der DeepSec, die 2007 zum ersten Mal stattfand. Mittlerweile hat die Wiener Konferenz 200 Teilnehmer. Längst zählen nicht mehr nur Entwickler, Netzwerktechniker und Administratoren zum Besucherkreis.
DeepSec führt Interessierte aus unterschiedlichsten Bereichen wie Bildungseinrichtungen, Finanzinstitute oder Gesundheits- und Versicherungsorganisationen mit IT-Security Experten zusammen.

Kontakt / Pressekontakt
DeepSec GmbH
René Pfeiffer & Michael Kafka
Weyringergasse 30a/10
1040 Wien, Austria
rpfeiffer@deepsec.net
Mobiltelefon: +43/676/5626390
Bürotelefon: +43/720/349387

P R E S S E I N F O R M A T I O N

Datum: 24.10.2013

Autor: René Pfeiffer, Birgit E. Astl-Kurz

Herzschrittmacher, Insulinpumpen und unser Wert im Web Haben nichts miteinander zu tun? Im Gegenteil!

Auf der DeepSec diskutieren darüber:

• Hacking Medical Devices – Florian Grunow, ERNW GmbH

• Prism Break - The Value of Online Identities - Frank Ackermann

Wien, 24. Oktober 2013 – Es ist noch knapp ein Monat bis zur DeepSec ISDC -
In Depth Security Conference im Imperial Riding School Renaissance Vienna Hotel
(ehemals Penta Hotel Wien 3) vom 19. bis 22. November 2013.
René Pfeiffer und Michael Kafka präsentieren diesmal zwei deutsche Experten:
Florian Grunow, ERNW GmbH, und Frank Ackermann, passionierter IT-Security Profi.
Dick Cheney lässt Wireless Funktion im Herzschrittmacher ausschalten!
Schrieben Spiegel und englische Medien. „I found it credible“ meinte Cheney schon 2007, als er seinen Arzt bat, den Fernzugriff abzuschalten, um sich vor möglichen Terroranschlägen via Drahtlos-Funktion zu schützen. Dass er jetzt damit an die Öffentlichkeit geht, trifft sich zugegebenermaßen gut mit dem DeepSec Talk von Florian Grunow, der sich mit der Möglichkeit von Angriffen auf medizinische Gerätschaften beschäftigt.
Und es lässt die Meinung zu, Cheney muss wissen, wovor er Angst haben kann.
Insulinpumpen oder Herzschrittmacher sind schon lang mit Wireless-Zugangsfunktionen – für Ärzte oder Hersteller – ausgestattet. Dies macht viel Sinn, denn implantierte, oft lebensrettende Geräte müssen ohne operativen Aufwand von außen zu überwachen bzw. zu adjustieren sein.

Alle Geräte mit Wireless Funktion können auch angegriffen werden.
Das ist in der IT-Branche eine akzeptierte Tatsache.
Grunow geht es weniger um einen tatsächlichen Angriff auf das Leben des Patienten, als vielmehr darum, Werksspionage und wirtschaftlich motivierte Angriffe auf einen Hersteller durch Sicherheitslücken in seinen Computersystemen aufzuzeigen. Diese können enorme Auswirkungen auf Endgeräte wie Insulinpumpen, OP-Geräte, Überwachungsmonitore etc. haben.
Florian Grunow ist Security Analyst bei ERNW in Heidelberg, Deutschland, mit Fokus auf Application Security. Er besitzt ein Bachelor's Degree in Medical Computer Sciences und Master's Degree in Software Engineering und verfügt über Hintergrundwissen im Spitalwesen

und in der täglichen Arbeit mit Informationstechnologien des medizinischen Personals.

Wie hoch ist mein Wert im Web? Prism Break

Frank Ackermann beschreibt in seinem nicht technischen Talk, wie viel Online Identitäten wert sind und wie die damit verbundenen Informationen von den Internetplattformen verarbeitet werden. Er leitet daraus Bedrohungen und Risiken für unsere Datenprofile ab: Neben dem durchaus bekannten Aspekt des „gläsernen Surfers“ bieten Online Identitäten ein hohes Missbrauchspotential unterschiedlicher Art. Das beginnt beim ‚Eintritt' in den Webdienst und den Wegen, dich ich im Netz wähle. Professionelle Schnüffler generieren daraus Muster, die dazu führen können, dass ich plötzlich in einer Weise und in einem Zusammenhang auffalle, der mir nicht bewusst war…

Ziel des Vortrages ist, den Teilnehmern ein besseres Verständnis davon zu geben, dass Prism, Suchmaschinen, Clouds, Big Data bei allen Online-Aktivitäten immer mitspielen und Informationen abgreifen können.

Frank Ackermann, Senior Security Professional in Düsseldorf. arbeitet seit über 13 Jahren in IT- und Information Security. Sein Credo lautet: 'Security is not my job – it is my passion'

Bitte melden Sie Interview Anfragen bei uns an – wir organisieren gern vorab Gespräche.

Akkreditierungen für die Konferenz und die Workshops nehmen wir ab sofort entgegen:

Aufgrund limitierter Plätze bitten wir um rasche Anmeldungen:

info@deepsec.net oder René Pfeiffer: 043 676 /562 63 90

Das laufend aktualisierte Programm finden Sie auf http://deepsec.net/schedule.html

Übersicht aller Sprecher & Themen: http://deepsec.net/speaker.html

Kurzprofil DeepSec:

Die DeepSEC bildet die neutrale Plattform für ein unabhängiges Zusammentreffen von weltweit renommierten Sicherheitsexperten von Universitäten, Regierungen, der Industrie, sowie unabhängigen Wissenschaftlern, Autoren und der zumeist im Untergrund tätigen Hacker Community und interessierten Gäste aus der ganzen Welt, die sich im engeren oder weiteren Sinn mit Sicherheitsbelangen auseinandersetzen.

Die vielzitierte Vision „Leben im global vernetzten Dorf“ ist für die meisten von uns real und oft sogar Existenz bestimmend. Im selben Ausmaß wachsen auch die Bedeutung und somit die Teilnehmerbreite der DeepSec, die 2007 zum ersten Mal stattfand. Mittlerweile hat die Wiener Konferenz 200 Teilnehmer. Längst zählen nicht mehr nur Entwickler, Netzwerktechniker und Administratoren zum Besucherkreis. DeepSec führt Interessierte aus unterschiedlichsten Bereichen wie Bildungseinrichtungen, Finanzinstitute

oder Gesundheits- und Versicherungsorganisationen mit IT-Security Experten zusammen.

Kontakt / Pressekontakt

DeepSec GmbH

René Pfeiffer & Michael Kafka

Weyringergasse 30a/10

1040 Wien, Austria

rpfeiffer@deepsec.net

Mobiltelefon: +43/676/5626390

Bürotelefon: +43/720/349387

DEEPSEC

P R E S S E I N F O R M A T I O N

Herzschrittmacher, Insulinpumpen und unser Wert im Web

Haben nichts miteinander zu tun? Im Gegenteil!

Auf der DeepSec diskutieren darüber:

- ***Hacking Medical Devices – Florian Grunow, ERNW GmbH***
- ***Prism Break - The Value of Online Identities - Frank Ackermann***

Wien, 24. Oktober 2013 – Es ist noch knapp ein Monat bis zur DeepSec ISDC - In Depth Security Conference im Imperial Riding School Renaissance Vienna Hotel (ehemals Penta Hotel Wien 3) vom 19. bis 22. November 2013.
René Pfeiffer und Michael Kafka präsentieren diesmal zwei deutsche Experten: Florian Grunow, ERNW GmbH, und Frank Ackermann, passionierter IT-Security Profi.

Dick Cheney lässt Wireless Funktion im Herzschrittmacher ausschalten!

Schrieben Spiegel und englische Medien. „*I found it credible*“ meinte Cheney schon 2007, als er seinen Arzt bat, den Fernzugriff abzuschalten, um sich vor möglichen Terroranschlägen via Drahtlos-Funktion zu schützen. Dass er jetzt damit an die Öffentlichkeit geht, trifft sich zugegebenermaßen gut mit dem **DeepSec Talk von Florian Grunow,** der sich mit der Möglichkeit von Angriffen auf medizinische Gerätschaften beschäftigt.
Und es lässt die Meinung zu, Cheney muss wissen, wovor er Angst haben kann.

Insulinpumpen oder Herzschrittmacher sind schon lang mit Wireless-Zugangsfunktionen – für Ärzte oder Hersteller – ausgestattet. Dies macht viel Sinn, denn implantierte, oft lebensrettende Geräte müssen ohne operativen Aufwand von außen zu überwachen bzw. zu adjustieren sein.

Alle Geräte mit Wireless Funktion können auch angegriffen werden.
Das ist in der IT-Branche eine akzeptierte Tatsache.

Grunow geht es weniger um einen tatsächlichen Angriff auf das Leben des Patienten, als vielmehr darum, Werksspionage und wirtschaftlich motivierte Angriffe auf einen Hersteller durch Sicherheitslücken in seinen Computersystemen aufzuzeigen. Diese können enorme Auswirkungen auf Endgeräte wie Insulinpumpen, OP-Geräte, Überwachungsmonitore etc. haben.

Florian Grunow ist Security Analyst bei ERNW in Heidelberg, Deutschland, mit Fokus auf Application Security. Er besitzt ein Bachelor's Degree in Medical Computer Sciences und Master's Degree in Software Engineering und verfügt über Hintergrundwissen im Spitalwesen und in der täglichen Arbeit mit Informationstechnologien des medizinischen Personals.

Wie hoch ist mein Wert im Web? Prism Break

Frank Ackermann beschreibt in seinem nicht technischen Talk, wie viel Online Identitäten wert sind und wie die damit verbundenen Informationen von den Internetplattformen verarbeitet werden. Er leitet daraus Bedrohungen und Risiken für unsere Datenprofile ab: Neben dem durchaus bekannten Aspekt des „gläsernen Surfers“ bieten Online Identitäten ein hohes Missbrauchspotential unterschiedlicher Art. Das beginnt beim ‚Eintritt’ in den Webdienst und den Wegen, dich ich im Netz wähle. Professionelle Schnüffler generieren daraus Muster, die dazu führen können, dass ich plötzlich in einer Weise und in einem Zusammenhang auffalle, der mir nicht bewusst war…

Ziel des Vortrages ist, den Teilnehmern ein besseres Verständnis davon zu geben, dass Prism, Suchmaschinen, Clouds, Big Data bei allen Online-Aktivitäten immer mitspielen und Informationen abgreifen können.

Frank Ackermann, Senior Security Professional in Düsseldorf. arbeitet seit über 13 Jahren in IT- und Information Security. Sein Credo lautet: *'Security is not my job – it is my passion’*

Bitte melden Sie **Interview Anfragen** bei uns an – wir organisieren gern vorab Gespräche.

Akkreditierungen für die Konferenz und die Workshops nehmen wir ab sofort entgegen:

Aufgrund limitierter Plätze bitten wir um rasche Anmeldungen:

info@deepsec.net oder René Pfeiffer: 043 676 /562 63 90

Das laufend aktualisierte Programm finden Sie auf http://deepsec.net/schedule.html

Übersicht aller Sprecher & Themen: http://deepsec.net/speaker.html

Kurzprofil DeepSec:
Die DeepSEC bildet die neutrale Plattform für ein unabhängiges Zusammentreffen von weltweit renommierten Sicherheitsexperten von Universitäten, Regierungen, der Industrie, sowie unabhängigen Wissenschaftlern, Autoren und der zumeist im Untergrund tätigen Hacker Community und interessierten Gäste aus der ganzen Welt, die sich im engeren oder weiteren Sinn mit Sicherheitsbelangen auseinandersetzen.
Die vielzitierte Vision „Leben im global vernetzten Dorf“ ist für die meisten von uns real und oft sogar Existenz bestimmend. Im selben Ausmaß wachsen auch die Bedeutung und somit die Teilnehmerbreite der DeepSec, die 2007 zum ersten Mal stattfand. Mittlerweile hat die Wiener Konferenz 200 Teilnehmer. Längst zählen nicht mehr nur Entwickler, Netzwerktechniker und Administratoren zum Besucherkreis. DeepSec führt Interessierte aus unterschiedlichsten Bereichen wie Bildungseinrichtungen, Finanzinstitute oder Gesundheits- und Versicherungsorganisationen mit IT-Security Experten zusammen.

Kontakt / Pressekontakt
DeepSec GmbH
René Pfeiffer & Michael Kafka
Weyringergasse 30a/10
1040 Wien, Austria
rpfeiffer@deepsec.net
Mobiltelefon: +43/676/5626390
Bürotelefon: +43/720/349387

P R E S S E I N F O R M A T I O N

Datum: 09.10.2013

Autor: René Pfeiffer, Birgit E. Astl-Kurz

Der Countdown zur DeepSec 2013 läuft

- Vom 19. bis 22.11.2013 referieren internationale Sicherheitsexperten in Wien

- Wir stellen Sprecher und Schwerpunkte vor

Wien, 9. Oktober 2012 – Vom 19. bis 22. November 2013 findet die DeepSec ISDC - In Depth Security Conference im Imperial Riding School Renaissance Vienna Hotel (ehemals Penta Hotel Wien 3) statt.

Heuriges Motto dieser 7. Konferenz ist “All about Secrets, Failures and Vision“.

Am 19.11. wird mit einem zweitägigen Workshop gestartet. Die Konferenz folgt am 21.11.2013.

Die Keynote hält Marcus J. Ranum. Am Anschluss daran findet die Pressekonferenz statt.

DeepSec Veranstalter René Pfeiffer und Michael Kafka gewannen auch 2013 wieder renommierte Experten aus Europa (u.a. Schweiz, Deutschland, Ungarn) sowie USA und Asien. Auf hohem Niveau diskutieren die Experten über Sicherheit in der mobilen Welt, welche Geheimnisse, Fehler und Visionen uns schon jetzt beschäftigen sollten, um auf die wachsenden Herausforderungen besser vorbereitet zu sein.

Geopolitics And The Internet: The Meaning Of "Hegemony", Marcus J. Ranum

Was die Vorherrschaft der USA im Internet und für die gesamte mobile Welt bedeutet, und was man ihr entgegensetzen kann und muss – darüber referiert Marcus J. Ranum (Tenable Network Security).

Der 1962 geborene US-Amerikaner gilt als IT-Sicherheits-Pionier, hält seit den 80er Jahren Top-Positionen in IT-Sicherheitsfirmen und publiziert regelmäßig Artikel sowie Sachbücher, u.a. „The Myth of Homeland Security“.

Ranum versteht das Internet als „Kolonie der US-Amerikaner“, in der sie ihre uneingeschränkte Machtposition laufend ausbauen – man denke beispielsweise an Stuxnet oder an den globalen Spionageskandal. Mittlerweile fordern einzelne europäische Regierungen ein Nachdenken über die Notwendigkeit einer europäischen ITK-Souveränität, um in der Informationstechnik nicht von den US-Amerikanern oder anderen Mächten abhängig zu sein.

Auch die europäische Wirtschaft bildet sich langsam eine Meinung dazu: Politiker verstünden nichts von der Thematik und interessieren sich daher auch nicht für Sicherheit bzw. erkennen die Brisanz nicht. Dass Politiker von unzähligen Lobbyisten – Diener unterschiedlicher Herren – beraten werden, mache

die Sache nicht einfacher; im Gegenteil.

Der menschlichen Psyche widmet sich Stefan Schumacher vom Magdeburger Institut für Sicherheitsforschung: Psychology of Security - A Research Programme

Warum gelingt es Betrügern dermaßen leicht via Porno-Apps, Sexbildern und fingierter Partnersuche auf Webplattformen Menschen und ganze Unternehmen auszuspionieren, zu erpressen und zu schädigen?

Warum fallen Menschen immer wieder auf schlecht gemachte Passwort-Fischer herein?

Weil fast 50% aller Smartphone Nutzer weltweit ihre Handys in keinster Weise sichern und oft sogar Codes und Passwörter offen darin aufbewahren? (Zahlen: aktueller Norton Bericht 2013)

Weil IT-Security nur als technisches Problem angesehen wird, statt anzuerkennen, dass Entscheidungen von Menschen getroffen werden und somit Sicherheitsprobleme und –strategien auch mit psychologischen Methoden untersucht werden sollten?

Stefan Schumacher stellt Ergebnisse aus seinem aktuellen Forschungsprojekt vor:

Es geht dabei u.a. darum, wie Menschen IT-Security erleben, was sie motiviert? Wie lernen sie und warum machen viele immer wieder dieselben Fehler und wie kann dieser Kreislauf nachhaltig unterbrochen werden?

Des weiteren geht es um die psychologischen Profile der Angreifer, die neben ihren technischen Möglichkeiten genauso entscheidend für die Abwehr von Angriffen sind.

Kontroverse Themen wie diese diskutieren wir auf der DeepSec 2013.

Bitte melden Sie Interview Anfragen bei uns an – wir organisieren auch vorab Gespräche.

Akkreditierungen für die Konferenz und die Workshops nehmen wir ab sofort entgegen:

Aufgrund limitierter Plätze bitten wir um rasche Anmeldungen:

info@deepsec.net oder René Pfeiffer: 043 676 /562 63 90

Das laufend aktualisierte Programm finden Sie auf http://deepsec.net/schedule.html

Übersicht aller Sprecher & Themen: http://deepsec.net/speaker.html

09.10.2013 3/3

Kurzprofil DeepSec:

Die DeepSEC bildet die neutrale Plattform für ein unabhängiges Zusammentreffen von weltweit renommierten Sicherheitsexperten von Universitäten, Regierungen, der Industrie, sowie unabhängigen Wissenschaftlern, Autoren und der zumeist im Untergrund tätigen Hacker Community und interessierten Gäste aus der ganzen Welt, die sich im engeren oder weiteren Sinn mit Sicherheitsbelangen auseinandersetzen.

Die vielzitierte Vision „Leben im global vernetzten Dorf“ ist für die meisten von uns real und oft sogar Existenz bestimmend. Im selben Ausmaß wachsen auch die Bedeutung und somit die Teilnehmerbreite der DeepSec, die2007 zum ersten Mal stattfand. Mittlerweile hat die Wiener Konferenz 200 Teilnehmer. Längst zählen nicht

mehrnur Entwickler, Netzwerktechniker und Administratoren zum Besucherkreis. DeepSec führt Interessierte aus unterschiedlichsten Bereichen wie Bildungseinrichtungen, Finanzinstitute oder Gesundheits- und Versicherungsorganisationen mit IT-Security Experten zusammen.

Kontakt / Pressekontakt

DeepSec GmbH

René Pfeiffer & Michael Kafka

Weyringergasse 30a/10

1040 Wien, Austria

rpfeiffer@deepsec.net

Mobiltelefon: +43/676/5626390

Bürotelefon: +43/720/349387

DEEPSEC

P R E S S E I N F O R M A T I O N

Der Countdown zur DeepSec 2013 läuft

- ***Vom 19. bis 22.11.2013 referieren internationale Sicherheitsexperten in Wien***
- ***Wir stellen Sprecher und Schwerpunkte vor***

Wien, 9. Oktober 2012 – Vom 19. bis 22. November 2013 findet die DeepSec ISDC - In Depth Security Conference im Imperial Riding School Renaissance Vienna Hotel (ehemals Penta Hotel Wien 3) statt.
Heuriges Motto dieser 7. Konferenz ist "All about Secrets, Failures and Vision".
Am 19.11. wird mit einem zweitägigen Workshop gestartet. Die Konferenz folgt am 21.11.2013.
Die Keynote hält Marcus J. Ranum. Am Anschluss daran findet die Pressekonferenz statt.

DeepSec Veranstalter René Pfeiffer und Michael Kafka gewannen auch 2013 wieder renommierte Experten aus Europa (u.a. Schweiz, Deutschland, Ungarn) sowie USA und Asien. Auf hohem Niveau diskutieren die Experten über Sicherheit in der mobilen Welt, welche Geheimnisse, Fehler und Visionen uns schon jetzt beschäftigen sollten, um auf die wachsenden Herausforderungen besser vorbereitet zu sein.

Geopolitics And The Internet: The Meaning Of "Hegemony", Marcus J. Ranum
Was die Vorherrschaft der USA im Internet und für die gesamte mobile Welt bedeutet, und was man ihr entgegensetzen kann und muss – darüber referiert Marcus J. Ranum (Tenable Network Security).
Der 1962 geborene US-Amerikaner gilt als IT-Sicherheits-Pionier, hält seit den 80er Jahren Top-Positionen in IT-Sicherheitsfirmen und publiziert regelmäßig Artikel sowie Sachbücher, u.a. „The Myth of Homeland Security".

Ranum versteht das Internet als **„Kolonie der US-Amerikaner",** in der sie ihre uneingeschränkte Machtposition laufend ausbauen – man denke beispielsweise an Stuxnet oder an den globalen Spionageskandal. Mittlerweile fordern einzelne europäische Regierungen ein Nachdenken über die **Notwendigkeit einer europäischen ITK-Souveränität,** um in der Informationstechnik nicht von den US-Amerikanern oder anderen Mächten abhängig zu sein.

Auch die europäische Wirtschaft bildet sich langsam eine Meinung dazu: Politiker verstünden nichts von der Thematik und interessieren sich daher auch nicht für Sicherheit bzw. erkennen die Brisanz nicht. Dass Politiker von unzähligen Lobbyisten – Diener unterschiedlicher Herren – beraten werden, mache die Sache nicht einfacher; im Gegenteil.

Der menschlichen Psyche widmet sich Stefan Schumacher vom Magdeburger Institut für Sicherheitsforschung: Psychology of Security - A Research Programme

Warum gelingt es Betrügern dermaßen leicht via Porno-Apps, Sexbildern und fingierter Partnersuche auf Webplattformen Menschen und ganze Unternehmen auszuspionieren, zu erpressen und zu schädigen?
Warum fallen Menschen immer wieder auf schlecht gemachte Passwort-Fischer herein?
Weil fast 50% aller Smartphone Nutzer weltweit ihre Handys in keinster Weise sichern und oft sogar Codes und Passwörter offen darin aufbewahren? *(Zahlen: aktueller Norton Bericht 2013*)

Weil IT-Security nur als technisches Problem angesehen wird, statt anzuerkennen, dass Entscheidungen von Menschen getroffen werden und somit Sicherheitsprobleme und –strategien auch mit psychologischen Methoden untersucht werden sollten?

Stefan Schumacher stellt Ergebnisse aus seinem aktuellen Forschungsprojekt vor:

Es geht dabei u.a. darum, wie Menschen IT-Security erleben, was sie motiviert? Wie lernen sie und warum machen viele immer wieder dieselben Fehler und wie kann dieser Kreislauf nachhaltig unterbrochen werden?
Des weiteren geht es um die psychologischen Profile der Angreifer, die neben ihren technischen Möglichkeiten genauso entscheidend für die Abwehr von Angriffen sind.

Kontroverse Themen wie diese diskutieren wir auf der DeepSec 2013.

Bitte melden Sie **Interview Anfragen** bei uns an – wir organisieren auch vorab Gespräche.
Akkreditierungen für die Konferenz und die Workshops nehmen wir ab sofort entgegen:
Aufgrund limitierter Plätze bitten wir um rasche Anmeldungen:
info@deepsec.net oder René Pfeiffer: 043 676 /562 63 90

Das laufend aktualisierte Programm finden Sie auf http://deepsec.net/schedule.html

Übersicht aller Sprecher & Themen: http://deepsec.net/speaker.html

Kurzprofil DeepSec:
Die DeepSEC bildet die neutrale Plattform für ein unabhängiges Zusammentreffen von weltweit renommierten Sicherheitsexperten von Universitäten, Regierungen, der Industrie, sowie unabhängigen Wissenschaftlern, Autoren und der zumeist im Untergrund tätigen Hacker Community und interessierten Gäste aus der ganzen Welt, die sich im engeren oder weiteren Sinn mit Sicherheitsbelangen auseinandersetzen.
Die vielzitierte Vision „Leben im global vernetzten Dorf“ ist für die meisten von uns real und oft sogar Existenz bestimmend. Im selben Ausmaß wachsen auch die Bedeutung und somit die Teilnehmerbreite der DeepSec, die 2007 zum ersten Mal stattfand. Mittlerweile hat die Wiener Konferenz 200 Teilnehmer. Längst zählen nicht mehr nur Entwickler, Netzwerktechniker und Administratoren zum Besucherkreis.
DeepSec führt Interessierte aus unterschiedlichsten Bereichen wie Bildungseinrichtungen, Finanzinstitute oder Gesundheits- und Versicherungsorganisationen mit IT-Security Experten zusammen.

Kontakt / Pressekontakt
DeepSec GmbH
René Pfeiffer & Michael Kafka
Weyringergasse 30a/10
1040 Wien, Austria
rpfeiffer@deepsec.net
Mobiltelefon: +43/676/5626390
Bürotelefon: +43/720/349387

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