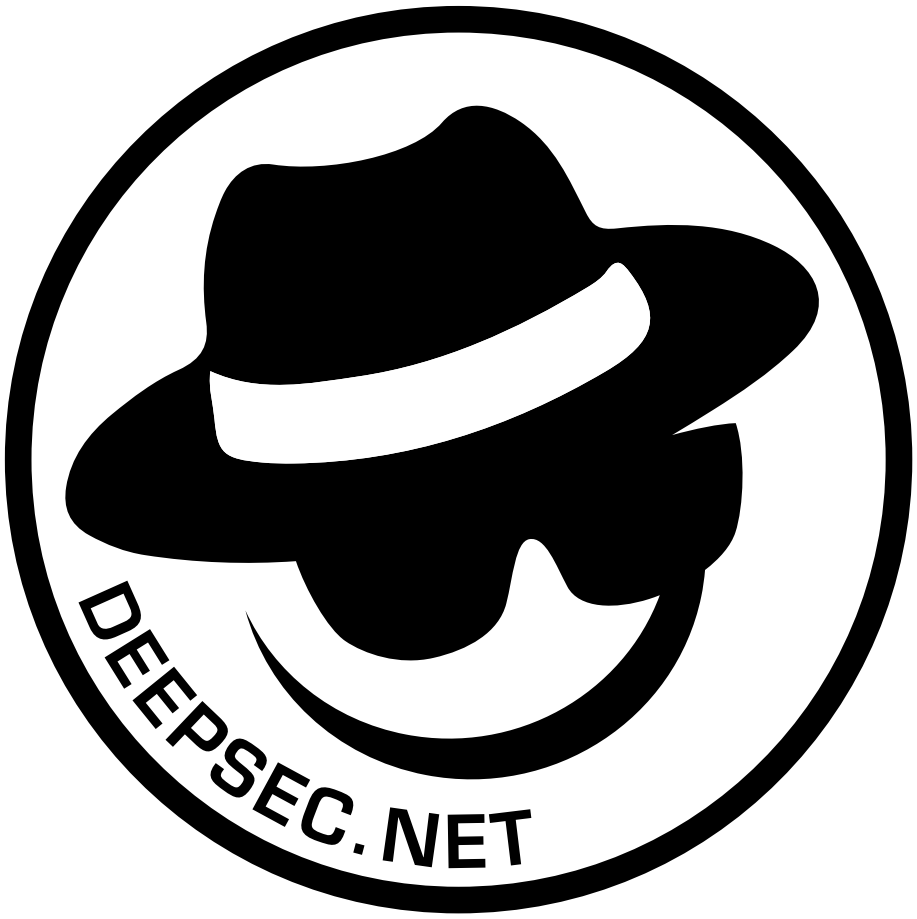


press review 2019

media coverage

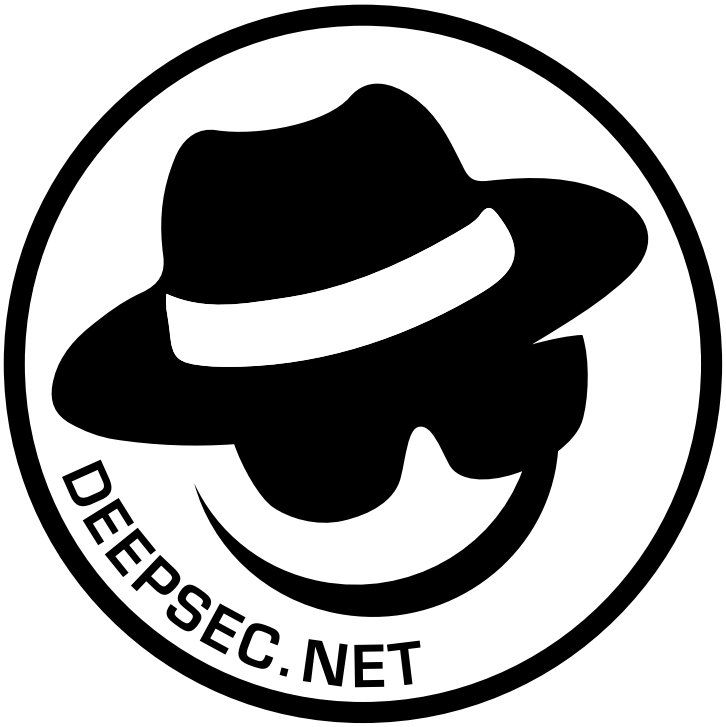
2019

contents

press releases

2019

media coverage 2019



https://xn--verschlsselt-jlb.it/deepsec-2019-nachlese-zum-grossen-it-sicherheit-event/

08.12.2019

DEEPSEC 2019 – Nachlese zum großen IT-Sicherheit Event

Auch dieses Jahr fand im November die große In-Depth Security Konferenz DEEPSEC 2019 in der Imperial Riding School Vienna im Wien statt. Rund 300 Teilnehmer und zahlreiche Sponsoren und Fachredner trafen sich vom 26. bis 29. November 2019 zum Training und Erfahrungsaustausch.

Mit 54 hochkarätigen Sessions in drei großzügigen Seminarräumen bot das Event für alle Interessentengruppen wie Security Officers, Security Professionals and Produkthersteller, IT Entscheider, Berater und Ersteller von Richtlinien, Security-/Network-/Firewall-Admins, Hackers and Software Developers umfassende Einblicke in aktuelle und zukünftige Security Konzepte aber auch Bedrohungen.

Besonders hat mich der DEEPSEC Vortrag von Michael Walser von der SEMATICON AG mit dem Titel „Demystifying Hardware Security Modules – How to Protect Keys in Hardware“ interessiert über den Vortrag ich hier im Detail berichten möchte.

Michael Walser, CTO der SEMATICON AG

Die Sematicon AG beschäftigt sich neben Remote-Management für Industriesteuerungen mit angewandter Kryptographie im IIoT Bereich. Michael Walser ist als CTO verantwortlich für die Technologische Ausrichtung des Produkt- und Schulungsportfolios.

Demystifying Hardware Security Modules – How to Protect Keys in Hardware

Der schwungvolle Einstieg in den DEEPSEC Vortrag gelang Michael mit der Frage was genau ein HSM ist, wobei der festhält, dass es wichtig ist kryptographische Ressourcen nicht zu teilen und seine Schüssel bestmöglich zu schützen. Warum? Das zeigt er kurze Zeit später.

Anmerkung: Allen seine Angriffen basieren nicht auf der kryptographischen Stärke der Verschlüsselungsmethode, siehe hierzu meinen Artikel Sind Krypto-Algorithmen wie AES knackbar?

Kryptographische Schlüssel sind möglichst zufällige Werte, die für die Verschlüsselung von Daten genutzt werden können. Hier hebt er hervor, dass gute Zufallszahlen nicht von der Funktion rand() oder dem Linux Device /dev/random kommen, sondern es spezielle Hardware erfordert solche Zahlen zu erzeugen.

Hardware Security Module – oder kurz HSM genannt – gibt es in unterschiedlichen Formen für die vielen Anwendungsfälle:

Als Smartcard oder Crypto-Token

Als Secure Element

als Datacenter HSM

Ein HSM unterstützt eine wichtige Funktion, nämlich die Separierung von Schlüssel für verschiedene Applikationen. Hier werden geschützte Container oder auch Partitionen erstellt wo die getrennten Applikationen ihre Schlüssel ablegen können. Wichtig ist, dass der authentisierte Zugriff einer Applikation keine Schlüssel einer anderen Applikation sehen bzw. nutzen kann. Die Anzahl der separierten Bereiche ist in der Regel sehr stark limitiert, oft sind das nur wenige Container bzw. Partitionen pro HSM.

Schlüssel werden in einem HSM nicht gespeichert, sondern sind dort speziell verwahrt und gibt eine hochsichere Schlüsselseparierung für die Schlüssel. Die Schlüssel kann man nicht wie Dateien öffnen und einfach lesen, sondern es gibt Schnittstellen über diese Software mit den Schlüsseln arbeiten kann. Zu den wichtigsten Schnittstellen zählen:

PKCS#11 (Unix, Linux, Windows per SO oder DLL)

CryptoAPI (Windows)

Minidriver oder KSP (Windows)

Java (Unix, Linux, Windows oft ein Wrapper für PKCS#11)

Meine Schlüssel sind geschützt … ich benötige kein HSM …

Den Tag eines Sicherheitsverantwortlichen oder IT-Administrators zu ruinieren ist nur eine Frage von rd. 5 KByte!

Bei einer typischen Windows 2016 CA mit den Standard Einstellungen des Betriebssystems basiert die Microsoft CA auf dem Microsoft Software Base CSP. Die CA wird in den Standardeinstellungen mit einem 4096 Bit RSA-Schlüssel mit SHA256-Hash erstellt. Es gibt nur einen Root-CA Schlüssel und im Enterprise CA Modus ist es mit der AD Domäne verbunden.

DEEPSEC Hack #1 – einen exportgeschützten CA Schlüssel kopieren

Michael Walser zeigt in seinem moderierten 5 Minuten Video wie man:

Das Root CA Zertifikat (mit dem öffentlichen Schlüssel) sichern kann

wie man von einem entfernten oder dem lokalen Server aus dem Computer Account den Root CA Zertifikat (privaten

Schlüssel + öffentlichen Schlüssel) sichern kann

wie man das Root CA Zertifikat mit dem privaten Schlüssel löschen kann

wie man das zuvor gesicherte Root CA Zertifikat mit erhöhten Sicherheitseinstellungen, nämlich dem Export-Schutz für den privaten Schlüssel wieder importieren kann

UND… wie man im Anschluss trotzdem mit dem Hacker Tool mimikatz das vermeintlich exportgeschützte Root CA Zertifikat mit dem privaten RSA 4096 Schlüssel in wenigen Sekunden stehlen kann.

DEEPSEC Hack #2 – ein gefälschtes Userzertifikat für die Domainanmeldung nutzen

Das zuvor geklaute CA Zertifikat mit dem privaten Schlüssel lässt sich hervorragend missbrauchen. Mit einem kleinen Windows Command Line Batch (modernen wäre natürlich ein PowerShell Script) erstellt er in wenigen Sekunden zwei Microsoft virtuelle Smartcards (VSC) wo er mit dem CA Zertifikat jeweils selbsterstellte Benutzerzertifikate für die Domainenanmeldung signiert. Der Benutzerprinzipalname (UPN) im Zertifikat muss, mit dem in der Domaine gespeicherten UPN übereinstimmen.

Nach dem Logoff von Windows, sieht man beim Windows-Logon dann unter „Sign-in options“ (englisches Windows) bzw. „Anmeldeoptionen“ (deutsches Windows) zwei neue Optionen für die Anmeldung mit virtuellen Smartcards.

Die gefälschten Zertifikate werden von der Domaine sofort den zugehörigen Benutzerkennungen zugeordnet und der Angreifer kann alle Datenzugriffe des nun gehackten Benutzeraccounts nutzen.

Nicht gezeigt hat Michael Walser, ob man so auch einen Domain-Administrator fälschen kann, aber ich denke das auch das möglich ist.

Ghost CA – die Gefahren eines verlorenen CA Schlüssels

Eine parallele CA eines Angreifers nennt er Ghost CA und diese CA ist äußerst gefährlich.

Leider erfahren Domain Administratoren nur in den seltensten Fällen von einer Ghost CA und dass ein CA Schlüssel gestohlen wurde. Aber auch wenn der Administrator es erfährt, er kann nahezu nichts gehen den Hack machen, da es keine Revokations-Liste für die Root CA gibt. Der Administrator kann nur die gesamte CA neu aufsetzen und versuchen alle Trusts der alten CA aus allen Teilen des Netzwerkes zu löschen. Bei einer Enterprise Umgebung eines Konzernes eine unglaublich schwierige Aufgabe.

Die Lösung: ein Hardware Security Modul (HSM)

Um sich vor dem Diebstahl von privaten Schlüsseln – in dem oberen Fall den privaten Root CA Schlüssel – zu schützen,

empfiehlt Michael Walser in seinem DEEPSEC 2019 Vortrag die Nutzung von Hardware Security Modulen und lädt die Besucher ein sich die HSMs der Hersteller nCipher (vormals Thales nShield) und Thales / Gemalto / SafeNet auf seinem DEEPSEC Stand anzusehen.

Beyond IT: Smart* kann gehackt werden und wurde schon gehackt!
In zahlreichen Berichten wie beispielsweise den von Wired, sind die TSA-Schlüssel die Behörden das Öffnen von Gepäckstücken ermöglichen, bereits vor einigen Jahren geleaket und können heute im 3D Drucker einfach nachgedruckt werden. Genauso sind auch Zahlreiche vorverteilte Krypto-Schlüssel von Smart Bulps ebenfalls geleaked.

DEEPSEC Hack #3 – einen geschützten AES Schlüssel aus einem Microcontroller extrahieren
Aber, wie kommt man an solche Schlüssel ran? Ein Microprozessor rechnet natürlich mit den Krypto-Schlüsseln und verbraucht damit Strom. Dieser charakteristische Stromverbrauch kann über den VCC Pin des Microprozessors über einen vorgeschalteten kleinen Ohmwiederstand gemessen werden. Hierzu benötigt man ein Speicheroszilloskop um wenige Hundert Euro.Durch das Messen des Stromverbrauchen der wichtigen Krypto-Operationen Count, Multiply Divide werden diese Operationen genau erkannt und korreliert. Diese Korrelierung ergibt dann rd. 20 Millionen Möglichkeiten bei einem AES-128 Schlüssel. Diese 20 Millionen lassen sich mit einer Methode die sich Partitional Guessing Entropy (PGE) nennt auf einen richtigen AES Schlüssel zurückrechnen. Der ganze Vorgang dauert nur 21 Sekunden…

Dein Appell für diese Microprozessor Demo lautet: „Denke immer über Security bevor Du eine Produktentwicklung startest“.Zum Abschluss präsentiert er wie er an einem Nachmittag den Verschlüsselungsschlüssel einer verschlüsselten Firmware extrahiert hat. Den Exploit hat er bereits an den Hardware Hersteller gemeldet, leider jedoch ganz ohne Rückmeldung des Herstellers.

Leider wollte er nicht verraten um welches gängige Consumer Produkt, wie z.B. einen DSL Router, WLAN Access Point, NAS Appliance, oder um welchen Hersteller es sich handelt. Ich denke mal in ein paar Wochen lesen wir davon schon in Heise.de.

Mit seiner Firma Sematicon AG in München erarbeitet er sichere Krypto-Konzepte immer unter dem Motto „Keys in Hardware!“.

Wie? Das präsentierte er auf seinem Stand auf der DEEPSEC 2019.
Michael Walser ist auf Xing und LinkedIn zu finden und natürlich kann man ihn gerne über seine Webseite https://www.sematicon.com/ kontaktieren.

DEEPSEC 2019 – Nachlese zum großen IT-Sicherheit Event

Auch dieses Jahr fand im November die große In-Depth Security Konferenz DEEPSEC 2019 in der Imperial Riding School Vienna im Wien statt. Rund 300 Teilnehmer und zahlreiche Sponsoren und Fachredner trafen sich vom 26. bis 29. November 2019 zum Training und Erfahrungsaustausch.

Mit 54 hochkarätigen Sessions in drei großzügigen Seminarräumen bot das Event für alle Interessentengruppen wie Security Officers, Security Professionals and Produkthersteller, IT Entscheider, Berater und Ersteller von Richtlinien, Security-/Network-/Firewall-Admins, Hackers and Software Developers umfassende Einblicke in aktuelle und zukünftige Security Konzepte aber auch Bedrohungen.

Two Days of Conference (28./29. November)

Throughout the conference you will get the opportunity of meeting experts at the Hacker's Lounge to discuss security issues and see demonstrations.

Conference, day 1 - Thu, 28 Nov

	Left Pirouette	Right Pirouette	Riding School (ROOTS)
08:00	Registration opens		
09:00		Opening Ceremony René Pfeiffer (DeepSec In-Depth Security Conference)	
09:10		Computer Security is simple, the World is not. Raphael Vinot and Quinn Norton (-)	
10:00	Comparing GnuPG With Signal is like Comparing Apples with Smart Light Bulbs Hans Fritag (Conosphere GmbH (CEO), Metalab (Hackspace), CCC)	Chinese Police and CloudPets Abraham Aranguren (7ASecurity)	RevEngE is a dish served cold: Debug-Oriented Malware Decompilation and Reassembly Marcus Botacin (Federal University of Paraná / UNICAMP / University of Campinas - Institute of Computing / UFPR)
10:50	Coffee Break		
11:10	SD-WAN Secure Communications Design and Vulnerabilities Denis Kolegov (BiZone, Tomsk State University)	Mastering AWS Pentesting and Methodology Ankit Giri (Independent Security Researcher)	Automatic Modulation Parameter Detection in Practice Johannes Pohl (University of Applied Sciences Stralsund)
12:00	Still Secure. We Empower What We Harden Because We Can Conceal Yury Chemerkin (Advanced Monitoring)	Security Analytics and Zero Trust - How Do We Tackle That? Holger Arends (Telstra)	Horizer Roller: Linker-Based Instrumentation for Enhanced Embedded Security Testing Katharina Bogad (Fraunhofer Institute for Applied and Integrated Security)
12:50	Lunch		
14:00	Android Malware Adventures: Analyzing Samples and Breaking into C&C Kürşat Oğuzhan Akıncı & Mert Can Coşkuner (STM AS & Trendyol)	Beyond Windows Forensics with Built-in Microsoft Tooling Thomas Fischer (FVT SecOps Consulting)	Shallow Security: on the Creation of Adversarial Variants to Evade ML-Based Malware Detectors Fabricio Ceschin (Federal University of Paraná / University of Waikato)
14:50	The Turtle Gone Ninja - Investigation of an Unusual Crypto-Mining Campaign Ophir Harpaz, Daniel Goldberg (Guardicore)	30 CVEs in 30 Days Eran Shimony (CyberArk)	T.B.A.
15:40	Coffee Break		
16:00	Emoji, how do they even work and how they break Security MacLemon (-)	"The Daily Malware Grind" – Looking Beyond the Cyberx Tim Berghoff, Hauke Gienow (G DATA Software AG)	Hands-On Workshop: Attacks on the Diffie-Hellman Protocol Denis Kolegov, Innokenti Sennovskii (BiZone LLC / Tomsk State University)
16:50	Demystifying Hardware Security Modules - How to Protect Keys in Hardware Michael Walser (sumatrocon AG)	The Future Is Here - Modern Attack Surface On Automotive Lior Yaari (Cymotive & Imperium Security)	Hands-On Workshop: Attacks on the Diffie-Hellman Protocol Denis Kolegov, Innokenti Sennovskii (BiZone LLC / Tomsk State University)
17:40	Practical Security Awareness - Lessons Learnt and Best Practices Stefan Schumacher (Magdeburger Institut für Sicherheitsforschung)	New Tales of Wireless Input Devices Matthias Deeg (SySS GmbH)	Hands-On Workshop: Attacks on the Diffie-Hellman Protocol Denis Kolegov, Innokenti Sennovskii (BiZone LLC / Tomsk State University)
20:00	Speaker's Dinner		

Conference, day 2 - Fri, 29 Nov

	Left Pirouette	Right Pirouette	Riding School (ROOTS)
09:00	What Has Data Science Got To Do With It? Thordis Thorsteins (Paraseer)	How To Create a Botnet of GSM-devices Aleksandr Kolcharov (Independent security researcher)	T.B.A.

Besonders hat mich der DEEPSEC Vortrag von Michael Walser von der SEMATICON AG mit dem Titel „Demystifying Hardware Security Modules – How to Protect Keys in Hardware“ interessiert über den Vortrag ich hier im Detail berichten möchte.

Michael Walser, CTO der SEMATICON AG

Die Sematicon AG beschäftigt sich neben Remote-Management für Industriesteuerungen mit angewandter Kryptographie im IIoT Bereich. Michael Walser ist als CTO verantwortlich für die Technologische Ausrichtung des Produkt- und Schulungsportfolios.

Demystifying Hardware Security Modules – How to Protect Keys in Hardware

Demystifying HSMs

Der schwungvolle Einstieg in den DEEPSEC Vortrag gelang Michael mit der Frage was genau ein HSM ist, wobei der festhält, dass es wichtig ist kryptographische Ressourcen nicht zu teilen und seine Schüssel bestmöglich zu schützen. Warum? Das zeigt er kurze Zeit später.

> *Anmerkung: Allen seine Angriffen basieren nicht auf der kryptographischen Stärke der Verschlüsselungsmethode, siehe hierzu meinen Artikel* ***Sind Krypto-Algorithmen wie AES knackbar?***

Kryptographische Schlüssel sind möglichst zufällige Werte, die für die Verschlüsselung von Daten genutzt werden können. Hier hebt er hervor, dass gute Zufallszahlen nicht von der Funktion rand() oder dem Linux Device /dev/random kommen, sondern es spezielle Hardware erfordert solche Zahlen zu erzeugen.

Hardware Security Module – oder kurz HSM genannt – gibt es in unterschiedlichen Formen für die vielen Anwendungsfälle:

1. Als Smartcard oder Crypto-Token
2. Als Secure Element
3. als Datacenter HSM

HSM Modelle

Ein HSM unterstützt eine wichtige Funktion, nämlich die Separierung von Schlüssel für verschiedene Applikationen. Hier werden geschützte Container oder auch Partitionen erstellt wo die getrennten Applikationen ihre Schlüssel ablegen können. Wichtig ist, dass der authentisierte Zugriff einer Applikation keine Schlüssel einer anderen Applikation sehen bzw. nutzen kann. Die Anzahl der separierten Bereiche ist in der Regel sehr stark limitiert, oft sind das nur wenige Container bzw. Partitionen pro HSM.

Schlüssel werden in einem HSM nicht gespeichert, sondern sind dort speziell verwahrt und gibt eine hochsichere Schlüsselseparierung für die Schlüssel. Die Schlüssel kann man nicht wie Dateien öffnen und einfach lesen, sondern es gibt Schnittstellen über diese Software mit den Schlüsseln arbeiten kann. Zu den wichtigsten Schnittstellen zählen:

1. PKCS#11 (Unix, Linux, Windows per SO oder DLL)
2. CryptoAPI (Windows)
3. Minidriver oder KSP (Windows)
4. Java (Unix, Linux, Windows oft ein Wrapper für PKCS#11)

Meine Schlüssel sind geschützt ... ich benötige kein HSM ...

Den Tag eines Sicherheitsverantwortlichen oder IT-Administrators zu ruinieren ist nur eine Frage von rd. 5 KByte!

Bei einer typischen Windows 2016 CA mit den Standard Einstellungen des Betriebssystems basiert die Microsoft CA auf dem Microsoft Software Base CSP. Die CA wird in den Standardeinstellungen mit einem **4096 Bit RSA-Schlüssel** mit **SHA256-Hash** erstellt. Es gibt nur einen Root-CA Schlüssel und im Enterprise CA Modus ist es **mit der AD Domäne verbunden.**

DEEPSEC Hack #1 – einen exportgeschützten CA Schlüssel kopieren

Michael Walser zeigt in seinem moderierten 5 Minuten Video wie man:

1. Das Root CA Zertifikat (mit dem öffentlichen Schlüssel) sichern kann
2. wie man von einem entfernten oder dem lokalen Server aus dem Computer Account den **Root CA Zertifikat (privaten Schlüssel + öffentlichen Schlüssel) sichern** kann
3. wie man das Root CA Zertifikat mit dem **privaten Schlüssel löschen** kann
4. wie man das zuvor gesicherte Root CA Zertifikat mit erhöhten Sicherheitseinstellungen, nämlich dem Export-Schutz für den **privaten Schlüssel wieder importieren** kann
5. **UND…** wie man im Anschluss trotzdem mit dem Hacker Tool *mimikatz* das vermeintlich **exportgeschützte Root CA Zertifikat mit dem privaten RSA 4096 Schlüssel in wenigen Sekunden stehlen kann**.

DEEPSEC Hack #2 – ein gefälschtes Userzertifikat für die Domainanmeldung nutzen

Das zuvor geklaute CA Zertifikat mit dem privaten Schlüssel lässt sich hervorragend missbrauchen. Mit einem kleinen Windows Command Line Batch (modernen wäre natürlich ein PowerShell Script) erstellt er in wenigen Sekunden zwei Microsoft virtuelle Smartcards (VSC) wo er mit dem CA Zertifikat jeweils selbsterstellte Benutzerzertifikate für die Domainenanmeldung signiert. Der Benutzerprinzipalname (UPN) im Zertifikat muss, mit dem in der Domaine gespeicherten UPN übereinstimmen.

Nach dem Logoff von Windows, sieht man beim Windows-Logon dann unter „Sign-in options“ (englisches Windows) bzw. „Anmeldeoptionen“ (deutsches Windows) zwei neue Optionen für die Anmeldung mit virtuellen Smartcards.

Die gefälschten Zertifikate werden von der Domaine sofort den zugehörigen Benutzerkennungen zugeordnet und der Angreifer kann alle Datenzugriffe des nun gehackten Benutzeraccounts nutzen.

Nicht gezeigt hat Michael Walser, ob man so auch einen Domain-Administrator fälschen kann, aber ich denke das auch das möglich ist.

Ghost CA – die Gefahren eines verlorenen CA Schlüssels

Eine parallele CA eines Angreifers nennt er Ghost CA und diese CA ist äußerst gefährlich.

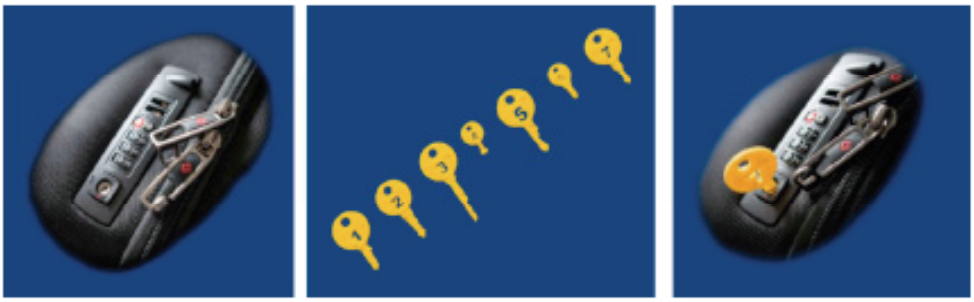
Leider erfahren Domain Administratoren nur in den seltensten Fällen von einer Ghost CA und dass ein CA Schlüssel gestohlen wurde. Aber auch wenn der Administrator es erfährt, er kann nahezu nichts gehen den Hack machen, da es keine Revokations-Liste für die Root CA gibt. Der Administrator kann nur die gesamte CA neu aufsetzen und versuchen alle Trusts der alten CA aus allen Teilen des Netzwerkes zu löschen. Bei einer Enterprise Umgebung eines Konzernes eine unglaublich schwierige Aufgabe.

Die Lösung: ein Hardware Security Modul (HSM)

Um sich vor dem Diebstahl von privaten Schlüsseln – in dem oberen Fall den privaten Root CA Schlüssel – zu schützen, empfiehlt Michael Walser in seinem DEEPSEC 2019 Vortrag die Nutzung von Hardware Security Modulen und lädt die Besucher ein sich die HSMs der Hersteller nCipher (vormals Thales nShield) und Thales / Gemalto / SafeNet auf seinem DEEPSEC Stand anzusehen.

Beyond IT: Smart* kann gehackt werden und wurde schon gehackt!

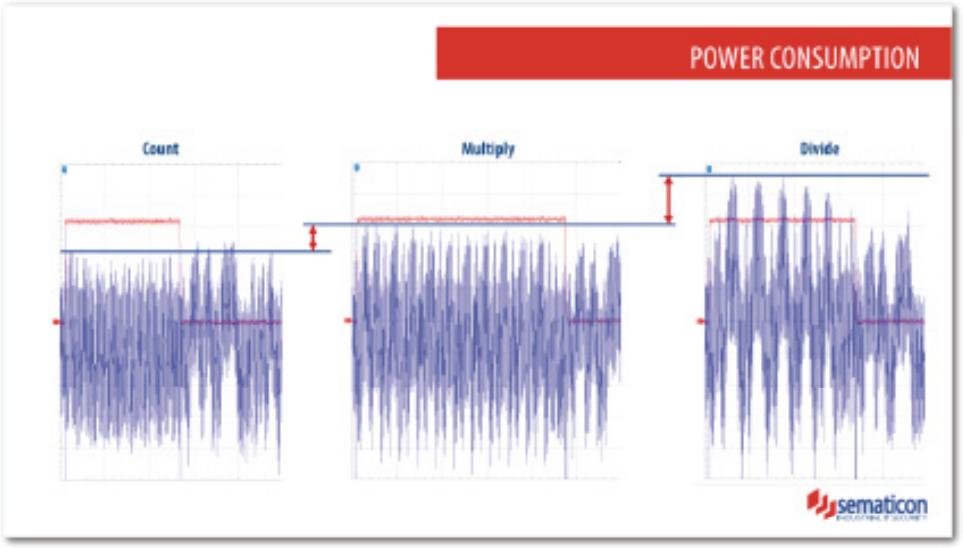
In zahlreichen Berichten wie beispielsweise den von **Wired, sind die TSA-Schlüssel die Behörden das Öffnen von Gepäckstücken ermöglichen, bereits vor einigen Jahren geleaket und können heute im 3D Drucker einfach nachgedruckt werden. Genauso sind auch Zahlreiche vorverteilte Krypto-Schlüssel von Smart Bulps ebenfalls geleaked.**



TSA Schlüssel aus dem 3D Drucker

DEEPSEC Hack #3 – einen geschützten AES Schlüssel aus einem Microcontroller extrahieren

Aber, wie kommt man an solche Schlüssel ran? Ein Microprozessor rechnet natürlich mit den Krypto-Schlüsseln und verbraucht damit Strom. Dieser charakteristische Stromverbrauch kann über den VCC Pin des Microprozessors über einen vorgeschalteten kleinen Ohmwiederstand gemessen werden. Hierzu benötigt man ein Speicheroszilloskop um wenige Hundert Euro.



Microcontroller – Stromverbrauch bei AES Krypto-Operationen

Durch das Messen des Stromverbrauchen der wichtigen Krypto-Operationen Count, Multiply Divide werden diese Operationen genau erkannt und korreliert. Diese Korrelierung ergibt dann rd. 20 Millionen Möglichkeiten bei einem AES-128 Schlüssel. Diese 20 Millionen lassen sich mit einer Methode die sich Partitional Guessing Entropy (PGE) nennt auf einen richtigen AES Schlüssel zurückrechnen. Der ganze Vorgang dauert nur 21 Sekunden…

Dein Appell für diese Microprozessor Demo lautet: „Denke immer über Security **bevor** Du eine Produktentwicklung startest".

Zum Abschluss präsentiert er wie er an einem Nachmittag den Verschlüsselungsschlüssel einer verschlüsselten Firmware extrahiert hat. Den Exploit hat er bereits an den Hardware Hersteller gemeldet, leider jedoch ganz ohne Rückmeldung des Herstellers.

Leider wollte er nicht verraten um welches gängige Consumer Produkt, wie z.B. einen DSL Router, WLAN Access Point, NAS Appliance, oder um welchen Hersteller es sich handelt. Ich denke mal in ein paar Wochen lesen wir davon schon in **Heise.de**.

Mit seiner Firma Sematicon AG in München erarbeitet er sichere Krypto-Konzepte immer unter dem Motto „Keys in Hardware!".

Wie? Das präsentierte er auf seinem Stand auf der DEEPSEC 2019.

Michael Walser ist auf **Xing** und **LinkedIn** zu finden und natürlich kann man ihn gerne über seine Webseite **https://www.sematicon.com/** kontaktieren.

8. Dezember 2019 Andreas Schuster IT-Sicherheit, Verschlüsselung

https://www.wired.com/story/rcs-texting-security/

04.12.2019

The Future of Texting Is Far Too Easy to Hack

Rich Communication Services promises to be the new standard for texting. Thanks to sloppy implementation, it's also a security mess.

Ask practically any phone carrier, and they'll tell you that the future of smartphone features from texting to video calls is a protocol called Rich Communication Services. Think of RCS as the successor to SMS, an answer to iMessage that can also handle phone and video calls. Last month, Google announced it would begin rolling RCS out to its Messages app in all US Android phones. It's easy to imagine a near-future where RCS is the default for a billion people or more. But when security researchers looked under the hood, they found the way carriers and Google have implemented the protocol creates a basket of worrisome vulnerabilities.

At the Black Hat security conference in London on Tuesday, German security consultancy SRLabs demonstrated a collection of problems in how RCS is implemented by both phone carriers and Google in modern Android phones. Those implementation flaws, the researchers say, could allow texts and calls to be intercepted, spoofed, or altered at will, in some cases by a hacker merely sitting on the same Wi-Fi network and using relatively simple tricks. SRLabs previously described those flaws at the DeepSec security conference in Vienna last week, and at Black Hat also showed how those RCS hijacking attacks would work in videos like the one below:

SRLabs founder Karsten Nohl, a researcher with a track record of exposing security flaws in telephony systems, argues that RCS is in many ways no better than SS7, the decades-old phone system carriers still used for calling and texting, which has long been known to be vulnerable to interception and spoofing attacks. While using end-to-end encrypted internet-based tools like iMessage and WhatsApp obviates many of those of SS7 issues, Nohl says that flawed implementations of RCS make it not much safer than the SMS system it hopes to replace.

"You’re going to be more vulnerable to hackers because your network decided to activate RCS," says Nohl. "RCS gives us the capability to read your text messages and listen to your calls. That's a capability that we had with SS7, but SS7 is a protocol from the '80s. Now some of these issues are being reintroduced in a modern protocol, and with support from Google."

The RCS rollout still has a ways to go, and will continue to be a patchwork even with Google's backing. Some Android manufacturers use proprietary messaging apps as the default rather than the stock Messages app, and most

carriers push their own versions as well. The iPhone doesn't support it at all, and Apple has given no indication that it will. But as RCS rolls out more broadly, its security issues merit attention—especially since it's those implementations that create the problems in the first place.

"If you put out a new technology for a billion people, you should define the whole security concept."

The SRLabs videos demonstrate a grab bag of different techniques to exploit RCS problems, all of which are caused by either Google's or one of the phone carriers' flawed implementations. The video above, for instance, shows that once a phone has authenticated itself to a carrier's RCS server with its unique credentials, the server uses the phone's IP address and phone number as a kind of identifier going forward. That means an attacker who knows the victim's phone number and who is on the same Wi-Fi network—anyone from a coworker in the same corporate office to someone at the neighboring table at Starbucks—can potentially use that number and IP address to impersonate them.

Using a different technique, the researchers showed how an Android phone using RCS can be vulnerable to a man-in-the-middle attack. Whether it's a hacker controlling a malicious Wi-Fi network or an ISP or nation-state spies with access to an ISP's servers, an attacker can alter the domain name system request that the phone uses to find the RCS server that acts as the relay between senders and recipients of a message. SRLabs found that while Android's RCS-enabled messaging app checks to see if the server the phone is connecting to has a valid TLS certificate—in the same way your browser checks the validity of an HTTPS website—it will accept any valid certificate, even for the attacker's server.

It's like a security guard who only checks if someone's ID matches their face, rather than if their name is on the approved list in the first place. "It's a really stupid mistake," adds Nohl.

The result is that the man-in-the-middle can intercept and alter messages at will, as shown in this video:

Another attack takes advantage of a flaw in the initial setup for RCS devices. When a phone is first registered in the RCS system, it downloads a configuration file that contains the device's credentials. But to identify itself to the server and download that configuration file, a device only needs to have the IP address the carrier believes is meant to be associated with that device's phone number. Nohl points out, however, that any malicious app that ends up on a phone—even without special app permissions in Android—can reach out from the same IP address, steal the device's unique RCS credentials, and start impersonating it, as shown in the video below. That configura-

tion file attack can be used even against someone who has never enabled RCS on their phone, Nohl points out.

In some cases, carriers try to guard against that attack by sending a one-time code to the user's device that they have to enter. But SRLabs found that some carriers failed to limit the number of tries at guessing that code; a hacker can try every possible number in just five minutes. "In five minutes we have your configuration file, and forever after we can listen to all your phone calls and read all your texts," Nohl says.

All of these attacks become even more serious when RCS messaging is used as a second factor in two-factor authentication. In that case, RCS interception could allow hackers to steal one-time codes and gain access to other, even more sensitive accounts like email, as shown in this video:

When WIRED reached out to the GSM Association phone carrier industry group and Google, the company responded with a statement thanking the researchers but arguing that "many of these issues have already been addressed"—it declined to say which ones—"and as part of our close collaboration with the ecosystem, we're actively advising partners as they resolve the remaining issues." The GSMA claimed that it already knew of the issues SRLabs highlighted, and that "countermeasures and mitigation actions are available" for carriers to fix their RCS flaws. Nohl countered that those fixes haven't been implemented yet for any of the issues SRLabs presented on at Black Hat.

The GSMA further argued that SRLabs had pointed out problems with the implementation of the RCS standard, rather than the standard itself. "The findings highlight issues with some RCS implementations but not every deployment, or the RCS specifications themselves, are impacted," the GSMA statement reads.

Nohl argues, however, that the existence of so many flaws in the standard's implementations is in fact a problem with the standard. "If you put out a new technology for a billion people, you should define the whole security concept. Instead RCS leaves a lot undefined, and telcos make a lot of individual mistakes when trying to implement this standard," Nohl says. "This is a technology being introduced quietly to over a billion people already. And it exposes them to threats they didn't have to worry about previously."

ANDY GREENBERG SECURITY 12.04.2019 08:48 PM

The Future of Texting Is Far Too Easy to Hack

Rich Communication Services promises to be the new standard for texting. Thanks to sloppy implementation, it's also a security mess.

PHOTOGRAPH: RICHARD BAKER/GETTY IMAGES

Ask practically any phone carrier, and they'll tell you that the future of smartphone features from texting to video calls is a protocol called Rich Communication Services. Think of RCS as the successor to SMS, an answer to iMessage that can also handle phone and video calls. Last month, Google announced it would begin rolling RCS out to its Messages app in all US Android phones. It's easy to imagine a near-future where RCS is the default for a billion people or more. But when security researchers looked under the hood, they found the way carriers and Google have implemented the protocol creates a basket of worrisome vulnerabilities.

At the Black Hat security conference in London on Tuesday, German security consultancy SRLabs demonstrated a collection of problems in how RCS is implemented by both phone carriers and Google

DeepSec security conference in Vienna last week, and at Black Hat also showed how those RCS hijacking attacks would work in videos like the one below:

SRLabs founder Karsten Nohl, a researcher with a track record of exposing security flaws in telephony systems, argues that RCS is in many ways no better than SS7, the decades-old phone system carriers still used for calling and texting, which has long been known to be vulnerable to interception and spoofing attacks. While using end-to-end encrypted internet-based tools like iMessage and WhatsApp obviates many of those of SS7 issues, Nohl says that flawed implementations of RCS make it not much safer than the SMS system it hopes to replace.

"You're going to be more vulnerable to hackers because your network decided to activate RCS," says Nohl. "RCS gives us the capability to read your text messages and listen to your calls. That's a capability that we had with SS7, but SS7 is a protocol from the '80s. Now some of these issues are being reintroduced in a modern protocol, and with support from Google."

The RCS rollout still has a ways to go, and will continue to be a patchwork even with Google's backing. Some Android manufacturers use proprietary messaging apps as the default rather than the stock Messages app, and most carriers push their own versions as well. The iPhone doesn't support it at all, and Apple has given no indication that it will. But as RCS rolls out more broadly, its security issues merit attention—especially since it's those implementations that create the problems in the first place.

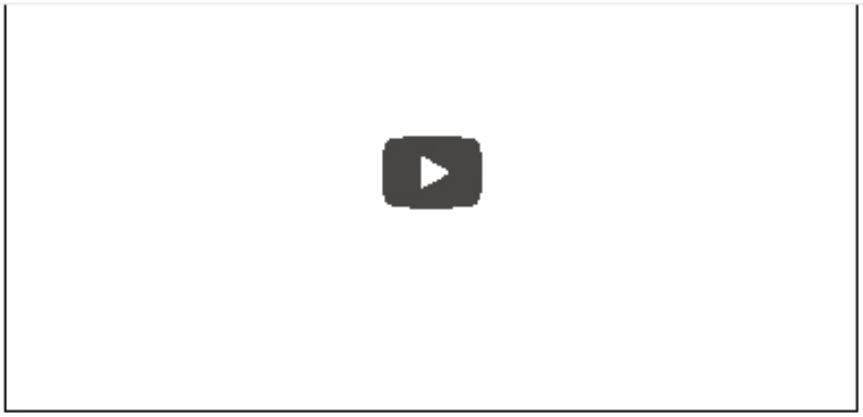
— KARSTEN NOHL, SRLABS

The SRLabs videos demonstrate a grab bag of different techniques to exploit RCS problems, all of which are caused by either Google's or one of the phone carriers' flawed implementations. The video above, for instance, shows that once a phone has authenticated itself to a carrier's RCS server with its unique credentials, the server uses the phone's IP address and phone number as a kind of identifier going forward. That means an attacker who knows the victim's phone number and who is on the same Wi-Fi network—anyone from a coworker in the same corporate office to someone at the neighboring table at Starbucks—can potentially use that number and IP address to impersonate them.

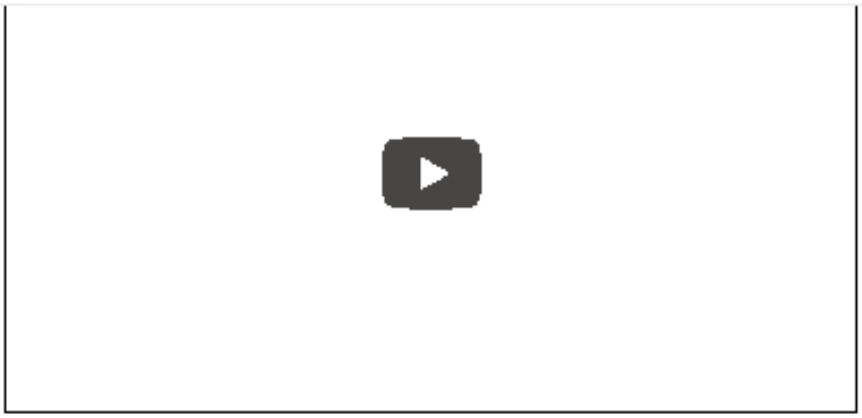
Using a different technique, the researchers showed how an Android phone using RCS can be vulnerable to a man-in-the-middle attack. Whether it's a hacker controlling a malicious Wi-Fi network or an ISP or nation-state spies with access to an ISP's servers, an attacker can alter the domain name system request that the phone uses to find the RCS server that acts as the relay between senders and recipients of a message. SRLabs found that while Android's RCS-enabled messaging app checks to see if the server the phone is connecting to has a valid TLS certificate—in the same way your browser checks the validity of an HTTPS website—it will accept any valid certificate, even for the attacker's server.

It's like a security guard who only checks if someone's ID matches their face, rather than if their name is on the approved list in the first place. "It's a really stupid mistake," adds Nohl.

The result is that the man-in-the-middle can intercept and alter messages at will, as shown in this video:

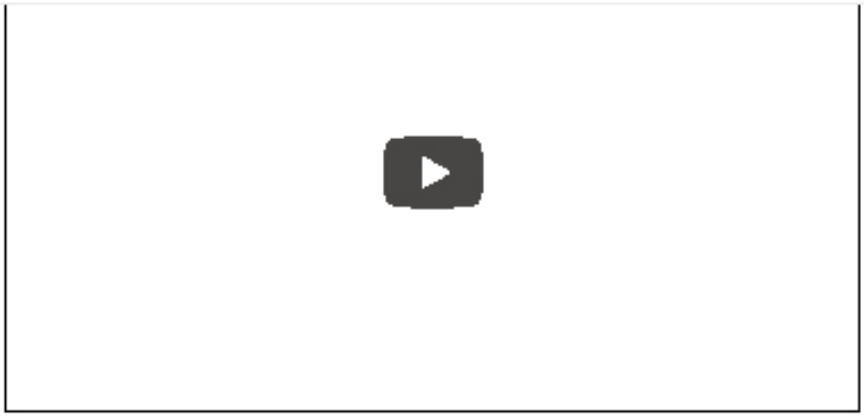


Another attack takes advantage of a flaw in the initial setup for RCS devices. When a phone is first registered in the RCS system, it downloads a configuration file that contains the device's credentials. But to identify itself to the server and download that configuration file, a device only needs to have the IP address the carrier believes is meant to be associated with that device's phone number. Nohl points out, however, that any malicious app that ends up on a phone—even without special app permissions in Android—can reach out from the same IP address, steal the device's unique RCS credentials, and start impersonating it, as shown in the video below. That configuration file attack can be used even against someone who has never enabled RCS on their phone, Nohl points out.



In some cases, carriers try to guard against that attack by sending a one-time code to the user's device that they have to enter. But SRLabs found that some carriers failed to limit the number of tries at guessing that code; a hacker can try every possible number in just five minutes. "In five minutes we have your configuration file, and forever after we can listen to all your phone calls and read all your texts," Nohl says.

All of these attacks become even more serious when RCS messaging is used as a second factor in two-factor authentication. In that case, RCS interception could allow hackers to steal one-time codes and gain access to other, even more sensitive accounts like email, as shown in this video:



When WIRED reached out to the GSM Association phone carrier industry group and Google, the company responded with a statement thanking the researchers but arguing that "many of these issues have already been addressed"—it declined to say which ones—"and as part of our close collaboration with the ecosystem, we're actively advising partners as they resolve the remaining issues." The GSMA claimed that it already knew of the issues SRLabs highlighted, and that "countermeasures and mitigation actions are available" for carriers to fix their RCS flaws. Nohl countered that those fixes haven't been implemented yet for any of the issues SRLabs presented on at Black Hat.

The GSMA further argued that SRLabs had pointed out problems with the implementation of the RCS standard, rather than the standard itself. "The findings highlight issues with some RCS implementations but not every deployment, or the RCS specifications themselves, are impacted," the GSMA statement reads.

Nohl argues, however, that the existence of so many flaws in the standard's implementations *is* in fact a problem with the standard. "If you put out a new technology for a billion people, you should define the whole security concept. Instead RCS leaves a lot undefined, and telcos make a lot of individual mistakes when trying to implement this standard," Nohl says. "This is a technology being introduced quietly to over a billion people already. And it exposes them to threats they didn't have to worry about previously."

More Great WIRED Stories

https://the-parallax.com/2019/12/03/rcs-security-vulnerabilities/

RCS delivers new texting features—and old security vulnerabilities

SETH ROSENBLATT DECEMBER 3, 2019

TOKYO—Google is aggressively boosting a new technology standard for text messages called RCS that it thinks should replace SMS around the world. But first, tech giants and telecommunications network providers will have to fix its major security flaws, researchers say.

RCS, or Rich Communication Services, brings a feature boost to the 30-year-old Short Message Service standard to make texting more like messaging with iMessage or WhatsApp. RCS data is sent using an Internet address, which means that consumers whose mobile network providers support RCS (available on all four major U.S. networks, as well as more than 100 networks in 67 countries, many in Europe) can send and receive messages, even when mobile network data is unavailable over Wi-Fi; they can receive "message read" notifications; they can send and receive high-quality photos and video; and they can see a three-dot ellipsis notification when the person with whom they're texting is in the process of writing a message.

Unlike similar but proprietary messaging services like those made by Apple and Facebook, RCS is designed to be an open standard that any tech company or network provider could support. Google has been advocating for RCS since 2015, when it acquired Jibe Mobile, the startup that invented the standard. RCS underpins a version of Google's Chat messaging app that the company debuted in the United Kingdom and France in June, and is now pushing globally.

At the PacSec conference here in November, researchers at Berlin-based Security Research Labs presented security vulnerabilities in RCS texts and calls the company's founder and CEO, Karsten Nohl, had discovered. (They also presented their findings last week at DeepSec in Austria, and plan to present an "extended set" of their findings again on Wednesday at Black Hat Europe in London.)

Hackers with what Nohl describes as "basic" abilities could take advantage of RCS vulnerabilities to track users, conduct fraud, impersonate users, prevent users from sending texts using a denial-of-service attack and, depending on the network, intercept texts. All of these actions, he stresses, can be prevented if network carriers implement widely used security protocols such as authenticating via the SIM card or secure chip on the phone; using "strong" one-time PIN codes that are at least eight alphanumeric characters; using rate limiting to prevent attackers from

trying an infinite series of OTP combinations; validating SIP sessions, which helps connect two or more devices to each other for voice and data calls; stripping sensitive information from SIP requests; and ensuring that Internet addresses linked to by certificates are validated.

“These are not structural hacks; these are avoidable mistakes,” Nohl says. “We don’t need to change the standard. It’s just up to a few vendors to change their implementation to get it right.”

RCS’ vulnerabilities can impact devices running Google’s Android mobile operating system, which currently account for about three-fourths of the world’s smartphones. They also can impact devices running Apple’s iOS. Because iMessage is only end-to-end encrypted when a message is sent between two Apple devices, anytime an iPhone user texts with an Android user, the message is sent over whichever network protocol the carrier is using. Historically, that’s been SMS, but as RCS becomes the standard for texting, it will increasingly be RCS, Nohl says.

Carriers Verizon, AT&T, T-Mobile, Sprint, Telefonica, and Google and Apple, did not respond to requests for comment. Australian carrier Optus declined to comment.

“The carriers are reinventing old security problems that the industry had previously solved.”—Karsten Nohl, CEO, Security Research Labs.

Deutsche Telekom spokesperson Christian Fischer said in an emailed statement that the network is “grateful for the feedback provided by the researchers.” Fischer alleged that Deutsche Telekom has “further improved the RCS security measures already this week,” but did not respond to requests to clarify what changes the network made.

Vodafone told The Parallax in an emailed statement that it is “aware” of the research. “We will review these protections in light of the research and, if required, take any further protective measures,” Vodafone representative Otso Iho said.

The mobile network trade group GSM Association said in a statement to The Parallax that SR Labs’ research is “complementary” to “an ongoing RCS risk assessment being conducted by the GSMA’s Fraud and Security Group.”

“Preliminary consideration of the research notes that countermeasures and mitigation actions are available to protect RCS implementations against the known vulnerabilities,” GSM Association spokeswoman Claire Cranton wrote,

adding that SR Labs is expected to present its findings to the GSM Association's Fraud and Security Group next week.

The struggle to secure RCS underscores challenges in improving legacy technology, such as SMS, with open standards. Text messages carry a greater security burden than ever before: One-time use and second-factor authentication codes designed to protect our most personal online accounts, such as Google and Facebook, as well as our online banking accounts, often are sent over text message. As currently implemented, RCS leaves those messages more open to interception than its technological predecessor, and the only way to secure them depends on mobile networks taking action.

By purchasing SIM cards from multiple carriers and checking which Internet addresses they connected to that were associated with RCS communications, Nohl and his colleagues at SR Labs were able to identify five ways to hack RCS texts. Many of them start with acquiring a SIM card from the targeted network, but that's not required in all cases.

From there, the hacker can exploit numerous misconfigurations of RCS for intercepting messages and calls. One involves a carrier sending a user a one-time code to verify their identity. Because RCS hasn't been configured to limit how many attempts the user can make, a hacker could try a brute-force attack to crack the one-time code by trying 1 million codes in five minutes; a successful attack would let the hacker fake that user's identity on the network.

The second attack involves sharing configuration files between the RCS-messaging app and the phone itself, which could let the hacker create an app that could take advantage of shared usernames and passwords to access texts and calls without alerting the user.

The third attack SR Labs discovered would allow a hacker with a fake mobile cell tower or Internet access point, or who is using the same legitimate tower or access point a target phone is using, to create and inject Internet traffic on to the phone.

The fourth enables the hacker to use RCS phones in denial-of-service attacks against a website by exploiting a command to automatically download a target file from the website. But this attack can also be used to track the IP address of the user, as well as take over the account of a user, if the RCS app sends back to the hacker the active-session token. The token is a small piece of software code that verifies the user and device's identity.

The fifth attack exploits signals from the RCS communication so that the hacker can maliciously set call forwarding, fake the user's identity on the network, redirect traffic to malicious websites and Web servers, and intercept all traffic to and from the device. Some of these attacks can be carried out with nothing more complicated than a rogue Wi-Fi hot spot, a known risk in public spaces such as coffee shops and airports.

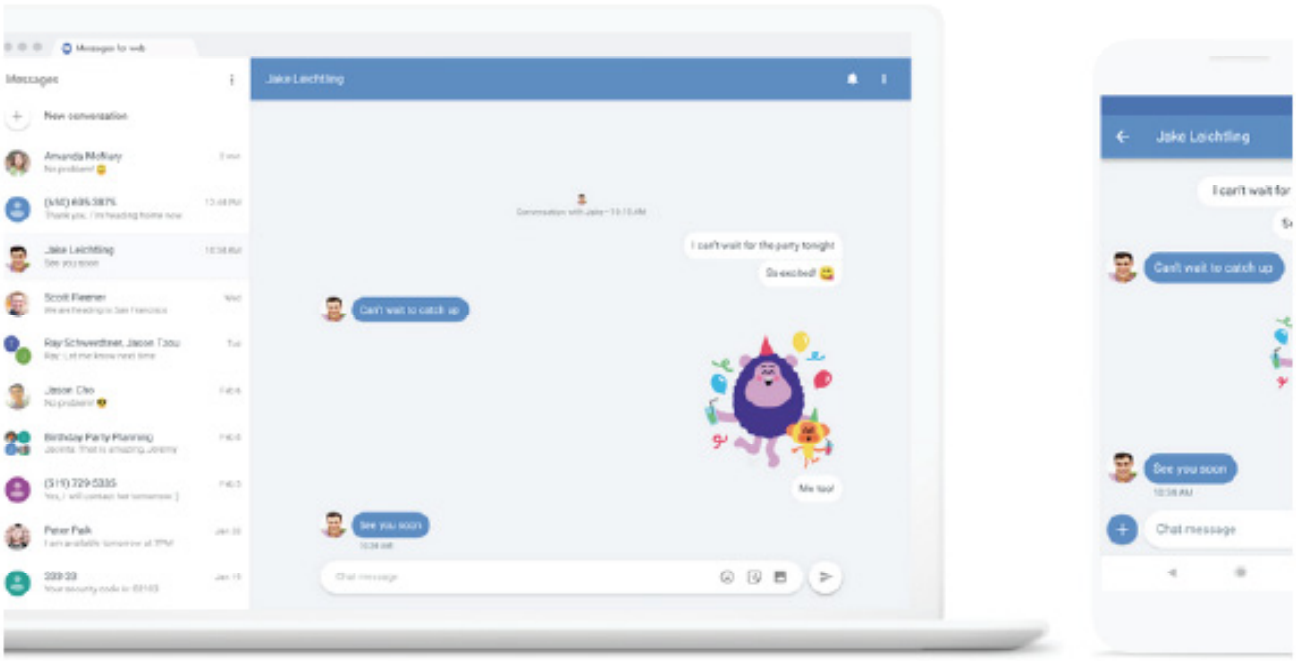
"The carriers are reinventing old security problems that the industry had previously solved," Nohl says. "Security responsibility in RCS has fragmented. Google controls the phone side but not the network side."

Since our original interview in November, Nohl has uncovered another method of intercepting RCS texts and calls that exploits how the messaging app validates the certificate. SR Labs plans to include this discovery in its Black Hat Europe presentation. If the attacker can redirect the domain name server to where the certificate is pointing, "the hacker can be in the middle of the encrypted connection," Nohl wrote in an email to The Parallax.

Because RCS is relatively new, and not as widespread as SMS, Nohl is hopeful that networks will take steps to fix their implementations of it. There haven't been enough consumers using RCS to make it worthwhile for hackers to exploit yet, he says. But as RCS use spreads with aggressive backing from Google and carriers, he believes that RCS will become an attractive target. And because each network has a slightly different implementation, he's concerned that RCS vulnerabilities are here to stay far longer than a stereotypical, ephemeral text.

"There's a clear progression in mobile security from 2G to 3G to 4G to 5G that each adds sensible security standards. But RCS tears holes into otherwise secure networks. As some standards are getting more secure, this one isn't," Nohl says.

Disclosure: PacSec's organizers covered part of The Parallax's conference travel expenses.



A mock-up of one of RCS's most-anticipated features that lets users send and receive text messages on their laptops. *Illustration courtesy Google.*

(https://the-parallax.com/wp-content/uploads/2019/12/PARALLAX-Google-RCS-mockup.png)

RCS delivers new texting features—and old security vulnerabilities

SETH ROSENBLATT (HTTPS://THE-PARALLAX.COM/AUTHOR/SETH-ROSENBLATT/) × DECEMBER 3, 2019

FEATURES (HTTPS://THE-PARALLAX.COM/CATEGORY/FEATURES/)

Share with:

TOKYO—Google is aggressively boosting a new technology standard for text messages called RCS that it thinks should replace SMS around the world (https://www.cnn.com/2019/11/15/business/google-rcs-android/index.html). But first, tech giants and telecommunications network providers will have to fix its major security flaws, researchers say.

RCS, or Rich Communication Services, brings a feature boost to the 30-year-old Short Message Service standard (http://news.bbc.co.uk/1/hi/uk/2538083.stm) to make texting more like messaging with iMessage or WhatsApp. RCS data is sent using an Internet address, which means that consumers whose mobile network providers support RCS (available on all four major U.S. networks, as well as more than 100 networks in 67 countries, many in Europe) can send and

receive messages, even when mobile network data is unavailable over Wi-Fi; they can receive "message read" notifications; they can send and receive high-quality photos and video; and they can see a three-dot ellipsis notification when the person with whom they're texting is in the process of writing a message.

Unlike similar but proprietary messaging services like those made by Apple and Facebook, RCS is designed to be an open standard that any tech company or network provider could support. Google has been advocating for RCS since 2015, when it acquired Jibe Mobile, the startup that invented the standard (https://venturebeat.com/2015/09/30/google-acquires-jibe-mobile-to-help-implement-the-rcs-carrier-messaging-standard-in-android/). RCS underpins a version of Google's Chat messaging app that the company debuted in the United Kingdom and France in June (https://www.cnn.com/2019/06/18/business/google-rcs-protocol-chat-android-imessage/index.html), and is now pushing globally.

READ MORE ON PHONE SECURITY AND PRIVACY

Android Q adds privacy, fragmentation (https://the-parallax.com/2019/05/10/android-q-fragmented-privacy-security/)
Google Play is an 'order of magnitude' better at blocking malware (https://the-parallax.com/2018/01/30/google-play-better-blocking-malware/)
Get a new phone? Consider your Fifth Amendment rights (https://the-parallax.com/2018/06/08/new-phone-fifth-amendment/)
For $3,900, DriveSavers says it can open locked smartphones (https://the-parallax.com/2018/12/06/drivesavers-unlock-iphone-android/)
Primer: Why are Androids less secure than iPhones? (https://the-parallax.com/2016/02/16/parallax-primer-why-are-androids-less-secure-than-iphones/)
How to FBI-proof your Android (https://the-parallax.com/2016/03/11/how-to-fbi-proof-your-android/)
How to wipe your phone (or tablet) for resale (https://the-parallax.com/2016/09/21/wipe-phone-resale/)

At the PacSec conference (https://pacsec.jp/) here in November, researchers at Berlin-based Security Research Labs presented (https://srlabs.de/bites/rcs-hacking/) security vulnerabilities in RCS texts and calls the company's founder and CEO, Karsten Nohl, had discovered. (They also presented their findings last week at DeepSec (https://deepsec.net/) in Austria, and plan to present an "extended set" of their findings again on Wednesday at Black Hat Europe (https://www.blackhat.com/eu-19/briefings/schedule/#mobile-network-hacking-ip-edition-17617) in London.)

Hackers with what Nohl describes as "basic" abilities could take advantage of RCS vulnerabilities to track users, conduct fraud, impersonate users, prevent users from sending texts using a denial-of-service attack (https://the-parallax.com/2018/06/13/primer-ddos-attacks-iot/) and, depending on the network, intercept texts. All of these actions, he stresses, can be prevented if network carriers implement widely used security protocols such as authenticating via the SIM card or secure chip on the phone; using "strong" one-time PIN codes (https://www.infobip.com/en/glossary/otp-one-time-pin-code) that are at least eight alphanumeric characters; using rate limiting to prevent attackers from trying an infinite series of OTP combinations; validating SIP sessions (https://www.networkworld.com/article/2332980/lan-wan-what-is-sip.html), which helps connect two or more devices to each other for voice and data calls; stripping sensitive information from SIP requests; and ensuring that Internet addresses linked to by certificates are validated.

"These are not structural hacks; these are avoidable mistakes," Nohl says. "We don't need to change the standard. It's just up to a few vendors to change their implementation to get it right."

RCS' vulnerabilities can impact devices running Google's Android mobile operating system, which currently account for about three-fourths of the world's smartphones (https://gs.statcounter.com/os-market-share/mobile/worldwide). They also can impact devices running Apple's iOS. Because iMessage is only end-to-end encrypted when a message is sent between two Apple devices, anytime an iPhone user texts with an Android user, the message is sent over whichever network protocol the carrier is using. Historically, that's been SMS, but as RCS becomes the standard for texting, it will increasingly be RCS, Nohl says.

Carriers Verizon, AT&T, T-Mobile, Sprint, Telefonica, and Google and Apple, did not respond to requests for comment. Australian carrier Optus declined to comment.

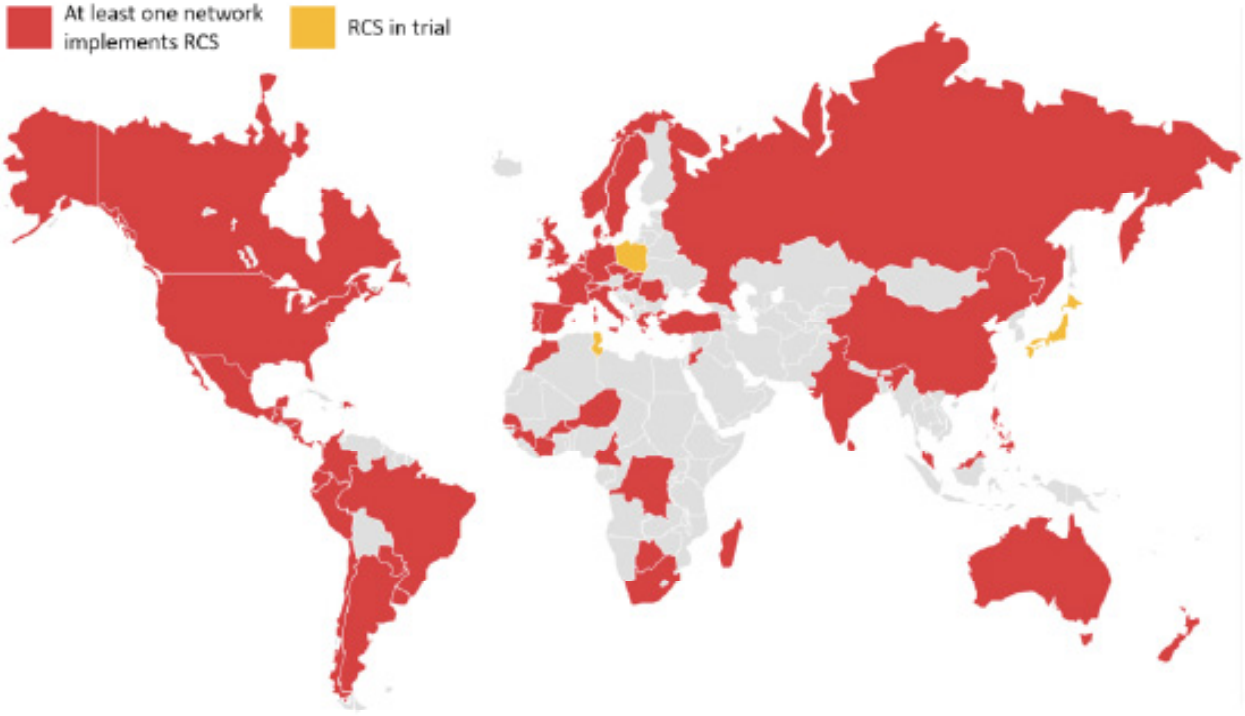
> *"The carriers are reinventing old security problems that the industry had previously solved."—Karsten Nohl, CEO, Security Research Labs.*

Deutsche Telekom spokesperson Christian Fischer said in an emailed statement that the network is "grateful for the feedback provided by the researchers." Fischer alleged that Deutsche Telekom has "further improved the RCS security measures already this week," but did not respond to requests to clarify what changes the network made.

Vodafone told The Parallax in an emailed statement that it is "aware" of the research. "We will review these protections in light of the research and, if required, take any further protective measures," Vodafone representative Otso Iho said.

The mobile network trade group GSM Association said in a statement to The Parallax that SR Labs' research is "complementary" to "an ongoing RCS risk assessment being conducted by the GSMA's Fraud and Security Group."

"Preliminary consideration of the research notes that countermeasures and mitigation actions are available to protect RCS implementations against the known vulnerabilities," GSM Association spokeswoman Claire Cranton wrote, adding that SR Labs is expected to present its findings to the GSM Association's Fraud and Security Group next week.



SR Labs map of global RCS use.

The struggle to secure RCS underscores challenges in improving legacy technology, such as SMS, with open standards. Text messages carry a greater security burden than ever before: One-time use and second-factor authentication codes (https://the-parallax.com/2015/10/22/how-to-set-up-two-factor-authentication/) designed to protect our most personal online accounts, such as Google and Facebook, as well as our online banking accounts, often are sent over text message. As currently implemented, RCS leaves those messages more open to interception than its technological predecessor, and the only way to secure them depends on mobile networks taking action.

By purchasing SIM cards from multiple carriers and checking which Internet addresses they connected to that were associated with RCS communications, Nohl and his colleagues at SR Labs were able to identify five ways to hack RCS texts. Many of them start with acquiring a SIM card from the targeted network, but that's not required in all cases.

From there, the hacker can exploit numerous misconfigurations of RCS for intercepting messages and calls. One involves a carrier sending a user a one-time code to verify their identity. Because RCS hasn't been configured to limit how many attempts the user can make, a hacker could try a brute-force (https://the-parallax.com/2016/12/29/flight-itinerary-boarding-pass-hacked/) attack to crack the one-time code by trying 1 million codes in five minutes; a successful attack would let the hacker fake that user's identity on the network.

Example hacking goal		Example method using RCS	Attack scope
Track users	A	Get IP address of victim / verify if user is online	These hacks should work against many RCS deployments as they do not require secret information about the victim; they do rely on configuration issues in the network
Impersonate users	B	Caller-ID spoofing in calls / messages	
Conduct fraud	C	Inject traffic / hijack session if victim is behind the same NAT	
Website DDoS	D	Send file attachment forcing auto-preview on victim	
Intercept texts	E	Connect to RCS with user credentials or hijack user session	Requires victim's config file or DNS MITM capabilities

SR Labs chart of RCS vulnerabilities.

The second attack involves sharing configuration files between the RCS-messaging app and the phone itself, which could let the hacker create an app that could take advantage of shared usernames and passwords to access texts and calls without alerting the user.

The third attack SR Labs discovered would allow a hacker with a fake mobile cell tower or Internet access point, or who is using the same legitimate tower or access point a target phone is using, to create and inject Internet traffic on to the phone.

The fourth enables the hacker to use RCS phones in denial-of-service attacks against a website by exploiting a command to automatically download a target file from the website. But this attack can also be used to track the IP address of the user, as well as take over the account of a user, if the RCS app sends back to the hacker the active-session token. The token is a small piece of software code that verifies the user and device's identity.

Area	Best practice	Implementation details	Affected components
Client provisioning	Authenticate using SIM / secure element	User authentication should be GBA/BSF based	RCS configuration server
	or		
	Use strong OTP verification codes	OTP should be at least 8 alphanumeric characters	RCS configuration server
	Apply rate limiting	Limit OTP validity to 5 minutes and 3 HTTP request attempts	RCS configuration server, SBC/P-CSCF
RCS services	Validate client identity	Validate SIP session using state (e.g. source IP, cookie, ...)	SBC/P-CSCF
	Avoid information leakage	Strip sensitive information from SIP requests	SBC/P-CSCF, RCS client
	Filter uploaded contents	Check/restrict content-type and size provided by clients	SBC/P-CSCF, FT server
RCS client	Enforce chain of trust	Connect only to trusted domains, validate certificates	RCS client, DNS

SR Labs chart of how to fix RCS security vulnerabilities.

The fifth attack exploits signals from the RCS communication so that the hacker can maliciously set call forwarding, fake the user's identity on the network, redirect traffic to malicious websites and Web servers, and intercept all traffic to and from the device. Some of these attacks can be carried out with nothing more complicated than a rogue Wi-Fi hot spot (https://the-parallax.com/2017/08/31/hackers-love-wi-fi-protect/), a known risk in public spaces such as coffee shops and airports.

"The carriers are reinventing old security problems that the industry had previously solved," Nohl says. "Security responsibility in RCS has fragmented. Google controls the phone side but not the network side."

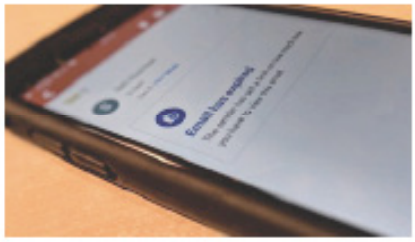
Since our original interview in November, Nohl has uncovered another method of intercepting RCS texts and calls that exploits how the messaging app validates the certificate. SR Labs plans to include this discovery in its Black Hat Europe presentation. If the attacker can redirect the domain name server to where the certificate is pointing, "the hacker can be in the middle of the encrypted connection," Nohl wrote in an email to The Parallax.

Because RCS is relatively new, and not as widespread as SMS, Nohl is hopeful that networks will take steps to fix their implementations of it. There haven't been enough consumers using RCS to make it worthwhile for hackers to exploit yet, he says. But as RCS use spreads with aggressive backing from Google and carriers, he believes that RCS will become an attractive target. And because each network has a slightly different implementation, he's concerned that RCS vulnerabilities are here to stay far longer than a stereotypical, ephemeral text.

"There's a clear progression in mobile security from 2G to 3G to 4G to 5G that each adds sensible security standards. But RCS tears holes into otherwise secure networks. As some standards are getting more secure, this one isn't," Nohl says.

Disclosure: PacSec's organizers covered part of The Parallax's conference travel expenses.

Related



(https://the-parallax.com/2018/12/10/gmail-confidential-mode-safe-bet/)
Is Gmail's Confidential Mode a safe bet? (https://the-parallax.com/2018/12/10/gmail-confidential-mode-safe-bet/)

(https://the-parallax.com/2016/01/12/want-end-to-end-encryption-use-these-apps/)
Want end-to-end encryption? Use these apps (https://the-parallax.com/2016/01/12/want-end-to-end-encryption-use-these-apps/)

(https://the-parallax.com/2016/08/01/send-money-securely/)
How to send money securely (https://the-parallax.com/2016/08/01/send-money-securely/)

ANDROID (HTTPS://THE-PARALLAX.COM/TAG/ANDROID/) APPLE (HTTPS://THE-PARALLAX.COM/TAG/APPLE/) GOOGLE (HTTPS://THE-PARALLAX.COM/TAG/GOOGLE/) IPHONE (HTTPS://THE-PARALLAX.COM/TAG/IPHONE/) KARSTEN NOHL (HTTPS://THE-PARALLAX.COM/TAG/KARSTEN-NOHL/) MOBILE (HTTPS://THE-PARALLAX.COM/TAG/MOBILE/) NETWORK (HTTPS://THE-PARALLAX.COM/TAG/NETWORK/) PACSEC (HTTPS://THE-PARALLAX.COM/TAG/PACSEC/) PACSEC 2019 (HTTPS://THE-PARALLAX.COM/TAG/PACSEC-2019/) RCS (HTTPS://THE-PARALLAX.COM/TAG/RCS/) RICH COMMUNICATION SERVICES (HTTPS://THE-PARALLAX.COM/TAG/RICH-COMMUNICATION-SERVICES/) SECURITY (HTTPS://THE-PARALLAX.COM/TAG/SECURITY/) SECURITY RESEARCH LABS (HTTPS://THE-PARALLAX.COM/TAG/SECURITY-RESEARCH-LABS/) SMARTPHONE (HTTPS://THE-PARALLAX.COM/TAG/SMARTPHONE/) SMS (HTTPS://THE-PARALLAX.COM/TAG/SMS/)

SETH ROSENBLATT (HTTPS://THE-PARALLAX.COM/AUTHOR/SETH-ROSENBLATT/)
EDITOR-IN-CHIEF

Seth is editor-in-chief and founder of The Parallax. He has worked in online journalism since 1999, including eight years at CNET News, where he led coverage of security, privacy, and Google. Based in San Francisco, he also writes about connected technology and pop culture.

https://www.randorisec.fr/deepsec-2019-training-conference-mobile-hacking/

02.12.2019

[TRAINING/CONFERENCE] DEEPSEC 2019

Training

During the DeepSec event, we gave our Mobile Hacking training (this training was also provided at Hack In Paris). This training presented the toolset needed when assessing mobile applications (such as adb, Apktool, Jadx, Androguard, Cycript, Frida, Needle and MobSF) and, also, the techniques to help you to work faster and in a more efficient way in the mobile ecosystem. This 2-days training focused on Android and iOS applications. The main topics of the training were:

Introduce the OWASP MSTG (Mobile Security Testing Guide) and the MASVS (Mobile Application Security Verification Standard)
Learn Android and iOS security basics
Know how to build an Android and iOS pentest toolset
Learn how to review the codebase of a mobile application (aka static analysis)
Run the mobile application on a rooted device (to check data security issues)
Inspect the app via instrumentation and manipulate the runtime (aka runtime analysis)
Man in The Middle all the network communications (aka inspect the traffic)
We had the pleasure to have 8 students following our training:DeepSec 2019 - Training students

We received really good feedbacks, especially regarding the hands-on exercices and the content of the training. In the case of the DeepSec event, the only limitation is the duration of the training. Students wanted a longer training to have time to go deeper on the topics presented.

That’s why we are going to provide a 3-days training at Hack in the Box. Don’t hesitate to register right now, if you want to enjoy the early bird (2599 euros) before 31st January!

Conference

Just after the trainings, the conference took place at the Imperial Riding School hotel during 2 days. Guillaume Lopes had the oportunity to present his research about the Google Play Billing API. If you want to know how to bypass the payment process on Android apps, you can download the slides

Regarding the other presentations, we really enjoyed the following ones:

Chinese Police and CloudPets

Abraham Aranguren presented the results of 3 different audits performed against Android applications. The first target was about the toy CloudPets. In short, it is a connected toy allowing parents to send messages to their kids using the toy. An Android app is used to interact with the connected toy. Abraham found many critical issues such as no HTTPS used for communication, S3 buckets open publicly with all the customers data, unprotected MongoDB, etc. The security was so bad that major resellers like Walmart and Amazon decided to remove CloudPets from their catalog!

Then, two other apps used by Chinese police were assessed: IJOP and BXAQ. For those apps, the objective was to find the information collected by the police. The IJOP app allows to collect information about the Muslim population and the type of data collected is really scaring (record of blood type, electricity usage at home, phone usage and especially if the phone becomes inactive, etc.). The BXAQ app is a trojan installed on tourist phones in order to collect many personal information such as contacts, calendar, phone calls, SMS, etc.). All the data collected is saved on a ZIP file on the SDCARD (sometimes it happens that the ZIP file is not correctly removed :)).

Mastering AWS Pentesting and Methodology

Ankit Giri reviewed the security best practices to set-up in AWS environments such as :

performing the inventory of your AWS account (the aws-inventory can be used to this purpose)

blocking public access to S3 buckets

enabling CloudWatch

enabling CloudTrail

setting Billing alerts

Finally, a demonstration of the tool Prowler was performed.

Saving Private Brian

Michael Burke presented various techniques to perform forensics analysis on iOS devices in order to identify if a malware/spyware is installed. The idea is not to use expensive tools but to manually perform a quick and dirty basic level forensic by checking:

the settings for modified configuration (VPN, profiles)

the installed apps (network / battery consumption, permissions)

your iCloud account (syncing, look me up, find my …)

suspicious safari “website data” statistics

He also explained a nice trick to obtain a lot of verbose logs: the sysdiagnose tool which can be triggered by pressing simultaneously the power button, the volume up and down buttons.

If you want a more complete overview of the presentations, Xavier Mertens already provided a complete wrap-up of the conference in his blog:

DeepSec 2019 Wrap-Up Day #1

DeepSec 2019 Wrap-Up Day #2

[TRAINING/CONFERENCE] DEEPSEC 2019

BY GUILLAUME LOPES | DECEMBER 2, 2019

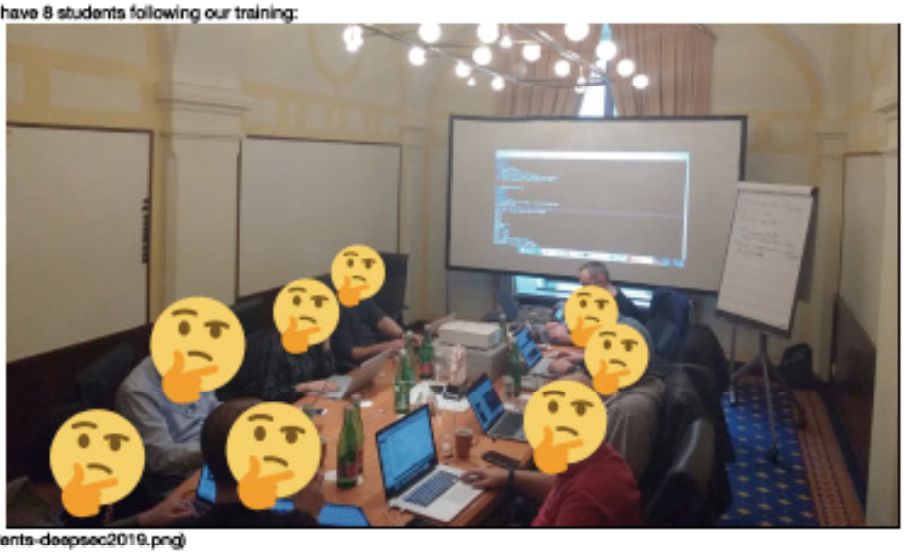
Training

During the DeepSec event, we gave our Mobile Hacking training (this training was also provided at Hack in Paris (https://hackinparis.com/)).

This training presented the toolset needed when assessing mobile applications (such as adb, Apktool, Jadx, Androguard, Cycript, Frida, Needle and MobSF) and, also, the techniques to help you to work faster and in a more efficient way in the mobile ecosystem. This 2-days training focused on Android and iOS applications. The main topics of the training were:

- Introduce the OWASP MSTG (Mobile Security Testing Guide) and the MASVS (Mobile Application Security Verification Standard)
- Learn Android and iOS security basics
- Know how to build an Android and iOS pentest toolset
- Learn how to review the codebase of a mobile application (aka static analysis)
- Run the mobile application on a rooted device (to check data security issues)
- Inspect the app via instrumentation and manipulate the runtime (aka runtime analysis)
- Man in The Middle all the network communications (aka inspect the traffic)

We had the pleasure to have 8 students following our training:



(/img/blog/training-students-deepsec2019.png)

We received really good feedbacks, especially regarding the hands-on exercices and the content of the training. In the case of the DeepSec event, the only limitation is the duration of the training. Students wanted a longer training to have time to go deeper on the topics presented.

That's why we are going to provide a 3-days training at Hack in the Box (https://conference.hitb.org/hitbsecconf2020ams/sessions/3-day-training-8-mobile-hacking-training/). Don't hesitate to register right now, if you want to enjoy the early bird (2599 euros) before 31st January!

Conference

Just after the trainings, the conference took place at the Imperial Riding School hotel during 2 days. Guillaume Lopes (https://twitter.com/@Guillaume_Lopes) had the oportunity to present his research about the Google Play Billing API. If you want to know how to bypass the payment process on Android apps, you can download the slides (/publications/DeepSec2019-Abusing_Google_Play_Billing_for_fun_and_unlimited_credits.pdf)

Regarding the other presentations, we really enjoyed the following ones:

Chinese Police and CloudPets

Abraham Aranguren presented the results of 3 different audits performed against Android applications. The first target was about the toy CloudPets. In short, it is a connected toy allowing parents to send messages to their kids using the toy. An Android app is used to interact with the connected toy. Abraham found many critical issues such as no HTTPS used for communication, S3 buckets open publicly with all the customers data, unprotected MongoDB, etc. The security was so bad that major resellers like Walmart and Amazon decided to remove CloudPets from their catalog!

Then, two other apps used by Chinese police were assessed: IJOP and BXAQ. For those apps, the objective was to find the information collected by the police. The IJOP app allows to collect information about the Muslim population and the type of data collected is really scaring (record of blood type, electricity usage at home, phone usage and especially if the phone becomes inactive, etc.). The BXAQ app is a trojan installed on tourist phones in order to collect many personal information such as contacts, calendar, phone calls, SMS, etc.). All the data collected is saved on a ZIP file on the SDCARD (sometimes it happens that the ZIP file is not correctly removed :)).

Mastering AWS Pentesting and Methodology

Ankit Giri reviewed the security best practices to set-up in AWS environments such as :

- performing the inventory of your AWS account (the aws-inventory (https://github.com/nccgroup/aws-inventory) can be used to this purpose)
- blocking public access to S3 buckets
- enabling CloudWatch
- enabling CloudTrail
- setting Billing alerts

Finally, a demonstration of the tool Prowler (https://github.com/toniblyx/prowler) was performed.

Saving Private Brian

Michael Burke presented various techniques to perform forensics analysis on iOS devices in order to identify if a malware/spyware is installed. The idea is not to use expensive tools but to manually perform a quick and dirty basic level forensic by checking:

- the settings for modified configuration (VPN, profiles)
- the installed apps (network / battery consumption, permissions)
- your iCloud account (syncing, look me up, find my ...)
- suspicious safari "website data" statistics

He also explained a nice trick to obtain a lot of verbose logs: the sysdiagnose tool which can be triggered by pressing simultaneously the power button, the volume up and down buttons.

If you want a more complete overview of the presentations, Xavier Mertens (https://twitter.com/xme) already provided a complete wrap-up of the conference in his blog:

- DeepSec 2019 Wrap-Up Day #1 (https://blog.rootshell.be/2019/11/29/deepsec-2019-wrap-up-day-1/)
- DeepSec 2019 Wrap-Up Day #2 (https://blog.rootshell.be/2019/11/29/deepsec-2019-wrap-up-day-2/)

SEARCH

Search

CATEGORIES

0day (10) (https://www.randorisec.fr/categories/0day)

bugbounty (2) (https://www.randorisec.fr/categories/bugbounty)

conference (10) (https://www.randorisec.fr/categories/conference)

general (5) (https://www.randorisec.fr/categories/general)

gestion-de-crise (1) (https://www.randorisec.fr/categories/gestion-de-crise)

pentest (27) (https://www.randorisec.fr/categories/pentest)

publications (12) (https://www.randorisec.fr/categories/publications)

responsible_disclosure (12) (https://www.randorisec.fr/categories/responsible_disclosure)

swift (1) (https://www.randorisec.fr/categories/swift)

training (9) (https://www.randorisec.fr/categories/training)

TAGS

0DAY (HTTPS://WWW.RANDORISEC.FR/TAGS/0DAY) ANDROID (HTTPS://WWW.RANDORISEC.FR/TAGS/ANDROID)

ANTIVIRUS (HTTPS://WWW.RANDORISEC.FR/TAGS/ANTIVIRUS) ASTERISK (HTTPS://WWW.RANDORISEC.FR/TAGS/ASTERISK)

BIAIS-COGNITIFS (HTTPS://WWW.RANDORISEC.FR/TAGS/BIAIS-COGNITIFS)

BUG-BOUNTY (HTTPS://WWW.RANDORISEC.FR/TAGS/BUG-BOUNTY) BUGBOUNTY (HTTPS://WWW.RANDORISEC.FR/TAGS/BUGBOUNTY)

BULL (HTTPS://WWW.RANDORISEC.FR/TAGS/BULL) BURP (HTTPS://WWW.RANDORISEC.FR/TAGS/BURP)

CAMERA (HTTPS://WWW.RANDORISEC.FR/TAGS/CAMERA) CERT (HTTPS://WWW.RANDORISEC.FR/TAGS/CERT)

CERT-EU (HTTPS://WWW.RANDORISEC.FR/TAGS/CERT-EU) CHECKMARX (HTTPS://WWW.RANDORISEC.FR/TAGS/CHECKMARX)

CLIENT-SIDE (HTTPS://WWW.RANDORISEC.FR/TAGS/CLIENT-SIDE) CLUSIF (HTTPS://WWW.RANDORISEC.FR/TAGS/CLUSIF)

https://e-commerce.blog/deepsec-2019-wrap-up-day-2/

30.11.2019

DeepSec 2019 Wrap-Up Day #2

Here we amble for the second wrap-up! DeepSec is over, flying again the following day to Belgium. My first different nowadays was to lend a hand: “How To Produce a Botnet of GSM-devices” by Aleksandr Kolchanov. Don’t neglect that GSM devices are no longer finest “telephones”. Aleksandr lined good devices dangle apprehension systems, electric sockets, tidy-home controllers, industrial controllers, trackers and… smartwatches for youth!

They all possess aspects dangle to ship notifications by strategy of SMS, call pre-configured numbers nonetheless additionally be configured or polled by strategy of SMS. Instance of assaults? Brute-power the PIN code, spoof calls, use “hidden” SMS commands. Ok, nonetheless what are the reasons to hack them? We possess say assaults (free up the door, consume stuff) or spying: abuse the constructed-in microphone. Attacks on the property are additionally involving: switch off electric devices (a water pump, a heating gadget). Also terrorism or political actions? Monetary assaults (call or ship SMS to premium numbers). Why a botnet? The salvage some money! Moral use it to ship gigantic amounts of SMS nonetheless additionally to DoS or for political/terrorism actions: Can you imagine hundreds of alarms at the same time. Attributable to worthy advertising and marketing, members capture them so we now possess many devices in the wild:

Default settings Boring vulnerabilitiesNot effectively installed Panicked by default Cheap! Absence of certification After the introduction, Aleksandr explained how he performed assaults against diversified devices. It’s straightforward to hack them nonetheless the actual articulate is to bag targets. How? It’s doubtless you’ll well presumably also invent a mass scanning and call all numbers nonetheless it with out a doubt will rate money and some operators will detect you (“Why are your calling xxx times per day?”) search with out making a call? They’re web products and companies equipped by some operators that lend a hand to salvage info about aged numbers, they’re starting up API, databases, leaked data, and tons others… If it is doubtless you’ll well presumably possess enough legit devices, it’s time to device the botnet:

Scan>Name>Attack>Commerce settings>Profit!

It was an involving talk over with kick off the day!

The next talk was about… pacemakers! Wait, the complete lot has been said about these devices, actual? A lot

of field cloth has already been published. The extensive myth was in 2017 when a big flaw was stumbled on. The debate introduced by Tobias Zillner was called “500.000 Recalled Pacemakers, 2 Billion $ Inventory Brand Loss – The Yarn On the again of”.

When or no longer it is far a have to want to assess such scientific devices, where to salvage one? On a second-hand webshop! Moral possess a glimpse at dotmed.com, their inventory of scientific devices is awesome! The eco-gadget tested was: pacemakers / programmers/home monitors and the “Merlin Accumulate” alias “the cloud”. The well-known attack vector lined by Tobias was the fresh period of devices that use wireless applied sciences (SDR), low energy, short-fluctuate (2M) – 401-406Mhz). bag technical specs? Moral test the FCC-ID and impress for it. Google remains constantly your finest buddy. The vulnerabilities stumbled on possess been an energy depletion attack (draining the battery) and a… break of the pacemaker! The next target was the “Merlin@Dwelling” instrument which is a home monitoring gadget. They’re straightforward to bag on eBay:

Moral raze an attack dangle against any embedded Linux instrument: Connect a console, boot it, press a key to salvage the bootloader, commerce the boot record add “init=/bin/bash” dangle every Linux and boot in single-consumer mode! As soon as during the box, it’s straightforward to bag relatively a ramification of data left by developers (offer code, SSH keys, encryption keys, offer code, … The second half of the controversy was dedicated to the total-disclosure process.

After a transient espresso spoil, Fabio Nigi introduced “IPFS As a Dispensed Various to Logs Assortment”. The premise leisurely this talk was to possess a look at out to clear up a classic headache for people that are fascinated by log management projects. This can like a flash become a nightmare as a outcome of the ever-altering topologies, the series of sources, quantity of logs to build up and process. Storage is a trouble to manage.

So, Fabio had the foundation to use IPFS. IPFS skill “Interplanetary file gadget” and is a P2P distributed file gadget that helps to store data in a pair of areas. He introduced the instrument, how it genuinely works (it search for involving, I wasn’t aware about it). Then he demonstrated interconnect it with a log series answer the usage of diversified tools dangle IPFS GW, React, Brig or Minerva. It’s an involving plan, then as soon as more, the venture is soundless in the vogue phase (as said on the gain page)…

There possess been many involving talks nowadays and, with a twin-track convention, it’s no longer constantly straightforward to secure the particular person that might be the most involving or involving. My next different was “Extracting a 19-Year-Feeble Code Execution from WinRAR” by Nadav Grossman.

WinRAR is a effectively-recognized instrument to handle many archive codecs. Because the instrument is terribly neatly-liked, it's a important target for attackers since it is far installed on many computer systems! After a truly long half about fuzzing (the tactics, tools dangle WinAFL), Nadav explained how the vulnerability was stumbled on. It was located in a DLL aged to process ACE data. Many critical aspects possess been disclosed and, in the event it is doubtless you'll well presumably very effectively be , there is a blog post on hand here. Label that since the vulnerability has been stumbled on and disclosed, the enhance of ACE archives has been eradicated from the rest versions of WinRAR!

After the lunch spoil, I attended "Constructing an Opensource Risk Detection Program" by Lance Buttars (Ingo Cash). This was an involving discuss tools which that you just can deploy to offer protection to your web products and companies nonetheless additionally counterattack the irascible guys. Many tools are aged in Lance's arsenal (ModSecurity, Reverse proxies, Fail2ban, and tons others…)

Lance additionally explained what honeypots are and the diversified forms of data that you just accumulate: domains, data, ports, SQL tables or DB. For every kind, he gave some examples. Label that "crammed with life defense" is no longer allowed in many countries!

And the day persevered with "As soon as Upon a Time in the West – A myth on DNS Attacks" by Valentina Palacín and Ruth Esmeralda Barbacil. They reviewed effectively-recognized DNS attack tactics (DNS tunneling, hijacking, and poisoning) then they introduced a timeline of well-known threats that affected DNS products and companies and that abused the protocols dangle:

DNSChangerOperation Ghost ClickSyrian Electronic ArmyCraiglist HijackedOilrig: Suspected Iranian Mission Sauron (suspected USA)Darkhydrus (Bernhard PoSFIN7DNSpionageSeaTurtleFor each of them, they utilized the Mitre ATT&CK framework. Nothing genuinely fresh nonetheless an actual recap which concludes that DNS is a key protocol and that it needs to be fastidiously controlled.

The 2 next talks centered more on penetration testing: "What's Substandard with WebSocket APIs? Unveiling Vulnerabilities in WebSocket APIs" by Mikhail Egorov. He already published relatively a ramification of researches spherical WebSocket and started with a overview of the protocol. Then he described diversified forms of assaults. The second one was "Abusing Google Play Billing for Fun and Unlimited Credits!" by Guillaume Lopes. Guillaume explained how Google offers a payment framework for developers. Just like the earlier talk, it started with a over-

view of the framework then how it was abused. He tested 50 apps, 29 possess been prone to this attack. All developers possess been contacted and finest 1 responded!

To close the day, Robert Sell introduced “Tactics and Tools for Becoming an Intelligence Operator“. Initiate-offer intelligence will also be aged in many fields: forensics, study, and tons others. Robert defines it as “Recordsdata that’s no longer easy to bag nonetheless freely on hand”.

He explained put collectively your self to raze investigations, which tools to use, community connections, introduction of profiles on social community and tons more. The checklist of tools and URLs equipped by Robert was extraordinary! Don’t neglect that actual OpSec is serious. For of us that’re aroused to see for data about your target, (s)he received’t potentially be as aroused as you! Also, remember, that every tactics aged can additionally be aged against you!

That’s all Of us! DeepSec is over! Thanks as soon as more to the organizers for a important tournament!

The E-Commerce Blog

Delivering the best E-Commerce News

E-COMMERCE

DeepSec 2019 Wrap-Up Day #2

By ecb - November 30, 2019

Time to Read: 7 min - 1408 words

Here we amble for the second wrap-up! DeepSec is over, flying again the following day to Belgium. My first different nowadays was to lend a hand: "How To Produce a Botnet of GSM-devices" by Aleksandr Kolchanov. Don't neglect that GSM devices are no longer finest "telephones". Aleksandr lined good devices dangle apprehension systems, electric sockets, tidy-home controllers, industrial controllers, trackers and... smartwatches for youth!

They all possess aspects dangle to ship notifications by strategy of SMS, call pre-configured numbers nonetheless additionally be configured or polled by strategy of SMS. Instance of assaults? Brute-power the PIN code, spoof calls, use "hidden" SMS commands. Ok, nonetheless what are the reasons to hack them? We possess say assaults (free up the door, consume stuff) or spying: abuse the constructed-in microphone. Attacks on the property are additionally involving: switch off electric devices (a water pump, a heating gadget). Also terrorism or political actions? Monetary assaults (call or ship SMS to premium numbers). Why a botnet? The salvage some money! Moral use it to ship gigantic amounts of SMS nonetheless additionally to DoS or for political/terrorism

actions: Can you imagine hundreds of alarms at the same time. Attributable to worthy advertising and marketing, members capture them so we now possess many devices in the wild:

Default settings Boring vulnerabilitiesNot effectively installed Panicked by default Cheap! Absence of certification After the introduction, Aleksandr explained how he performed assaults against diversified devices. It's straightforward to hack them nonetheless the actual articulate is to bag targets. How? It's doubtless you'll well presumably also invent a mass scanning and call all numbers nonetheless it with out a doubt will rate money and some operators will detect you ("Why are your calling xxx times per day?") search with out making a call? They're web products and companies equipped by some operators that lend a hand to salvage info about aged numbers, they're starting up API, databases, leaked data, and tons others... If it is doubtless you'll well presumably possess enough legit devices, it's time to device the botnet:

Scan>Name>Attack>Commerce settings>Profit!

It was an involving talk over with kick off the day!

The next talk was about... pacemakers! Wait, the complete lot has been said about these devices, actual? A lot of field cloth has already been published. The extensive myth was in 2017 when a big flaw was stumbled on. The debate introduced by Tobias Zillner was called "500.000 Recalled Pacemakers, 2 Billion $ Inventory Brand Loss – The Yarn On the again of".

When or no longer it is far a have to want to assess such scientific devices, where to salvage one? On a second-hand webshop! Moral possess a glimpse at dotmed.com, their inventory of scientific devices is awesome! The eco-gadget tested was: pacemakers / programmers/home monitors and the "Merlin Accumulate" alias "the cloud". The well-known attack vector lined by Tobias was the fresh period of devices that use wireless applied sciences (SDR), low energy, short-fluctuate (2M) – 401-406Mhz). bag technical specs? Moral test the FCC-ID and impress for it. Google remains constantly your finest buddy. The vulnerabilities stumbled on possess been an energy depletion attack (draining the battery) and a... break of the pacemaker! The next target was the "Merlin@Dwelling" instrument which is a home monitoring gadget. They're straightforward to bag on eBay:

Moral raze an attack dangle against any embedded Linux instrument: Connect a console, boot it, press a key to salvage the bootloader, commerce the boot record add "init=/bin/bash" dangle every Linux and boot in single-consumer mode! As soon as during the box, it's straightforward to bag relatively a ramification of data left by developers (offer code, SSH keys, encryption keys,

offer code, … The second half of the controversy was dedicated to the total-disclosure process.

After a transient espresso spoil, Fabio Nigi introduced "IPFS As a Dispensed Various to Logs Assortment". The premise leisurely this talk was to possess a look at out to clear up a classic headache for people that are fascinated by log management projects. This can like a flash become a nightmare as a outcome of the ever-altering topologies, the series of sources, quantity of logs to build up and process. Storage is a trouble to manage.

So, Fabio had the foundation to use IPFS. IPFS skill "Interplanetary file gadget" and is a P2P distributed file gadget that helps to store data in a pair of areas. He introduced the instrument, how it genuinely works (it search for involving, I wasn't aware about it). Then he demonstrated interconnect it with a log series answer the usage of diversified tools dangle IPFS GW, React, Brig or Minerva. It's an involving plan, then as soon as more, the venture is soundless in the vogue phase (as said on the gain page)…

There possess been many involving talks nowadays and, with a twin-track convention, it's no longer constantly straightforward to secure the particular person that might be the most involving or involving. My next different was "Extracting a 19-Year-Feeble Code Execution from WinRAR" by Nadav Grossman.

WinRAR is a effectively-recognized instrument to handle many archive codecs. Because the instrument is terribly neatly-liked, it's a important target for attackers since it is far installed on many computer systems! After a truly long half about fuzzing (the tactics, tools dangle WinAFL), Nadav explained how the vulnerability was stumbled on. It was located in a DLL aged to process ACE data. Many critical aspects possess been disclosed and, in the event it is doubtless you'll well presumably very effectively be , there is a blog post on hand here. Label that since the vulnerability has been stumbled on and disclosed, the enhance of ACE archives has been eradicated from the rest versions of WinRAR!

After the lunch spoil, I attended "Constructing an Opensource Risk Detection Program" by Lance Buttars (Ingo Cash). This was an involving discuss tools which that you just can deploy to offer protection to your web products and companies nonetheless additionally counterattack the irascible guys. Many tools are aged in Lance's arsenal (ModSecurity, Reverse proxies, Fail2ban, and tons others…)

Lance additionally explained what honeypots are and the diversified forms of data that you just accumulate: domains, data, ports, SQL tables or DB. For every kind, he gave some examples. Label that "crammed with life defense" is no longer allowed in many countries!

And the day persevered with "As soon as Upon a Time in the West – A myth on DNS Attacks" by Valentina Palacín and Ruth Esmeralda Barbacil. They reviewed effectively-recognized DNS attack tactics (DNS tunneling, hijacking, and poisoning) then they introduced a timeline of well-known threats that affected DNS products and companies and that abused the protocols dangle:

DNSChangerOperation Ghost ClickSyrian Electronic ArmyCraiglist HijackedOilrig: Suspected Iranian Mission Sauron (suspected USA)Darkhydrus (Bernhard PoSFIN7DNSpionageSeaTurtleFor each of them, they utilized the Mitre ATT&CK framework. Nothing genuinely fresh nonetheless an actual recap which concludes that DNS is a key protocol and that it needs to be fastidiously controlled.

The 2 next talks centered more on penetration testing: "What's Substandard with WebSocket APIs? Unveiling Vulnerabilities in WebSocket APIs" by Mikhail Egorov. He already published relatively a ramification of researches spherical WebSocket and started with a overview of the protocol. Then he described diversified forms of assaults. The second one was "Abusing Google Play Billing for Fun and Unlimited Credits!" by Guillaume Lopes. Guillaume explained how Google offers a payment framework for developers. Just like the earlier talk, it started with a overview of the framework then how it was abused. He tested 50 apps, 29 possess been prone to this attack. All developers possess been contacted and finest 1 responded!

To close the day, Robert Sell introduced "Tactics and Tools for Becoming an Intelligence Operator". Initiate-offer intelligence will also be aged in many fields: forensics, study, and tons others. Robert defines it as "Recordsdata that's no longer easy to bag nonetheless freely on hand".

He explained put collectively your self to raze investigations, which tools to use, community connections, introduction of profiles on social community and tons more. The checklist of tools and URLs equipped by Robert was extraordinary! Don't neglect that actual OpSec is serious. For of us that're aroused to see for data about your target, (s)he received't potentially be as aroused as you! Also, remember, that every tactics aged can additionally be aged against you!

That's all Of us! DeepSec is over! Thanks as soon as more to the organizers for a important tournament!

Read more!

Tag: #DeepSec #ecommerce #Wrap-Up

https://blog.rootshell.be/2019/11/29/deepsec-2019-wrap-up-day-2/

DeepSec 2019 Wrap-Up Day #2

29.11.2019

Here we go for the second wrap-up! DeepSec is over, flying back tomorrow to Belgium. My first choice today was to attend: “How To Create a Botnet of GSM-devices” by Aleksandr Kolchanov. Don’t forget that GSM devices are not only “phones”. Aleksandr covered nice devices like alarm systems, electric sockets, smart-home controllers, industrial controllers, trackers and… smartwatches for kids!

They all have features like to send notifications via SMS, call pre-configured numbers but also be configured or polled via SMS. Example of attacks? Brute-force the PIN code, spoof calls, use “hidden” SMS commands. Ok, but what are the reasons to hack them? We have direct attacks (unlock the door, steal stuff) or spying: abuse the built-in microphone. Attacks on the property are also interesting: switch off electric devices (a water pump, a heating system). Also terrorism or political actions? Financial attacks (call or send SMS to premium numbers). Why a botnet? The get some money! Just use it to send huge amounts of SMS but also to DoS or for political/terrorism actions: Can you imagine thousands of alarms at the same time. Thanks to powerful marketing, people buy them so we have many devices in the wild:

Default settings
Stupid vulnerabilities
Not properly installed
Insecure by default
Cheap!
Absence of certification

After the introduction, Aleksandr explained how he performed attacks against different devices. It’s easy to hack them but the real challenge is to find targets. How? You can do a mass scanning and call all numbers but it will cost money and some operators will detect you (“Why are your calling xxx times per day?”) How to search without making a call? They are web services provided by some operators that help to get info about used numbers, they are open API, databases, leaked data, etc… Once you have enough valid devices, it’s time to build the botnet:

Scan > Identify > Attack > Change settings > Profit!

It was an interesting talk to kick off the day!

The next talk was about… pacemakers! Wait, everything has been said about those devices, right? A lot of material has already been published. The big story was in 2017 when a big flaw was discovered. The talk presented by Tobias Zillner was called “500.000 Recalled Pacemakers, 2 Billion $ Stock Value Loss – The Story Behind”.

When you need to assess such medical devices, where to get one? On a second-hand webshop! Just have a look at dotmed.com, their stock of medical devices is awesome! The eco-system tested was: pacemakers / programmers/home monitors and the “Merlin Net” alias “the cloud”. The first attack vector covered by Tobias was the new generation of devices that use wireless technologies (SDR), low power, short-range (2M) – 401-406Mhz). How to find technical specs? Just check the FCC-ID and search for it. Google remains always your best friend. The vulnerabilities found were an energy depletion attack (draining the battery) and a… crash of the pacemaker! The next target was the “Merlin@Home” device which is a home monitoring system. They are easy to find on eBay:

Just perform an attack like against any embedded Linux device: Connect a console, boot it, press a key to get the bootloader, change the boot command add “init=/bin/bash” like any Linux and boot in single-user mode! Once inside the box, it’s easy to find a lot of data left by developers (source code, SSH keys, encryption keys, source code, … The second part of the talk was dedicated to the full-disclosure process.

After a short coffee break, Fabio Nigi presented “IPFS As a Distributed Alternative to Logs Collection”. The idea behind this talk was to try to solve a classic headache for people who are involved in log management tasks. This can quickly become a nightmare due to the ever-changing topologies, the number of assets, amount of logs to collect and process. Storage is a pain to manage.

So, Fabio had the idea to use IPFS. IPFS means “Interplanetary file system” and is a P2P distributed file system that helps to store files in multiple locations. He introduced the tool, how it works (it look interesting, I wasn’t aware of it). Then he demonstrated how to interconnect it with a log collection solution using different tools like IPFS GW, React, Brig or Minerva. It’s an interesting approach, however, the project is still in the development phase (as stated on the website)…

There were many interesting talks today and, with a dual-track conference, it's not always easy to choose the one that will be the most entertaining or interesting. My next choice was "Extracting a 19-Year-Old Code Execution from WinRAR" by Nadav Grossman.

WinRAR is a well-known tool to handle many archive formats. As the tool is very popular, it's a great target for attackers because it is installed on many computers! After a very long part about fuzzing (the techniques, tools like WinAFL), Nadav explained how the vulnerability was found. It was located in a DLL used to process ACE files. Many details were disclosed and, if you are interested, there is a blog post available here. Note that since the vulnerability has been found and disclosed, the support of ACE archives has been removed from the last versions of WinRAR!

After the lunch break, I attended "Setting up an Opensource Threat Detection Program" by Lance Buttars (Ingo Money). This was an interesting talk about tools that you can deploy to protect your web services but also counter-attack the bad guys. Many tools are used in Lance's arsenal (ModSecurity, Reverse proxies, Fail2ban, etc…)

Lance also explained what honeypots are and the different types of data that you collect: domains, files, ports, SQL tables or DB. For each type, he gave some examples. Note that "active defense" is not allowed in many countries!

And the day continued with "Once Upon a Time in the West – A story on DNS Attacks" by Valentina Palacín and Ruth Esmeralda Barbacil. They reviewed well-known DNS attack techniques (DNS tunneling, hijacking, and poisoning) then they presented a timeline of major threats that affected DNS services and that abused the protocols like:

DNSChangerOperation Ghost Click
Syrian Electronic Army
Craiglist Hijacked
Oilrig: Suspected Iranian
Project Sauron (suspected USA)Darkhydrus (
Bernhard PoS
FIN7

DNSpionage

SeaTurtle

For each of them, they applied the Mitre ATT&CK framework. Nothing really new but a good recap which concludes that DNS is a key protocol and that it must be carefully controlled.

The two next talks focused more on penetration testing: “What’s Wrong with WebSocket APIs? Unveiling Vulnerabilities in WebSocket APIs“
by Mikhail Egorov. He already published a lot of researches around WebSocket and started with a review of the protocol. Then he described different types of attacks. The second one was “Abusing Google Play Billing for Fun and Unlimited Credits!” by Guillaume Lopes. Guillaume explained how Google provides a payment framework for developers. Like the previous talk, it started with a review of the framework then how it was abused. He tested 50 apps, 29 were vulnerable to this attack. All developers were contacted and only 1 replied!

To close the day, Robert Sell presented “Techniques and Tools for Becoming an Intelligence Operator“. Open-source intelligence can be used in many fields: forensics, research, etc. Robert defines it as “Information that is hard to find but freely available”.

He explained how to prepare yourself to perform investigations, which tools to use, network connections, creation of profiles on social network and many more. The list of tools and URLs provided by Robert was amazing! Don’t forget that good OpSec is important. If you’re excited to search for information about your target, (s)he won’t probably be as excited as you! Also, keep in mind, that all techniques used can also be used against you!

That’s all Folks! DeepSec is over! Thanks again to the organizers for a great event!

孫子兵法 /dev/random

"If the enemy leaves a door open, you must rush in." – Sun Tzu

Search ...

About Me | Disclaimer | Tools

DeepSec 2019 Wrap-Up Day #2

November 29, 2019 Event, Security Leave a comment

Here we go for the second wrap-up! DeepSec is over, flying back tomorrow to Belgium. My first choice today was to attend: "*How To Create a Botnet of GSM-devices*" by Aleksandr Kolchanov. Don't forget that GSM devices are not only "phones". Aleksandr covered nice devices like alarm systems, electric sockets, smart-home controllers, industrial controllers, trackers and... smartwatches for kids!

Stay in Touch

Upcoming Events

Here is a list of events that I will attend and cover via Twitter and wrap-ups. Ping me if you want to meet! The list is regularly updated.

Recent Articles

- [SANS ISC] Code & Data Reuse in the Malware Ecosystem

They all have features like to send notifications via SMS, call pre-configured numbers but also be configured or polled via SMS. Example of attacks? Brute-force the PIN code, spoof calls, use "hidden" SMS commands. Ok, but what are the reasons to hack them? We have direct attacks (unlock the door, steal stuff) or spying: abuse the built-in microphone. Attacks on the property are also interesting: switch off electric devices (a water pump, a heating system). Also terrorism or political actions? Financial attacks (call or send SMS to premium numbers). Why a botnet? The get some money! Just use it to send huge amounts of SMS but also to DoS or for political/terrorism actions: Can you imagine thousands of alarms at the same time. Thanks to powerful marketing, people buy them so we have many devices in the wild:

- Default settings
- Stupid vulnerabilities
- Not properly installed
- Insecure by default
- Cheap!
- Absence of certification

BotConf 2019 Wrap-Up Day #3
BotConf 2019 Wrap-Up Day #2
BotConf 2019 Wrap-Up Day #1
DeepSec 2019 Wrap-Up Day #2

Popular Articles

Show me your SSID's, I'll Tell Who You Are!
37,808 views

Keep an Eye on SSH Forwarding!
36,151 views

Sending Windows Event Logs to Logstash
29,489 views

Socat, Another Network Swiss Army Knife
26,019 views

Check Point Firewall Logs and Logstash (ELK) Integration
25,759 views

Forensics: Reconstructing Data from Pcap Files
21,839 views

dns2tcp: How to bypass firewalls or

After the introduction, Aleksandr explained how he performed attacks against different devices. It's easy to hack them but the real challenge is to find targets. How? You can do a mass scanning and call all numbers but it will cost money and some operators will detect you ("Why are your calling xxx times per day?") How to search without making a call? They are web services provided by some operators that help to get info about used numbers, they are open API, databases, leaked data, etc... Once you have enough valid devices, it's time to build the botnet:

```
Scan > Identify > Attack > Change settings > Profit!
```

It was an interesting talk to kick off the day!

The next talk was about... pacemakers! Wait, everything has been said about those devices, right? A lot of material has already been published. The big story was in 2017 when a big flaw was discovered. The talk presented by Tobias Zillner was called "*500.000 Recalled Pacemakers, 2 Billion $ Stock Value Loss – The Story Behind*".

When you need to assess such medical devices, where to get one? On a second-hand webshop! Just have a look at dotmed.com, their stock of medical devices is awesome! The

captive portals?
20,874 views

- Vulnerability Scanner within Nmap
18,678 views

- Post-BruCON Experience - Running a Wall of Sheep in the Wild
17,357 views

- Bash: History to Syslog
15,434 views

Recent Tweets

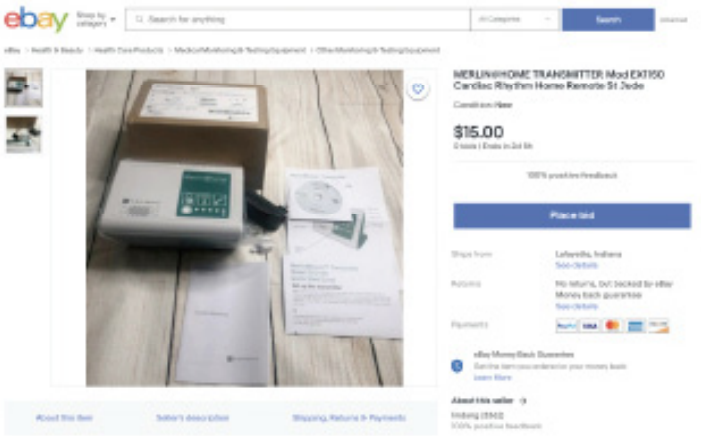
What are the top techniques used by adversaries? @likethecoins explains that it depends. The point of view matters:... twitter.com/i/web/status/12166...

16 minutes ago

Good morning London! Ready for #THIREurope pic.twitter.com/X7X3qZ0o2y

About 2 hours ago

eco-system tested was: pacemakers / programmers/home monitors and the "Merlin Net" alias "the cloud". The first attack vector covered by Tobias was the new generation of devices that use wireless technologies (SDR), low power, short-range (2M) – 401-406Mhz). How to find technical specs? Just check the FCC-ID and search for it. Google remains always your best friend. The vulnerabilities found were an energy depletion attack (draining the battery) and a... crash of the pacemaker! The next target was the "Merlin@Home" device which is a home monitoring system. They are easy to find on eBay:



Just perform an attack like against any embedded Linux device: Connect a console, boot it, press a key to get the bootloader, change the boot command add "init=/bin/bash" like any Linux and boot in single-user mode! Once inside the box, it's easy to find a lot of data left by developers (source code, SSH keys, encryption keys, source code, ... The second part of the talk was dedicated to the full-disclosure process.

After a short coffee break, Fabio Nigi presented "*IPFS As a Distributed Alternative to Logs Collection*". The idea behind this talk was to try to solve a classic headache for people who are involved in log management tasks. This can quickly become a nightmare due to the ever-changing topologies, the number of assets, amount of logs to collect and process. Storage is a pain to manage.

So, Fabio had the idea to use IPFS. IPFS means "*Interplanetary file system*" and is a P2P distributed file system that helps to store files in multiple locations. He introduced the tool, how it works (it look interesting, I wasn't aware of it). Then he demonstrated how to interconnect it with a log collection solution using different tools like IPFS GW, React, Brig or Minerva. It's an interesting approach, however, the project is still in the development phase (as stated on the website)...

There were many interesting talks today and, with a dual-track conference, it's not always easy to choose the one that will be the most entertaining or interesting. My next choice was "*Extracting a 19-Year-Old Code Execution from WinRAR*" by Nadav Grossman.

NVD Vulnerabilities Feed

- CVE-2012-3806 (kies) January 9, 2020
  Samsung Kies before 2.5.0.12094_27_11 contains a NULL pointer dereference vulnerability which could allow remote attackers to perform a denial of service.
- CVE-2012-3808 (kies) January 9, 2020
  Samsung Kies before 2.5.0.12094_27_11 has arbitrary file modification.
- CVE-2012-3809 (kies) January 9, 2020
  Samsung Kies before 2.5.0.12094_27_11 has arbitrary directory modification.
- CVE-2012-3810 (kies) January 9, 2020
  Samsung Kies before 2.5.0.12094_27_11

WinRAR is a well-known tool to handle many archive formats. As the tool is very popular, it's a great target for attackers because it is installed on many computers! After a very long part about fuzzing (the techniques, tools like WinAFL), Nadav explained how the vulnerability was found. It was located in a DLL used to process ACE files. Many details were disclosed and, if you are interested, there is a blog post available here. Note that since the vulnerability has been found and disclosed, the support of ACE archives has been removed from the last versions of WinRAR!

After the lunch break, I attended "*Setting up an Opensource Threat Detection Program*" by Lance Buttars (Ingo Money). This was an interesting talk about tools that you can deploy to protect your web services but also counterattack the bad guys. Many tools are used in Lance's arsenal (ModSecurity, Reverse proxies, Fail2ban, etc...)

has registry modification.

- CVE-2012-4434 (fwknop) January 9, 2020
  fwknop before 2.0.3 allow remote authenticated users to cause a denial of service (server crash) or possibly execute arbitrary code.
- CVE-2019-18859 (anywhereusb/14_firmware) January 9, 2020
  Digi AnywhereUSB 14 allows XSS via a link for the Digi Page.
- CVE-2020-6166 (minimal_coming_soon_&_maintenance_mode) January 9, 2020
  A flaw in the WordPress plugin, Minimal Coming Soon & Maintenance Mode through 2.15, allows authenticated users with basic access to export settings and change maintenance-mode themes.
- CVE-2020-6168 (minimal_coming_soon_&_maintenanc

Lance also explained what honeypots are and the different types of data that you collect: domains, files, ports, SQL tables or DB. For each type, he gave some examples. Note that "*active defense*" is not allowed in many countries!

And the day continued with "*Once Upon a Time in the West – A story on DNS Attacks*" by Valentina Palacín and Ruth Esmeralda Barbacil. They reviewed well-known DNS attack techniques (DNS tunneling, hijacking, and poisoning) then they presented a timeline of major threats that affected DNS services and that abused the protocols like:

e_mode) January 9, 2020
A flaw in the WordPress plugin, Minimal Coming Soon & Maintenance Mode through 2.10, allows authenticated users with basic access to enable and disable maintenance-mode settings (impacting the availability and confidentiality of a vulnerable site, along with the integrity of the setting).

- DNSChangerOperation Ghost Click
- Syrian Electronic Army
- Craiglist Hijacked
- Oilrig: Suspected Iranian
- Project Sauron (suspected USA)Darkhydrus (
- Bernhard PoS
- FIN7
- DNSpionage
- SeaTurtle

For each of them, they applied the Mitre ATT&CK framework. Nothing really new but a good recap which concludes that DNS is a key protocol and that it must be carefully controlled.

The two next talks focused more on penetration testing: *"What's Wrong with WebSocket APIs? Unveiling Vulnerabilities in WebSocket APIs"* by Mikhail Egorov. He already published a lot of researches around WebSocket and started with a review of the protocol. Then he described different types of attacks. The second one was "Abusing Google Play Billing for Fun and Unlimited Credits!" by Guillaume Lopes. Guillaume explained how Google provides a payment framework for developers. Like the previous talk, it started with a review of the framework then how it was abused. He tested 50 apps, 29 were vulnerable to this attack. All developers were contacted and only 1 replied!

To close the day, Robert Sell presented "*Techniques and Tools for Becoming an Intelligence Operator*". Open-source intelligence can be used in many fields: forensics, research, etc. Robert defines it as "*Information that is hard to find but freely available*".

He explained how to prepare yourself to perform investigations, which tools to use, network connections, creation of profiles on social network and many more. The list of tools and URLs provided by Robert was amazing! Don't forget that good OpSec is important. If you're excited to search for information about your target, (s)he won't probably be as excited as you! Also, keep in mind, that all techniques used can also be used against you!

That's all Folks! DeepSec is over! Thanks again to the organizers for a great event!

DeepSec

« DeepSec 2019 Wrap-Up Day #1 BotConf 2019 Wrap-Up Day #1 »

https://blog.rootshell.be/2019/11/29/deepsec-2019-wrap-up-day-1/

DeepSec 2019 Wrap-Up Day #1

29.11. 2019

Hello from Vienna where I'm at the DeepSec conference. Initially, I was scheduled to give my OSSEC training but it was canceled due to a lack of students. Anyway, the organizers proposed to me to join (huge thanks to them!). So, here is a wrap-up of the first day!

After the short opening ceremony by René Pfeiffer, the DeepSec organizer, the day started with a keynote. The slot was assigned to Raphaël Vinot and Quinn Norton: "Computer security is simple, the world is not".

I was curious based on the title but the idea was very interesting. Every day, as security practitioners, we deal with computers but we also have to deal with people that use a computer we are protecting! We have to take them into account. Based on different stories, Raphaël and Quinn gave their view of how to communicate with our users. First principle: Listen to them! Let them explain with their own words and shut up. Even if it's technically incorrect, they could have interesting information for us. The second principle is the following: If you don't listen to your users, you don't know how to make your job! The next principle is to learn how they work because you must adapt to them. More close to your users you are, the more you can understand the risks they are facing. Also, don't say "Do this, then this, …" but explain what is behind the action, why they have to do this. Don't go too technical if people don't ask details. Don't scare your users! The classic example is the motivated user that has to finish his/her presentation for tomorrow morning. She/he must transfer files to home but how? If you block all the classic file transfer services, be sure that the worst one will be used. Instead, promote a tool that you trust and that is reliable! Very interesting keynote!

The first regular talk was presented by Abraham Aranguren: "Chinese Police & Cloudpets". If you don't Cloudpets, have a look at this video. What could go wrong? A lot! The security of this connected toy was so bad that major resellers like Walmart or Amazon decided to stop selling it. It's a connected toy linked to mobile apps to exchange messages between parents and kids. Nice isn't it? But they made a lot of mistakes regarding the security of the products. Abraham reviewed them:

Bad BlueTooth implementation, no control to pair or push/fetch data from the toy

Unprotected MongoDB indexed by Shodan, attacked multiple times by ransomware

Unencrypted firmware

Can be used as a spy device

The domain used to interact with the toy is now for sale (mycloudpets.com)

No HTTPS support

All recordings available in an S3 bucket (800K customers!)

The next part of the talk was about mobile apps used by Chinese police to track people, especially the Muslim population in Xinjiang: IJOP & BXAQ. IJOP means “Integrated Joint Operations Platform” and is an application used to collect private information about people and to perform big data analysis. The idea is to collect unusual behaviors and report them to central services for further investigations. The app was analyzed, reverse-engineered and what they found is scaring. Collected data are:

Recording of height & blood type

Anomaly detection

Political data

Religious data

Education level

Abnormal electricity use

Problematic tools -> to make explosives?

IF stopped using phone

The BXAQ app is a trojan that is installed even on tourists phones to collect “interesting” data about them:

It scans the device on which it is installed

Collected info: calendar, contacts, calls, SMS, IMEI, IMSI, hardware details

Scan files on SD card (hash comparison)

A zip file created (without any password) and uploaded to police server

After a welcomed coffee break, I came back to the same track to attend “Mastering AWS pen testing and methodology” by Ankit Giri. The idea behind this talk is to get a better idea about how to pentest an AWS environment.

The talk was full of tips & tricks but also references to tools. The idea is to start by enumerating the AWS accounts used by the platform as well as the services. To achieve this, you can use aws-inventory. Then check for Cloud-

Watch, CloudTrail of BillingAlerts. Check the configuration of services being used. Make notes of services interacting with each other. S3 buckets are, of course, juicy targets. Another tool presented was S3SCanner. Then keep an eye on the IAM: how accounts are managed, what are the access rights, keys, roles. In this case, PMApper can be useful. EV2 virtual systems must be reviewed to find open ports, ingress/egress traffic, and their security groups! If you are interested in testing AWS environments, have a look at this arsenal. To complete the presentation, a demo of prowler was performed by Ankit.

Then Yuri Chemerkin presented "Still Secure. We Empower What We Harden Because We Can Conceal". To be honest with you, I did not understand the goal of the presentation, the speaker was not very engaging and many content was in Russian… Apparently, while discussing with other people who attended the talk, it was related to the leak of information from many tools and how to use them in security testing…

The next one was much more interesting: "Android Malware Adventures: Analyzing Samples and Breaking into C&C" presented by Kürşat Oğuzhan Akıncı & Mert Can Coşkuner. The talk covered the hunt for malware in the mobile apps ecosystem, mainly Android (>70% of new malware are targeting Android phones). Even if Google implemented checks for all apps submitted to the Play store, the solution is not bullet-proof and, like on Windows systems, malware developers have techniques to bypass sandbox detection… They explained how they spotted a campaign targetting Turkey. They analyzed the malware and successfully exploited the C2 server which was vulnerable to:

Directory listing
Lack of encryption keys
Password found in source code
Weak upload feature, they uploaded a webshell
SQLi
Stored XSS
In the end, they uncovered the campaign, they hacked back (with proper authorization!), they restored stolen data and prevented further incidents. Eight threat actors were arrested.

My next choice was again a presentation about the analysis of a known campaign: "The Turtle Gone Ninja – Investigation of an Unusual Crypto-Mining Campaign" presented by Ophir Harpaz, Daniel Goldberg.

The campaign was “NanshOu” and it’s not a classic one. Ophir & Daniel gave many technical details about the malware, how it infected thousands of MSSQL servers to deploy a crypto-miner. Why servers? Because they require less interaction, they have better uptime, they have lot of resources and are maintained by poor IT teams ;-). The infection path was: scanning for MSSQL servers, brute force them, enable execution of code (via xp-cmd-shell()), drop files and execute them.

Then, Tim Berghoff and Hauke Gierow presented “The Daily Malware Grind” – Looking Beyond the Cybers“. They performed a review of the threat landscape, ransomware, crypto-miners, RATs, etc… Interesting fact: old malware remains active.

Lior Yaari talked about a hot topic these days: “The Future Is Here – Modern Attack Surface On Automotive“. Do you know that IDS are coming to connected cars automotive today? It’s a fact, cars are ultra-connected today and it will be worse in the future. If, in the year 2005, cars had an AUX connected and USB ports, today they have GPS, 4G, BT, WiFi and a lot of telemetrics data sent to the manufacturer! By 2025, cars will be part of clouds, be connected to PLC, talk to electric chargers, gas stations, etc. Instead of using ODB2 connections, we will use regular apps to interact with them. Lior gave multiple examples of potential issues that people will face with their connected cards. A great topic!

To close the first day, I attended “Practical Security Awareness – Lessons Learnt and Best Practices” by Stefan Schumacher. He explained in detail why awareness trainings are not always successful.

It’s over for today! Stay tuned for the next wrap-up tomorrow! I’m expecting a lot from some presentations!

孫子兵法 /dev/random

"If the enemy leaves a door open, you must rush in." – Sun Tzu

Search ...

About Me Disclaimer Tools

DeepSec 2019 Wrap-Up Day #1

November 29, 2019 Event, Forensics, Security 2 comments

Hello from Vienna where I'm at the DeepSec conference. Initially, I was scheduled to give my OSSEC training but it was canceled due to a lack of students. Anyway, the organizers proposed to me to join (huge thanks to them!). So, here is a wrap-up of the first day!

After the short opening ceremony by René Pfeiffer, the DeepSec organizer, the day started with a keynote. The slot was assigned to Raphaël Vinot and Quinn Norton: "*Computer security is simple, the world is not*".

Stay in Touch

Upcoming Events

Here is a list of events that I will attend and cover via Twitter and wrap-ups. Ping me if you want to meet! The list is regularly updated.

Recent Articles

- [SANS ISC] Code & Data Reuse in the Malware Ecosystem

I was curious based on the title but the idea was very interesting. Every day, as security practitioners, we deal with computers but we also have to deal with people that use a computer we are protecting! We have to take them into account. Based on different stories, Raphaël and Quinn gave their view of how to communicate with our users. First principle: Listen to them! Let them explain with their own words and shut up. Even if it's technically incorrect, they could have interesting information for us. The second principle is the following: If you don't listen to your users, you don't know how to make your job! The next principle is to learn how they work because you must adapt to them. More close to your users you are, the more you can understand the risks they are facing. Also, don't say "Do this, then this, ..." but explain what is behind the action, why they have to do this. Don't go too technical if people don't ask details. Don't scare your users! The classic example is the motivated user that has to finish his/her presentation for tomorrow morning. She/he must transfer files to home but how? If you block all the classic file transfer services, be sure that the worst one will be used. Instead, promote a tool that you trust and that is reliable! Very interesting keynote!

- BotConf 2019 Wrap-Up Day #3
- BotConf 2019 Wrap-Up Day #2
- BotConf 2019 Wrap-Up Day #1
- DeepSec 2019 Wrap-Up Day #2

Popular Articles

- Show me your SSID's, I'll Tell Who You Are!
  37,808 views
- Keep an Eye on SSH Forwarding!
  36,151 views
- Sending Windows Event Logs to Logstash
  29,489 views
- Socat, Another Network Swiss Army Knife
  26,019 views
- Check Point Firewall Logs and Logstash (ELK) Integration
  25,759 views
- Forensics: Reconstructing Data from Pcap Files
  21,839 views
- dns2tcp: How to bypass firewalls or

The first regular talk was presented by Abraham Aranguren: "*Chinese Police & Cloudpets*". If you don't Cloudpets, have a look at this video. What could go wrong? A lot! The security of this connected toy was so bad that major resellers like Walmart or Amazon decided to stop selling it. It's a connected toy linked to mobile apps to exchange messages between parents and kids. Nice isn't it? But they made a lot of mistakes regarding the security of the products. Abraham reviewed them:

- Bad BlueTooth implementation, no control to pair or push/fetch data from the toy
- Unprotected MongoDB indexed by Shodan, attacked multiple times by ransomware
- Unencrypted firmware
- Can be used as a spy device
- The domain used to interact with the toy is now for sale (mycloudpets.com)
- No HTTPS support
- All recordings available in an S3 bucket (800K customers!)

The next part of the talk was about mobile apps used by Chinese police to track people, especially the Muslim

captive portals?
20,874 views

- Vulnerability Scanner within Nmap
18,678 views
- Post-BruCON Experience - Running a Wall of Sheep in the Wild
17,357 views
- Bash: History to Syslog
15,434 views

Recent Tweets

What are the top techniques used by adversaries? @likethecoins explains that it depends. The point of view matters:... twitter.com/i/web/status/12166...

16 minutes ago

Good morning London! Ready for #THIREurope pic.twitter.com/X7X3qZ0o2y

About 2 hours ago

population in Xinjiang: IJOP & BXAQ. IJOP means "*Integrated Joint Operations Platform*" and is an application used to collect private information about people and to perform big data analysis. The idea is to collect unusual behaviors and report them to central services for further investigations. The app was analyzed, reverse-engineered and what they found is scaring. Collected data are:

- Recording of height & blood type
- Anomaly detection
- Political data
- Religious data
- Education level
- Abnormal electricity use
- Problematic tools -> to make explosives?
- IF stopped using phone

The BXAQ app is a trojan that is installed even on tourists phones to collect "interesting" data about them:

- It scans the device on which it is installed
- Collected info: calendar, contacts, calls, SMS, IMEI, IMSI, hardware details
- Scan files on SD card (hash comparison)
- A zip file created (without any password) and uploaded to police server

After a welcomed coffee break, I came back to the same track to attend "*Mastering AWS pen testing and methodology*" by Ankit Giri. The idea behind this talk is to get a better idea about how to pentest an AWS environment.

What an open file share that has been encrypted looks like? #ransomware pic.twitter.com/diRVVD59PF

January 11, 2020 15:02

Is typing 2 x the complete alphabet a strong password? :-) pic.twitter.com/MrnJDeLjH9

January 10, 2020 14:03

"Apple to scan your photos and videos searching for child pornography and report to authorities" (... twitter.com/i/web/status/12155...

January 10, 2020 07:35

Time Machine

Select Month

The talk was full of tips & tricks but also references to tools. The idea is to start by enumerating the AWS accounts used by the platform as well as the services. To achieve this, you can use aws-inventory. Then check for CloudWatch, CloudTrail of BillingAlerts. Check the configuration of services being used. Make notes of services interacting with each other. S3 buckets are, of course, juicy targets. Another tool presented was S3SCanner. Then keep an eye on the IAM: how accounts are managed, what are the access rights, keys, roles. In this case, PMApper can be useful. EV2 virtual systems must be reviewed to find open ports, ingress/egress traffic, and their security groups! If you are interested in testing AWS environments, have a look at this arsenal. To complete the presentation, a demo of prowler was performed by Ankit.

Then Yuri Chemerkin presented "*Still Secure. We Empower What We Harden Because We Can Conceal*". To be honest with you, I did not understand the goal of the presentation, the speaker was not very engaging and many content was in Russian... Apparently, while discussing with other people who attended the talk, it was related to the leak of information from many tools and how to use them in security testing...

The next one was much more interesting: "*Android Malware Adventures: Analyzing Samples and Breaking into C&C*" presented by Kürşat Oğuzhan Akıncı & Mert Can Coşkuner. The talk covered the hunt for malware in the mobile apps ecosystem, mainly Android (>70% of new malware are

NVD Vulnerabilities Feed

- CVE-2012-3806 (kies) January 9, 2020
  Samsung Kies before 2.5.0.12094_27_11 contains a NULL pointer dereference vulnerability which could allow remote attackers to perform a denial of service.
- CVE-2012-3808 (kies) January 9, 2020
  Samsung Kies before 2.5.0.12094_27_11 has arbitrary file modification.
- CVE-2012-3809 (kies) January 9, 2020
  Samsung Kies before 2.5.0.12094_27_11 has arbitrary directory modification.
- CVE-2012-3810 (kies) January 9, 2020
  Samsung Kies before 2.5.0.12094_27_11

targeting Android phones). Even if Google implemented checks for all apps submitted to the Play store, the solution is not bullet-proof and, like on Windows systems, malware developers have techniques to bypass sandbox detection... They explained how they spotted a campaign targetting Turkey. They analyzed the malware and successfully exploited the C2 server which was vulnerable to:

- Directory listing
- Lack of encryption keys
- Password found in source code
- Weak upload feature, they uploaded a webshell
- SQLi
- Stored XSS

In the end, they uncovered the campaign, they hacked back (with proper authorization!), they restored stolen data and prevented further incidents. Eight threat actors were arrested.

My next choice was again a presentation about the analysis of a known campaign: "*The Turtle Gone Ninja – Investigation of an Unusual Crypto-Mining Campaign*" presented by Ophir Harpaz, Daniel Goldberg.

The campaign was "NanshOu" and it's not a classic one. Ophir & Daniel gave many technical details about the malware, how it infected thousands of MSSQL servers to deploy a crypto-miner. Why servers? Because they require less interaction, they have better uptime, they have lot of

has registry modification.

- CVE-2012-4434 (fwknop) January 9, 2020
  fwknop before 2.0.3 allow remote authenticated users to cause a denial of service (server crash) or possibly execute arbitrary code.
- CVE-2019-18859 (anywhereusb/14_firmware) January 9, 2020
  Digi AnywhereUSB 14 allows XSS via a link for the Digi Page.
- CVE-2020-6166 (minimal_coming_soon_&_maintenance_mode) January 9, 2020
  A flaw in the WordPress plugin, Minimal Coming Soon & Maintenance Mode through 2.15, allows authenticated users with basic access to export settings and change maintenance-mode themes.
- CVE-2020-6168 (minimal_coming_soon_&_maintenanc

resources and are maintained by poor IT teams ;-). The infection path was: scanning for MSSQL servers, brute force them, enable execution of code (via xp-cmdshell()), drop files and execute them.

Then, Tim Berghoff and Hauke Gierow presented "*The Daily Malware Grind" – Looking Beyond the Cybers*". They performed a review of the threat landscape, ransomware, crypto-miners, RATs, etc... Interesting fact: old malware remains active.

Lior Yaari talked about a hot topic these days: "*The Future Is Here – Modern Attack Surface On Automotive*". Do you know that IDS are coming to connected cars automotive today? It's a fact, cars are ultra-connected today and it will be worse in the future. If, in the year 2005, cars had an AUX connected and USB ports, today they have GPS, 4G, BT, WiFi and a lot of telemetrics data sent to the manufacturer! By 2025, cars will be part of clouds, be connected to PLC, talk to electric chargers, gas stations, etc. Instead of using ODB2 connections, we will use regular apps to interact with them. Lior gave multiple examples of potential issues that people will face with their connected cards. A great topic!

e_mode) January 9, 2020
A flaw in the WordPress plugin, Minimal Coming Soon & Maintenance Mode through 2.10, allows authenticated users with basic access to enable and disable maintenance-mode settings (impacting the availability and confidentiality of a vulnerable site, along with the integrity of the setting).

To close the first day, I attended "*Practical Security Awareness – Lessons Learnt and Best Practices*" by Stefan Schumacher. He explained in detail why awareness trainings are not always successful.

It's over for today! Stay tuned for the next wrap-up tomorrow! I'm expecting a lot from some presentations!

Conference | DeepSec | Event | Vienna | Wrap-up

« [SANS ISC] My Little DoH Setup | DeepSec 2019 Wrap-Up Day #2 »

2 comments

Pingback: BotConf 2019 Wrap-Up Day #1 | /dev/random

Lior Yaari says:
December 1, 2019 at 16:42

Thanks for writing about my talk! This conference was amazing!

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Post Comment

This site uses Akismet to reduce spam. Learn how your comment data is processed.

https://olhardigital.com.br/noticia/instalacoes-de-rcs-trazem-vulnerabilidades-a-usuarios/93694

Instalações de RCS trazem vulnerabilidades a usuários

Fabrício Filho, editado por Maria Lutfi 29/11/2019 15h50

Pesquisadores apontaram que implementações do novo padrão de mensagens de algumas operadoras podem trazer diversas falhas no celular, deixando-os vulneráveis e expostos a acessos de terceiros

Operadoras de diversas partes do mundo trabalham para implementar o RCS, o novo padrão de mensagens e sucessor do SMS. No entanto, pesquisadores de segurança da SRLabs descobriram uma série de vulnerabilidades na integração do sistema, que pode comprometer dados de localização do usuário e permitir que mensagens e chamadas sejam interceptadas e o número de telefone falsificado.

Veja também:
[EXCLUSIVO] Falha de segurança no site do Carrefour expõe dados pessoais de clientes
Falha deixa API de proteção da Kaspersky exposta para invasores
Google vai pagar US$ 1,5 milhão a quem identificar falha no Android
Twitter desativa recurso de publicações via SMS após invasão
App de SMS do Android permite seleção múltipla para mensagens individuais

Em um dos casos, a falha pode ocorrer logo após a implementação de uma operadora sem nome, que possibilita qualquer aplicativo instalado no telefone baixar a configuração RCS e obter dados pessoais e conversas privadas. Já em outro, o código de seis dígitos usado para verificar a identidade do usuário fica vulnerável e também permite o acesso de terceiros. Ambos os problemas foram detectados após análises de amostras de cartões SIM de várias operadoras diferentes.

A SRLabs não compartilhou quais empresas possuem os erros identificados, mas divulgou que o padrão ocorre em ao menos 100, incluindo as quatro principais dos Estados Unidos no ramo. “Achamos que isso é realmente um passo atrás para muitas redes (em comparação com o SMS)”, afirmou Karsten Nohl, especialista em segurança da SRLabs. “Esses erros dos anos 90 estão sendo reinventados, reintroduzidos”.

A GSMA, órgão comercial que representa as operadoras de rede, destacou a importância da descoberta para a melhoria do serviço. “Somos gratos aos pesquisadores por permitirem à indústria a oportunidade de compartilhar suas descobertas. A GSMA agradece qualquer pesquisa que aprimore a segurança e a confiança do usuário dos

serviços móveis", afirmou um porta-voz.

RCS

O RCS é um novo padrão de mensagens projetado para substituir o SMS como um meio de enviar mensagens de texto. Ele suporta muitos dos apps usados pelas pessoas atualmente, como iMessage e WhatsApp, incluindo recibos de leitura e indicadores de digitação (embora não criptografe de ponta a ponta), em um padrão de plataforma cruzada com o qual diferentes empresas podem se integrar.

Apesar de suas vantagens em relação ao SMS, o novo padrão tem demorado para ser introduzido. Mesmo anunciado no ano passado, o Google decidiu utilizá-lo como a principal plataforma de mensagens de texto do Android Messages somente neste mês. A mudança da gigante de busca não afetará a Samsung, fabricante de aparelhos Android mais vendido nos EUA, pois a empresa oferece aos seus clientes um sistema de mensagens próprio.

A partir de 2020, companhias como AT&T, Verizon, T-Mobile e Sprint também oferecerão seus próprios serviços referentes a mensagens de texto, enquanto a Apple ainda não comunicou se apoiará ou não o RCS. O SRLabs apresentará suas descobertas detalhadamente na conferência Black Hat Europe, em dezembro, depois de mostrar alguns trabalhos na conferência DeepSec, que ocorrerá nesta sexta-feira.

Compartilhe com seus seguidores

Ouvir: 0:00 ouvima

Pesquisadores apontaram que implementações do novo padrão de mensagens de algumas operadoras podem trazer diversas falhas no celular, deixando-os vulneráveis e expostos a acessos de terceiros

Operadoras de diversas partes do mundo trabalham para implementar o RCS, o novo padrão de mensagens e sucessor do SMS. No entanto, pesquisadores de segurança da SRLabs descobriram uma série de vulnerabilidades na integração do sistema, que pode comprometer dados de localização do usuário e permitir que mensagens e chamadas sejam interceptadas e o número de telefone falsificado.

Veja também:

[EXCLUSIVO] Falha de segurança no site do Carrefour expõe dados pessoais de clientes

Falha deixa API de proteção da Kaspersky exposta para invasores

OLHAR DIGITAL

Twitter desativa recurso de publicações via SMS após invasão

App de SMS do Android permite seleção múltipla para mensagens individuais

Em um dos casos, a falha pode ocorrer logo após a implementação de uma operadora sem nome, que possibilita qualquer aplicativo instalado no telefone baixar a configuração RCS e obter dados pessoais e conversas privadas. Já em outro, o código de seis dígitos usado para verificar a identidade do usuário fica vulnerável e também permite o acesso de terceiros. Ambos os problemas foram detectados após análises de amostras de cartões SIM de várias operadoras diferentes.

A SRLabs não compartilhou quais empresas possuem os erros identificados, mas divulgou que o padrão ocorre em ao menos 100, incluindo as quatro principais dos Estados Unidos no ramo. "Achamos que isso é realmente um passo atrás para muitas redes (em comparação com o SMS)", afirmou Karsten Nohl, especialista em segurança da SRLabs. "Esses erros dos anos 90 estão sendo reinventados, reintroduzidos".

A GSMA, órgão comercial que representa as operadoras de rede, destacou a importância da descoberta para a melhoria do serviço. "Somos gratos aos pesquisadores por permitirem à indústria a oportunidade de compartilhar suas descobertas. A GSMA agradece qualquer pesquisa que aprimore a segurança e a confiança do usuário dos serviços móveis", afirmou um porta-voz.

RCS

O RCS é um novo padrão de mensagens projetado para substituir o SMS como um meio de enviar mensagens de texto. Ele suporta muitos dos apps usados pelas pessoas atualmente, como iMessage e WhatsApp, incluindo recibos de leitura e indicadores de digitação (embora não criptografe de ponta a ponta), em um padrão de

Apesar de suas vantagens em relação ao SMS, o novo padrão tem demorado para ser introduzido. Mesmo anunciado no ano passado, o Google decidiu utilizá-lo como a principal plataforma de mensagens de texto do Android Messages somente neste mês. A mudança da gigante de busca não afetará a Samsung, fabricante de aparelhos Android mais vendido nos EUA, pois a empresa oferece aos seus clientes um sistema de mensagens próprio.

A partir de 2020, companhias como AT&T, Verizon, T-Mobile e Sprint também oferecerão seus próprios serviços referentes a mensagens de texto, enquanto a Apple ainda não comunicou se apoiará ou não o RCS. O SRLabs apresentará suas descobertas detalhadamente na conferência Black Hat Europe, em dezembro, depois de mostrar alguns trabalhos na conferência DeepSec, que ocorrerá nesta sexta-feira.

Via: The Verge

GOOGLE APPLE ANDROID SMS AT&T
OPERADORAS VULNERABILIDADE FALHA DE SEGURANÇA
MENSAGENS T-MOBILE FALHA DE PRIVACIDADE
CELULAR RCS

https://www.theverge.com/2019/11/29/20987738/bad-rcs-implementations-are-creating-big-vulnerabilities-security-researchers-claim

Bad RCS implementations are creating big vulnerabilities, security researchers claim

Carriers are creating problems for users

By Jon Porter@JonPorty Nov 29, 2019, 7:44am

Security researchers at SRLabs have found a number of vulnerabilities with the way carriers around the world are implementing RCS, the new messaging standard designed to replace SMS, Motherboard reports. In some cases, these issues could compromise a user's location data, they could allow their text messages or calls to be intercepted, or they might allow their phone number to be spoofed.

One issue identified on an unnamed carrier's implementation could allow any app on your phone to download your RCS configuration file, for example, giving the app your username and password and allowing it to access all your voice calls and text messages. In another case, the six-digit code a carrier uses to verify a user's identity was vulnerable to being guessed through brute force by a third-party. These problems were found after researchers analyzed a sample of SIM cards from several different carriers.

"ALL OF THESE MISTAKES FROM THE 90S ARE BEING REINVENTED, REINTRODUCED"

RCS is a new messaging standard that's designed to one day replace SMS as a means of sending text messages. It supports many of the features introduced by modern messaging clients like iMessage and WhatsApp including read receipts and typing indicators (although not end-to-end encryption), in a cross-platform standard that different companies can integrate with. The researchers did not identify any problems with the standard itself; it's the way carriers are rolling it out that's the problem.

SRLabs didn't share which security holes were found with which carriers, but noted that the standard is being implemented by at least 100 carriers around the world, including the four US majors. "We find that is actually a step backwards for a lot of networks [compared to SMS]," Karsten Nohl from SRLabs told Motherboard. "All of these mistakes from the 90s are being reinvented, reintroduced."

When contacted for comment, a spokesperson for the trade body that represents network operators, the GSMA, told Motherboard that researchers from SRLabs will be presenting their findings to the organization next week, and

that they believed their are countermeasures available to fix the issues they've identified. "We are grateful to the researchers for allowing the industry the opportunity to consider their findings. The GSMA welcomes any research that enhances the security and user confidence of mobile services," the spokesperson said.

Despite its advantages over SMS, RCS has been slow to roll out. The standard was announced last year, but it wasn't until this month that Google started making it the primary texting platform for Android Messages, and that change won't affect the best-selling Android phone manufacturer in the US, Samsung, because by default it offers its own messaging client. AT&T, Verizon, T-Mobile, and Sprint are also planning on offering support via their own texting app next year. Meanwhile, Apple has declined to comment on whether it will support the standard.

SRLabs will be presenting its findings at the Black Hat Europe conference in December, after showing off some of its work at the DeepSec conference today.

TECH CYBERSECURITY

19

Bad RCS implementations are creating big vulnerabilities, security researchers claim

Carriers are creating problems for users

By Jon Porter | @JonPorty | Nov 29, 2019, 7:44am EST

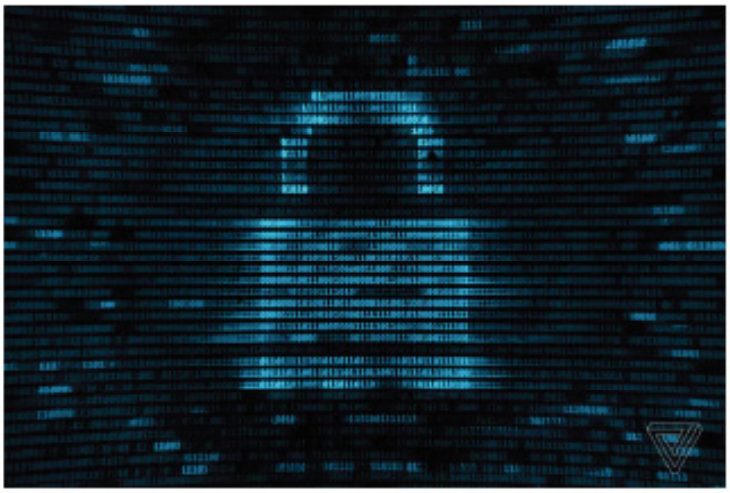


Illustration by Alex Castro / The Verge

Security researchers at SRLabs have found a number of vulnerabilities with the way carriers around the world are implementing RCS, the new messaging standard designed to replace SMS, *Motherboard* reports. In some cases, these issues could compromise a user's location data, they could allow their text messages or calls to be intercepted, or they might allow their phone number to be spoofed.

One issue identified on an unnamed carrier's implementation could allow any app on your phone to download your RCS configuration file, for example, giving the app your username and password and allowing it to access all your voice calls and text messages. In another case, the six-digit code a

carrier uses to verify a user's identity was vulnerable to being guessed through brute force by a third-party. These problems were found after researchers analyzed a sample of SIM cards from several different carriers.

> "ALL OF THESE MISTAKES FROM THE 90S ARE BEING REINVENTED, REINTRODUCED"

RCS is a new messaging standard that's designed to one day replace SMS as a means of sending text messages. It supports many of the features introduced by modern messaging clients like iMessage and WhatsApp including read receipts and typing indicators (although not end-to-end encryption), in a cross-platform standard that different companies can integrate with. The researchers did not identify any problems with the standard itself; it's the way carriers are rolling it out that's the problem.

SRLabs didn't share which security holes were found with which carriers, but noted that the standard is being implemented by at least 100 carriers around the world, including the four US majors. "We find that is actually a step backwards for a lot of networks [compared to SMS]," Karsten Nohl from SRLabs told *Motherboard*. "All of these mistakes from the 90s are being reinvented, reintroduced."

When contacted for comment, a spokesperson for the trade body that represents network operators, the GSMA, told *Motherboard* that researchers from SRLabs will be presenting their findings to the organization next week, and that they believed their are countermeasures available to fix the issues they've identified. "We are grateful to the researchers for allowing the industry the opportunity to consider their findings. The GSMA welcomes any research that enhances the security and user confidence of mobile services," the spokesperson said.

Despite its advantages over SMS, RCS has been slow to roll out. The standard was announced last year, but it wasn't until this month that Google started making it the primary texting platform for Android Messages, and that change won't affect the best-selling Android phone manufacturer in the US, Samsung, because by default it offers its own messaging client. AT&T, Verizon, T-Mobile, and Sprint are also planning on offering support via their own texting app next year. Meanwhile, Apple has declined to comment on whether it will support the standard.

SRLabs will be presenting its findings at the Black Hat Europe conference in December, after showing off some of its work at the DeepSec conference today.

RELATED

RCS: What it is and why you might want it

https://www.vice.com/en_us/article/j5ywxb/rcs-rich-communications-services-text-call-interception

SMS Replacement is Exposing Users to Text, Call Interception Thanks to Sloppy Telecos

Researchers from SRLabs found that telecos are implementing the RCS standard in vulnerable ways, which bring back techniques to attack phone networks.

By Joseph Cox

Nov 29 2019, 7:00am

A standard used by phone carriers around the world can leave users open to all sorts of attacks, like text message and call interception, spoofed phone numbers, and leaking their coarse location, new research reveals.

The Rich Communication Services (RCS) standard is essentially the replacement for SMS. The news shows how even as carriers move onto more modern protocols for communication, phone network security continues to be an exposed area with multiple avenues for attack in some implementations of RCS.

“I’m surprised that large companies, like Vodafone, introduce a technology that exposes literally hundreds of millions of people, without asking them, without telling them,” Karsten Nohl from cybersecurity firm Security Research Labs (SRLabs) told Motherboard in a phone call.

SRLabs researchers Luca Melette and Sina Yazdanmehr will present their RCS findings at the upcoming Black Hat Europe conference in December, and discussed some of their work at security conference DeepSec on Friday.

RCS is a relatively new standard for carrier messaging and includes more features than SMS, such as photos, group chats, and file transfers. Back in 2015, Google announced it would be adopting RCS to move users away from SMS, and that it had acquired a company called Jibe Mobile to help with the transition. RCS essentially runs as an app on your phone that logs into a service with a username and password, Nohl explained.

SRLabs estimated RCS is already implemented by at least 100 mobile operators, with many of the deployments being in Europe. SRLabs said that all the major U.S. carriers—AT&T, T-Mobile, Sprint, and Verizon—were using RCS.

Do you work for AT&T, T-Mobile, Sprint, or Verizon? We’d love to hear from you. Using a non-work phone or computer, you can contact Joseph Cox securely on Signal on +44 20 8133 5190, Wickr on josephcox, OTR chat on jfcox@jabber.ccc.de, or email joseph.cox@vice.com.

SRLabs didn't find an issue in the RCS standard itself, but rather how it is being implemented by different telecos. Because some of the standard is undefined, there's a good chance companies may deploy it in their own way and make mistakes.

"Everybody seems to get it wrong right now, but in different ways," Nohl said. SRLabs took a sample of SIM cards from a variety of carriers and checked for RCS-related domains, and then looked into particular security issues with each. SRLabs didn't say which issues impacted which particular telecos.

Some of those issues include how devices receive RCS configuration files. In one instance, a server provides the configuration file for the right device by identifying them by their IP address. But because they also use that IP address, "Any app that you install on your phone, even if you give it no permissions whatsoever, it can request this file. So now every app can get your username and password to all your text messages and all your voice calls. That's unexpected," Nohl said.

In another instance, a teleco sends a text message with a six-digit code to verify that the RCS user is who they say they are, but "then give you an unlimited number of tries" to input the code, Nohl said. "One million attempts takes five minutes," he added, meaning that it could be possible to brute force through the authentication process.

"All of these mistakes from the 90s are being reinvented, reintroduced," Nohl said. "It is being rolled out for upwards of a billion people already who are all affected by this."

Verizon did not respond to a request for comment and T-Mobile did not provide a statement in time for publication.

Vodafone said in a statement, "We are aware of the research by SRLabs. We take security very seriously and we have a number of measures in place to protect RCS services. We will review these protections in light of the research and, if required, take any further protective measures."

AT&T and Sprint directed questions to the GSM Association (GSMA), a trade body for network operators.

Claire Cranton, a spokesperson for the GSMA, wrote in an email, "The GSMA is aware of research undertaken by SRLabs into RCS security in which some previously known, but no new, vulnerabilities are reported. The findings highlight issues with some RCS implementations but not every deployment, or the RCS specifications themselves, are impacted."

Cranton said the researchers will present their findings to an expert group at GSMA next week, and that an initial analysis of the research shows there are countermeasures to the uncovered issues.

“We are grateful to the researchers for allowing the industry the opportunity to consider their findings. The GSMA welcomes any research that enhances the security and user confidence of mobile services and encourages all researchers to submit their work to our Coordinated Vulnerability Disclosure (CVD) Programme which enables them to share findings and to contribute to industry’s ongoing work to drive security improvements,” Cranton wrote.

Nohl said of the move to RCS, “We find that is actually a step backwards for a lot of networks.”

MOTHERBOARD
TECH BY VICE

SMS Replacement is Exposing Users to Text, Call Interception Thanks to Sloppy Telecos

Researchers from SRLabs found that telecos are implementing the RCS standard in vulnerable ways, which bring back techniques to attack phone networks.

By Joseph Cox

Nov 29 2019, 7:00am

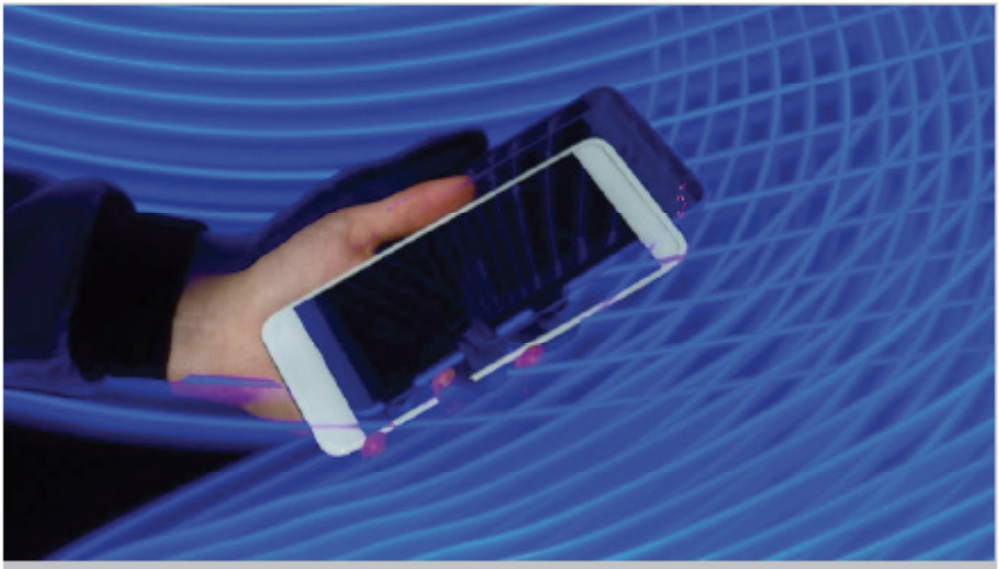


IMAGE: AITOR DIAGO

A standard used by phone carriers around the world can leave users open to all sorts of attacks, **like text message and call interception**, spoofed phone numbers, and leaking their coarse location, new research reveals.

The Rich Communication Services (RCS) standard is essentially the replacement for SMS. The news shows how even as carriers move onto more modern protocols for communication, phone network security continues to be an exposed area with multiple avenues for attack in some implementations of RCS.

"I'm surprised that large companies, like Vodafone, introduce a technology that exposes literally hundreds of millions of people, without asking them, without telling them," Karsten Nohl from **cybersecurity firm Security Research Labs (SRLabs)** told Motherboard in a phone call.

SRLabs researchers Luca Melette and Sina Yazdanmehr will present their RCS findings at the upcoming Black Hat Europe conference in December, and discussed some of their work at security conference DeepSec on Friday.

RCS is a relatively new standard for carrier messaging and includes more features than SMS, such as photos, group chats, and file transfers. Back in 2015, **Google announced it would be adopting RCS** to move users away from SMS, and that it had acquired a company called Jibe Mobile to help with the transition. RCS essentially runs as an app on your phone that logs into a service with a username and password, Nohl explained.

SRLabs estimated RCS is already implemented by at least 100 mobile operators, with many of the deployments being in Europe. SRLabs said that all the major U.S. carriers—AT&T, T-Mobile, Sprint, and Verizon—were using RCS.

> ***Do you work for AT&T, T-Mobile, Sprint, or Verizon? We'd love to hear from you. Using a non-work phone or computer, you can contact Joseph Cox securely on Signal on +44 20 8133 5190, Wickr on josephcox, OTR chat on jfcox@jabber.ccc.de, or email joseph.cox@vice.com.***

SRLabs didn't find an issue in the RCS standard itself, but rather how it is being implemented by different telecos. Because some of the standard is

undefined, there's a good chance companies may deploy it in their own way and make mistakes.

"Everybody seems to get it wrong right now, but in different ways," Nohl said. SRLabs took a sample of SIM cards from a variety of carriers and checked for RCS-related domains, and then looked into particular security issues with each. SRLabs didn't say which issues impacted which particular telecos.

Some of those issues include how devices receive RCS configuration files. In one instance, a server provides the configuration file for the right device by identifying them by their IP address. But because they also use that IP address, "Any app that you install on your phone, even if you give it no permissions whatsoever, it can request this file. So now every app can get your username and password to all your text messages and all your voice calls. That's unexpected," Nohl said.

In another instance, a teleco sends a text message with a six-digit code to verify that the RCS user is who they say they are, but "then give you an unlimited number of tries" to input the code, Nohl said. "One million attempts takes five minutes," he added, meaning that it could be possible to brute force through the authentication process.

"All of these mistakes from the 90s are being reinvented, reintroduced," Nohl said. "It is being rolled out for upwards of a billion people already who are all affected by this."

Verizon did not respond to a request for comment and T-Mobile did not provide a statement in time for publication.

Vodafone said in a statement, "We are aware of the research by SRLabs. We take security very seriously and we have a number of measures in place to protect RCS services. We will review these protections in light of the research and, if required, take any further protective measures."

AT&T and Sprint directed questions to the GSM Association (GSMA), a trade body for network operators.

Claire Cranton, a spokesperson for the GSMA, wrote in an email, "The GSMA is aware of research undertaken by SRLabs into RCS security in which some previously known, but no new, vulnerabilities are reported. The findings

highlight issues with some RCS implementations but not every deployment, or the RCS specifications themselves, are impacted."

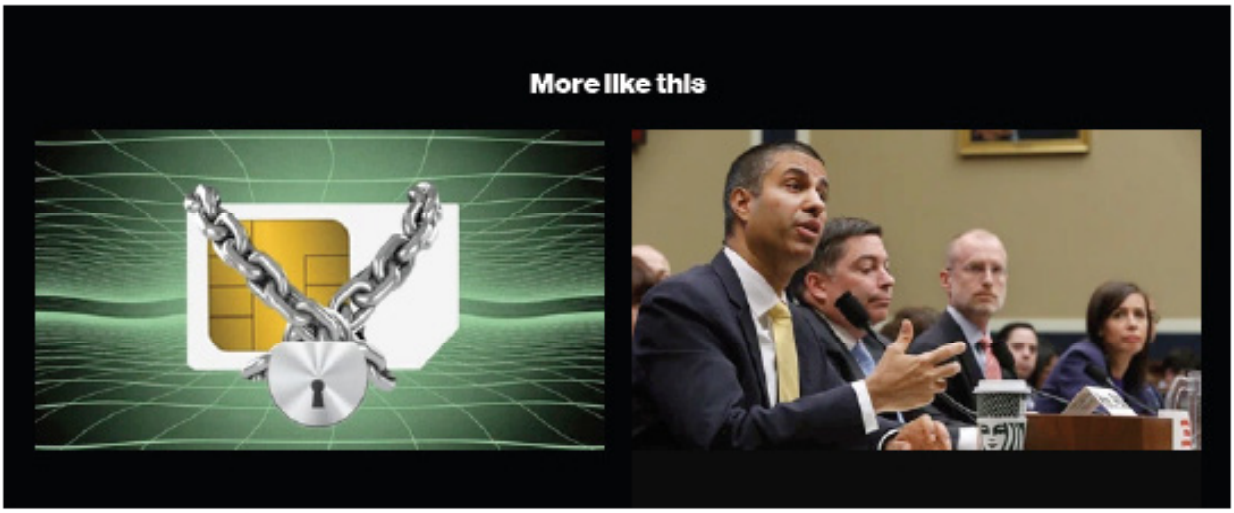
Cranton said the researchers will present their findings to an expert group at GSMA next week, and that an initial analysis of the research shows there are countermeasures to the uncovered issues.

"We are grateful to the researchers for allowing the industry the opportunity to consider their findings. The GSMA welcomes any research that enhances the security and user confidence of mobile services and encourages all researchers to submit their work to our Coordinated Vulnerability Disclosure (CVD) Programme which enables them to share findings and to contribute to industry's ongoing work to drive security improvements," Cranton wrote.

Nohl said of the move to RCS, "We find that is actually a step backwards for a lot of networks."

Subscribe to our cybersecurity podcast, CYBER.

TAGGED: GOOGLE, HACKERS, VERIZON, AT&T, SS7, CELL PHONE NETWORKS, RCS, PHONE NETWORKS, RICH COMMUNICATIONS SERVICES



https://futurezone.at/apps/wie-sicher-ist-das-chatten-ueber-whatsapp-signal-und-co/400685609

Wie sicher ist das Chatten über WhatsApp, Signal und Co?

Messenger-Dienste sind eng mit Datenschutzbedenken verbunden. Was dahintersteckt.

von Andreea Iosa, 28.11.2019

Über Messenger-Apps versenden jeden Tag hunderte Millionen Nutzer ihre privaten Fotos und Nachrichten. Inhalte, bei denen niemand will, dass ein Dritter mitliest. Deshalb sind Messenger-Dienste und soziale Netzwerke wie Facebook fast untrennbar mit Datenschutzbedenken verbunden. Bei den meisten Nutzern bestehen nicht ganz unberechtigte Sorgen, dass ihre Daten in falsche Hände geraten.

Verschlüsselung

Um diesen Bedenken entgegenzutreten, gibt es bei den unten angeführten Messenger-Diensten eine so genannte Ende-zu-Ende-Verschlüsselung. Dadurch soll gewährleistet werden, dass private Nachrichten nicht mitgelesen werden können, da diese Inhalte am gesamten Transportweg verschlüsselt sind. Das bedeutet, dass sie tatsächlich auch nur von Sender und Empfänger lesbar sind. Wie sicher diese Messenger-Apps sind, darüber hat Sicherheitsexperte René Pfeiffer von der IT-Sicherheitsfirma DeepSec mit der futurezone gesprochen.

SMS in jedem Fall unverschlüsselt

Den Short Message Service (SMS) zur Übertragung von Textnachrichten gibt es bereits seit 1992. Der Dienst wurde zunächst für den GSM-Mobilfunk (Global System for Mobile Communications) verfügbar gemacht, ist teilweise aber auch als Festnetz-Variante verfügbar. Das Problem laut Pfeiffer: „SMS ist prinzipiell unverschlüsselt, längen- und formatbeschränkt." Dafür sei der Dienst aber universell, also von jedem Handy aus verfügbar – „auch wenn es kein Smartphone ist", sagt der Experte. Die Sicherheit hängt zudem vom Mobilfunkanbieter ab.

WhatsApp nutzt Metadaten

WhatsApp ist ein Instant-Messaging-Dienst und gehört seit 2014 Facebook. Nutzer können Textnachrichten, Bild-, Video- und Ton-Dateien sowie Standortinformationen, Dokumente und Kontaktdaten austauschen. Pfeiffer: „WhatsApp hat zwar eine Ende-zu-Ende-Verschlüsselung, aber nur, wenn sie aktiv ist. Das Problem ist, dass man sie abschalten kann." Zudem stünden Metadaten – also wer mit wem kommuniziert – Facebook zur Verfügung, auch wenn es eine Ende-zu-Ende-Verschlüsselung gebe. Laut Sicherheitsexperten ist WhatsApp weniger ratsam. WhatsApp ist kostenlos für iOS und Android erhältlich.

Facebook Messenger unsicher

Facebook hat in der Vergangenheit des Öfteren mit seinen weitreichenden Datenlecks von sich sprechen gemacht. Unter anderem wurden persönliche Daten an Dritte, etwa an Behörden, weitergegeben. „Facebook wollte die Applikation getrennt von WhatsApp führen. Bei dem Unternehmen besteht aber kein Zweifel, dass von Daten bis hin zu Metadaten alles verwendet wird“, so Pfeiffer. Wer Sicherheitsansprüche an seinen Messenger-Dienst stellt, sollte diesen nicht verwenden. Ende-zu-Ende-Verschlüsselung ist bei diesem Dienst außerdem nicht Standard.
Der Facebook Messenger ist kostenlos für iOS und Android erhältlich.

Signal immer verschlüsselt

Signal ist für viele Sicherheitsexperten und Datenschutzorganisationen die erste Wahl. „Signal ist anders und hat definitiv immer eine Ende-zu-Ende-Verschlüsselung. Die kann man auch nicht abschalten“, so Pfeiffer. Eine Datensammlung stehe ebenfalls nicht dahinter, Kontakte und Telefonnummern seien verschlüsselt. „Signal unternimmt sehr große Anstrengungen, diese Kontaktdaten auch vor sich selbst zu isolieren.“ Die Infrastruktur wird von Whisper Systems betrieben. Sicherheitsforscher schätzen das Unternehmen als vertrauenswürdig ein.
Signal ist kostenlos für iOS und Android erhältlich.

Telegram bewirbt sich als “sicher”

Telegram ist ein Cloud-basierter Instant-Messaging-Dienst, der vom Russen Pawel Durow gegründet wurde. Nachrichten werden dauerhaft auf dem Server gespeichert und sind für Betreiber sowie jede Person mit Serverzugriff sichtbar. „Geheime Chats“ können nur optional aktiviert werden, wofür eine Ende-zu-Ende-Verschlüsselung verwendet wird. „Telegram wirbt immer mit dem Schutz der Privatsphäre, hat in der Vergangenheit aber mehrere technische Schwächen gehabt. Den Dienst würde ich nur bedingt empfehlen“, sagt Experte Pfeiffer.
Telegram ist kostenlos für iOS und Android erhältlich.

eMail ist dezentrales Medium

Die „electronic Mail“ ist laut Pfeiffer ein dezentrales Kommunikationsmedium. Das heißt, dass dahinter keine spezifische Firma steckt. Wie sicher der Transportweg dieses Standard-Nachrichtendienstes ist, hängt vom Dienstleister ab – etwa Google, Yahoo oder der Arbeitgeber. Das Verschlüsseln der elektronischen Post ist laut Pfeiffer jedoch schwierig. Je nach Nutzung – etwa über Smartphone-Apps oder Webmail – ist sie schwierig zu implementieren und kann ausfallen. Sie muss auch auf jedem Gerät, auf dem eMails abgerufen werden, installiert werden.

APPS

28.11.2019

Wie sicher ist das Chatten über WhatsApp, Signal und Co?

Messenger-Dienste sind eng mit Datenschutzbedenken verbunden. Was dahintersteckt.

von Andreea Iosa

Über Messenger-Apps versenden jeden Tag hunderte Millionen Nutzer ihre privaten Fotos und Nachrichten. Inhalte, bei denen niemand will, dass ein Dritter mitliest. Deshalb sind Messenger-Dienste und soziale Netzwerke wie Facebook fast untrennbar mit Datenschutzbedenken verbunden. Bei den meisten Nutzern bestehen nicht ganz unberechtigte Sorgen, dass ihre Daten in falsche Hände geraten.

Verschlüsselung

Um diesen Bedenken entgegenzutreten, gibt es bei den unten angeführten Messenger-Diensten eine so genannte Ende-zu-Ende-Verschlüsselung. Dadurch soll gewährleistet werden, dass private Nachrichten nicht mitgelesen werden können, da diese Inhalte am gesamten Transportweg verschlüsselt sind. Das bedeutet, dass sie tatsächlich auch nur von Sender und Empfänger lesbar sind. Wie sicher diese Messenger-Apps sind, darüber hat Sicherheitsexperte René Pfeiffer von der IT-Sicherheitsfirma DeepSec mit der futurezone gesprochen.

[illegible]n jedem Fall unverschlüsselt

Den Short Message Service (SMS) zur Übertragung von Textnachrichten gibt es bereits seit 1992. Der Dienst wurde zunächst für den GSM-Mobilfunk (Global System for Mobile Communications) verfügbar gemacht, ist teilweise aber auch als Festnetz-Variante verfügbar. Das Problem laut Pfeiffer: „SMS ist prinzipiell unverschlüsselt, längen- und formatbeschränkt." Dafür sei der Dienst aber universell, also von jedem Handy aus verfügbar – „auch wenn es kein Smartphone ist", sagt der Experte. Die Sicherheit hängt zudem vom Mobilfunkanbieter ab.

WhatsApp nutzt Metadaten

WhatsApp ist ein Instant-Messaging-Dienst und gehört seit 2014 Facebook. Nutzer können Textnachrichten, Bild-, Video- und Ton-Dateien sowie Standortinformationen, Dokumente und Kontaktdaten austauschen. Pfeiffer: „WhatsApp hat zwar eine Ende-zu-Ende-Verschlüsselung, aber nur, wenn sie aktiv ist. Das Problem ist, dass man sie abschalten kann." Zudem stünden Metadaten – also wer mit wem kommuniziert – Facebook zur Verfügung, auch wenn es eine Ende-zu-Ende-Verschlüsselung gebe. Laut Sicherheitsexperten ist WhatsApp weniger ratsam.

WhatsApp ist kostenlos für iOS und Android erhältlich.

Facebook Messenger unsicher

Facebook hat in der Vergangenheit des Öfteren mit seinen weitreichenden Datenlecks von sich sprechen gemacht. Unter anderem wurden persönliche Daten an Dritte, etwa an Behörden, weitergegeben. „Facebook wollte die Applikation getrennt von WhatsApp führen. Bei dem Unternehmen besteht aber kein Zweifel, dass von Daten bis hin zu Metadaten alles verwendet wird", so Pfeiffer. Wer Sicherheitsansprüche an seinen Messenger-Dienst stellt, sollte diesen nicht verwenden. Ende-zu-Ende-Verschlüsselung ist bei diesem Dienst außerdem nicht Standard.

Der Facebook Messenger ist kostenlos für iOS und Android erhältlich.

Signal immer verschlüsselt

Signal ist für viele Sicherheitsexperten und Datenschutzorganisationen die erste Wahl. „Signal ist anders und hat definitiv immer eine Ende-zu-Ende-Verschlüsselung. Die kann man auch nicht abschalten", so Pfeiffer. Eine Datensammlung stehe ebenfalls nicht dahinter, Kontakte und Telefonnummern seien verschlüsselt. „Signal unternimmt sehr große Anstrengungen, diese Kontaktdaten auch vor sich selbst zu isolieren." Die Infrastruktur wird von Whisper Systems betrieben. Sicherheitsforscher schätzen das Unternehmen als vertrauenswürdig ein.

Signal ist kostenlos für iOS und Android erhältlich.

Telegram bewirbt sich als "sicher"

Telegram ist ein Cloud-basierter Instant-Messaging-Dienst, der vom Russen Pawel Durow gegründet wurde. Nachrichten werden dauerhaft auf dem Server gespeichert und sind für Betreiber sowie jede Person mit Serverzugriff sichtbar. „Geheime Chats" können nur optional aktiviert werden, wofür eine Ende-zu-Ende-Verschlüsselung verwendet wird. „Telegram wirbt immer mit dem Schutz der Privatsphäre, hat in der Vergangenheit aber mehrere technische Schwächen gehabt. Den Dienst würde ich nur bedingt empfehlen", sagt Experte Pfeiffer.

Telegram ist kostenlos für iOS und Android erhältlich.

eMail ist dezentrales Medium

[illegible]ectronic Mail" ist laut Pfeiffer ein dezentrales Kommunikationsmedium. Das heißt, dass dahinter keine [illegible]sche Firma steckt. Wie sicher der Transportweg dieses Standard-Nachrichtendienstes ist, hängt vom

Dienstleister ab – etwa Google, Yahoo oder der Arbeitgeber. Das Verschlüsseln der elektronischen Post ist laut Pfeiffer jedoch schwierig. Je nach Nutzung – etwa über Smartphone-Apps oder Webmail – ist sie schwierig zu implementieren und kann ausfallen. Sie muss auch auf jedem Gerät, auf dem eMails abgerufen werden, installiert werden.

Ihr habt auch eine Frage aus unserem Themengebiete, die wir für euch beantworten sollen? Schickt uns eine E-Mail an redaktion@futurezone.at - Betreff: "frag die futurezone".

APPS
Schwere Sicherheitslücke in WhatsApp entdeckt

NETZPOLITIK
EU-Parlament lässt Abgeordnete kein Signal installieren

[futurezone] | Stand: 28.11.2019, 06:00

So sicher sind WhatsApp und SMS

Kommunikation. Messenger-Dienste sind eng mit Datenschutzbedenken verbunden.Was dahinter steckt

VON ANDREEA IOSA, Dienstag 26.11.2019

Über Messenger-Apps versenden jeden TagHunderte Millionen Nutzer ihre privaten Fotos und Nachrichten. Inhalte, bei denen niemand will, dass ein Dritter mitliest.

Deshalb sind Messenger-Dienste und soziale Netzwerke wie Facebook fast untrennbar mit Datenschutzbedenken verbunden. Bei den meisten Nutzern bestehen nicht ganz unberechtigte Sorgen, dass ihre Daten in falsche Hände geraten.

Verschlüsselung

Um diesen Bedenken entgegenzutreten, gibt es bei den unten angeführten Messenger-Diensten eine sogenannte Ende-zu-Ende-Verschlüsselung. Dadurch soll gewährleistet werden, dass private Nachrichten nicht mitgelesen werden können, da diese Inhalte am gesamten Transportweg verschlüsselt sind. Das bedeutet, dass sie tatsächlich auch nur von Sender und Empfänger

lesbar sind. Wie sicher diese Messenger-Apps sind, darüber hat Sicherheitsexperte René Pfeiffer von der IT-Sicherheitsfirma Deep-Sec mit dem KURIER gesprochen.

SMS in jedem Fall unverschlüsselt

Den Short Message Service (SMS) zur Übertragung von Textnachrichten gibt es bereits seit 1992. Der Dienst wurde zunächst für den GSM-Mobilfunk (Global System for Mobile Communications)

verfügbar gemacht, ist teilweise aber auch als Festnetz- Variante verfügbar. Das Problem laut Pfeiffer: „SMS ist prinzipiell unverschlüsselt, längen- und formatbeschränkt." Dafür sei der Dienst aber universell, also von jedem Handy aus verfügbar – „auch wenn es kein Smartphone ist", sagt der Experte. Die Sicherheit hängt zudem vom Mobilfunkanbieter ab.

WhatsApp nutzt Metadaten

WhatsApp ist ein Instant-Messaging- Dienst und gehört seit 2014 Facebook. Nutzer

können Textnachrichten, Bild-, Video- und Ton-Dateien sowie Standortinformationen, Dokumente und Kontaktdaten austauschen. Pfeiffer: „WhatsApp hat zwar eine Ende-zu-Ende-Verschlüsselung, aber

nur, wenn sie aktiv ist. Das Problem ist, dass man sie abschalten kann." Zudem stünden Metadaten

– also wer mit wem kommuniziert – Facebook zur Verfügung, auch wenn es eine Ende-zu-Ende-Verschlüsselung gebe. Laut Sicherheitsexperten ist WhatsApp weniger ratsam.

Facebook Messenger ist unsicher

Facebook hat in der Vergangenheit des Öfteren mit seinen weitreichenden Datenlecks von sich reden gemacht. Unter anderem wurden persönliche Daten an Dritte, etwa an Behörden, weitergegeben.

„Facebook wollte die Applikation getrennt von Whats- App führen. Bei dem Unternehmen besteht aber kein Zweifel, dass von Daten bis hin zu Metadaten alles verwendet wird“, so Pfeiffer. Wer Sicherheitsansprüche an seinen Messenger-Dienst stellt, sollte diesen nicht verwenden.

Ende-zu-Ende-Verschlüsselung ist bei diesem Dienst außerdem nicht Standard.

Signal ist definitiv immer verschlüsselt

Signal ist für viele Sicherheitsexperten und Datenschutzorganisationen die erste Wahl. „Signal ist anders und hat definitiv immer eine Ende-zu-Ende-Verschlüsselung. Die kann man auch nicht abschalten“, so Pfeiffer. Eine Datensammlung stehe ebenfalls nicht dahinter, Kontakte und Telefonnummern seien verschlüsselt. „Signal unternimmt sehr große Anstrengungen, diese Kontaktdaten auch vor sich selbst zu isolieren.“ Die Infrastruktur wird von Whisper Systems betrieben. Sicherheitsforscher schätzen das Unternehmen als vertrauenswürdig ein.

Telegram bewirbt sich als “sicher”

Telegram ist ein Cloud-basierter Instant-Messaging-Dienst, der vom Russen Pawel Durow gegründet wurde. Nachrichten werden dauerhaft auf dem Server gespeichert und sind für Betreiber sowie jede Person mit Serverzugriff sichtbar. „Geheime Chats“ können nur optional aktiviert werden, wofür eine Ende-zu-Ende-Verschlüsselung verwendet wird. „Telegram wirbt immer mit dem Schutz der Privatsphäre, hat in der Vergangenheit aber mehrere technische Schwächen gehabt. Den Dienst würde ich nur bedingt empfehlen“, sagt Experte Pfeiffer.

eMail ist ein dezentrales Medium

Die „electronic Mail“ ist laut Pfeiffer ein dezentrales Kommunikationsmedium.

Das heißt, dass dahinter keine spezifische Firma steckt. Wie sicher der Transportweg dieses Standard-Nachrichtendienstes ist, hängt vom Dienstleister ab – etwa Google, Yahoo oder der Arbeitgeber. Das Verschlüsseln der elektronischen Post ist laut Pfeiffer jedoch schwierig. Je nach Nutzung – etwa über Smartphone-Apps oder Webmail – ist sie schwierig zu implementieren

und kann ausfallen. Sie muss auch auf jedem Gerät, auf dem eMails abgerufen werden, installiert werden.

So sicher sind WhatsApp und SMS

[illegible]

SMS in jedem Fall unverschlüsselt

[illegible]

WhatsApp nutzt Metadaten

[illegible]

Facebook Messenger unsicher

[illegible]

Signal ist definitiv immer verschlüsselt

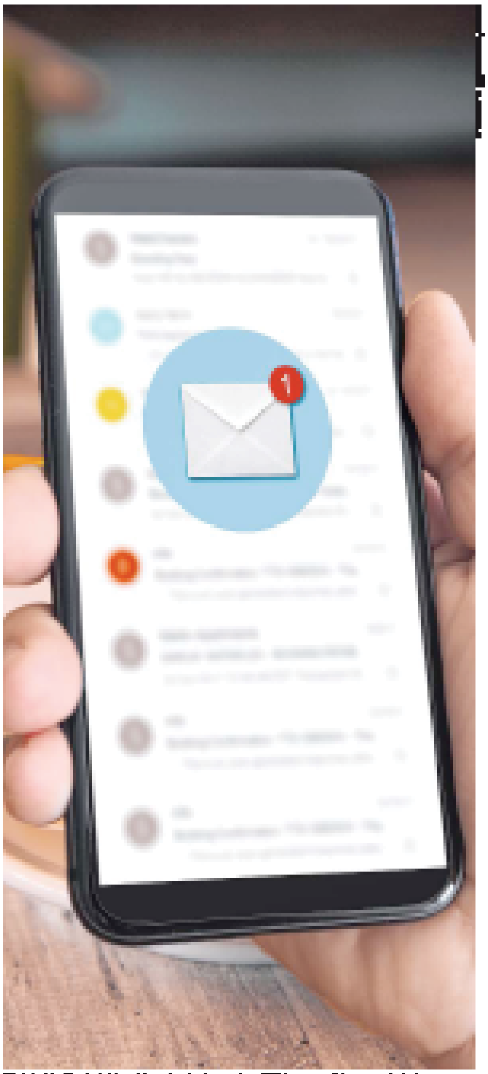
[illegible]

Telegram bewirbt sich als „sicher"

[illegible]

eMail ist dezentrales Medium

[illegible]



[illegible]

https://computerwelt.at/news/dekonstruktion-und-analyse-moderner-it-bedrohungen/

Dekonstruktion und Analyse moderner IT-Bedrohungen

04.11.2019, Klaus Lorbeer

Die jedes Jahr in Wien stattfindende DeepINTEL Security Intelligence Konferenz möchte eine Plattform bieten, auf der Behörden, Unternehmen, Forscher und Hacker produktiv in einem geschlossenen Kreis Eigenschaften und Gegenmaßnahmen von Bedrohungen diskutieren können.Skizzierte Analyse eines Netzwerkangriffs.
Skizzierte Analyse eines Netzwerkangriffs. (c) Florian Stocker, Crowes Agency OG
Wirtschaftsspionage wird sehr gerne als Beispiel für Bedrohungen im Bereich der Informationen angeführt. Spionage gibt es aber auf allen Ebenen. Im Mai 2019 wurde bekannt, dass man über WhatsApp-Anrufe Smartphones infizieren kann. Das Annehmen des Anrufs war nicht notwendig. Ausgenutzt wurde diese Schwachstelle von einer in Israel produzierten kommerziellen Spionagesoftware. Ausspioniert wurden damit keine Firmen, sondern Bürgerrechtlerinnen und Bürgerrechtler im Nahen Osten. Doch die Software ist vielseitig einsetzbar und könnte genauso auf Geschäftsführerinnen und Angestellte losgelassen werden. Schließlich sitzen die Kunden der israelischen Firma nicht nur im Nahen Osten, sondern auch in westlichen Staaten, wie die Veranstalter der DeepSec-Konferenz betonen

Der Knackpunkt ist das Finden von Schwachstellen, um die Verteidigung zu brechen oder zu umgehen. Die Kenntnis über solche Lücken wird mit viel Geld belohnt und gehandelt. Auch Schadcode ist – bei allen vorhandenen Unterschieden – eine Waffe. Die Attacken durch die Schadsoftware Petya und Wannacry in den Jahren 2016 bzw. 2017 unterstreichen diese Analogie, da die Ausnutzung der Schwachstelle, über die beide Programme eindringen konnten, sehr wahrscheinlich durch die US-amerikanische National Security Agency (NSA) entwickelt wurde. Konkrete Beweise über das tatsächliche Entkommen der Schwachstelle fehlen allerdings – die Theorien reichen von der Aktion eines Whistleblowers bis hin zu Tätern aus Russland. Gewissheit wird es wohl nie geben.

Für Sicherheitsverantwortliche in Unternehmen spielen die Spekulationen keine Rolle. Die Fakten zeigen, dass sich die digitale Welt direkt in geopolitischen Spannungsfeldern bewegt. Es wird daher höchste Zeit, diesen Umstand in interne Abläufe zu integrieren.

Geopolitik ist längst Teil von Unternehmensentscheidungen

Die Wirtschaft wird gerne und oft abseits der Politik wahrgenommen. Dies gilt insbesondere für digitale Dienstleistungen. Beim Streaming, der internen Dokumentenablage, E-Mail-Kommunikation oder Social-Media-Plattformen-

besitzen nur noch wenige Organisationen eine eigene Infrastruktur. „Wolkige Dienstleister verwalten fremde digitale Güter“, so die DeepSec-Veranstalter. Der sehr beliebte Begriff der Digitalen Souveränität verliere damit jede Bedeutung, wenn die Geschäftsführung nicht mehr sagen könne wo sich alle Unternehmensdaten genau befänden und wer sie verwalte. Man kann nichts beschützen dessen Aufenthaltsort man nicht kennt. Das gilt insbesondere für Prototypen wie die vom deutschen Wirtschaftsministerium vorgeschlagene Gaia-X-Infrastruktur. Sie soll eine Alternative zur Datenhaltung und -verarbeitung außerhalb der Grenzen Europas bieten. Damit ist Geopolitik zum Alltag in der Wirtschaft geworden – Software kann genau so wie die Hardware auch in Handelskriege verstrickt werden.

Die Beispiele illustrieren, dass sich die Unternehmensführungen endlich auch mit Themen beschäftigen müssen, die bisher die Außenpolitik und das Militär beschäftigt haben. Die IT-Sicherheit hat das schon längst erkannt und den Bereich der Security Intelligence geschaffen. Dort beschäftigt man sich mit dem strategischen Blick auf Bedrohungen und die Fähigkeiten der Gegner gegen die man sich verteidigen muss. Die technischen Details sind dabei zwar Rüstzeug, jedoch sekundär. Es geht um das Aufklären der Identitäten, Kapazitäten und Absichten gegnerischer Organisationen, welche die eigenen Daten und die eigene Infrastruktur attackieren können. Die klassische Informationssicherheit liefert die Werkzeuge, aber Analytiker müssen die Puzzlesteine richtig zusammensetzen. Genau dort setzt die jährlich in Wien stattfindende DeepINTEL Konferenz an – Austausch von Erkenntnissen in einer geschlossenen Gruppe.

Erfahrungsaustausch ist wichtig

Möchte man über echte Vorfälle und konkrete Einbrüche reden, so ist es ratsam, dies konzentriert im Rahmen von Diskussionen unter Expertinnen und Experten zu tun. Der Erfahrungsaustausch ist von unschätzbarem Wert und verbessert die Verteidigung nachhaltig. Die DeepINTEL ist eine solche Plattform. Fokus in diesem Jahr sind Attacken auf Energieversorger, Ausschaltung von Infrastruktur (Netzwerke, Stromversorgung), Analyse von Netzwerkverkehr zum Schutz autonomer Systeme, Aufklärung in globalen Netzwerken (Internet, Domain Name Service) und das Aufspüren von versteckten Kommunikationskanälen.

Der Fokus sind die Zusammenhänge zwischen Vorfällen und der Verwendung bestimmter Angriffswege. Beispielsweise erfährt man aus herkömmlicher Berichterstattung meist, welche Schadsoftware zugeschlagen hat. Man lernt aber sehr wenig über die tatsächlichen Infektionswege, welche Teile der Infrastruktur betroffen sind und was eigentlich das Ziel war. Diese Details lassen sich nur in kleinem Rahmen und Blick auf die Strategie besprechen. Speziell in der digitalen Welt sind Zusammenhänge oft schwer erkennbar, da das Internet global zur Verfügung steht. Die klare Zuordnung von Tätern – seien es Einzelpersonen, Organisationen oder Staaten – ist dabei sehr

schwierig bis unmöglich. Auch in bei diesen Überlegungen möchte die DeepINTEL allen Teilnehmern Hilfestellung geben.

Die notwendigen Daten für eine strategische Betrachtung der eigenen Informationstechnologie sind kritisch für eine aussagekräftige Analyse. Am Markt gibt es viele Dienstleister, die erfasste Daten zusammenführen und mit Sensornetzwerken ergänzen. Es kann aber niemand die Kenntnisse über die eigenen Prozesse und die interne Organisation ersetzen. Daher wird während der DeepINTEL Konferenz auch die Erfassung, die Bewertung und die richtige Auswertung der Informationen diskutiert, die bereits zur Verfügung stehen.

Programme und Buchung

Die DeepINTEL-Konferenz findet am 27. November 2019 in Wien statt. Tickets sind auf der Webseite https://deepintel.net/ erhältlich.

Die DeepSec- und DeepINTEL-Konferenz findet im Hotel The Imperial Riding School Vienna – A Renaissance Hotel, in der Ungargasse 60 im dritten Wiener Gemeindebezirk statt.

Das Programm der im Anschluss stattfindenden DeepSec-Konferenz ist unter https://deepsec.net/schedule.html ersichtlich. Das Programm der DeepINTEL wird ausschließlich auf Anfrage (deepsec@deepsec.net) zur Verfügung gestellt, weil es sich bei der DeepINTEL um eine nichtöffentliche Konferenz handelt.

Tickets für die DeepSec-Konferenz sowie für die DeepINTEL-Veranstaltung und die DeepSec-Trainings können Interessierte unter dem Link https://deepsec.net/register.html oder per E-Mail an deepsec@deepsec.net bestellen.

4. November 2019 Klaus Lorbeer/pi

Dekonstruktion und Analyse moderner IT-Bedrohungen

Die jedes Jahr in Wien stattfindende DeepINTEL Security Intelligence Konferenz möchte eine Plattform bieten, auf der Behörden, Unternehmen, Forscher und Hacker produktiv in einem geschlossenen Kreis Eigenschaften und Gegenmaßnahmen von Bedrohungen diskutieren können.

Skizzierte Analyse eines Netzwerkangriffs. (c) Florian Stocker, Crowes Agency OG

Wirtschaftsspionage wird sehr gerne als Beispiel für Bedrohungen im Bereich der Informationen angeführt. Spionage gibt es aber auf allen Ebenen. Im Mai 2019 wurde bekannt, dass man über WhatsApp-Anrufe Smartphones infizieren kann. Das Annehmen des Anrufs war nicht notwendig. Ausgenutzt wurde diese Schwachstelle von einer in Israel produzierten kommerziellen Spionagesoftware. Ausspioniert wurden damit keine Firmen, sondern Bürgerrechtlerinnen und Bürgerrechtler im Nahen Osten. Doch die Software ist vielseitig einsetzbar und könnte genauso auf Geschäftsführerinnen und Angestellte losgelassen werden. Schließlich sitzen die Kunden der israelischen Firma nicht nur im Nahen Osten, sondern auch in westlichen Staaten, wie die Veranstalter der DeepSec-Konferenz betonen

Der Knackpunkt ist das Finden von Schwachstellen, um die Verteidigung zu brechen oder zu umgehen. Die Kenntnis über solche Lücken wird mit viel Geld belohnt und gehandelt. Auch Schadcode ist – bei allen vorhandenen Unterschieden – eine Waffe. Die Attacken durch die Schadsoftware Petya und Wannacry in den Jahren 2016 bzw. 2017 unterstreichen diese Analogie, da die Ausnutzung der Schwachstelle, über die beide Programme eindringen konnten, sehr wahrscheinlich durch die US-amerikanische National Security Agency (NSA) entwickelt wurde. Konkrete Beweise über das tatsächliche Entkommen der Schwachstelle fehlen allerdings – die Theorien reichen von der Aktion eines Whistleblowers bis hin zu Tätern aus Russland. Gewissheit wird es wohl nie geben.

Für Sicherheitsverantwortliche in Unternehmen spielen die Spekulationen keine Rolle. Die Fakten zeigen, dass sich die digitale Welt direkt in geopolitischen Spannungsfeldern bewegt. Es wird daher höchste Zeit, diesen Umstand in interne Abläufe zu integrieren.

Geopolitik ist längst Teil von Unternehmensentscheidungen

Die Wirtschaft wird gerne und oft abseits der Politik wahrgenommen. Dies gilt insbesondere für digitale Dienstleistungen. Beim Streaming, der internen Dokumentenablage, E-Mail-Kommunikation oder Social-Media-Plattformenbesitzen

Begriff der Digitalen Souveränität verliere damit jede Bedeutung, wenn die Geschäftsführung nicht mehr sagen könne wo sich alle Unternehmensdaten genau befänden und wer sie verwalte. Man kann nichts beschützen dessen Aufenthaltsort man nicht kennt. Das gilt insbesondere für Prototypen wie die vom deutschen Wirtschaftsministerium vorgeschlagene Gaia-X-Infrastruktur. Sie soll eine Alternative zur Datenhaltung und -verarbeitung außerhalb der Grenzen Europas bieten. Damit ist Geopolitik zum Alltag in der Wirtschaft geworden – Software kann genau so wie die Hardware auch in Handelskriege verstrickt werden.

Die Beispiele illustrieren, dass sich die Unternehmensführungen endlich auch mit Themen beschäftigen müssen, die bisher die Außenpolitik und das Militär beschäftigt haben. Die IT-Sicherheit hat das schon längst erkannt und den Bereich der Security Intelligence geschaffen. Dort beschäftigt man sich mit dem strategischen Blick auf Bedrohungen und die Fähigkeiten der Gegner gegen die man sich verteidigen muss. Die technischen Details sind dabei zwar Rüstzeug, jedoch sekundär. Es geht um das Aufklären der Identitäten, Kapazitäten und Absichten gegnerischer Organisationen, welche die eigenen Daten und die eigene Infrastruktur attackieren können. Die klassische Informationssicherheit liefert die Werkzeuge, aber Analytiker müssen die Puzzlesteine richtig zusammensetzen. Genau dort setzt die jährlich in Wien stattfindende DeepINTEL Konferenz an – Austausch von Erkenntnissen in einer geschlossenen Gruppe.

Erfahrungsaustausch ist wichtig

Möchte man über echte Vorfälle und konkrete Einbrüche reden, so ist es ratsam, dies konzentriert im Rahmen von Diskussionen unter Expertinnen und Experten zu tun. Der Erfahrungsaustausch ist von unschätzbarem Wert und verbessert die Verteidigung nachhaltig. Die DeepINTEL ist eine solche Plattform. Fokus in diesem Jahr sind Attacken auf Energieversorger, Ausschaltung von Infrastruktur (Netzwerke, Stromversorgung), Analyse von Netzwerkverkehr zum Schutz autonomer Systeme, Aufklärung in globalen Netzwerken (Internet, Domain Name Service) und das Aufspüren von versteckten Kommunikationskanälen.

Der Fokus sind die Zusammenhänge zwischen Vorfällen und der Verwendung bestimmter Angriffswege. Beispielsweise erfährt man aus herkömmlicher Berichterstattung meist, welche Schadsoftware zugeschlagen hat. Man lernt aber sehr wenig über die tatsächlichen Infektionswege, welche Teile der Infrastruktur betroffen sind und was eigentlich das Ziel war. Diese Details lassen sich nur in kleinem Rahmen und Blick auf die Strategie besprechen. Speziell in der digitalen Welt sind Zusammenhänge oft schwer erkennbar, da das Internet global zur Verfügung steht. Die klare Zuordnung von Tätern – seien es Einzelpersonen, Organisationen oder Staaten – ist dabei sehr schwierig bis unmöglich. Auch in bei diesen Überlegungen möchte die DeepINTEL allen Teilnehmern Hilfestellung geben.

Die notwendigen Daten für eine strategische Betrachtung der eigenen Informationstechnologie sind kritisch für eine aussagekräftige Analyse. Am Markt gibt es viele Dienstleister, die erfasste Daten zusammenführen und mit Sensornetzwerken ergänzen. Es kann aber niemand die Kenntnisse über die eigenen Prozesse und die interne Organisation ersetzen. Daher wird während der DeepINTEL Konferenz auch die Erfassung, die Bewertung und die richtige Auswertung der Informationen diskutiert, die bereits zur Verfügung stehen.

Programme und Buchung

Die DeepINTEL-Konferenz findet am 27. November 2019 in Wien statt. Tickets sind auf der Webseite **https://deepintel.net/ erhältlich.**

Die DeepSec- und DeepINTEL-Konferenz findet im Hotel The Imperial Riding School Vienna – A Renaissance Hotel, in der Ungargasse 60 im dritten Wiener Gemeindebezirk statt.

wird ausschließlich auf Anfrage (deepsec@deepsec.net) zur Verfügung gestellt, weil es sich bei der DeepINTEL um eine nichtöffentliche Konferenz handelt.

Tickets für die DeepSec-Konferenz sowie für die DeepINTEL-Veranstaltung und die DeepSec-Trainings können Interessierte unter dem Link https://deepsec.net/register.html oder per E-Mail an deepsec@deepsec.net bestellen.

KONFERENZ SECURITY WIEN

MEHR ARTIKEL

NEWS

Drei wichtige IT-Trends für 2020

NEWS

KI: Hype oder kritischer Faktor für effiziente IT- und Datennutzung?

CASE-STUDY

Kendox realisiert „elektronische Studierendendossiers" für die ZHAW

CASE-STUDY

Schmitz Cargobull migriert SAP-Landschaft in Microsoft Azure

NEWS

Deutsche Fußball-Bundesliga setzt auf KI aus der Amazon-Cloud

NEWS

Ausblick 2020: Prognosen für Cloud-Lösungen

NEWS

Apple tauscht Smart Battery Cases aus

NEWS

TikTok will „sicheren" Stream für Brands

NEWS

TCL lanciert 5G-Smartphone

BE THE FIRST TO COMMENT

Leave a Reply

Your email address will not be published.

https://www.wko.at/service/Veranstaltung.html?id=cdd736e3-5d98-4e94-b3b7-fc019aa48cb9

Rabattcode DeepSec-Conference

Sichern Sie sich Ihren Rabattcode für die diesjährige ‘DeepSec-Conference’

Datum: 26.11.2019

Veranstalter: Fachgruppe UBIT Wien

Beginn: 00:00

Ende: 00:00

Veranstaltungstyp: Informationsveranstaltung

Ansprechpartner: UBIT Wien

Veranstaltungsort: Imperial Riding School Renaissance Vienna Hotel

Ungargasse 60

1030 Wien Wien

Anmeldung bis 17.11.2019

Liebe Mitglieder der UBIT,

nutzten Sie die Chance und nehmen Sie an der diesjährige DeepSec-Conference teil. Details über die Conference finden Sie hier.

Bei dieser Veranstaltung treffen die weltweit renommiertesten Sicherheitsexperten aus Wissenschaft, Regierung, Industrie und der Underground-Hacking-Community zusammen.

Insgesamt stehen 20 Rabattcodes zur Verfügung (1 Code pro Mitglied).

Melden Sie sich für einen der Codes über den Button unten an!

Den Code erhalten Sie nach der Anmeldefrist.

Wir freuen uns auf Ihr Kommen und wünschen Ihnen eine interessante Veranstaltung!

Freundliche Grüße

Ihr

Mag. Martin Puaschitz

Obmann der Fachgruppe UBIT

November
26
Dienstag

InPlanung - Rabattcode DeepSec-Conference

Sichern Sie sich Ihren Rabattcode für die diesjährige 'DeepSec-Conference'

Datum **26.11.2019**

Veranstalter **Fachgruppe UBIT Wien**

Beginn **00:00**

Ende **00:00**

Veranstaltungstyp **Informationsveranstaltung**

Ansprechpartner **UBIT Wien**

Veranstaltungsort **Imperial Riding School Renaissance Vienna Hotel**
Ungargasse 60
1030 Wien Wien

Anmeldung bis **17.11.2019**

Liebe Mitglieder der UBIT,

nutzten Sie die Chance und nehmen Sie an der diesjährige DeepSec-Conference teil. Details über die Conference finden Sie hier.
Bei dieser Veranstaltung treffen die weltweit renommiertesten Sicherheitsexperten aus Wissenschaft, Regierung, Industrie und der Underground-Hacking-Community zusammen.

Insgesamt stehen 20 Rabattcodes zur Verfügung (1 Code pro Mitglied).
Melden Sie sich für einen der Codes über den Button unten an!

Den Code erhalten Sie nach der Anmeldefrist.

Wir freuen uns auf Ihr Kommen und wünschen Ihnen eine interessante Veranstaltung!

Freundliche Grüße
Ihr
Mag. Martin Puaschitz
Obmann der Fachgruppe UBIT

› Zur Veranstaltung anmelden

Termin exportieren

Das könnte Sie auch interessieren

› Normenseminare e-Marke 2019/2020

› Kreativwirtschafts-Coworking in London

Mekka für kreative Querdenker

https://computerwelt.at/news/deepsec-und-deepintel-konferenzen-veroeffentlichen-programm/

02.09.2019

DeepSec- und DeepINTEL-Konferenzen veröffentlichen Programm

Die zunehmende Vernetzung erreicht immer mehr Bereiche des Alltags und der Gesellschaft. Die diesjährigen Sicherheitskonferenzen DeepSec und DeepINTEL möchten daher das Internet der Fakten und der Furcht nüchtern aus dem Blickwinkel der Informationssicherheit betrachten.Die DeepSec-Konferenz findet in Wien am 28. und 29. November statt.

Die DeepSec-Konferenz findet in Wien am 28. und 29. November statt. (c) DeepSec GmbH

Systeme sind derzeit weniger isoliert und viel komplexer als es sicherheitstechnisch vertretbar ist. Die DeepSec widmet sich daher in zwei Tagen Konferenz und zwei Tagen Trainings aktuellen Technologien und deren Verwundbarkeiten. Parallel dazu wird in der DeepINTEL-Seminarkonferenz das Verhältnis zwischen Geopolitik und IT-Sicherheit anhand von Vorfällen diskutiert.

Internet der Angriffe statt der Dinge

Sobald man ein System mit dem Internet verbindet, bekommt man es sofort zu spüren. Lohnende oder verwundbare Ziele werden automatisch gesucht und angegriffen. Verbindet man Sensoren, Geräte oder Aktore (bekannt als „Dinge“ im Internet der Dinge) mit einem Netzwerk, so ist es nicht anders. Die Vorträge der diesjährigen DeepSec-Konferenz versuchen die Verbindungen zwischen verschiedenen Aspekten der IT-Sicherheit mit diesem Hintergrund herzustellen. Mobile Endgeräte sind seit ihrer Existenz bedroht. Moderne Mobilfunktechnologien setzen auf Daten. Es ist daher keine Überraschung, dass Luca Melette in seiner Präsentation vorstellt, wie man mobile Systeme ausschließlich über das Internetprotokoll angreift. Aleksandr Kolchanov wird zeigen, wie man bestimmte Mobilfunkgeräte kompromittieren und massenweise auslesen kann. Lior Yaari teilt seine Erfahrung aus dem Bereich des Automobilbaus. Er hat zukünftige Komponenten moderner Autos analysiert, Komponenten, die noch nicht auf dem Markt, aber bereits in Entwicklung sind. Lior wird über Schwachstellen berichten, die möglicherweise in einigen Jahren über unsere Straßen rollen.

Training mit Sicherheitsexperten

Die DeepSec-Konferenz bietet jedes Jahr eine Weiterbildung von Sicherheitsexperten für Experten in Ihrem Unternehmen an. Austausch von Wissen ist die Grundlage jeder guten Verteidigung, nicht nur digital. Durch die Kurzlebigkeit in der Informationstechnologie ist der eigene Wissensstand und die eigene Weiterbildung maßgeblich für den Umgang mit Angriffen und der ständigen Vernetzung. Im Programm sind daher drei verschiedene Workshops, die sich um den Umgang mit Angreifern drehen. Xavier Mertens lehrt die Aufklärung von Bedrohungen mit Open-Source-Security. Verwendet werden öffentlich zugängliche Quellen, um den Umgang damit und den Aufbau

von internen Prozessen zu vermitteln. Darüber hinaus werden an Fallstudien Beispiele für das Detektieren von verdächtigen Mustern gelehrt.

Peter Manev und Eric Leblond zeigen in ihrem Workshop, wie man mit dem Intrusion-Detection-Werkzeug „Suricata“ Angriffe und verdächtige Vorgänge im Netzwerk erkennen kann. Suricata ist leicht einzusetzen und bietet sehr viele Funktionen. Da beide Trainer im Entwicklungsteam von Suricata sind, erfährt man direkt Details über die internen Abläufe der Software. Zusätzlich werden die Teilnehmer an echtem Netzwerkverkehr das Erstellen von Regeln üben. Das Training ist laut Veranstalter praxisorientiert und wendet sich an alle, die Netzwerksicherheit betreiben müssen.

Thomas Fischer und Craig Jones zeigen in ihrem Workshop, wie man mit Sicherheitsvorfällen umgeht und wie man Spuren der Angreifer findet. Auch hier wird an echten Fällen und realen Beispielen der Umgang mit den richtigen Werkzeugen vermittelt.

Technik ist keine Insel

Oft wird bei der Betrachtung von Sicherheitsproblemen nur der technische Standpunkt berücksichtigt. Es gibt in der Informationstechnologie, genau wie in anderen Bereichen, externe Faktoren, die bestimmte Rahmenbedingungen vorgeben. Ein prominentes Beispiel ist die seit den 1990er Jahren immer wiederkehrende Diskussion um Hintertüren in digitalen Systemen und Kommunikationsnetzwerken. Was mit der Verschlüsselung von Mobilfunk und E-Mail anfing, das setzt sich jetzt bei 5G, Messenger und Softwareentwicklung fort. Die australische Regierung hat 2018 ein Gesetz erlassen, das Tech-Firmen zwingen kann Hintertüren in ihre Produkte einzubauen. Diese Sollbruchstellen werden künftig von Angreifern ebenfalls verwendet werden.

Die Mathematik der Verschlüsselung ist beim Thema Sicherheit unerbittlich. Entweder man hat eine sichere Kommunikation, oder man hat sie nicht. Die aktuellen Handelskriege betreffen die IT-Welt ebenso nachhaltig und stellen die Weichen für Umsetzungen neuer Technologien in den nächsten Jahren. Aus diesem Grund werden auf der diesjährigen DeepSec und DeepINTEL die Wechselwirkungen der Informationssicherheit mit geopolitischen Aspekten untersucht. Die Vorträge beider Veranstaltungen wurden unter diesem Aspekt ausgesucht. Diskutiert werden unter anderem Mittel und Wege von Angriffen, die Einordnung der Ziele und welche Bedingungen sich für den Einsatz von Sicherheitsmaßnahmen ergeben. Die Veranstalter empfehlen Sicherheitsverantwortlichen dringend den eigenen Horizont um diese Aspekte zu erweitern.

Programme und Buchung

Die DeepSec-2019-Konferenztage finden am 28. und 29. November statt. Die DeepSec-Trainings sind zwei Tage zuvor angesetzt, am 26. und 27. November.

Die DeepINTEL-Konferenz findet am 27. November statt. Das Programm senden die Veranstalter auf Anfrage an deepsec@deepsec.net gerne zu, weil es sich bei der DeepINTEL um eine nichtöffentliche Konferenz handelt. Tickets sind auf der Webseite https://deepintel.net erhältlich. Das Programm der DeepSec-Konferenz ist wiederum unter https://deepsec.net/schedule.html einsehbar.

Tickets für die DeepSec-Konferenz sowie für die DeepINTEL-Veranstaltung und die DeepSec-Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html bestellen.

Der Veranstaltungsort für DeepSec und DeepINTEL ist das Hotel The Imperial Riding School Vienna – A Renaissance Hotel, Ungargasse 60, 1030 Wien.

2. September 2019 Klaus Lorbeer/pi

DeepSec- und DeepINTEL-Konferenzen veröffentlichen Programm

Die zunehmende Vernetzung erreicht immer mehr Bereiche des Alltags und der Gesellschaft. Die diesjährigen Sicherheitskonferenzen DeepSec und DeepINTEL möchten daher das Internet der Fakten und der Furcht nüchtern aus dem Blickwinkel der Informationssicherheit betrachten.

Die DeepSec-Konferenz findet in Wien am 28. und 29. November statt. (c) DeepSec GmbH

Systeme sind derzeit weniger isoliert und viel komplexer als es sicherheitstechnisch vertretbar ist. Die DeepSec widmet sich daher in zwei Tagen Konferenz und zwei Tagen Trainings aktuellen Technologien und deren Verwundbarkeiten. Parallel dazu wird in der DeepINTEL-Seminarkonferenz das Verhältnis zwischen Geopolitik und IT-Sicherheit anhand von Vorfällen diskutiert.

Internet der Angriffe statt der Dinge

Sobald man ein System mit dem Internet verbindet, bekommt man es sofort zu spüren. Lohnende oder verwundbare Ziele werden automatisch gesucht und angegriffen. Verbindet man Sensoren, Geräte oder Aktore (bekannt als „Dinge" im Internet der Dinge) mit einem Netzwerk, so ist es nicht anders. Die Vorträge der diesjährigen DeepSec-Konferenz versuchen die Verbindungen zwischen verschiedenen Aspekten der IT-Sicherheit mit diesem Hintergrund herzustellen. Mobile Endgeräte sind seit ihrer Existenz bedroht. Moderne Mobilfunktechnologien setzen auf Daten. Es ist daher keine Überraschung, dass Luca Melette in seiner Präsentation vorstellt, wie man mobile Systeme ausschließlich über das Internetprotokoll angreift. Aleksandr Kolchanov wird zeigen, wie man bestimmte Mobilfunkgeräte kompromittieren und massenweise auslesen kann. Lior Yaari teilt seine Erfahrung aus dem Bereich des Automobilbaus. Er hat zukünftige Komponenten moderner Autos analysiert, Komponenten, die noch nicht auf dem Markt, aber bereits in Entwicklung sind. Lior wird über Schwachstellen berichten, die möglicherweise in einigen Jahren über unsere Straßen rollen.

Training mit Sicherheitsexperten

Die DeepSec-Konferenz bietet jedes Jahr eine Weiterbildung von Sicherheitsexperten für Experten in Ihrem Unternehmen an. Austausch von Wissen ist die Grundlage jeder guten Verteidigung, nicht nur digital. Durch die Kurzlebigkeit in der Informationstechnologie ist der eigene Wissensstand und die eigene Weiterbildung maßgeblich für den Umgang mit Angriffen und der ständigen Vernetzung. Im Programm sind daher drei verschiedene Workshops, die sich um den Umgang mit Angreifern drehen. Xavier Mertens lehrt die Aufklärung von Bedrohungen mit Open-Source-Security. Verwendet werden öffentlich zugängliche Quellen, um den Umgang

Peter Manev und Eric Leblond zeigen in ihrem Workshop, wie man mit dem Intrusion-Detection-Werkzeug „Suricata" Angriffe und verdächtige Vorgänge im Netzwerk erkennen kann. Suricata ist leicht einzusetzen und bietet sehr viele Funktionen. Da beide Trainer im Entwicklungsteam von Suricata sind, erfährt man direkt Details über die internen Abläufe der Software. Zusätzlich werden die Teilnehmer an echtem Netzwerkverkehr das Erstellen von Regeln üben. Das Training ist laut Veranstalter praxisorientiert und wendet sich an alle, die Netzwerksicherheit betreiben müssen.

Thomas Fischer und Craig Jones zeigen in ihrem Workshop, wie man mit Sicherheitsvorfällen umgeht und wie man Spuren der Angreifer findet. Auch hier wird an echten Fällen und realen Beispielen der Umgang mit den richtigen Werkzeugen vermittelt.

Technik ist keine Insel

Oft wird bei der Betrachtung von Sicherheitsproblemen nur der technische Standpunkt berücksichtigt. Es gibt in der Informationstechnologie, genau wie in anderen Bereichen, externe Faktoren, die bestimmte Rahmenbedingungen vorgeben. Ein prominentes Beispiel ist die seit den 1990er Jahren immer wiederkehrende Diskussion um Hintertüren in digitalen Systemen und Kommunikationsnetzwerken. Was mit der Verschlüsselung von Mobilfunk und E-Mail anfing, das setzt sich jetzt bei 5G, Messenger und Softwareentwicklung fort. Die australische Regierung hat 2018 ein Gesetz erlassen, das Tech-Firmen zwingen kann Hintertüren in ihre Produkte einzubauen. Diese Sollbruchstellen werden künftig von Angreifern ebenfalls verwendet werden.

Die Mathematik der Verschlüsselung ist beim Thema Sicherheit unerbittlich. Entweder man hat eine sichere Kommunikation, oder man hat sie nicht. Die aktuellen Handelskriege betreffen die IT-Welt ebenso nachhaltig und stellen die Weichen für Umsetzungen neuer Technologien in den nächsten Jahren. Aus diesem Grund werden auf der diesjährigen DeepSec und DeepINTEL die Wechselwirkungen der Informationssicherheit mit geopolitischen Aspekten untersucht. Die Vorträge beider Veranstaltungen wurden unter diesem Aspekt ausgesucht. Diskutiert werden unter anderem Mittel und Wege von Angriffen, die Einordnung der Ziele und welche Bedingungen sich für den Einsatz von Sicherheitsmaßnahmen ergeben. Die Veranstalter empfehlen Sicherheitsverantwortlichen dringend den eigenen Horizont um diese Aspekte zu erweitern.

Programme und Buchung

Die DeepSec-2019-Konferenztage finden am 28. und 29. November statt. Die DeepSec-Trainings sind zwei Tage zuvor angesetzt, am 26. und 27. November.

Die DeepINTEL-Konferenz findet am 27. November statt. Das Programm senden die Veranstalter auf Anfrage an deepsec@deepsec.net gerne zu, weil es sich bei der DeepINTEL um eine nichtöffentliche Konferenz handelt. Tickets sind auf der Webseite https://deepintel.net erhältlich. Das Programm der DeepSec-Konferenz ist wiederum unter https://deepsec.net/schedule.html einsehbar.

Tickets für die DeepSec-Konferenz sowie für die DeepINTEL-Veranstaltung und die DeepSec-Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html bestellen.

Der Veranstaltungsort für DeepSec und DeepINTEL ist das Hotel The Imperial Riding School Vienna – A Renaissance Hotel, Ungargasse 60, 1030 Wien.

KONFERENZ SECURITY WIEN

https://medium.com/@deepsec/deepsec-2019-preliminary-schedule-is-online-837e8c47793b

DeepSec 2019 Preliminary Schedule is online *

Aug 14, 2019 · 2 min read

We have reviewed all submissions, and we have published the preliminary schedule. It wasn't easy to pick, because we received more submission than in the years before. Even though we start the reviews early, as soon as they arrive, it usually takes a couple of days to get to a stable version. The process is very similar to other forms of content creation with components, such as software development, or creative/technical writing. The most important fact is the preliminary schedule of DeepSec 2019. You can view it online. We are working on a new calendar export, so that you can view it on the go as well.

Some slots are still vacant. The reason is the ongoing review process, and cancellations due to conflicts regarding our speakers. We will fill the remaining slots during the next weeks. The online version of the schedule is always the correct version.

We also debugged our ticket shop. The creation of the DeepSec and DeepINTEL 2019 event introduced some bugs regarding the categories. We have fixed this. If you have any questions about the different categories, please let us know. Anyone interested in attending our trainings should book tickets as early as possible! Trainings cannot be conducted if the number of participants is below a certain threshold, because the trainer has to get to Vienna. As always, book early, and book often. It helps us a lot.

*Originally published at https://blog.deepsec.net on August 14, 2019.

DeepSec 2019 Preliminary Schedule is online *

DeepSec Conference Follow
Aug 14, 2019 · 2 min read

We have reviewed all submissions, and we have published the preliminary schedule. It wasn't easy to pick, because we received more submission than in the years before. Even though we start the reviews early, as soon as they arrive, it usually takes a couple of days to get to a stable version. The process is very similar to other forms of content creation with components, such as software development, or creative/technical writing. The most important fact is the preliminary schedule of DeepSec 2019. You can view it online. We are working on a new calendar export, so that you can view it on the go as well.

Some slots are still vacant. The reason is the ongoing review process, and cancellations due to conflicts regarding our speakers. We will fill the remaining slots during the next weeks. The online version of the schedule is always the correct version.

We also debugged our ticket shop. The creation of the DeepSec and DeepINTEL 2019 event introduced some bugs regarding the categories. We have fixed this. If you have any questions about the different categories, please let us know. *Anyone interested in attending our trainings should book tickets as early as possible!* Trainings cannot be conducted if the number of participants is below a certain threshold, because the trainer has to get to Vienna. As always, book early, and book often. It helps us a lot.

. . .

Originally published at https://blog.deepsec.net on August 14, 2019.

https://www.it-daily.net/shortnews/20666-it-sicherheit-steht-zunehmend-im-zeichen-der-geopolitik

DEEPSEC KONFERENZ

IT-SICHERHEIT STEHT ZUNEHMEND IM ZEICHEN DER GEOPOLITIK

20.02.2019

Die DeepSec Konferenz möchte dieses Jahr das Augenmerk auf die Verbindung zwischen Geopolitik und Informationssicherheit legen. Sie widmet sich den technischen Herausforderungen des Internets der Dinge, den kommenden Netzwerktechnologien und den geopolitischen Randbedingungen diktiert durch Schlüsselereignisse der letzten 6 Jahre.

Wer den Technologie Teil des jeweiligen Lieblingsmagazins liest, kann sich vor den Versprechungen kommender Netzwerktechnologien kaum retten. Das eigene Auto wird zum Smartphone. Der sprechende Kühlschrank wird zur Therapeutin. 5G-Mobilfunknetze versprechen glasfaserschnelles Streaming von Daten auf dem geschwindigkeitsbeschränkten Elektroroller. Beim zweiten Lesen offenbahrt sich die Bedeutung des Buchstabens G in 5G - er steht für Geopolitik. Es gibt im Zuge des Netzwerkausbaus Diskussionen um versteckte Killswitches zwecks Notabschaltungen ganze Netzwerke und Hintertüren zur Belauschung der Kunden. Die im November stattfindende DeepSec-In-Depth-Security-Konferenz widmet sich den technischen Herausforderungen des Internets der Dinge, den kommenden Netzwerktechnologien und den geopolitischen Randbedingungen diktiert durch Schlüsselereignisse der letzten 6 Jahre.

5G ALS FORTSETZUNG DER HANDELSKRIEGE

Es gibt weltweit sehr wenige Anbieter von Mobilfunknetzwerktechnologie. Der Name Huawei wird in den letzten Monaten in der Berichterstattung recht oft erwähnt. Diskutiert werden dann selten die Vorzüge der angebotenen Produkte oder die tatsächlichen Implementationen des neuen Mobilfunkstandards 5G. Stattdessen geht es um den Vorwurf heimlich eingebauter Notabschaltungen, die auf einen Schlag das komplette Mobilfunknetz eines Betreibers lahmlegen können. Angeklagt wird auch vermeintlicher versteckter Code, der Fernzugriff und das Kopieren von Daten aus dem Netzwerk erlaubt. Gerüstet mit vielen Vorwürfen ohne konkrete Beweise wird gerade in bestimmten westlichen Ländern ein Ausschluss chinesischer Telekommunikationsausrüster öffentlich diskutiert.

Die Sorgen sind berechtigt, jedoch sind sie Sicherheitsforschern nicht fremd. Fast alle Computer, die in Europa und anderswo eingesetzt werden, stammen selten aus den Ländern, in denen sie ihre Arbeit tatsächlich verrichten.

Die Chips, die Firmware und viele weitere Zutaten in Hard- und Software werden woanders gebaut. Da man in den letzten Dekaden systematisch darauf verzichtet hat, den Inhalt der Box hinter Tastatur oder Touchscreen zu hinterfragen, geschweige zu verstehen, blühen die Anschuldigungen getrieben von der Phantasie.

Die IT-Security-Forschung kann dem nur mit Fakten und solider Recherche begegnen. Robert Hannigan, der ehemalige Chef des britischen Geheimdiensts GCHQ, hat bestätigt, dass sich das britische National Cyber Security Centre (NCSC) lange Jahre mit Komponenten aus chinesischen Lieferketten beschäftigt hat. Bisher hat es laut seiner Aussage keine Indizien für staatlich verordnete verdeckte Angriffe durch Huawei Hardware gegeben. NCSC hat seit 2010 mit Hilfe des Huawei Security Evaluation Centres (HSEC) Zugang zum Quellcode der Produkte.

Der Sinn dahinter ist eine Zertifizierung durch das NCSC bevor Technologie in sensitiven Bereichen eingesetzt werden kann. Robert Hannigan widerspricht damit direkt den Vorwürfen aus den USA und der Einschätzung von Gerhard Schindler, dem früheren Präsident des deutschen Bundesnachrichtendienstes (BND). Darüber hinaus ignorieren die Kritiker die bereits jetzt in Europa vorgeschriebenen gesetzlichen Überwachungsschnittstellen, standardisiert durch das Europäische Institut für Telekommunikationsnormen (ETSI). Diese Vorgaben gelten übrigens für alle Anbieter, die in Europa Netzwerke bauen oder bauen lassen möchten.

INTRANET STATT INTERNET

Die aktuelle Nachrichtenlage illustriert daher sehr gut was man alles in der Informationssicherheit beachten sollte. Die Absicherung der eigenen Daten ist längst nicht mehr mit einzelnen isolierten Betrachtungen getan. Die DeepSec Konferenz hat obendrein eine lange Tradition der Sicherheitsforschung im Mobilfunkbereich, angefangen von der ersten öffentlichen Publikation von Schwachstellen des A5/1 Verschlüsselungsalgorithmus (zwischen Telefon und Funkzelle) bis hin zu Sicherheitsproblemen bei Smartphones. Dieser Bereich ist nur ein Beispiel, und hat durch die rasante Verbreitung von Mobiltechnologie immens an Bedeutung gewonnen.

Um den diskutierten Killswitch in Netzwerken wieder aufzugreifen: Die Idee in einem nationalen Notfall Informationsnetzwerke zu kontrollieren ist nicht neu. Präsident Franklin D. Roosevelt hat dies im Communications Act of 1934 schon umgesetzt. Damals ging es um Medien. Im vorgeschlagenen Protecting Cyberspace as a National Asset Act of 2010 wollte man dasselbe für das Internet umsetzen, mit dem Unterschied der Abschaltung statt Kontrolle. Das vorgeschlagene Gesetz von 2010 verfiel ohne Stimmen zu bekommen, weil die technische Umsetzung nicht klar war und nach wie vor auch nicht ist. Der Gedanken mit einem simplen Schalter Kommunikationsnetzwerke nach Belieben lahmzulegen funktionierte auf der Kinoleinwand oder im Fernsehen noch gut - leider nur in der Vergangenheit, denn mittlerweile werden Informationen per Internet gestreamt.

Die Alternative ist ein strikt nationales Netzwerk. Die iranische Regierung arbeitet an einem iranischen Intranet, angespornt durch Proteste im Jahre 2009. Die chinesische Firewall versucht etwas ähnliches, allerdings durch strenge Filter gesteuert durch Redaktionen. Rußland probt derzeit ebenfalls eine Abkopplung vom Internet. Die Kommunikationsnetzwerke sollen dann zwar noch funktionieren, aber man plant sie vom Rest der Welt zu trennen. Das ist de fakto einfach die fettarme Variante des Killswitches. Beide Ansätze demonstrieren wie enorm die Bedeutung des Internets mittlerweile geworden ist - es kann nicht mehr ignoriert werden. Das gilt für Unternehmen noch viel mehr als für Länder.

DIGITALER REALISMUS

Realistisch betrachtet macht es wenig Sinn die eigene Bevölkerung und den Staat zunächst von einem Netzwerk abhängig zu machen, um das dann wieder abzuschalten. Die Sehnsucht nach lokalen Netzwerken beweist das. In Unternehmen ist es nicht anders. Daten müssen ausgetauscht und Kommunikation muss stattfinden. Seriöse Informationssicherheit muss daher untersuchen wie sich die Integrität der Infrastruktur und von Daten auch unter widrigen Umständen erhalten lassen. Wichtigster Punkt ist dabei das sichere Design von Applikationen von Anfang an. Dazu gab es bei den vergangenen DeepSec-Konferenzen reichlich Vorträge und Trainings als Weiterbildung für Entwicklerinnen und Planer.

Der IT-Security haftet der Ruf eines Verhinderers an. Tatsächlich ist das Gegenteil der Fall. Vergangene Sicherheitsvorfälle und publizierte Dokumente über organisierte Schwachstellen wie beispielsweise durch Edward Snowden sind und waren wesentliche Bausteine für eine Verbesserung der Sicherheit in unserem Alltag. Voraussetzung dafür ist paradoxerweise ein freier Austausch zwischen Sicherheitsforschern. Ein nationales Intranet, Verbote von kryptographischen Algorithmen, Filter für publizierte Inhalte oder ähnliche Restriktionen sind daher der maximal unsicherste Kontrapunkt zu notwendiger Sicherheit in der digitalen Welt.

Die DeepSec Konferenz möchte daher explizit nicht nur Sicherheitsexperten ansprechen. Die Durchdringung digitaler Netze erfordert für eine sinnvolle Weiterentwicklung der IT-Sicherheitsmaßnahmen die Einbindung von Unternehmen, Entwicklerinnen, der Hacker Community, Behörden, Anwendern, Infrastrukturbetreibern, Designern und interdisziplinären Wissenschaftlerinnen. Menschen in beratender Funktion sind ausdrücklich eingeladen an dem Austausch von Erfahrungen und Ideen im November in Wien teilzunehmen.

Weitere Informationen zur DeepSec Konferenz:

BEITRÄGE GESUCHT - CALL FOR PAPERS

Die DeepSec Konferenz möchte dieses Jahr das Augenmerk auf die Verbindung zwischen Geopolitik und Informationssicherheit legen. Bis zum 31. Juli 2019 werden daher Vorträge gesucht, welche sich mit Technologien beschäftigen, die beide Welten berühren. Konkret sind das die Herausforderungen für Industrie- und Steuerungssysteme, der Internet der Dinge, sämtliche mobil eingesetzte Kommunikationstechnologie (vom Auto bis zum Telefon), Einsatz von Algorithmen und moderne Datenhaltung. Wir erleben gerade eine beschleunigte Vermischung neuer und vorhandener Methoden. Es sind Sicherheitsforscherinnen gefragtt, die sich kreativ mit den aktuellen Möglichkeiten auseinandersetzen und Schwachstellen aufzeigen. Risiken lassen sich erst dann managen, wenn man sie kennt. Das Programmkommittee freut sich daher auf möglichst viele Einreichungen, die Trends und sogenannte Zukunftstechnologien ganz genau unter das digitale Mikroskop legen.

Die zweitägigen Trainings vor der DeepSec Konferenz sind auch Teil des Call for Papers. Trainerinnen, die ihr Wissen weitergeben möchten, sind herzlich eingeladen Kurse einzureichen. Akzeptierte Kurse werden vorzeitig bekanntgegeben, um den Teilnehmern die Planung beim Buchen zu erleichtern.

PROGRAMME UND BUCHUNG

Die DeepSec 2019-Konferenztage sind am 28. und 29. November. Parallel finden die ROOTS 2019 Vorträge in einem separaten Saal ebenso am 28. und 29. November statt. Die DeepSec Trainings finden an den zwei vorangehenden Tagen, dem 26. und 27. November statt. Die DeepINTEL Konferenz findet am 27. November statt. Das Programm senden wir auf Anfragen an deepsec@deepsec.net gerne zu. Tickets sind auf der Webseite https://deepintel.net erhältlich.

Der Veranstaltungsort für DeepSec, DeepINTEL und ROOTS 2019 ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Einreichungen können unter https://deepsec.net/cfp.html abgegeben werden. Das aktuelle Programm der Veranstaltungen wird nach dem Abschluss der Einreichungsfristen bekanntgegeben.

Tickets für die DeepSec Konferenz sowie ROOTS 2019 und die DeepSec Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html bestellen.

deepsec.net

Shortnews (/shortnews)

DEEPSEC KONFERENZ

IT-SICHERHEIT STEHT ZUNEHMEND IM ZEICHEN DER GEOPOLITIK

20. Februar 2019

Die DeepSec Konferenz möchte dieses Jahr das Augenmerk auf die Verbindung zwischen Geopolitik und Informationssicherheit legen. Sie widmet sich den technischen Herausforderungen des Internets der Dinge, den kommenden Netzwerktechnologien und den geopolitischen Randbedingungen diktiert durch

Kühlschrank wird zur Therapeutin. 5G-Mobilfunknetze versprechen glasfaserschnelles Streaming von Daten auf dem geschwindigkeitsbeschränkten Elektroroller. Beim zweiten Lesen offenbahrt sich die Bedeutung des Buchstabens G in 5G - er steht für Geopolitik. Es gibt im Zuge des Netzwerkausbaus Diskussionen um versteckte Killswitches zwecks Notabschaltungen ganze Netzwerke und Hintertüren zur Belauschung der Kunden. Die im November stattfindende DeepSec-In-Depth-Security-Konferenz widmet sich den technischen Herausforderungen des Internets der Dinge, den kommenden Netzwerktechnologien und den geopolitischen Randbedingungen diktiert durch Schlüsselereignisse der letzten 6 Jahre.

5G ALS FORTSETZUNG DER HANDELSKRIEGE

Es gibt weltweit sehr wenige Anbieter von Mobilfunknetzwerktechnologie. Der Name Huawei wird in den letzten Monaten in der Berichterstattung recht oft erwähnt. Diskutiert werden dann selten die Vorzüge der angebotenen Produkte oder die tatsächlichen Implementationen des neuen Mobilfunkstandards 5G. Stattdessen geht es um den Vorwurf heimlich eingebauter Notabschaltungen, die auf einen Schlag das komplette Mobilfunknetz eines Betreibers lahmlegen können. Angeklagt wird auch vermeintlicher versteckter Code, der Fernzugriff und das Kopieren von Daten aus dem Netzwerk erlaubt. Gerüstet mit vielen Vorwürfen ohne konkrete Beweise wird gerade in bestimmten westlichen Ländern ein Ausschluss chinesischer Telekommunikationsausrüster öffentlich diskutiert.

Die Sorgen sind berechtigt, jedoch sind sie Sicherheitsforschern nicht fremd. Fast alle Computer, die in Europa und anderswo eingesetzt werden, stammen selten aus den Ländern, in denen sie ihre Arbeit tatsächlich verrichten. Die Chips, die Firmware und viele weitere Zutaten in Hard- und Software werden woanders gebaut. Da man in den letzten Dekaden systematisch darauf verzichtet hat, den Inhalt der Box hinter Tastatur oder Touchscreen zu hinterfragen, geschweige zu verstehen, blühen die Anschuldigungen getrieben von der Phantasie.

Die IT-Security-Forschung kann dem nur mit Fakten und solider Recherche begegnen. Robert Hannigan, der ehemalige Chef des britischen Geheimdiensts GCHQ, hat bestätigt, dass sich das britische National Cyber Security Centre (NCSC) lange Jahre mit Komponenten aus chinesischen Lieferketten beschäftigt hat. Bisher hat es laut seiner Aussage keine Indizien für staatlich verordnete verdeckte Angriffe durch Huawei Hardware gegeben. NCSC hat seit 2010 mit Hilfe des Huawei Security Evaluation Centres (HSEC) Zugang zum Quellcode der Produkte.

Der Sinn dahinter ist eine Zertifizierung durch das NCSC bevor Technologie in sensitiven Bereichen eingesetzt werden kann. Robert Hannigan widerspricht damit direkt den Vorwürfen aus den USA und der Einschätzung von

ignorieren die Kritiker die bereits jetzt in Europa vorgeschriebenen gesetzlichen Überwachungsschnittstellen, standardisiert durch das Europäische Institut für Telekommunikationsnormen (ETSI). Diese Vorgaben gelten übrigens für alle Anbieter, die in Europa Netzwerke bauen oder bauen lassen möchten.

INTRANET STATT INTERNET

Die aktuelle Nachrichtenlage illustriert daher sehr gut was man alles in der Informationssicherheit beachten sollte. Die Absicherung der eigenen Daten ist längst nicht mehr mit einzelnen isolierten Betrachtungen getan. Die DeepSec Konferenz hat obendrein eine lange Tradition der Sicherheitsforschung im Mobilfunkbereich, angefangen von der ersten öffentlichen Publikation von Schwachstellen des A5/1 Verschlüsselungsalgorithmus (zwischen Telefon und Funkzelle) bis hin zu Sicherheitsproblemen bei Smartphones. Dieser Bereich ist nur ein Beispiel, und hat durch die rasante Verbreitung von Mobiltechnologie immens an Bedeutung gewonnen.

Um den diskutierten Killswitch in Netzwerken wieder aufzugreifen: Die Idee in einem nationalen Notfall Informationsnetzwerke zu kontrollieren ist nicht neu. Präsident Franklin D. Roosevelt hat dies im Communications Act of 1934 schon umgesetzt. Damals ging es um Medien. Im vorgeschlagenen Protecting Cyberspace as a National Asset Act of 2010 wollte man dasselbe für das Internet umsetzen, mit dem Unterschied der Abschaltung statt Kontrolle. Das vorgeschlagene Gesetz von 2010 verfiel ohne Stimmen zu bekommen, weil die technische Umsetzung nicht klar war und nach wie vor auch nicht ist. Der Gedanken mit einem simplen Schalter Kommunikationsnetzwerke nach Belieben lahmzulegen funktionierte auf der Kinoleinwand oder im Fernsehen noch gut - leider nur in der Vergangenheit, denn mittlerweile werden Informationen per Internet gestreamt.

Die Alternative ist ein strikt nationales Netzwerk. Die iranische Regierung arbeitet an einem iranischen Intranet, angespornt durch Proteste im Jahre 2009. Die chinesische Firewall versucht etwas ähnliches, allerdings durch strenge Filter gesteuert durch Redaktionen. Rußland probt derzeit ebenfalls eine Abkopplung vom Internet. Die Kommunikationsnetzwerke sollen dann zwar noch funktionieren, aber man plant sie vom Rest der Welt zu trennen. Das ist de fakto einfach die fettarme Variante des Killswitches. Beide Ansätze demonstrieren wie enorm die Bedeutung des Internets mittlerweile geworden ist - es kann nicht mehr ignoriert werden. Das gilt für Unternehmen noch viel mehr als für Länder.

DIGITALER REALISMUS

Realistisch betrachtet macht es wenig Sinn die eigene Bevölkerung und den Staat zunächst von einem Netzwerk abhängig zu machen, um das dann wieder abzuschalten. Die Sehnsucht nach lokalen Netzwerken beweist das. In Unternehmen ist es nicht anders. Daten müssen ausgetauscht und Kommunikation muss stattfinden. Seriöse

dabei das sichere Design von Applikationen von Anfang an. Dazu gab es bei den vergangenen DeepSec-Konferenzen reichlich Vorträge und Trainings als Weiterbildung für Entwicklerinnen und Planer.

Der IT-Security haftet der Ruf eines Verhinderers an. Tatsächlich ist das Gegenteil der Fall. Vergangene Sicherheitsvorfälle und publizierte Dokumente über organisierte Schwachstellen wie beispielsweise durch Edward Snowden sind und waren wesentliche Bausteine für eine Verbesserung der Sicherheit in unserem Alltag. Voraussetzung dafür ist paradoxerweise ein freier Austausch zwischen Sicherheitsforschern. Ein nationales Intranet, Verbote von kryptographischen Algorithmen, Filter für publizierte Inhalte oder ähnliche Restriktionen sind daher der maximal unsicherste Kontrapunkt zu notwendiger Sicherheit in der digitalen Welt.

Die DeepSec Konferenz möchte daher explizit nicht nur Sicherheitsexperten ansprechen. Die Durchdringung digitaler Netze erfordert für eine sinnvolle Weiterentwicklung der IT-Sicherheitsmaßnahmen die Einbindung von Unternehmen, Entwicklerinnen, der Hacker Community, Behörden, Anwendern, Infrastrukturbetreibern, Designern und interdisziplinären Wissenschaftlerinnen. Menschen in beratender Funktion sind ausdrücklich eingeladen an dem Austausch von Erfahrungen und Ideen im November in Wien teilzunehmen.

Weitere Informationen zur DeepSec Konferenz:

BEITRÄGE GESUCHT - CALL FOR PAPERS

Die DeepSec Konferenz möchte dieses Jahr das Augenmerk auf die Verbindung zwischen Geopolitik und Informationssicherheit legen. Bis zum 31. Juli 2019 werden daher Vorträge gesucht, welche sich mit Technologien beschäftigen, die beide Welten berühren. Konkret sind das die Herausforderungen für Industrie- und Steuerungssysteme, der Internet der Dinge, sämtliche mobil eingesetzte Kommunikationstechnologie (vom Auto bis zum Telefon), Einsatz von Algorithmen und moderne Datenhaltung. Wir erleben gerade eine beschleunigte Vermischung neuer und vorhandener Methoden. Es sind Sicherheitsforscherinnen gefragt, die sich kreativ mit den aktuellen Möglichkeiten auseinandersetzen und Schwachstellen aufzeigen. Risiken lassen sich erst dann managen, wenn man sie kennt. Das Programmkommittee freut sich daher auf möglichst viele Einreichungen, die Trends und sogenannte Zukunftstechnologien ganz genau unter das digitale Mikroskop legen.

Die zweitägigen Trainings vor der DeepSec Konferenz sind auch Teil des Call for Papers. Trainerinnen, die ihr Wissen weitergeben möchten, sind herzlich eingeladen Kurse einzureichen. Akzeptierte Kurse werden vorzeitig bekanntgegeben, um den Teilnehmern die Planung beim Buchen zu erleichtern.

PROGRAMME UND BUCHUNG

November. Parallel finden die ROOTS 2019 Vorträge in einem separaten Saal ebenso am 28. und 29. November statt. Die DeepSec Trainings finden an den zwei vorangehenden Tagen, dem 26. und 27. November statt. Die DeepINTEL Konferenz findet am 27. November statt. Das Programm senden wir auf Anfragen an deepsec@deepsec.net (mailto:deepsec@deepsec.net) gerne zu. Tickets sind auf der Webseite https://deepintel.net erhältlich.

Der Veranstaltungsort für DeepSec, DeepINTEL und ROOTS 2019 ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Einreichungen können unter https://deepsec.net/cfp.html abgegeben werden. Das aktuelle Programm der Veranstaltungen wird nach dem Abschluss der Einreichungsfristen bekanntgegeben.

Tickets für die DeepSec Konferenz sowie ROOTS 2019 und die DeepSec Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html bestellen.

deepsec.net (https://deepintel.net)

GRID LIST

(/shortnews/23201-alibaba-kuendigt-partnerschaft-mit-der-faw-gruppe-an)

(/shortnews/23200-amazon-bekommt-mehr-konkurrenz)

(/shortnews/23185-supportende-fuer-windows-7-als-unterschaetztes-sicherheitsrisiko)

https://computerwelt.at/news/topmeldung/it-sicherheit-steht-zunehmend-im-zeichen-der-geopolitik/

18.02.2019

IT-Sicherheit steht zunehmend im Zeichen der Geopolitik

Die im November stattfindende DeepSec-In-Depth-Security-Konferenz widmet sich den technischen Herausforderungen des Internets der Dinge, den kommenden Netzwerktechnologien und den geopolitischen Randbedingungen diktiert durch Schlüsselereignisse der letzten sechs Jahre.Die DeepSec-Konferenz findet in Wien am 28. und 29. November statt.

Die DeepSec-Konferenz findet in Wien am 28. und 29. November statt. (c) DeepSec GmbH

Es gibt weltweit sehr wenige Anbieter von Mobilfunknetzwerktechnologie. Der Name Huawei wird in den letzten Monaten in der Berichterstattung recht oft erwähnt. Diskutiert werden dann selten die Vorzüge der angebotenen Produkte oder die tatsächlichen Implementationen des neuen Mobilfunkstandards 5G. Stattdessen geht es um den Vorwurf heimlich eingebauter Notabschaltungen, die auf einen Schlag das komplette Mobilfunknetz eines Betreibers lahmlegen können. Angeklagt wird auch vermeintlicher versteckter Code, der Fernzugriff und das Kopieren von Daten aus dem Netzwerk erlaubt. Gerüstet mit vielen Vorwürfen ohne konkrete Beweise wird gerade in bestimmten westlichen Ländern ein Ausschluss chinesischer Telekommunikationsausrüster öffentlich diskutiert.

Die Sorgen sind berechtigt, jedoch sind sie Sicherheitsforschern nicht fremd. Fast alle Computer, die in Europa und anderswo eingesetzt werden, stammen selten aus den Ländern, in denen sie ihre Arbeit tatsächlich verrichten. Die Chips, die Firmware und viele weitere Zutaten in Hard- und Software werden woanders gebaut. Da man in den letzten Dekaden systematisch darauf verzichtet hat, den Inhalt der Box hinter Tastatur oder Touchscreen zu hinterfragen, geschweige zu verstehen, blühen die Anschuldigungen getrieben von der Fantasie.

Fakten von Fiktion trennen

Die IT-Security-Forschung kann dem nur mit Fakten und solider Recherche begegnen. Robert Hannigan, der ehemalige Chef des britischen Geheimdiensts GCHQ, hat bestätigt, dass sich das britische National Cyber Security Centre (NCSC) lange Jahre mit Komponenten aus chinesischen Lieferketten beschäftigt hat. Bisher hat es laut seiner Aussage keine Indizien für staatlich verordnete verdeckte Angriffe durch Huawei-Hardware gegeben. NCSC hat seit 2010 mit Hilfe des Huawei Security Evaluation Centres (HSEC) Zugang zum Quellcode der Produkte.

Der Sinn dahinter ist eine Zertifizierung durch das NCSC bevor Technologie in sensitiven Bereichen eingesetzt werden kann. Robert Hannigan widerspricht damit direkt den Vorwürfen aus den USA und der Einschätzung von Gerhard Schindler, dem früheren Präsident des deutschen Bundesnachrichtendienstes (BND). Darüber hinaus

ignorieren die Kritiker die bereits jetzt in Europa vorgeschriebenen gesetzlichen Überwachungsschnittstellen, standardisiert durch das Europäische Institut für Telekommunikationsnormen (ETSI). Diese Vorgaben gelten übrigens für alle Anbieter, die in Europa Netzwerke bauen oder bauen lassen möchten.

Intranet statt Internet

Die aktuelle Nachrichtenlage illustriert daher sehr gut, was man alles in der Informationssicherheit beachten sollte. Die Absicherung der eigenen Daten ist längst nicht mehr mit einzelnen isolierten Betrachtungen getan. Die DeepSec-Konferenz hat obendrein eine lange Tradition der Sicherheitsforschung im Mobilfunkbereich, angefangen von der ersten öffentlichen Publikation von Schwachstellen des A5/1 Verschlüsselungsalgorithmus (zwischen Telefon und Funkzelle) bis hin zu Sicherheitsproblemen bei Smartphones. Dieser Bereich ist nur ein Beispiel, und hat durch die rasante Verbreitung von Mobiltechnologie immens an Bedeutung gewonnen.

Um den diskutierten Killswitch in Netzwerken wieder aufzugreifen: Die Idee in einem nationalen Notfall Informationsnetzwerke zu kontrollieren ist nicht neu. Präsident Franklin D. Roosevelt hat dies im Communications Act of 1934 schon umgesetzt. Damals ging es um Medien. Im vorgeschlagenen „Protecting Cyberspace as a National Asset Act of 2010“ wollte man dasselbe für das Internet umsetzen, mit dem Unterschied der Abschaltung statt Kontrolle. Das vorgeschlagene Gesetz von 2010 verfiel ohne Stimmen zu bekommen, weil die technische Umsetzung nicht klar war und nach wie vor auch nicht ist. Der Gedanken mit einem simplen Schalter Kommunikationsnetzwerke nach Belieben lahmzulegen funktionierte auf der Kinoleinwand oder im Fernsehen noch gut – leider nur in der Vergangenheit, denn mittlerweile werden Informationen per Internet gestreamt.

Die Alternative ist ein strikt nationales Netzwerk. Die iranische Regierung arbeitet an einem iranischen Intranet, angespornt durch Proteste im Jahre 2009. Die chinesische Firewall versucht etwas ähnliches, allerdings durch strenge Filter gesteuert durch Redaktionen. Russland probt derzeit ebenfalls eine Abkopplung vom Internet. Die Kommunikationsnetzwerke sollen dann zwar noch funktionieren, aber man plant sie vom Rest der Welt zu trennen. Das ist de fakto einfach die fettarme Variante des Killswitches. Beide Ansätze demonstrieren wie essentiell die Bedeutung des Internets mittlerweile geworden ist. Das gilt für Unternehmen noch viel mehr als für Länder.

Digitaler Realismus

Realistisch betrachtet ist es wenig sinnvoll, die eigene Bevölkerung und den Staat zunächst von einem Netzwerk abhängig zu machen, um das dann wieder abzuschalten, sind die DeepSec-Konferenz-Versanstalter überzeugt. Die Sehnsucht nach lokalen Netzwerken beweist das. In Unternehmen ist es nicht anders. Daten müssen ausgetauscht werden. Seriöse Informationssicherheit muss daher untersuchen wie sich die Integrität der Infrastruktur und

von Daten auch unter widrigen Umständen erhalten lassen. Wichtigster Punkt ist dabei das sichere Design von Applikationen von Beginn an. Dazu gab es bei den vergangenen DeepSec-Konferenzen reichlich Vorträge und Trainings als Weiterbildung für Entwickler und Planer.

Der IT-Security haftet oft der Ruf eines Verhinderers an. Tatsächlich ist das Gegenteil der Fall. Vergangene Sicherheitsvorfälle und publizierte Dokumente über organisierte Schwachstellen wie beispielsweise durch Edward Snowden sind und waren wesentliche Bausteine für eine Verbesserung der Sicherheit in unserem Alltag. Voraussetzung dafür ist paradoxerweise ein freier Austausch zwischen Sicherheitsforschern. Ein nationales Intranet, Verbote von kryptografischen Algorithmen, Filter für publizierte Inhalte oder ähnliche Restriktionen sind laut DeepSec-Experten daher der maximal unsicherste Kontrapunkt zu notwendiger Sicherheit in der digitalen Welt.

Die DeepSec-Konferenz möchte daher explizit nicht nur Sicherheitsexperten ansprechen. Die Durchdringung digitaler Netze erfordert für eine sinnvolle Weiterentwicklung der IT-Sicherheitsmaßnahmen die Einbindung von Unternehmen, Entwicklern, der Hacker-Community, Behörden, Anwendern, Infrastrukturbetreibern, Designern und interdisziplinären Wissenschaftlern. Menschen in beratender Funktion sind ausdrücklich eingeladen an dem Austausch von Erfahrungen und Ideen im November in Wien teilzunehmen.

Beiträge gesucht – Call for Papers

Die DeepSec-Konferenz legt dieses Jahr das Augenmerk auf die Verbindung zwischen Geopolitik und Informationssicherheit. Bis zum 31. Juli 2019 werden daher Vorträge gesucht, die sich mit Technologien beschäftigen, die beide Welten berühren. Konkret sind das die Herausforderungen für Industrie- und Steuerungssysteme, das Internet der Dinge, sämtliche mobil eingesetzte Kommunikationstechnologie (vom Auto bis zum Telefon), Einsatz von Algorithmen und moderne Datenhaltung. Wir erleben gerade eine sich beschleunigende Vermischung neuer und vorhandener Methoden. Es sind Sicherheitsforscher gefragt, die sich kreativ mit den aktuellen Möglichkeiten auseinandersetzen und Schwachstellen aufzeigen. Risiken lassen sich erst dann managen, wenn man sie kennt. Das Programmkommittee freut sich daher auf möglichst viele Einreichungen, die Trends und sogenannte Zukunftstechnologien ganz genau unter das digitale Mikroskop legen.

Die zweitägigen Trainings vor der DeepSec-Konferenz sind auch Teil des „Call for Papers“. Trainer und Trainerinnen, die ihr Wissen weitergeben möchten, sind herzlich eingeladen Kurse einzureichen. Akzeptierte Kurse werden vorzeitig bekanntgegeben, um den Teilnehmern die Planung beim Buchen zu erleichtern.

Programme und Buchung

Die DeepSec-2019-Konferenztage sind am 28. und 29. November. Parallel finden die ROOTS 2019 Vorträge in einem separaten Saal ebenso am 28. und 29. November statt. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 26. und 27. November statt. Die DeepINTEL-Konferenz ist für den 27. November angesetzt. Anfragen für Programm unter deepsec@deepsec.net , es wird dann zugesandt. Tickets sind auf der Webseite https://deepintel.net erhältlich.

Die Konferenzen DeepSec, DeepINTEL und ROOTS 2019 finden im Hotel The Imperial Riding School Vienna – A Renaissance Hotel in der Ungargasse 60 im dritten Wiener Gemendebezirk statt.

Einreichungen können unter https://deepsec.net/cfp.html abgegeben werden. Das aktuelle Programm der Veranstaltungen wird nach dem Abschluss der Einreichungsfristen bekanntgegeben.#

Tickets für die DeepSec Konferenz sowie ROOTS 2019 und die DeepSec Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html bestellen.

18. Februar 2019 Klaus Lorbeer/pi

IT-Sicherheit steht zunehmend im Zeichen der Geopolitik

Die im November stattfindende DeepSec-In-Depth-Security-Konferenz widmet sich den technischen Herausforderungen des Internets der Dinge, den kommenden Netzwerktechnologien und den geopolitischen Randbedingungen diktiert durch Schlüsselereignisse der letzten sechs Jahre.

Die DeepSec-Konferenz findet in Wien am 28. und 29. November statt. (c) DeepSec GmbH

Es gibt weltweit sehr wenige Anbieter von Mobilfunknetzwerktechnologie. Der Name Huawei wird in den letzten Monaten in der Berichterstattung recht oft erwähnt. Diskutiert werden dann selten die Vorzüge der angebotenen Produkte oder die tatsächlichen Implementationen des neuen Mobilfunkstandards 5G. Stattdessen geht es um den Vorwurf heimlich eingebauter Notabschaltungen, die auf einen Schlag das komplette Mobilfunknetz eines Betreibers lahmlegen können. Angeklagt wird auch vermeintlicher versteckter Code, der Fernzugriff und das Kopieren von Daten aus dem Netzwerk erlaubt. Gerüstet mit vielen Vorwürfen ohne konkrete Beweise wird gerade in bestimmten westlichen Ländern ein Ausschluss chinesischer Telekommunikationsausrüster öffentlich diskutiert.

Die Sorgen sind berechtigt, jedoch sind sie Sicherheitsforschern nicht fremd. Fast alle Computer, die in Europa und anderswo eingesetzt werden, stammen selten aus den Ländern, in denen sie ihre Arbeit tatsächlich verrichten. Die Chips, die Firmware und viele weitere Zutaten in Hard- und Software werden woanders gebaut. Da man in den letzten Dekaden systematisch darauf verzichtet hat, den Inhalt der Box hinter Tastatur oder Touchscreen zu hinterfragen, geschweige zu verstehen, blühen die Anschuldigungen getrieben von der Fantasie.

Fakten von Fiktion trennen

Die IT-Security-Forschung kann dem nur mit Fakten und solider Recherche begegnen. Robert Hannigan, der ehemalige Chef des britischen Geheimdiensts GCHQ, hat bestätigt, dass sich das britische National Cyber Security Centre (NCSC) lange Jahre mit Komponenten aus chinesischen Lieferketten beschäftigt hat. Bisher hat es laut seiner Aussage keine Indizien für staatlich verordnete verdeckte Angriffe durch Huawei-Hardware gegeben. NCSC hat seit 2010 mit Hilfe des Huawei Security Evaluation Centres (HSEC) Zugang zum Quellcode der Produkte.

Der Sinn dahinter ist eine Zertifizierung durch das NCSC bevor Technologie in sensitiven Bereichen eingesetzt werden kann. Robert Hannigan widerspricht damit direkt den Vorwürfen aus den USA und der Einschätzung von Gerhard Schindler, dem früheren Präsident des deutschen Bundesnachrichtendienstes (BND). Darüber hinaus ignorieren die Kritiker die bereits jetzt in Europa vorgeschriebenen gesetzlichen

Telekommunikationsnormen (ETSI). Diese Vorgaben gelten übrigens für alle Anbieter, die in Europa Netzwerke bauen oder bauen lassen möchten.

Intranet statt Internet

Die aktuelle Nachrichtenlage illustriert daher sehr gut, was man alles in der Informationssicherheit beachten sollte. Die Absicherung der eigenen Daten ist längst nicht mehr mit einzelnen isolierten Betrachtungen getan. Die DeepSec-Konferenz hat obendrein eine lange Tradition der Sicherheitsforschung im Mobilfunkbereich, angefangen von der ersten öffentlichen Publikation von Schwachstellen des A5/1 Verschlüsselungsalgorithmus (zwischen Telefon und Funkzelle) bis hin zu Sicherheitsproblemen bei Smartphones. Dieser Bereich ist nur ein Beispiel, und hat durch die rasante Verbreitung von Mobiltechnologie immens an Bedeutung gewonnen.

Um den diskutierten Killswitch in Netzwerken wieder aufzugreifen: Die Idee in einem nationalen Notfall Informationsnetzwerke zu kontrollieren ist nicht neu. Präsident Franklin D. Roosevelt hat dies im Communications Act of 1934 schon umgesetzt. Damals ging es um Medien. Im vorgeschlagenen „Protecting Cyberspace as a National Asset Act of 2010" wollte man dasselbe für das Internet umsetzen, mit dem Unterschied der Abschaltung statt Kontrolle. Das vorgeschlagene Gesetz von 2010 verfiel ohne Stimmen zu bekommen, weil die technische Umsetzung nicht klar war und nach wie vor auch nicht ist. Der Gedanken mit einem simplen Schalter Kommunikationsnetzwerke nach Belieben lahmzulegen funktionierte auf der Kinoleinwand oder im Fernsehen noch gut – leider nur in der Vergangenheit, denn mittlerweile werden Informationen per Internet gestreamt.

Die Alternative ist ein strikt nationales Netzwerk. Die iranische Regierung arbeitet an einem iranischen Intranet, angespornt durch Proteste im Jahre 2009. Die chinesische Firewall versucht etwas ähnliches, allerdings durch strenge Filter gesteuert durch Redaktionen. Russland probt derzeit ebenfalls eine Abkopplung vom Internet. Die Kommunikationsnetzwerke sollen dann zwar noch funktionieren, aber man plant sie vom Rest der Welt zu trennen. Das ist de fakto einfach die fettarme Variante des Killswitches. Beide Ansätze demonstrieren wie essentiell die Bedeutung des Internets mittlerweile geworden ist. Das gilt für Unternehmen noch viel mehr als für Länder.

Digitaler Realismus

Realistisch betrachtet ist es wenig sinnvoll, die eigene Bevölkerung und den Staat zunächst von einem Netzwerk abhängig zu machen, um das dann wieder abzuschalten, sind die DeepSec-Konferenz-Versanstalter überzeugt. Die Sehnsucht nach lokalen Netzwerken beweist das. In Unternehmen ist es nicht anders. Daten müssen ausgetauscht werden. Seriöse Informationssicherheit muss daher untersuchen wie sich die Integrität der Infrastruktur und von Daten auch unter widrigen Umständen erhalten lassen. Wichtigster Punkt ist dabei das sichere Design von Applikationen von Beginn an. Dazu gab es bei den vergangenen DeepSec-Konferenzen reichlich Vorträge und Trainings als Weiterbildung für Entwickler und Planer.

Der IT-Security haftet oft der Ruf eines Verhinderers an. Tatsächlich ist das Gegenteil der Fall. Vergangene Sicherheitsvorfälle und publizierte Dokumente über organisierte Schwachstellen wie beispielsweise durch Edward Snowden sind und waren wesentliche Bausteine für eine Verbesserung der Sicherheit in unserem Alltag. Voraussetzung dafür ist paradoxerweise ein freier Austausch zwischen Sicherheitsforschern. Ein nationales Intranet, Verbote von kryptografischen Algorithmen, Filter für publizierte Inhalte oder ähnliche Restriktionen sind laut DeepSec-Experten daher der maximal unsicherste Kontrapunkt zu notwendiger Sicherheit in der digitalen Welt.

Die DeepSec-Konferenz möchte daher explizit nicht nur Sicherheitsexperten ansprechen. Die Durchdringung digitaler Netze erfordert für eine sinnvolle

Designern und interdisziplinären Wissenschaftlern. Menschen in beratender Funktion sind ausdrücklich eingeladen an dem Austausch von Erfahrungen und Ideen im November in Wien teilzunehmen.

Beiträge gesucht – Call for Papers

Die DeepSec-Konferenz legt dieses Jahr das Augenmerk auf die Verbindung zwischen Geopolitik und Informationssicherheit. Bis zum 31. Juli 2019 werden daher Vorträge gesucht, die sich mit Technologien beschäftigen, die beide Welten berühren. Konkret sind das die Herausforderungen für Industrie- und Steuerungssysteme, das Internet der Dinge, sämtliche mobil eingesetzte Kommunikationstechnologie (vom Auto bis zum Telefon), Einsatz von Algorithmen und moderne Datenhaltung. Wir erleben gerade eine sich beschleunigende Vermischung neuer und vorhandener Methoden. Es sind Sicherheitsforscher gefragt, die sich kreativ mit den aktuellen Möglichkeiten auseinandersetzen und Schwachstellen aufzeigen. Risiken lassen sich erst dann managen, wenn man sie kennt. Das Programmkommittee freut sich daher auf möglichst viele Einreichungen, die Trends und sogenannte Zukunftstechnologien ganz genau unter das digitale Mikroskop legen.

Die zweitägigen Trainings vor der DeepSec-Konferenz sind auch Teil des „Call for Papers". Trainer und Trainerinnen, die ihr Wissen weitergeben möchten, sind herzlich eingeladen Kurse einzureichen. Akzeptierte Kurse werden vorzeitig bekanntgegeben, um den Teilnehmern die Planung beim Buchen zu erleichtern.

Programme und Buchung

Die DeepSec-2019-Konferenztage sind am 28. und 29. November. Parallel finden die ROOTS 2019 Vorträge in einem separaten Saal ebenso am 28. und 29. November statt. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 26. und 27. November statt. Die DeepINTEL-Konferenz ist für den 27. November angesetzt. Anfragen für Programm unter deepsec@deepsec.net , es wird dann zugesandt. Tickets sind auf der Webseite https://deepintel.net erhältlich.

Die Konferenzen DeepSec, DeepINTEL und ROOTS 2019 finden im Hotel The Imperial Riding School Vienna – A Renaissance Hotel in der Ungargasse 60 im dritten Wiener Gemendebezirk statt.

Einreichungen können unter https://deepsec.net/cfp.html abgegeben werden. Das aktuelle Programm der Veranstaltungen wird nach dem Abschluss der Einreichungsfristen bekanntgegeben.#

Tickets für die DeepSec Konferenz sowie ROOTS 2019 und die DeepSec Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html bestellen.

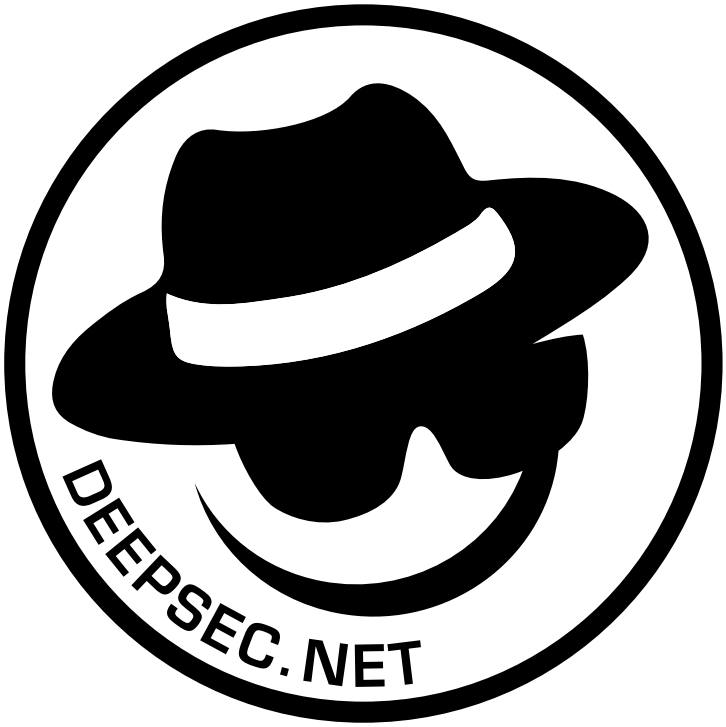
KONFERENZ SECURITY WIEN

MEHR ARTIKEL

Drei wichtige IT-Trends für 2020

KI: Hype oder kritischer Faktor für effiziente IT- und

Kendox realisiert „elektronische Studierendendossie


DEEPSEC.NET

https://www.pressetext.com/news/20191120006

Hochwertiger Zufall schützt Unternehmen

“Bugs” der 90er leben versteckt in IoT-Geräten, integrierten Systemen und Industriesteuerungen

Wien (pts006/20.11.2019/09:15) - Moderne Informationssicherheit kommt nicht ohne Mathematik aus. Dabei geht es weniger um Statistik in Form von Betriebsdaten oder Risikoanalysen. Es geht um Kryptographie, die wird ständig im Alltag einsetzen. Sie benutzt Elemente, welche auf hochwertigen Zufallszahlen aufbauen, um Informationen vor Attacken zu schützen. Die diesjährige DeepSec Sicherheitskonferenz widmet sich wichtigen Aspekten der Umsetzung in Produkten - Schutz von Daten bei Transport und Speicherung.

Schutz der digitalen Transformation

Egal ob “intelligente” Glühlampen und Leuchtmittel, Heizungs- oder Gebäudesteuerungen, Fernseher, Industrieanlagen oder ganze Produktionsstraßen - die digitale Transformation erfasst alle Bereiche unseres Lebens und führt zu Veränderungen.

Auf der einen Seite eröffnet die Digitalisierung Chancen wie die Optimierung von Prozessen, eine effizientere Nutzung eigener und externer Ressourcen, die Vernetzung von Wertschöpfungsketten oder digitale Wartung. Gleichzeitig ergeben sich jedoch nicht zu unterschätzende Risiken. Das Gewährleisten der Datensicherheit und -echtheit sowie die Einhaltung geforderter Sicherheitsstandards stellt viele Unternehmen vor große Herausforderungen. Dabei spielen die Kryptographie und der damit einhergehende Schutz der kryptographischen Schlüssel eine fundamentale Rolle - wer die Schlüssel besitzt hat die Kontrolle.

Auf der diesjährigen DeepSec Sicherheitskonferenz in Wien stehen Experten der sematicon AG bereit um Risiken und Gefahren aktueller Implementierungen zu zeigen. Darüber hinaus werden sie mit Praxisbeispielen den Nachweis erbringen, dass es für alle Bereiche dieser neuen Technik passende und einfache Lösungen sowie Werkzeuge gibt um die Sicherheit - durch den Einsatz starker Kryptographie - drastisch zu erhöhen. Hierbei müssen solche Implementierungen keinesfalls auf Benutzerfreundlichkeit oder Wartbarkeit verzichten. Als Nebeneffekt erhöhen korrekt implementierte Lösungen sogar die Geschwindigkeit und sparen Strom, was gerade bei dezentralen sowie batterie- oder solarbetrieben Systemen von großem Interesse ist.

Warum man die IT-Sicherheit dem Zufall überlassen sollte

Seit den Berichten von Edward Snowden über die durchdringende Überwachung von Kommunikation hat sich die Verwendung von Verschlüsselung im Internet stark erhöht. Kaum eine bekannte Webseite verzichtet noch hierauf. Auch für Systeme jenseits des Desktops von intelligenten Sensoren bis hin zu großen Industrieanlagen ist Verschlüsslung heute unabdingbar. Diese Schlüssel müssen zufällig erzeugt werden, damit sie nicht leicht erraten werden können. Hochqualitative Zufallszahlen sind dafür notwendig. Zufall ist aber keine “Funktion” einer Softwarelösung, sondern bedient sich speziellen physikalischen Effekten, um eine hochwertige Qualität der Zufallszahlen sicherzustellen. Lassen sich diese Erraten oder Nachvollziehen ist der Weg zur Errechnung des Schlüssels nicht mehr weit. Die Erzeugung der schützenswerten Schlüssel basiert auf dem Prinzip des qualitativen Zufalls - auch bekannt als Entropie. Wer viele davon benötigt oder die Qualität steigern möchte, der sucht sich passende Quellen wie beispielsweise Hardware-Sicherheitsmodule, auch Hardware Security Modules (HSMs) genannt.

Auf der diesjährigen DeepSec Sicherheitskonferenz in Wien wird in Zusammenarbeit mit dem Münchner Unternehmen sematicon gezeigt, dass es für alle Bereiche der Technik passende Lösungen gibt, und dass die Angst vor einem Einsatz im eigenen Unternehmen unbegründet ist.

Seitenkanalangriffe - oder wie man Krypto-Schlüssel aus geschützter Hardware extrahiert

Während der DeepSec Konferenz wird durch die Firma sematicon AG unter anderem gezeigt, wie einfach man mit Windows-Bordmitteln und einer falsch konfigurierten PKI Zugriff auf ganze Unternehmensnetzwerke erlangt, oder wie man kryptographische Schlüssel aus vermeintlich geschützten IoT- oder Embeded Geräten extrahiert und somit die Firmware manipulieren kann. So werden einfache Haushaltsgeräte wie Glühlampen zum Einfallstor für Hacker. Ebenfalls wird kurz darauf eingegangen, wie Geheimnisse von Industrie-Equipment erlangt werden können, wenn die Sicherheit nicht von Anfang an korrekt implementiert wurde. Dabei handelt es sich keinesfalls um speziell präparierte Systeme, sondern um klassische Implementierungen wie man diese in der Wirtschaft findet. Es geht dabei keinesfalls um “Live Hacking”, sondern um fachliche Expertise von Krypto-Experten die schon sehr viele Jahre in der Branche tätig sind und reichhaltig Erfahrung mitbringen. Gedacht ist diese Vorführung für alle die in ihrer Infrastruktur sichere Datenübertragung einbauen müssen, ganz egal auf welcher Ebene.

Kryptographie zugänglich vermittelt

Trotz dem thematischen Anteil höherer Mathematik ist es der DeepSec Konferenz und der sematicon AG ein Anli-

egen die Bedeutung der eingesetzten Methoden und Technologien für den Praxiseinsatz einem breitem Fachpublikum zu vermitteln. Die Demonstrationen und Vorträge richten sich nicht nur an Techniker und Entwicklerinnen, sondern auch an Projektverantwortliche, Manager und Designer von Produkten. Es sollen alle Ebenen eingebunden werden, da Informationssicherheit ein interdisziplinäres Unterfangen ist. Furcht vor der Materie ist daher völlig unbegründet. Die Vorträge und Veranstaltungen während der Konferenz bieten mehrere Wege zum Einstieg und zur Fortbildung durch Austausch mit Experten. Nutzen Sie diese Möglichkeit.

Programme und Buchung

Die DeepSec 2019 Konferenztage sind am 28. und 29. November. Die zweitägigen DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 26. und 27. November statt.

Der Veranstaltungsort für die DeepSec-Veranstaltung ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Tickets für die DeepSec Konferenz selbst und die Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html bestellen.

(/)

HIGHTECH

pts20181120006 Forschung/Entwicklung, Produkte/Innovationen

Hochwertiger Zufall schützt Unternehmen

"Bugs" der 90er leben versteckt in IoT-Geräten, integrierten Systemen und Industriesteuerungen

Wien (pts006/20.11.2019/09:15) - Moderne Informationssicherheit kommt nicht ohne Mathematik aus. Dabei geht es weniger um Statistik in Form von Betriebsdaten oder Risikoanalysen. Es geht um Kryptographie, die wird ständig im Alltag einsetzen. Sie benutzt Elemente, welche auf hochwertigen Zufallszahlen aufbauen, um Informationen vor Attacken zu schützen. Die diesjährige DeepSec Sicherheitskonferenz widmet sich wichtigen Aspekten der Umsetzung in Produkten - Schutz von Daten bei Transport und Speicherung.

Echter Zufall aus einem Generator (Quelle: René Pfeiffer, eigenes Werk)

Schutz der digitalen Transformation

Egal ob "intelligente" Glühlampen und Leuchtmittel, Heizungs- oder Gebäudesteuerungen, Fernseher, Industrieanlagen oder ganze Produktionsstraßen - die digitale Transformation erfasst alle Bereiche unseres Lebens und führt zu Veränderungen.

Auf der einen Seite eröffnet die Digitalisierung Chancen wie die Optimierung von Prozessen, eine effizientere Nutzung eigener und externer Ressourcen, die Vernetzung von Wertschöpfungsketten oder digitale Wartung. Gleichzeitig ergeben sich jedoch nicht zu unterschätzende Risiken. Das Gewährleisten der Datensicherheit und -echtheit sowie die Einhaltung geforderter Sicherheitsstandards stellt viele Unternehmen vor große Herausforderungen. Dabei spielen die Kryptographie und der damit einhergehende Schutz der kryptographischen Schlüssel eine fundamentale Rolle - wer die Schlüssel besitzt hat die Kontrolle.

Auf der diesjährigen DeepSec Sicherheitskonferenz in Wien stehen Experten der sematicon AG bereit um Risiken und Gefahren aktueller Implementierungen zu zeigen. Darüber hinaus werden sie mit Praxisbeispielen den Nachweis erbringen, dass es für alle Bereiche dieser neuen Technik passende und einfache Lösungen sowie Werkzeuge gibt um die Sicherheit - durch den Einsatz starker Kryptographie - drastisch zu erhöhen. Hierbei müssen solche Implementierungen keinesfalls auf Benutzerfreundlichkeit oder Wartbarkeit verzichten. Als Nebeneffekt erhöhen korrekt implementierte Lösungen sogar die Geschwindigkeit und sparen Strom, was gerade bei dezentralen sowie batterie- oder solarbetrieben Systemen von großem Interesse ist.

Warum man die IT-Sicherheit dem Zufall überlassen sollte

Seit den Berichten von Edward Snowden über die durchdringende Überwachung von Kommunikation hat sich die Verwendung von Verschlüsselung im Internet stark erhöht. Kaum eine bekannte Webseite verzichtet noch hierauf. Auch für Systeme jenseits des Desktops von intelligenten Sensoren bis hin zu großen Industrieanlagen ist Verschlüsslung heute unabdingbar. Diese Schlüssel müssen zufällig erzeugt werden, damit sie nicht leicht erraten werden können. Hochqualitative Zufallszahlen sind dafür notwendig. Zufall ist aber keine "Funktion" einer Softwarelösung, sondern bedient sich speziellen physikalischen Effekten, um eine hochwertige Qualität der Zufallszahlen sicherzustellen. Lassen sich diese Erraten oder Nachvollziehen ist der Weg zur Errechnung des Schlüssels nicht mehr weit. Die Erzeugung der schützenswerten Schlüssel basiert auf dem Prinzip des qualitativen Zufalls - auch bekannt als Entropie. Wer viele davon benötigt oder die Qualität steigern möchte, der sucht sich passende Quellen wie beispielsweise Hardware-Sicherheitsmodule, auch Hardware Security Modules (HSMs) genannt.

Auf der diesjährigen DeepSec Sicherheitskonferenz in Wien wird in Zusammenarbeit mit dem Münchner Unternehmen sematicon gezeigt, dass es für alle Bereiche der Technik passende Lösungen gibt, und dass die Angst vor einem Einsatz im eigenen Unternehmen unbegründet ist.

Seitenkanalangriffe - oder wie man Krypto-Schlüssel aus geschützter Hardware extrahiert

Während der DeepSec Konferenz wird durch die Firma sematicon AG unter anderem gezeigt, wie einfach man mit Windows-Bordmitteln und einer falsch konfigurierten PKI Zugriff auf ganze Unternehmensnetzwerke erlangt, oder wie man kryptographische Schlüssel aus vermeintlich geschützten IoT- oder Embeded Geräten extrahiert und somit die Firmware manipulieren kann. So werden einfache Haushaltsgeräte wie Glühlampen zum Einfallstor für Hacker. Ebenfalls wird kurz darauf eingegangen, wie Geheimnisse von Industrie-Equipment erlangt werden können, wenn die Sicherheit nicht von Anfang an korrekt implementiert wurde. Dabei handelt es sich keinesfalls um speziell präparierte Systeme, sondern um klassische Implementierungen wie man diese in der Wirtschaft findet. Es geht dabei keinesfalls um "Live Hacking", sondern um fachliche Expertise von Krypto-Experten die schon sehr viele Jahre in der Branche tätig sind und reichhaltig Erfahrung mitbringen. Gedacht ist diese Vorführung für alle die in ihrer Infrastruktur sichere Datenübertragung einbauen müssen, ganz egal auf welcher Ebene.

Kryptographie zugänglich vermittelt

Trotz dem thematischen Anteil höherer Mathematik ist es der DeepSec Konferenz und der sematicon AG ein Anliegen die Bedeutung der eingesetzten Methoden und Technologien für den Praxiseinsatz einem breitem Fachpublikum zu vermitteln. Die Demonstrationen und Vorträge richten sich nicht nur an Techniker und Entwicklerinnen, sondern auch an Projektverantwortliche, Manager und Designer von Produkten. Es sollen alle Ebenen eingebunden werden, da Informationssicherheit ein interdisziplinäres Unterfangen ist. Furcht vor der Materie ist daher völlig unbegründet. Die Vorträge und Veranstaltungen während der Konferenz bieten mehrere Wege zum Einstieg und zur Fortbildung durch Austausch mit Experten. Nutzen Sie diese Möglichkeit.

Programme und Buchung

Die DeepSec 2019 Konferenztage sind am 28. und 29. November. Die zweitägigen DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 26. und 27. November statt.

Der Veranstaltungsort für die DeepSec-Veranstaltung ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Tickets für die DeepSec Konferenz selbst und die Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html (https://deepsec.net/register.html) bestellen.

(Ende)

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

(http://deepsec.net)

https://www.pressetext.com/news/20191104009

Dekonstruktion und Analyse moderner IT-Bedrohungen

DeepINTEL Security Intelligence Konferenz entzaubert Komplexität von Sicherheitsbedrohungen

Wien (pts009/04.11.2019/09:45) - Die moderne digitale Welt wird ständig bedroht. Leider verstehen nur wenige, was dies tatsächlich bedeutet. Informationssicherheit wird immer in verfälschenden Klischees dargestellt, die mit der Realität nichts zu tun haben. Kein Angriff wird in Minuten durch Hämmern auf eine Tastatur umgesetzt. Die gefährlichsten Bedrohungen lassen sich nicht durch Kapuzenshirts oder Gesichtsmasken erkennen. Nichts in der digitalen Welt lässt sich mit einem einfachen Klick entschärfen. Das Gegenteil ist der Fall, weil Innen- und Außenpolitik globale Auswirkungen auf die digitale Infrastruktur aller Organisationen haben. Die jedes Jahr in Wien stattfindende DeepINTEL Security Intelligence Konferenz möchte daher eine Plattform bieten, auf der Behörden, Unternehmen, Forscher und Hacker produktiv in einem geschlossenen Kreis Eigenschaften und Gegenmaßnahmen von Bedrohungen diskutieren können.

Plakative Beispiele

Wirtschaftsspionage wird sehr gerne als Beispiel für Bedrohungen im Bereich der Informationen angeführt. Angriffe auf Informationssysteme haben oft das Ziel, Daten zu kopieren, um diese dann entweder zu handeln oder anderweitig zu verwenden. Spionage gibt es auf allen Ebenen. Im Mai 2019 wurde bekannt, dass man über WhatsApp-Anrufe Smartphones infizieren kann. Das Annehmen des Anrufs war nicht notwendig. Ausgenutzt wurde diese Schwachstelle von einer in Israel produzierten kommerziellen Spionagesoftware. Ausspioniert wurden zwar keine Firmen, sondern Bürgerrechtlerinnen und Bürgerrechtler im Nahen Osten. Die Software könnte genauso auf Geschäftsführerinnen und Angestellte losgelassen werden. Die Kunden der israelischen Firma sitzen nicht nur im Nahen Osten. Sie befinden sich auch in westlichen Staaten.

Der Knackpunkt ist das Finden von Schwachstellen, um die Verteidigung zu brechen oder zu umgehen. Die Kenntnis über solche Lücken wird mit viel Geld belohnt und gehandelt. Die Analogie zu Waffen liegt nahe, auch wenn es große technologische Unterschiede gibt. Schadcode hat mehr Verwandtschaft mit biologischen Waffen. Die Attacken durch die Schadsoftware Petya und Wannacry in den Jahren 2016 bzw. 2017 unterstreichen diese These, da die Ausnutzung der Schwachstelle, über die beide Programme eindringen konnten, sehr wahrscheinlich durch die US-amerikanische National Security Agency (NSA) entwickelt wurde. Konkrete Beweise über das tatsächliche Entkommen der Schwachstelle fehlen. Die entwickelten Theorien reichen von der Aktion eines Whistleblowers bis hin zu Tätern aus Russland. Gewissheit wird es keine geben.

Für Sicherheitsverantwortliche in Unternehmen spielen die Spekulationen keine Rolle. Die Fakten zeigen, dass sich die digitale Welt direkt in geopolitischen Spannungsfeldern bewegt. Es wird daher höchste Zeit, diesen Umstand in interne Abläufe zu integrieren.

Geopolitik ist längst Teil von Unternehmensentscheidungen

Die Wirtschaft wird gerne und oft abseits der Politik wahrgenommen. Dies gilt insbesondere für digitale Dienstleistungen. Beim Streaming, der internen Dokumentenablage, E-Mail Kommunikation, Social-Media-Plattformen oder den Dateiablage besitzen nur noch wenige Organisationen eine eigene Infrastruktur. Wolkige Dienstleister verwalten fremde digitale Güter. Der sehr beliebte Begriff der Digitalen Souveränität verliert jede Bedeutung, wenn die Geschäftsführung nicht mehr sagen kann wo sich alle Unternehmensdaten genau befinden und wer sie verwaltet. Man kann nichts beschützen dessen Aufenthaltsort man nicht kennt. Das gilt insbesondere für Prototypen wie die vom deutschen Wirtschaftsministerium vorgeschlagene Gaia-X-Infrastruktur. Sie soll eine Alternative zur Datenhaltung und -verarbeitung außerhalb der Grenzen Europas bieten. Der Kern des Ganzen? Geopolitik ist zum Alltag in der Wirtschaft geworden. Damit kann die Software genau so wie die Hardware auch in Handelskriege - oder Schlimmerem - verstrickt werden.

Die Beispiele illustrieren endringlich, dass sich die Unternehmensführungen nun endlich auch mit Themen beschäftigen müssen, die bislang die Außenpolitik und das Militär beschäftigt haben. Die IT Sicherheit hat das schon längst erkannt und den Bereich der Security Intelligence geschaffen. Dort beschäftigt man sich mit dem strategischen Blick auf Bedrohungen und die Fähigkeiten der Gegner gegen die man sich verteidigen muss. Die technischen Details sind dabei zwar Rüstzeug, jedoch sekundär. Es geht um das Aufklären der Identitäten, Kapazitäten und Absichten gegnerischer Organisationen, welche die eigenen Daten und die eigene Infrastruktur attackieren können. Die klassische Informationssicherheit liefert die Werkzeuge, aber Analytikerinnen müssen die Puzzlesteine richtig zusammensetzen. Genau dort setzt die jährlich in Wien stattfindende DeepINTEL Konferenz an - Austausch von Erkenntnissen in einer geschlossenen Gruppe.

Austausch am lebenden Objekt

Möchte man über echte Vorfälle und konkrete Einbrüche reden, so ist es ratsam, dies konzentriert im Rahmen von Diskussionen unter Expertinnen und Experten zu tun. Der Erfahrungsaustausch ist von unschätzbarem Wert und verbessert Ihre Verteidigung nachhaltig. Die DeepINTEL ist eine solche Plattform. Fokus in diesem Jahr sind Attacken auf Energieversorger, Ausschaltung von Infrastruktur (Netzwerke, Stromversorgung), Analyse von Netzwerkverkehr zum Schutz autonomer Systeme, Aufklärung in globalen Netzwerken (Internet, Domain Name Service) und das Aufspüren von versteckten Kommunikationskanälen.

Der Fokus sind die Zusammenhänge zwischen Vorfällen und der Verwendung bestimmter Angriffswege. Beispielsweise erfährt man aus herkömmlicher Berichterstattung meist, welche Schadsoftware zugeschlagen hat. Man lernt aber sehr wenig über die tatsächlichen Infektionswege, welche Teile der Infrastruktur betroffen sind und was eigentlich das Ziel war. Diese Details lassen sich nur in kleinem Rahmen und Blick auf die Strategie besprechen. Speziell in der digitalen Welt sind Zusammenhänge oft schwer erkennbar, da das Internet global zur Verfügung steht. Die klare Zuordnung von Tätern - seien es Einzelpersonen, Organisationen oder Staaten - ist dabei sehr schwierig bis unmöglich. Auch in bei diesen Überlegungen möchte die DeepINTEL allen Teilnehmern Hilfestellung geben.

Die notwendigen Daten für eine strategische Betrachtung der eigenen Informationstechnologie sind kritisch für eine aussagekräftige Analyse. Am Markt gibt es viele Dienstleister, die erfasste Daten zusammenführen und mit Sensornetzwerken ergänzen. Es kann aber niemand die Kenntnisse über die eigenen Prozesse und die interne Organisation ersetzen. Daher wird während der DeepINTEL Konferenz auch die Erfassung, die Bewertung und die richtige Auswertung der Informationen diskutiert, die bereits zur Verfügung stehen.

Programme und Buchung

Die DeepINTEL Konferenz findet am 27. November 2019 in Wien statt. Das Programm senden wir auf Anfragen an deepsec@deepsec.net nach Überprüfung gerne zu. Tickets sind auf der Webseite https://deepintel.net/ erhältlich.

Der Veranstaltungsort für DeepSec und DeepINTEL Konferenz ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Das Programm der im Anschluss stattfindenden DeepSec Konferenz ist unter https://deepsec.net/schedule.html ersichtlich. Das Programm der DeepINTEL wird ausschließlich auf Anfrage zur Verfügung gestellt, weil es sich bei der DeepINTEL um eine nichtöffentliche Konferenz handelt.

Tickets für die DeepSec Konferenz sowie für die DeepINTEL Veranstaltung und die DeepSec Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html oder per E-Mail an deepsec@deepsec.net bestellen.

(/)

BUSINESS

Mediabox

pts20191104009 Technologie/Digitalisierung, Forschung/Entwicklung

Dekonstruktion und Analyse moderner IT-Bedrohungen

DeepINTEL Security Intelligence Konferenz entzaubert Komplexität von Sicherheitsbedrohungen

Wien (pts009/04.11.2019/09:45) - **Die moderne digitale Welt wird ständig bedroht. Leider verstehen nur wenige, was dies tatsächlich bedeutet. Informationssicherheit wird immer in verfälschenden Klischees dargestellt, die mit der Realität nichts zu tun haben. Kein Angriff wird in Minuten durch Hämmern auf eine Tastatur umgesetzt. Die gefährlichsten Bedrohungen lassen sich nicht durch Kapuzenshirts oder Gesichtsmasken erkennen. Nichts in der digitalen Welt lässt sich mit einem einfachen Klick entschärfen. Das Gegenteil ist der Fall, weil Innen- und Außenpolitik globale Auswirkungen auf die digitale Infrastruktur aller Organisationen haben. Die jedes Jahr in Wien stattfindende DeepINTEL Security Intelligence Konferenz möchte daher eine Plattform bieten, auf der Behörden, Unternehmen, Forscher und Hacker produktiv in einem geschlossenen Kreis Eigenschaften und Gegenmaßnahmen von Bedrohungen diskutieren können.**

Plakative Beispiele

Wirtschaftsspionage wird sehr gerne als Beispiel für Bedrohungen im Bereich der Informationen angeführt. Angriffe auf Informationssysteme haben oft das Ziel, Daten zu kopieren, um diese dann entweder zu handeln oder anderweitig zu verwenden. Spionage gibt es auf allen Ebenen. Im Mai 2019 wurde bekannt, dass man über WhatsApp-Anrufe Smartphones infizieren kann. Das Annehmen des Anrufs war nicht notwendig. Ausgenutzt wurde diese Schwachstelle von einer in Israel produzierten kommerziellen Spionagesoftware. Ausspioniert wurden zwar keine Firmen, sondern Bürgerrechtlerinnen und Bürgerrechtler im Nahen Osten. Die Software könnte genauso auf Geschäftsführerinnen und Angestellte losgelassen werden. Die Kunden der israelischen Firma sitzen nicht nur im Nahen Osten. Sie befinden sich auch in westlichen Staaten.

Der Knackpunkt ist das Finden von Schwachstellen, um die Verteidigung zu brechen oder zu umgehen. Die Kenntnis über solche Lücken wird mit viel Geld belohnt und gehandelt. Die Analogie zu Waffen liegt nahe, auch wenn es große technologische Unterschiede gibt. Schadcode hat mehr Verwandtschaft mit biologischen

Waffen. Die Attacken durch die Schadsoftware Petya und Wannacry in den Jahren 2016 bzw. 2017 unterstreichen diese These, da die Ausnutzung der Schwachstelle, über die beide Programme eindringen konnten, sehr wahrscheinlich durch die US-amerikanische National Security Agency (NSA) entwickelt wurde. Konkrete Beweise über das tatsächliche Entkommen der Schwachstelle fehlen. Die entwickelten Theorien reichen von der Aktion eines Whistleblowers bis hin zu Tätern aus Russland. Gewissheit wird es keine geben.

Für Sicherheitsverantwortliche in Unternehmen spielen die Spekulationen keine Rolle. Die Fakten zeigen, dass sich die digitale Welt direkt in geopolitischen Spannungsfeldern bewegt. Es wird daher höchste Zeit, diesen Umstand in interne Abläufe zu integrieren.

Geopolitik ist längst Teil von Unternehmensentscheidungen

Die Wirtschaft wird gerne und oft abseits der Politik wahrgenommen. Dies gilt insbesondere für digitale Dienstleistungen. Beim Streaming, der internen Dokumentenablage, E-Mail Kommunikation, Social-Media-Plattformen oder den Dateiablage besitzen nur noch wenige Organisationen eine eigene Infrastruktur. Wolkige Dienstleister verwalten fremde digitale Güter. Der sehr beliebte Begriff der Digitalen Souveränität verliert jede Bedeutung, wenn die Geschäftsführung nicht mehr sagen kann wo sich alle Unternehmensdaten genau befinden und wer sie verwaltet. Man kann nichts beschützen dessen Aufenthaltsort man nicht kennt. Das gilt insbesondere für Prototypen wie die vom deutschen Wirtschaftsministerium vorgeschlagene Gaia-X-Infrastruktur. Sie soll eine Alternative zur Datenhaltung und -verarbeitung außerhalb der Grenzen Europas bieten. Der Kern des Ganzen? Geopolitik ist zum Alltag in der Wirtschaft geworden. Damit kann die Software genau so wie die Hardware auch in Handelskriege - oder Schlimmerem - verstrickt werden.

Die Beispiele illustrieren endringlich, dass sich die Unternehmensführungen nun endlich auch mit Themen beschäftigen müssen, die bislang die Außenpolitik und das Militär beschäftigt haben. Die IT Sicherheit hat das schon längst erkannt und den Bereich der Security Intelligence geschaffen. Dort beschäftigt man sich mit dem strategischen Blick auf Bedrohungen und die Fähigkeiten der Gegner gegen die man sich verteidigen muss. Die technischen Details sind dabei zwar Rüstzeug, jedoch sekundär. Es geht um das Aufklären der Identitäten, Kapazitäten und Absichten gegnerischer Organisationen, welche die eigenen Daten und die eigene Infrastruktur attackieren können. Die klassische Informationssicherheit liefert die Werkzeuge, aber Analytikerinnen müssen die Puzzlesteine richtig zusammensetzen. Genau dort setzt die jährlich in Wien stattfindende DeepINTEL Konferenz an - Austausch von Erkenntnissen in einer geschlossenen Gruppe.

Austausch am lebenden Objekt

Möchte man über echte Vorfälle und konkrete Einbrüche reden, so ist es ratsam, dies konzentriert im Rahmen von Diskussionen unter Expertinnen und Experten zu tun. Der Erfahrungsaustausch ist von unschätzbarem Wert und verbessert Ihre Verteidigung nachhaltig. Die DeepINTEL ist eine solche Plattform. Fokus in diesem Jahr sind Attacken auf Energieversorger, Ausschaltung von Infrastruktur (Netzwerke, Stromversorgung), Analyse von Netzwerkverkehr zum Schutz autonomer Systeme, Aufklärung in globalen Netzwerken (Internet, Domain Name Service) und das Aufspüren von versteckten Kommunikationskanälen.

Der Fokus sind die Zusammenhänge zwischen Vorfällen und der Verwendung bestimmter Angriffswege. Beispielsweise erfährt man aus herkömmlicher Berichterstattung meist, welche Schadsoftware zugeschlagen hat. Man lernt aber sehr wenig über die tatsächlichen Infektionswege, welche Teile der Infrastruktur betroffen sind und was eigentlich das Ziel war. Diese Details lassen sich nur in kleinem Rahmen und Blick auf die Strategie besprechen. Speziell in der digitalen Welt sind Zusammenhänge oft schwer erkennbar, da das Internet global zur Verfügung steht. Die klare Zuordnung von Tätern - seien es Einzelpersonen, Organisationen oder Staaten - ist dabei sehr schwierig bis unmöglich. Auch in bei diesen Überlegungen möchte die DeepINTEL allen Teilnehmern Hilfestellung geben.

Die notwendigen Daten für eine strategische Betrachtung der eigenen Informationstechnologie sind kritisch für eine aussagekräftige Analyse. Am Markt gibt es viele Dienstleister, die erfasste Daten zusammenführen und mit Sensornetzwerken ergänzen. Es kann aber niemand die Kenntnisse über die eigenen Prozesse und die

interne Organisation ersetzen. Daher wird während der DeepINTEL Konferenz auch die Erfassung, die Bewertung und die richtige Auswertung der Informationen diskutiert, die bereits zur Verfügung stehen.

Programme und Buchung

Die DeepINTEL Konferenz findet am 27. November 2019 in Wien statt. Das Programm senden wir auf Anfragen an deepsec@deepsec.net (mailto:deepsec@deepsec.net) nach Überprüfung gerne zu. Tickets sind auf der Webseite https://deepintel.net/ (https://deepintel.net/) erhältlich.

Der Veranstaltungsort für DeepSec und DeepINTEL Konferenz ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Das Programm der im Anschluss stattfindenden DeepSec Konferenz ist unter https://deepsec.net/schedule.html (https://deepsec.net/schedule.html) ersichtlich. Das Programm der DeepINTEL wird ausschließlich auf Anfrage zur Verfügung gestellt, weil es sich bei der DeepINTEL um eine nichtöffentliche Konferenz handelt.

Tickets für die DeepSec Konferenz sowie für die DeepINTEL Veranstaltung und die DeepSec Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html (https://deepsec.net/register.html) oder per E-Mail an deepsec@deepsec.net (mailto:deepsec@deepsec.net) bestellen.

(Ende)

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

(http://deepsec.net)

https://www.pressetext.com/news/20191017014

Bedrohungen und Lösungen für Supply-Chain-Attacken in der IT

DeepSec Konferenz beleuchtet die verkettete Logistik der Informationstechnologie

Wien (pts014/17.10.2019/10:30) - Im Netz tummeln sich Videos von sehr ausgeklügelten Aufbauten vieler Dominosteine. Stößt man dann einen Stein um, so folgt eine ganze Kaskade von atemberaubenden Aktionen. Der Dominoeffekt in der eigenen IT-Infrastruktur ist wesentlich weniger unterhaltsam. Auch dort fängt alles meist harmlos mit einer kleinen Aktion an - dem Lesen einer Nachricht, der Weiterleitung eines Dokuments, dem Zugriff auf einen Webserver oder dem Erhalt einer Kurznachricht von einem vermeintlichen Mitarbeiter. Besonders spannend wird es, wenn die Dominosteine dann die eigenen Lieferanten und Geschäftspartnerinnen sind. Die diesjährige DeepSec Sicherheitskonferenz bietet reichhaltige Inhalte zur Analyse der verwobenen Situation moderner Firmen und Organisationen.

Ohne Vertrauen geht es nicht in Netzwerken

In der Theorie gibt es immer ein Außen und ein Innen. Türen, Netzwerkfilter, Zugänge, ... Datenhaltung kennt diesen Ansatz. In allen IT-Architekturen findet daher immer eine Einteilung statt, die letztlich auch die Sicherheitszonen abbildet. Außen bedeutet oft nicht vertrauenswürdig. Haben Daten, Personen oder Tätigkeiten einmal eine Reihe von Sicherheitsprüfungen absolviert, so gelten sie als vertrauenswürdig. Dieser Zustand bleibt oft unverändert, weil keine weiteren oder zumindest weniger Prüfungen durchgeführt werden. Vertrauen macht sich breit. Kombiniert man nun diese Elemente durch Geschäftsbeziehungen, so baut man sich seine sehr persönliche Straße von Dominosteinen auf. Je komplexer die Abläufe, desto mehr Steine stehen auf dem Tisch. Eine Mischung aus Dienstleistern und Outsourcing potenziert das ganze Werk. Angreiferinnen müssen jetzt nur noch den richtigen Stein zum Anstoßen aussuchen.

In den vergangenen 12 Monaten betrafen mehrere Attacken auf Zulieferer den europäischen Luftfahrtkonzern Airbus. Der Konzern wurde über kleinere Firmen angegriffen, es wurden offenbar die Vertrauensverhältnisse ausgenutzt. Sicherheitsmaßnahmen sind schon allein wegen der verschiedenen Budgets in Organisationen nicht gleich. Umgekehrt kann auch die Größe täuschen, weil die bloße Präsenz von Daten auf einer Cloud-Plattform auch keine Aussage über die Sicherheit treffen kann. Das Geschäftsleben wird also von Dominosteinketten beherrscht, zumindest aus der Sicht der Informationssicherheit.

Überblick schlägt Größe der Organisation

Man darf nun keine übereilige Schlüsse aus den Lieferketten und deren Bedeutung für die Sicherheit ziehen, auch wenn Schlussfolgerungen auf Basis von lückenhaftem Wissen gerade modisch sind. Die Größe einer Firma bzw. deren Budget für Sicherheit ist keine Garantie gegen Vorfälle. Angreifer versuchen natürlich immer den effizientesten Weg zu nehmen, um ihr Ziel zu erreichen. Bei kleineren Unternehmen gibt es viel mehr Möglichkeiten Hebel anzusetzen. Die beste Gegenmaßnahme ist die eigenen Abhängigkeiten aufzuklären und sehr gut im Blick zu haben. Wie eingangs erwähnt, ganz ohne Vertrauen geht es nicht. Dennoch sollte man von möglichst wenig ungeprüften Annahmen ausgehen, wenn es um die intern und extern aufgebauten Vertrauensverhältnisse geht.

Die im November stattfindende DeepSec IT Sicherheitskonferenz bietet daher eine ganze Reihe von Trainings und Vorträgen an, die dabei helfen können die Aufstellung der eigenen Dominosteine besser kennenzulernen. In den zweitägigen Trainings wird der Umgang mit Bedrohungen gezielt gelehrt. Xavier Mertens zeigt in seinem Training vor wie man Gefährdungen durch Analyse frei verfügbarer Daten erkennt, isoliert und zu Ergebnissen kommt. In dem technischen Training von Davy Douhine und Guillaume Lopes werden mobile Endgeräte, in Dawid Czagans Training moderne Webapplikationen aus der Sicht der Informationssicherheit in ihre logischen Bestandteile zerlegt. Beide Technologien sind Teil aller Dominosteinketten in allen Bereichen der Wirtschaft.

Bei dem Training zur Entwicklung von Geräten im Bereich des Internets of Things (IoT) durch Lior Yaari geht es um Fallstricke bei der Produktentwicklung und beim Testen von IoT Komponenten. Arnauld Soullie führt zwei Tage lang durch Schwachstellen von Industrial Control Systems, die in Industrieanlagen europa- und weltweit zu finden sind. Weiterhin stellen Peter Manev und Eric Leblond in ihrem Training ihre Expertise im Bereich der Einbruchsanalyse in Netzwerken zur Verfügung. Beide sind renommierte Experten, die seit mehr als 10 Jahren Spuren von Attacken und Anomalien in Datentransfers analysieren und detektieren.

Und zu guter Letzt bieten Thomas Fischer und Craig Jones ihre praktischen Erfahrungen im Umgang mit den wichtigsten Schritten im Notfall an, wenn bereits ein Gruppe von Angreifern Fuß in der eigenen Infrastruktur - oder der eines Lieferanten - gefasst hat. In ihrem Training geht es ganz konkret um Maßnahmen der Informationsbeschaffung, dem Finden von Schwachstellen in der eigenen Infrastruktur, dem Verlauf des Einbruchs und das Aufspüren von dessen Spuren.

Mut zum technischen Verständnis unerlässlich

Die IT-Sicherheit hat, wie die Informationstechnologie selbst, mit der Komplexität der eingesetzten Hardware und Software zu kämpfen. Beim Sammeln der notwendigen Erfahrung und beim Erlernen des notwendigen Wissens werden leider oft technische Zusammenhänge ausgelassen. Diese sind allerdings ein wichtiges Werkzeug, um die verwendete Technologien im eigenen Unternehmen und bei den Partnern richtig einschätzen zu können. Man mag heute nicht mehr genau wissen wie ein Flugzeug fliegt und wie ein Auto fährt, aber eine Auseinandersetzung mit den jeweiligen Themen bedingt zwangsläufig Kenntnisse der Technologie.

Die DeepSec Konferenz führt aus diesem Grunde seit ihrer Gründung den Titel In-Depth Security Conference, weil es bei der Sicherheit immer um Details geht, nie um Oberflächlichkeiten. Die DeepSec Konferenz legt daher größten Wert auf die Expertise der Trainer und Vortragenden, und sie unterstützt darüber hinaus Forschung und Lehre, um neue Erkenntnisse daraus der Wirtschaft zur Verfügung zu stellen. Nutzen Sie die Gelegenheit und seien Sie kein Dominostein.

Programme und Buchung

Die DeepSec 2019 Konferenztage sind am 28. und 29. November. Die DeepSec Trainings finden an den zwei vorangehenden Tagen, dem 26. und 27. November statt.

Der Veranstaltungsort für die DeepSec Veranstaltung ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Tickets für die DeepSec Konferenz selbst und die Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html bestellen.

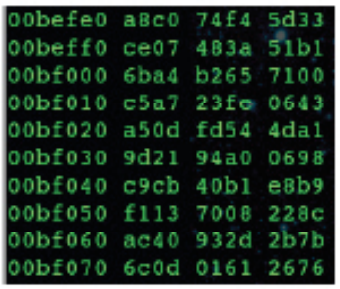
(/)

BUSINESS

pts20191017014 Unternehmen/Wirtschaft, Technologie/Digitalisierung

Bedrohungen und Lösungen für Supply-Chain-Attacken in der IT

DeepSec Konferenz beleuchtet die verkettete Logistik der Informationstechnologie



Daten von Partnerfirmen - gefährlich oder harmlos? (Illustration: René Pfeiffer)

Wien (pts014/17.10.2019/10:30) - **Im Netz tummeln sich Videos von sehr ausgeklügelten Aufbauten vieler Dominosteine. Stößt man dann einen Stein um, so folgt eine ganze Kaskade von atemberaubenden Aktionen. Der Dominoeffekt in der eigenen IT-Infrastruktur ist wesentlich weniger unterhaltsam. Auch dort fängt alles meist harmlos mit einer kleinen Aktion an - dem Lesen einer Nachricht, der Weiterleitung eines Dokuments, dem Zugriff auf einen Webserver oder dem Erhalt einer Kurznachricht von einem vermeintlichen Mitarbeiter. Besonders spannend wird es, wenn die Dominosteine dann die eigenen Lieferanten und Geschäftspartnerinnen sind. Die diesjährige DeepSec Sicherheitskonferenz bietet reichhaltige Inhalte zur Analyse der verwobenen Situation moderner Firmen und Organisationen.**

Ohne Vertrauen geht es nicht in Netzwerken

In der Theorie gibt es immer ein Außen und ein Innen. Türen, Netzwerkfilter, Zugänge, ... Datenhaltung kennt diesen Ansatz. In allen IT-Architekturen findet daher immer eine Einteilung statt, die letztlich auch die Sicherheitszonen abbildet. Außen bedeutet oft nicht vertrauenswürdig. Haben Daten, Personen oder Tätigkeiten einmal eine Reihe von Sicherheitsprüfungen absolviert, so gelten sie als vertrauenswürdig. Dieser Zustand bleibt oft unverändert, weil keine weiteren oder zumindest weniger Prüfungen durchgeführt werden. Vertrauen macht sich breit. Kombiniert man nun diese Elemente durch Geschäftsbeziehungen, so baut man sich seine sehr persönliche Straße von Dominosteinen auf. Je komplexer die Abläufe, desto mehr Steine stehen auf dem Tisch. Eine Mischung aus Dienstleistern und Outsourcing potenziert das ganze Werk. Angreiferinnen müssen jetzt nur noch den richtigen Stein zum Anstoßen aussuchen.

In den vergangenen 12 Monaten betrafen mehrere Attacken auf Zulieferer den europäischen Luftfahrtkonzern Airbus. Der Konzern wurde über kleinere Firmen angegriffen, es wurden offenbar die Vertrauensverhältnisse ausgenutzt. Sicherheitsmaßnahmen sind schon allein wegen der verschiedenen Budgets in Organisationen nicht gleich. Umgekehrt kann auch die Größe täuschen, weil die bloße Präsenz von Daten auf einer Cloud-Plattform auch keine Aussage über die Sicherheit treffen kann. Das Geschäftsleben wird also von Dominosteinketten beherrscht, zumindest aus der Sicht der Informationssicherheit.

Überblick schlägt Größe der Organisation

Man darf nun keine übereilige Schlüsse aus den Lieferketten und deren Bedeutung für die Sicherheit ziehen, auch wenn Schlussfolgerungen auf Basis von lückenhaftem Wissen gerade modisch sind. Die Größe einer Firma bzw. deren Budget für Sicherheit ist keine Garantie gegen Vorfälle. Angreifer versuchen natürlich immer den effizientesten Weg zu nehmen, um ihr Ziel zu erreichen. Bei kleineren Unternehmen gibt es viel mehr Möglichkeiten Hebel anzusetzen. Die beste Gegenmaßnahme ist die eigenen Abhängigkeiten aufzuklären und sehr gut im Blick zu haben. Wie eingangs erwähnt, ganz ohne Vertrauen geht es nicht. Dennoch sollte man von möglichst wenig ungeprüften Annahmen ausgehen, wenn es um die intern und extern aufgebauten Vertrauensverhältnisse geht.

Die im November stattfindende DeepSec IT Sicherheitskonferenz bietet daher eine ganze Reihe von Trainings und Vorträgen an, die dabei helfen können die Aufstellung der eigenen Dominosteine besser kennenzulernen. In den zweitägigen Trainings wird der Umgang mit Bedrohungen gezielt gelehrt. Xavier Mertens zeigt in seinem Training vor wie man Gefährdungen durch Analyse frei verfügbarer Daten erkennt, isoliert und zu Ergebnissen kommt. In dem technischen Training von Davy Douhine und Guillaume Lopes werden mobile Endgeräte, in Dawid Czagans Training moderne Webapplikationen aus der Sicht der Informationssicherheit in ihre logischen Bestandteile zerlegt. Beide Technologien sind Teil aller Dominosteinketten in allen Bereichen der Wirtschaft.

Bei dem Training zur Entwicklung von Geräten im Bereich des Internets of Things (IoT) durch Lior Yaari geht es um Fallstricke bei der Produktentwicklung und beim Testen von IoT Komponenten. Arnauld Soullie führt zwei Tage lang durch Schwachstellen von Industrial Control Systems, die in Industrieanlagen europa- und weltweit zu finden sind. Weiterhin stellen Peter Manev und Eric Leblond in ihrem Training ihre Expertise im Bereich der Einbruchsanalyse in Netzwerken zur Verfügung. Beide sind renommierte Experten, die seit mehr als 10 Jahren Spuren von Attacken und Anomalien in Datentransfers analysieren und detektieren.

Und zu guter Letzt bieten Thomas Fischer und Craig Jones ihre praktischen Erfahrungen im Umgang mit den wichtigsten Schritten im Notfall an, wenn bereits ein Gruppe von Angreifern Fuß in der eigenen Infrastruktur - oder der eines Lieferanten - gefasst hat. In ihrem Training geht es ganz konkret um Maßnahmen der Informationsbeschaffung, dem Finden von Schwachstellen in der eigenen Infrastruktur, dem Verlauf des Einbruchs und das Aufspüren von dessen Spuren.

Mut zum technischen Verständnis unerlässlich

Die IT-Sicherheit hat, wie die Informationstechnologie selbst, mit der Komplexität der eingesetzten Hardware und Software zu kämpfen. Beim Sammeln der notwendigen Erfahrung und beim Erlernen des notwendigen Wissens werden leider oft technische Zusammenhänge ausgelassen. Diese sind allerdings ein wichtiges Werkzeug, um die verwendete Technologien im eigenen Unternehmen und bei den Partnern richtig einschätzen zu können. Man mag heute nicht mehr genau wissen wie ein Flugzeug fliegt und wie ein Auto fährt, aber eine Auseinandersetzung mit den jeweiligen Themen bedingt zwangsläufig Kenntnisse der Technologie.

Die DeepSec Konferenz führt aus diesem Grunde seit ihrer Gründung den Titel In-Depth Security Conference, weil es bei der Sicherheit immer um Details geht, nie um Oberflächlichkeiten. Die DeepSec Konferenz legt daher größten Wert auf die Expertise der Trainer und Vortragenden, und sie unterstützt darüber hinaus Forschung und Lehre, um neue Erkenntnisse daraus der Wirtschaft zur Verfügung zu stellen. Nutzen Sie die Gelegenheit und seien Sie kein Dominostein.

Programme und Buchung

Die DeepSec 2019 Konferenztage sind am 28. und 29. November. Die DeepSec Trainings finden an den zwei vorangehenden Tagen, dem 26. und 27. November statt.

Der Veranstaltungsort für die DeepSec Veranstaltung ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Tickets für die DeepSec Konferenz selbst und die Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html (https://deepsec.net/register.html) bestellen.

(Ende)

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

(http://deepsec.net/)

https://www.pressetext.com/news/20191016009

L'Internet des faits et la peur dans la sécurité informatique

Les conférences DeepSec et DeepINTEL dévoilent leurs programmes - sécurité et géopolitique

Vienne (pts009/16.10.2019/09:15) - "No man is an island". Cette citation ("Aucun homme n'est une île") est de l'écrivain anglais John Donne. Si la phrase est devenue célèbre au XVIIe siècle, elle prend un tout autre sens à l'ère du numérique. La version moderne serait plutôt : il n'y a plus aucune île. De plus en plus de domaines du quotidien et de la société sont connectés. Cette année, les conférences sur la sécurité DeepSec et DeepINTEL souhaitent donc jeter un regard sobre sur l'Internet des faits et sur la peur sous l'angle de la sécurité de l'information. Actuellement, les systèmes sont moins isolés et bien plus complexes que ce qui est raisonnable du point de vue de la sécurité. La DeepSec se consacre donc aux nouvelles technologies et à leurs vulnérabilités au cours de deux journées de conférences et de formations. En parallèle, le séminaire DeepINTEL discutera de la relation entre la géopolitique et la sécurité informatique à l'aide d'exemples d'incidents.

L'Internet des attaques remplace l'Internet des objets

On s'en rend compte dès que l'on connecte un système à Internet. Les cibles intéressantes ou vulnérables sont immédiatement attaquées. Et c'est pareil lorsqu'on connecte des capteurs, des appareils ou des acteurs (les " objets " de l'Internet des objets) à un réseau. Cette année, les conférences de la DeepSec tenteront d'établir un lien entre différents aspects de la sécurité informatique dans ce contexte. Les appareils mobiles ont toujours été menacés. Les technologies sans fil d'aujourd'hui reposent sur les données. Pas étonnant donc que Luca Melette explique les attaques des systèmes mobiles exclusivement par le biais du protocole Internet. Aleksandr Kolchanov montrera comment compromettre et lire en masse certains appareils mobiles. Lior Yaari partagera son expérience dans le domaine de la construction auto. Il a analysé les composants de futures voitures qui ne sont pas encore sur le marché mais déjà en développement. Lior rendra compte des points faibles des technologies que l'on croisera peut-être sur nos routes dans quelques années.

Formation avec des experts en sécurité

La conférence DeepSec propose chaque année une formation continue par des experts en sécurité pour les experts de votre entreprise. L'échange de connaissances est la base de toute bonne défense, et pas que dans le

numérique. En raison de la courte durée de vie de la technologie de l'information, le niveau de connaissances et la formation continue de chacun sont décisifs pour faire face aux attaques et à la connexion constante. Le programme offre par conséquent trois ateliers différents indiquant comment gérer les attaques. Xavier Mertens expliquera les dangers de l'Open Source Security. Il utilisera des sources accessibles à tous pour expliquer comment y faire face et comment mettre en place des processus internes. Il donnera des exemples permettant de détecter des schémas suspects à l'aide d'études de cas.

Peter Manev et Eric Leblond montreront dans leur atelier comment détecter les attaques et les processus suspects dans un réseau avec le logiciel de détection d'intrusion Suricata. Suricata est facile à mettre en place et offre énormément de fonctionnalités. Les deux formateurs sont également développeurs chez Suricata et donnent des précisions de première main sur les processus internes du logiciel. Les participants s'essayeront en outre à la création de règles pour un vrai trafic réseau. La formation privilégie une approche concrète et s'adresse à tous ceux qui travaillent dans la sécurité réseau.

Dans leur atelier, Thomas Fischer et Craig Jones montrent comment gérer des incidents de sécurité et retrouver les traces des hackers. Là aussi, la formation repose sur des cas réels et de vrais exemples d'utilisation des bons outils.

La technologie n'est pas une île non plus

Souvent, seul le point de vue technique est pris en compte lors de l'examen des problèmes de sécurité. Dans la technologie de l'information comme dans d'autres domaines, des facteurs externes déterminent certaines conditions. Le débat sur les portes dérobées dans les systèmes numériques et les réseaux de communication, récurrent depuis les années 1990, en est un exemple frappant. Ce qui a commencé avec le cryptage des réseaux mobiles et des e-mails se poursuit à présent avec la 5G, la messagerie instantanée et le développement de logiciels. En 2018, le gouvernement australien a adopté une loi qui peut forcer les entreprises spécialisées dans la technologie à intégrer des portes dérobées dans leurs produits. Ces points faibles prédéterminés seront aussi utilisés par les hackers.

Les mathématiques du cryptage sont implacables quand il s'agit de sécurité. Soit la communication est sûre, soit elle ne l'est pas. Les conflits commerciaux actuels affectent tout autant le monde de l'informatique et posent les jalons de la mise en place de nouvelles technologies dans les années à venir. Par conséquent, les DeepSec et DeepINTEL de cette année explorent les interactions entre la sécurité de l'information et les aspects géopolitiques.

Les présentations de ces deux conférences ont été choisies pour approfondir ce sujet. Les moyens d'attaques, la classification des cibles et les conditions d'utilisation des mesures de sécurité y seront entre autres abordés. Nous recommandons à tous les responsables de la sécurité d'approfondir leurs connaissances dans ces domaines.

Programme et réservation

Les conférences DeepSec 2019 auront lieu les 28 et 29 novembre. Les formations DeepSec auront lieu les deux jours précédents, les 26 et 27 novembre.

La conférence DeepINTEL aura lieu le 27 novembre. Pour recevoir le programme, envoyez une demande à deepsec@deepsec.net. Les tickets sont disponibles sur https://deepintel.net .

DeepSec et DeepINTEL auront lieu à l'hôtel Imperial Riding School Renaissance Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Vienne.

Le programme de la conférence DeepSec peut être consulté sur https://deepsec.net/schedule.html . Le programme de DeepINTEL peut seulement être mis à disposition sur demande, car il s'agit d'une conférence privée.

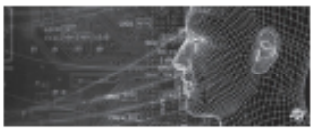
Vous pouvez commander vos tickets pour la conférence DeepSec, DeepINTEL et les formations DeepSec sur https://deepsec.net/register.html .

HIGHTECH

pts20191016009 Technologie/Digitalisierung, Unternehmen/Wirtschaft

L'Internet des faits et la peur dans la sécurité informatique

Les conférences DeepSec et DeepINTEL dévoilent leurs programmes - sécurité et géopolitique



Sujet sécurité de l'information (Copyright : Florian Stocker, Cronos Agency OG)

Vienne (pts009/16.10.2019/09:15) - **"No man is an island". Cette citation ("Aucun homme n'est une île") est de l'écrivain anglais John Donne. Si la phrase est devenue célèbre au XVIIe siècle, elle prend un tout autre sens à l'ère du numérique. La version moderne serait plutôt : il n'y a plus aucune île. De plus en plus de domaines du quotidien et de la société sont connectés. Cette année, les conférences sur la sécurité DeepSec et DeepINTEL souhaitent donc jeter un regard sobre sur l'Internet des faits et sur la peur sous l'angle de la sécurité de l'information. Actuellement, les systèmes sont moins isolés et bien plus complexes que ce qui est raisonnable du point de vue de la sécurité. La DeepSec se consacre donc aux nouvelles technologies et à leurs vulnérabilités au cours de deux journées de conférences et de formations. En parallèle, le séminaire DeepINTEL discutera de la relation entre la géopolitique et la sécurité informatique à l'aide d'exemples d'incidents.**

L'Internet des attaques remplace l'Internet des objets

On s'en rend compte dès que l'on connecte un système à Internet. Les cibles intéressantes ou vulnérables sont immédiatement attaquées. Et c'est pareil lorsqu'on connecte des capteurs, des appareils ou des acteurs (les " objets " de l'Internet des objets) à un réseau. Cette année, les conférences de la DeepSec tenteront d'établir un lien entre différents aspects de la sécurité informatique dans ce contexte. Les appareils mobiles ont toujours été menacés. Les technologies sans fil d'aujourd'hui reposent sur les données. Pas étonnant donc que Luca Melette explique les attaques des systèmes mobiles exclusivement par le biais du protocole Internet. Aleksandr Kolchanov montrera comment compromettre et lire en masse certains appareils mobiles. Lior Yaari partagera son expérience dans le domaine de la construction auto. Il a analysé les composants de futures voitures qui ne sont pas encore sur le marché mais déjà en développement. Lior rendra compte des points faibles des technologies que l'on croisera peut-être sur nos routes dans quelques années.

Formation avec des experts en sécurité

La conférence DeepSec propose chaque année une formation continue par des experts en sécurité pour les experts de votre entreprise. L'échange de connaissances est la base de toute bonne défense, et pas que dans le numérique. En raison de la courte durée de vie de la technologie de l'information, le niveau de connaissances et la formation continue de chacun sont décisifs pour faire face aux attaques et à la connexion constante. Le programme offre par conséquent trois ateliers différents indiquant comment gérer les attaques. Xavier Mertens expliquera les dangers de l'Open Source Security. Il utilisera des sources accessibles à tous pour expliquer comment y faire face et comment mettre en place des processus internes. Il donnera des exemples permettant de détecter des schémas suspects à l'aide d'études de cas.

Peter Manev et Eric Leblond montreront dans leur atelier comment détecter les attaques et les processus suspects dans un réseau avec le logiciel de détection d'intrusion Suricata. Suricata est facile à mettre en place et offre énormément de fonctionnalités. Les deux formateurs sont également développeurs chez Suricata et donnent des précisions de première main sur les processus internes du logiciel. Les participants s'essayeront en outre à la création de règles pour un vrai trafic réseau. La formation privilégie une approche concrète et s'adresse à tous ceux qui travaillent dans la sécurité réseau.

Dans leur atelier, Thomas Fischer et Craig Jones montrent comment gérer des incidents de sécurité et retrouver les traces des hackers. Là aussi, la formation repose sur des cas réels et de vrais exemples d'utilisation des bons outils.

La technologie n'est pas une île non plus

Souvent, seul le point de vue technique est pris en compte lors de l'examen des problèmes de sécurité. Dans la technologie de l'information comme dans d'autres domaines, des facteurs externes déterminent certaines conditions. Le débat sur les portes dérobées dans les systèmes numériques et les réseaux de communication, récurrent depuis les années 1990, en est un exemple frappant. Ce qui a commencé avec le cryptage des réseaux mobiles et des e-mails se poursuit à présent avec la 5G, la messagerie instantanée et le développement de logiciels. En 2018, le gouvernement australien a adopté une loi qui peut forcer les entreprises spécialisées dans la technologie à intégrer des portes dérobées dans leurs produits. Ces points faibles prédéterminés seront aussi utilisés par les hackers.

Les mathématiques du cryptage sont implacables quand il s'agit de sécurité. Soit la communication est sûre, soit elle ne l'est pas. Les conflits commerciaux actuels affectent tout autant le monde de l'informatique et posent les jalons de la mise en place de nouvelles technologies dans les années à venir. Par conséquent, les DeepSec et DeepINTEL de cette année explorent les interactions entre la sécurité de l'information et les aspects géopolitiques. Les présentations de ces deux conférences ont été choisies pour approfondir ce sujet. Les moyens d'attaques, la classification des cibles et les conditions d'utilisation des mesures de sécurité y seront entre autres abordés. Nous recommandons à tous les responsables de la sécurité d'approfondir leurs connaissances dans ces domaines.

Programme et réservation

Les conférences DeepSec 2019 auront lieu les 28 et 29 novembre. Les formations DeepSec auront lieu les deux jours précédents, les 26 et 27 novembre.

La conférence DeepINTEL aura lieu le 27 novembre. Pour recevoir le programme, envoyez une demande à deepsec@deepsec.net (mailto:deepsec@deepsec.net). Les tickets sont disponibles sur https://deepintel.net (https://deepintel.net) .

DeepSec et DeepINTEL auront lieu à l'hôtel Imperial Riding School Renaissance Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Vienne.

Le programme de la conférence DeepSec peut être consulté sur https://deepsec.net/schedule.html (https://deepsec.net/schedule.html) . Le programme de DeepINTEL peut seulement être mis à disposition sur demande, car il s'agit d'une conférence privée.

Vous pouvez commander vos tickets pour la conférence DeepSec, DeepINTEL et les formations DeepSec sur https://deepsec.net/register.html (https://deepsec.net/register.html) .

(Ende)

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

(http://deepsec.net/)

https://www.pressetext.com/news/20190909006

Industriespionage und Datenabgriffe sind Alltag in der IT

DeepSec Konferenz bietet Trainings zur Früherkennung, Analyse und Schadensbegrenzung

Wien (pts006/09.09.2019/09:30) - Die Aufregung war früher groß, wenn Organisationen, Parteien, Prominente, Firmen oder staatliche Stellen Einbrüche in ihre eigene oder angemietete digitale Infrastruktur vermeldet haben. Mittlerweile gehören Berichte über Datenlecks und kompromittierte Systeme fast schon zum Wetterbericht. Sicherheitsapplikationen auf Smartphones oder Portale bieten diese Informationen an, um dem User eine Prüfung zu ermöglichen ob man selbst betroffen sein könnte. Die vernetzte Welt des Alltags macht es scheinbar möglich Angriff und Verteidigung in einem Atemzug zu präsentieren. Betroffene, Angreifer, Verteidiger und Nutznießer rücken näher zusammen. Wer diesen Eindruck hat, ist der um sich greifenden Vereinfachung zum Opfer gefallen. Die moderne Informationstechnologie muss sich täglich gefährlichen Situationen stellen, die weit mehr Facetten haben. Dazu braucht es eine gehörige Portion Fachwissen und Erfahrung.

Ersthelfer, Analyse und Finden von Bedrohungen

Alle digitalen Systeme und Netzwerke haben mittlerweile eine Verteidigung. Das Spektrum reicht vom Minimum bis hin zu Absicherungen mit hohem Aufwand. Im Normalbetrieb prüft man die benötigten Funktionen und stellt gegebenenfalls die Sicherheitsmaßnahmen nach, wenn es neue Meldungen gibt. Das ändert sich schlagartig, wenn ein tatsächlicher Einbruch entdeckt wird. Die sogenannte Incident Response, also Reaktion bei einem Vorfall, unterscheidet sich grundlegend vom normalen Betrieb. Es gilt festzustellen, welche Systeme, Applikationen und Daten betroffen sind.

Was haben Angreifer verändert? Welche Beweise und Indizien gibt es dafür? Thomas Fischer und Craig Jones werden auf der diesjährigen DeepSec ein Training veranstalten, in dem man die Abläufe von Incident Response erlernen und ausprobieren kann. In solchen Situationen muss sehr strukturiert und sorgfältig vorgegangen werden. Die Übungen lehren auch wie man Bedrohungen in der eigenen Infrastruktur oder Organisation findet bevor sie potentielle Angreifer ausfindig machen. In den zwei Tagen des Trainings werden alle Aspekte dieser Vorgehensweise ausgeführt. Die Teilnehmerinnen lernen auch die notwendigen Werkzeuge kennen, die in solchen Fällen benötigt werden.

Einbrüche bleiben lange unbemerkt

Leider werden kompromittierte Systeme oft nicht sofort entdeckt. Fähige Gegner vermeiden es entdeckt zu werden, um möglichst lange von dem Einbruch zu profitieren. Die Zeitspanne zwischen Angriff und Entdeckung bewegt sich im Bereich von Wochen bis zu vielen Monaten. Man kann diesen Zeitraum verkürzen, indem man sich eingehend mit dem Normalbetrieb der eigenen Infrastruktur auseinandersetzt und versucht Abweichungen zu erkennen. Peter Manev und Eric Leblond, Spezialisten auf dem Gebiet der Netzwerkeinbruchsanalyse, lehren in einem zweitägigen Training an Hand von Beispielen wie das funktioniert. Beide sind seit über 10 Jahren im Entwicklungsteam der Network Intrusion Detection Software Suricata tätig. Sie haben durch ihre Arbeit tiefen Einblick in die Vorgänge von Netzwerkübertragungen und sehr viel Erfahrung im Finden von Anomalien.

Das Training wird echte Daten von historischen Vorfällen verwenden, um direkt Techniken ausprobieren zu können. Neben dem Umgang mit den Werkzeugen zur Entdeckung, lernt man auch den Einsatz von Ködern, um Angreifer leichter entdecken zu können. Darüber hinaus wird vermittelt wie man Fehlalarme und echte Alarme besser auseinander halten kann.

Bestehende Daten nutzen, neue Angriffe erkennen

Wege zur Erkennung von Ereignissen sind oft schon vorhanden. Logdaten sind in allen Bereichen der IT vorhanden. Systeme und Applikationen generieren selbst Daten, die extrem hilfreich für die Verteidigung sind. Xavier Mertens zeigt in seinem Workshop wie man diese Schätze hebt. Er wird Techniken zur Anomalieerkennung auf Systemen (OSSEC im Speziellen) mit extern verfügbaren Informationen kombinieren, um das Bild der Lage zu schärfen. Diese sogenannten Open Source Intelligence (OSINT) Quellen liefern wichtige Daten zur Ergänzung. Xavier Mertens wird mit Beispielen vermitteln wie man diese Daten in die eigene Verteidigung richtig integriert. Sein Workshop ist für erfahrene IT Administratoren gedacht, die den Stand ihrer Verteidigungsmaßnahmen steigern möchten.

Vermutungen sind immer fehl am Platz

Bei der Untersuchung von Sicherheitsvorfällen darf es keine Spekulationen geben. Alle Erkenntnisse müssen auf Fakten beruhen, die aus der Analyse der verfügbaren Daten stammen. Das ist ein wichtiger Punkt, an dem oft schwere Fehler begangen werden. Es schleichen sich gerne Annahmen ein, die sich im Laufe der Abhandlung des Vorfalls verfestigen. Man entwickelt dann gerne einen Tunnelblick und interpretiert Informationen nur einseitig. Das

gilt es zu vermeiden. Gemäß der Datenschutz-Grundverordnung (DSGVO) müssen Vorfälle, die Daten von Kunden oder Dritten betreffen, natürlich gemeldet werden. Das steht nicht im Widerspruch keine Annahmen zu verbreiten, sondern bestätigt das Vermeiden von Spekulationen.

Es gibt zahlreiche Beispiele in aktuellen und vergangenen Nachrichtenmeldungen. Das Datenleck im Jahre 2017 bei Equifax, einem US-amerikanischen Finanzdienstleistungsunternehmen mit Hauptsitz in Atlanta im Bundesstaat Georgia, ist gut dokumentiert. Ohne Details bekannt zu geben, wurden Betroffene aufgefordert auf einer Webseite eine Teil ihrer Sozialversicherungsnummer einzugeben. Der Zweck sollte die Feststellung sein, ob eigene Daten kopiert wurden oder nicht. Dieser Schnellschuss führte zu viel größerer Unsicherheit, die durch Nachbesserungen und zusätzliche Erklärungen nicht nachhaltig verbessert wurde. Antworten, die zu mehr Fragen führen, sind keine sinnvolle Erklärung. Sie führen maximal zu mehr medialer Reichweite, weil die Öffentlichkeit dann mit spekulieren kann. In einem seriösen Kontext hat dieser Ansatz nichts zu suchen.

Die angebotenen Trainings zur DeepSec Konferenz sind als Hilfestellung gedacht, um in einem angenehmen Umfeld Erfahrungen im Umgang mit Sicherheitsvorfällen zu sammeln und Prozesse für den Ernstfall sinnvoll gestalten zu können.

Programme und Buchung

Die DeepSec 2019 Konferenztage sind am 28. und 29. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 26. und 27. November statt.

Der Veranstaltungsort für die DeepSec-Veranstaltung ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Tickets für die DeepSec Konferenz selbst und die Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html bestellen.

BUSINESS

pts20190909006 Technologie/Digitalisierung, Unternehmen/Wirtschaft

Industriespionage und Datenabgriffe sind Alltag in der IT

DeepSec Konferenz bietet Trainings zur Früherkennung, Analyse und Schadensbegrenzung

Wien (pts006/09.09.2019/09:30) - **Die Aufregung war früher groß, wenn Organisationen, Parteien, Prominente, Firmen oder staatliche Stellen Einbrüche in ihre eigene oder angemietete digitale Infrastruktur vermeldet haben. Mittlerweile gehören Berichte über Datenlecks und kompromittierte Systeme fast schon zum Wetterbericht. Sicherheitsapplikationen auf Smartphones oder Portale bieten diese Informationen an, um dem User eine Prüfung zu ermöglichen ob man selbst betroffen sein könnte. Die vernetzte Welt des Alltags macht es scheinbar möglich Angriff und Verteidigung in einem Atemzug zu präsentieren. Betroffene, Angreifer, Verteidiger und Nutznießer rücken näher zusammen. Wer diesen Eindruck hat, ist der um sich greifenden Vereinfachung zum Opfer gefallen. Die moderne Informationstechnologie muss sich täglich gefährlichen Situationen stellen, die weit mehr Facetten haben. Dazu braucht es eine gehörige Portion Fachwissen und Erfahrung.**

Ersthelfer, Analyse und Finden von Bedrohungen

Alle digitalen Systeme und Netzwerke haben mittlerweile eine Verteidigung. Das Spektrum reicht vom Minimum bis hin zu Absicherungen mit hohem Aufwand. Im Normalbetrieb prüft man die benötigten Funktionen und stellt gegebenenfalls die Sicherheitsmaßnahmen nach, wenn es neue Meldungen gibt. Das ändert sich schlagartig, wenn ein tatsächlicher Einbruch entdeckt wird. Die sogenannte Incident Response, also Reaktion bei einem Vorfall, unterscheidet sich grundlegend vom normalen Betrieb. Es gilt festzustellen, welche Systeme, Applikationen und Daten betroffen sind.

Was haben Angreifer verändert? Welche Beweise und Indizien gibt es dafür? Thomas Fischer und Craig Jones werden auf der diesjährigen DeepSec ein Training veranstalten, in dem man die Abläufe von Incident Response erlernen und ausprobieren kann. In solchen Situationen muss sehr strukturiert und sorgfältig vorgegangen werden. Die Übungen lehren auch wie man Bedrohungen in der eigenen Infrastruktur oder Organisation findet bevor sie potentielle Angreifer ausfindig machen. In den zwei Tagen des Trainings werden alle Aspekte dieser Vorgehensweise ausgeführt. Die Teilnehmerinnen lernen auch die notwendigen Werkzeuge kennen, die in solchen Fällen benötigt werden.

Einbrüche bleiben lange unbemerkt

Leider werden kompromittierte Systeme oft nicht sofort entdeckt. Fähige Gegner vermeiden es entdeckt zu werden, um möglichst lange von dem Einbruch zu profitieren. Die Zeitspanne zwischen Angriff und Entdeckung bewegt sich im Bereich von Wochen bis zu vielen Monaten. Man kann diesen Zeitraum verkürzen, indem man sich eingehend mit dem Normalbetrieb der eigenen Infrastruktur auseinandersetzt und versucht Abweichungen zu erkennen. Peter Manev und Eric Leblond, Spezialisten auf dem Gebiet der Netzwerkeinbruchsanalyse, lehren in einem zweitägigen Training an Hand von Beispielen wie das funktioniert. Beide sind seit über 10 Jahren im Entwicklungsteam der Network Intrusion Detection Software Suricata tätig. Sie haben durch ihre Arbeit tiefen Einblick in die Vorgänge von Netzwerkübertragungen und sehr viel Erfahrung im Finden von Anomalien.

Das Training wird echte Daten von historischen Vorfällen verwenden, um direkt Techniken ausprobieren zu können. Neben dem Umgang mit den Werkzeugen zur Entdeckung, lernt man auch den Einsatz von Ködern, um Angreifer leichter entdecken zu können. Darüber hinaus wird vermittelt wie man Fehlalarme und echte Alarme besser auseinander halten kann.

Bestehende Daten nutzen, neue Angriffe erkennen

Wege zur Erkennung von Ereignissen sind oft schon vorhanden. Logdaten sind in allen Bereichen der IT vorhanden. Systeme und Applikationen generieren selbst Daten, die extrem hilfreich für die Verteidigung sind. Xavier Mertens zeigt in seinem Workshop wie man diese Schätze hebt. Er wird Techniken zur Anomalieerkennung auf Systemen (OSSEC im Speziellen) mit extern verfügbaren Informationen kombinieren, um das Bild der Lage zu schärfen. Diese sogenannten Open Source Intelligence (OSINT) Quellen liefern wichtige Daten zur Ergänzung. Xavier Mertens wird mit Beispielen vermitteln wie man diese Daten in die eigene Verteidigung richtig integriert. Sein Workshop ist für erfahrene IT Administratoren gedacht, die den Stand ihrer Verteidigungsmaßnahmen steigern möchten.

Vermutungen sind immer fehl am Platz

Bei der Untersuchung von Sicherheitsvorfällen darf es keine Spekulationen geben. Alle Erkenntnisse müssen auf Fakten beruhen, die aus der Analyse der verfügbaren Daten stammen. Das ist ein wichtiger Punkt, an dem oft schwere Fehler begangen werden. Es schleichen sich gerne Annahmen ein, die sich im Laufe der Abhandlung des Vorfalls verfestigen. Man entwickelt dann gerne einen Tunnelblick und

interpretiert Informationen nur einseitig. Das gilt es zu vermeiden. Gemäß der Datenschutz-Grundverordnung (DSGVO) müssen Vorfälle, die Daten von Kunden oder Dritten betreffen, natürlich gemeldet werden. Das steht nicht im Widerspruch keine Annahmen zu verbreiten, sondern bestätigt das Vermeiden von Spekulationen.

Es gibt zahlreiche Beispiele in aktuellen und vergangenen Nachrichtenmeldungen. Das Datenleck im Jahre 2017 bei Equifax, einem US-amerikanischen Finanzdienstleistungsunternehmen mit Hauptsitz in Atlanta im Bundesstaat Georgia, ist gut dokumentiert. Ohne Details bekannt zu geben, wurden Betroffene aufgefordert auf einer Webseite eine Teil ihrer Sozialversicherungsnummer einzugeben. Der Zweck sollte die Feststellung sein, ob eigene Daten kopiert wurden oder nicht. Dieser Schnellschuss führte zu viel größerer Unsicherheit, die durch Nachbesserungen und zusätzliche Erklärungen nicht nachhaltig verbessert wurde. Antworten, die zu mehr Fragen führen, sind keine sinnvolle Erklärung. Sie führen maximal zu mehr medialer Reichweite, weil die Öffentlichkeit dann mit spekulieren kann. In einem seriösen Kontext hat dieser Ansatz nichts zu suchen.

Die angebotenen Trainings zur DeepSec Konferenz sind als Hilfestellung gedacht, um in einem angenehmen Umfeld Erfahrungen im Umgang mit Sicherheitsvorfällen zu sammeln und Prozesse für den Ernstfall sinnvoll gestalten zu können.

Programme und Buchung

Die DeepSec 2019 Konferenztage sind am 28. und 29. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 26. und 27. November statt.

Der Veranstaltungsort für die DeepSec-Veranstaltung ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Tickets für die DeepSec Konferenz selbst und die Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html (https://deepsec.net/register.html) bestellen.

(Ende)

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

(http://deepsec.net/)

https://www.pressetext.com/news/20190829011

Internet der Fakten und Furcht im Zeichen der IT Security

DeepSec- und DeepINTEL-Konferenzen veröffentlichen Programm - Bits, Bytes, Sicherheit und Geopolitik

Wien (pts011/29.08.2019/09:05) - Niemand ist eine Insel. Diese Aussage wird dem englischen Schriftsteller John Donne zugeschrieben. Der Satz wurde im 17. Jahrhundert bekannt. Mittlerweile hat sich das durch die Digitalisierung verändert. Die moderne Fassung der Aussage müsste lauten: Es gibt keine Inseln mehr. Die zunehmende Vernetzung erreicht immer mehr Bereiche des Alltags und der Gesellschaft. Die diesjährigen Sicherheitskonferenzen DeepSec und DeepINTEL möchten daher das Internet der Fakten und der Furcht nüchtern aus dem Blickwinkel der Informationssicherheit betrachten. Systeme sind derzeit weniger isoliert und viel komplexer als es sicherheitstechnisch vertretbar ist. Die DeepSec widmet sich daher in zwei Tagen Konferenz und zwei Tagen Trainings aktuellen Technologien und deren Verwundbarkeiten. Parallel dazu wird in der DeepINTEL-Seminarkonferenz das Verhältnis zwischen Geopolitik und IT-Sicherheit anhand von Vorfällen diskutiert.

Internet der Angriffe statt der Dinge

Sobald man ein System mit dem Internet verbindet, bekommt man es sofort zu spüren. Lohnende oder verwundbare Ziele werden automatisch gesucht und angegriffen. Verbindet man Sensoren, Geräte oder Aktore (bekannt als “Dinge” im Internet der Dinge) mit einem Netzwerk, so ist es nicht anders. Die Vorträge der diesjährigen DeepSec-Konferenz versuchen die Verbindungen zwischen verschiedenen Aspekten der IT-Sicherheit mit diesem Hintergrund herzustellen. Mobile Endgeräte sind seit ihrer Existenz bedroht. Moderne Mobilfunktechnologien setzen auf Daten. Es ist daher keine Überraschung, dass Luca Melette in seiner Präsentation vorstellt, wie man mobile Systeme ausschließlich über das Internetprotokoll angreift. Aleksandr Kolchanov wird zeigen, wie man bestimmte Mobilfunkgeräte kompromittieren und massenweise auslesen kann. Lior Yaari teilt seine Erfahrung aus dem Bereich des Automobilbaus. Er hat zukünftige Komponenten moderner Autos analysiert, Komponenten, die noch nicht auf dem Markt, aber bereits in Entwicklung sind. Lior wird über Schwachstellen berichten, die möglicherweise in einigen Jahren über unsere Straßen rollen.

Training mit Sicherheitsexperten

Die DeepSec-Konferenz bietet jedes Jahr eine Weiterbildung von Sicherheitsexperten für Experten in Ihrem Un-

ternehmen an. Austausch von Wissen ist die Grundlage jeder guten Verteidigung, nicht nur digital. Durch die Kurzlebigkeit in der Informationstechnologie ist der eigene Wissensstand und die eigene Weiterbildung maßgeblich für den Umgang mit Angriffen und der ständigen Vernetzung. Im Programm sind daher drei verschiedene Workshops, die sich um den Umgang mit Angreiferinnen drehen. Xavier Mertens lehrt die Aufklärung von Bedrohungen mit Open Source Security. Verwendet werden öffentlich zugängliche Quellen, um den Umgang damit und den Aufbau von internen Prozessen zu vermitteln. Darüber hinaus werden an Fallstudien Beispiele für das Detektieren von verdächtigen Mustern gelehrt.

Peter Manev und Eric Leblond zeigen in ihrem Workshop, wie man mit dem Intrusion-Detection-Werkzeug “Suricata” Angriffe und verdächtige Vorgänge im Netzwerk erkennen kann. Suricata ist leicht einzusetzen und bietet sehr viele Funktionen. Da beide Trainer im Entwicklungsteam von Suricata sind, erfährt man direkt Details über die internen Abläufe der Software. Zusätzlich werden die Teilnehmer an echtem Netzwerkverkehr das Erstellen von Regeln üben. Das Training ist praxisorientiert und wendet sich an alle, die Netzwerksicherheit betreiben müssen.

Thomas Fischer und Craig Jones zeigen in ihrem Workshop, wie man mit Sicherheitsvorfällen umgeht und wie man Spuren der Angreifer findet. Auch hier wird an echten Fällen und realen Beispielen der Umgang mit den richtigen Werkzeugen vermittelt.

Technik ist auch keine Insel

Oft wird bei der Betrachtung von Sicherheitsproblemen nur der technische Standpunkt berücksichtigt. Es gibt in der Informationstechnologie, genau wie in anderen Bereichen, externe Faktoren, die bestimmte Rahmenbedingungen vorgeben. Ein prominentes Beispiel ist die seit den 1990er Jahren immer wiederkehrende Diskussion um Hintertüren in digitalen Systemen und Kommunikationsnetzwerken. Was mit der Verschlüsselung von Mobilfunk und E-Mail anfing, das setzt sich jetzt bei 5G, Messenger und Softwareentwicklung fort. Die australische Regierung hat 2018 ein Gesetz erlassen, welches Tech-Firmen zwingen kann Hintertüren in ihre Produkte einzubauen. Diese Sollbruchstellen werden künftig von Angreifern ebenfalls verwendet werden.

Die Mathematik der Verschlüsselung ist beim Thema Sicherheit unerbittlich. Entweder man hat eine sichere Kommunikation, oder man hat sie nicht. Die aktuellen Handelskriege betreffen die IT-Welt ebenso nachhaltig und stellen die Weichen für Umsetzungen neuer Technologien in den nächsten Jahren. Aus diesem Grund werden auf der diesjährigen DeepSec und DeepINTEL die Wechselwirkungen der Informationssicherheit mit geopolitischen Aspekten untersucht. Die Vorträge beider Veranstaltungen wurden unter diesem Aspekt ausgesucht. Diskutiert werden

unter anderem Mittel und Wege von Angriffen, die Einordnung der Ziele und welche Bedingungen sich für den Einsatz von Sicherheitsmaßnahmen ergeben. Wir empfehlen Sicherheitsverantwortlichen dringend den eigenen Horizont um diese Aspekte zu erweitern.

Programme und Buchung

Die DeepSec-2019-Konferenztage sind am 28. und 29. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, den 26. und 27. November, statt.

Die DeepINTEL-Konferenz findet am 27. November statt. Das Programm senden wir auf Anfragen an deepsec@deepsec.net gerne zu. Tickets sind auf der Webseite https://deepintel.net erhältlich.

Der Veranstaltungsort für DeepSec und DeepINTEL ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Das Programm der DeepSec Konferenz ist unter https://deepsec.net/schedule.html einsehbar. Das Programm der DeepINTEL wird auf Anfrage zur Verfügung gestellt, weil es sich bei der DeepINTEL um eine nichtöffentliche Konferenz handelt.

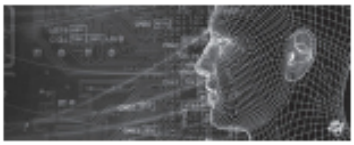
Tickets für die DeepSec-Konferenz sowie für die DeepINTEL-Veranstaltung und die DeepSec-Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html bestellen.

HIGHTECH

pts20190829011 Handel/Dienstleistungen, Unternehmen/Wirtschaft

Internet der Fakten und Furcht im Zeichen der IT Security

DeepSec- und DeepINTEL-Konferenzen veröffentlichen Programm - Bits, Bytes, Sicherheit und Geopolitik



Thema Informationssicherheit (Copyright: Florian Stocker, Crowes Agency OG)

Wien (pts011/29.08.2019/09:05) - **Niemand ist eine Insel. Diese Aussage wird dem englischen Schriftsteller John Donne zugeschrieben. Der Satz wurde im 17. Jahrhundert bekannt. Mittlerweile hat sich das durch die Digitalisierung verändert. Die moderne Fassung der Aussage müsste lauten: Es gibt keine Inseln mehr. Die zunehmende Vernetzung erreicht immer mehr Bereiche des Alltags und der Gesellschaft. Die diesjährigen Sicherheitskonferenzen DeepSec und DeepINTEL möchten daher das Internet der Fakten und der Furcht nüchtern aus dem Blickwinkel der Informationssicherheit betrachten. Systeme sind derzeit weniger isoliert und viel komplexer als es sicherheitstechnisch vertretbar ist. Die DeepSec widmet sich daher in zwei Tagen Konferenz und zwei Tagen Trainings aktuellen Technologien und deren Verwundbarkeiten. Parallel dazu wird in der DeepINTEL-Seminarkonferenz das Verhältnis zwischen Geopolitik und IT-Sicherheit anhand von Vorfällen diskutiert.**

Internet der Angriffe statt der Dinge

Sobald man ein System mit dem Internet verbindet, bekommt man es sofort zu spüren. Lohnende oder verwundbare Ziele werden automatisch gesucht und angegriffen. Verbindet man Sensoren, Geräte oder Aktore (bekannt als "Dinge" im Internet der Dinge) mit einem Netzwerk, so ist es nicht anders. Die Vorträge der diesjährigen DeepSec-Konferenz versuchen die Verbindungen zwischen verschiedenen Aspekten der IT-Sicherheit mit diesem Hintergrund herzustellen. Mobile Endgeräte sind seit ihrer Existenz bedroht. Moderne Mobilfunktechnologien setzen auf Daten. Es ist daher keine Überraschung, dass Luca Melette in seiner Präsentation vorstellt, wie man mobile Systeme ausschließlich über das Internetprotokoll angreift. Aleksandr Kolchanov wird zeigen, wie man bestimmte Mobilfunkgeräte kompromittieren und massenweise auslesen kann. Lior Yaari teilt seine Erfahrung aus dem Bereich des Automobilbaus. Er hat zukünftige Komponenten moderner Autos analysiert, Komponenten, die noch nicht auf dem Markt, aber bereits in Entwicklung sind. Lior wird über Schwachstellen berichten, die möglicherweise in einigen Jahren über unsere Straßen rollen.

Training mit Sicherheitsexperten

Die DeepSec-Konferenz bietet jedes Jahr eine Weiterbildung von Sicherheitsexperten für Experten in Ihrem Unternehmen an. Austausch von Wissen ist die Grundlage jeder guten Verteidigung, nicht nur digital. Durch die Kurzlebigkeit in der Informationstechnologie ist der eigene Wissensstand und die eigene Weiterbildung maßgeblich für den Umgang mit Angriffen und der ständigen Vernetzung. Im Programm sind daher drei verschiedene Workshops, die sich um den Umgang mit Angreiferinnen drehen. Xavier Mertens lehrt die Aufklärung von Bedrohungen mit Open Source Security. Verwendet werden öffentlich zugängliche Quellen, um den Umgang damit und den Aufbau von internen Prozessen zu vermitteln. Darüber hinaus werden an Fallstudien Beispiele für das Detektieren von verdächtigen Mustern gelehrt.

Peter Manev und Eric Leblond zeigen in ihrem Workshop, wie man mit dem Intrusion-Detection-Werkzeug "Suricata" Angriffe und verdächtige Vorgänge im Netzwerk erkennen kann. Suricata ist leicht einzusetzen und bietet sehr viele Funktionen. Da beide Trainer im Entwicklungsteam von Suricata sind, erfährt man direkt Details über die internen Abläufe der Software. Zusätzlich werden die Teilnehmer an echtem Netzwerkverkehr das Erstellen von Regeln üben. Das Training ist praxisorientiert und wendet sich an alle, die Netzwerksicherheit betreiben müssen.

Thomas Fischer und Craig Jones zeigen in ihrem Workshop, wie man mit Sicherheitsvorfällen umgeht und wie man Spuren der Angreifer findet. Auch hier wird an echten Fällen und realen Beispielen der Umgang mit den richtigen Werkzeugen vermittelt.

Technik ist auch keine Insel

Oft wird bei der Betrachtung von Sicherheitsproblemen nur der technische Standpunkt berücksichtigt. Es gibt in der Informationstechnologie, genau wie in anderen Bereichen, externe Faktoren, die bestimmte Rahmenbedingungen vorgeben. Ein prominentes Beispiel ist die seit den 1990er Jahren immer wiederkehrende Diskussion um Hintertüren in digitalen Systemen und Kommunikationsnetzwerken. Was mit der Verschlüsselung von Mobilfunk und E-Mail anfing, das setzt sich jetzt bei 5G, Messenger und Softwareentwicklung fort. Die australische Regierung hat 2018 ein Gesetz erlassen, welches Tech-Firmen zwingen kann Hintertüren in ihre Produkte einzubauen. Diese Sollbruchstellen werden künftig von Angreifern ebenfalls verwendet werden.

Die Mathematik der Verschlüsselung ist beim Thema Sicherheit unerbittlich. Entweder man hat eine sichere Kommunikation, oder man hat sie nicht. Die aktuellen Handelskriege betreffen die IT-Welt ebenso nachhaltig und stellen die Weichen für Umsetzungen neuer Technologien in den nächsten Jahren. Aus diesem Grund werden auf der diesjährigen DeepSec und DeepINTEL die Wechselwirkungen der Informationssicherheit mit geopolitischen Aspekten untersucht. Die Vorträge beider Veranstaltungen wurden unter diesem Aspekt ausgesucht. Diskutiert werden unter anderem Mittel und Wege von Angriffen, die Einordnung der Ziele und welche Bedingungen sich für den Einsatz von Sicherheitsmaßnahmen ergeben. Wir empfehlen Sicherheitsverantwortlichen dringend den eigenen Horizont um diese Aspekte zu erweitern.

Programme und Buchung

Die DeepSec-2019-Konferenztage sind am 28. und 29. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, den 26. und 27. November, statt.

Die DeepINTEL-Konferenz findet am 27. November statt. Das Programm senden wir auf Anfragen an deepsec@deepsec.net (mailto:deepsec@deepsec.net) gerne zu. Tickets sind auf der Webseite https://deepintel.net (https://deepintel.net) erhältlich.

Der Veranstaltungsort für DeepSec und DeepINTEL ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Das Programm der DeepSec Konferenz ist unter https://deepsec.net/schedule.html (https://deepsec.net/schedule.html) einsehbar. Das Programm der DeepINTEL wird auf Anfrage zur Verfügung gestellt, weil es sich bei der DeepINTEL um eine nichtöffentliche Konferenz handelt.

Tickets für die DeepSec-Konferenz sowie für die DeepINTEL-Veranstaltung und die DeepSec-Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html (https://deepsec.net/register.html) bestellen.

(Ende)

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

(http://www.deepsec.net)

https://www.pressetext.com/news/20190218005

IT-Sicherheit steht zunehmend im Zeichen der Geopolitik

DeepSec und DeepINTEL Konferenz eröffnen Call for Papers - Einreichung für Vorträge gefragt

Wien (pts005/18.02.2019/08:45) - Wer den Technologie Teil des jeweiligen Lieblingsmagazins liest, kann sich vor den Versprechungen kommender Netzwerktechnologien kaum retten. Das eigene Auto wird zum Smartphone. Der sprechende Kühlschrank wird zur Therapeutin. 5G-Mobilfunknetze versprechen glasfaserschnelles Streaming von Daten auf dem geschwindigkeitsbeschränkten Elektroroller. Beim zweiten Lesen offenbahrt sich die Bedeutung des Buchstabens G in 5G - er steht für Geopolitik. Es gibt im Zuge des Netzwerkausbaus Diskussionen um versteckte Killswitches zwecks Notabschaltungen ganze Netzwerke und Hintertüren zur Belauschung der Kunden. Die im November stattfindende DeepSec-In-Depth-Security-Konferenz widmet sich den technischen Herausforderungen des Internets der Dinge, den kommenden Netzwerktechnologien und den geopolitischen Randbedingungen diktiert durch Schlüsselereignisse der letzten 6 Jahre.

5G als Fortsetzung der Handelskriege

Es gibt weltweit sehr wenige Anbieter von Mobilfunknetzwerktechnologie. Der Name Huawei wird in den letzten Monaten in der Berichterstattung recht oft erwähnt. Diskutiert werden dann selten die Vorzüge der angebotenen Produkte oder die tatsächlichen Implementationen des neuen Mobilfunkstandards 5G. Stattdessen geht es um den Vorwurf heimlich eingebauter Notabschaltungen, die auf einen Schlag das komplette Mobilfunknetz eines Betreibers lahmlegen können. Angeklagt wird auch vermeintlicher versteckter Code, der Fernzugriff und das Kopieren von Daten aus dem Netzwerk erlaubt. Gerüstet mit vielen Vorwürfen ohne konkrete Beweise wird gerade in bestimmten westlichen Ländern ein Ausschluss chinesischer Telekommunikationsausrüster öffentlich diskutiert.

Die Sorgen sind berechtigt, jedoch sind sie Sicherheitsforschern nicht fremd. Fast alle Computer, die in Europa und anderswo eingesetzt werden, stammen selten aus den Ländern, in denen sie ihre Arbeit tatsächlich verrichten. Die Chips, die Firmware und viele weitere Zutaten in Hard- und Software werden woanders gebaut. Da man in den letzten Dekaden systematisch darauf verzichtet hat, den Inhalt der Box hinter Tastatur oder Touchscreen zu hinterfragen, geschweige zu verstehen, blühen die Anschuldigungen getrieben von der Phantasie.

Die IT-Security-Forschung kann dem nur mit Fakten und solider Recherche begegnen. Robert Hannigan, der

ehemalige Chef des britischen Geheimdiensts GCHQ, hat bestätigt, dass sich das britische National Cyber Security Centre (NCSC) lange Jahre mit Komponenten aus chinesischen Lieferketten beschäftigt hat. Bisher hat es laut seiner Aussage keine Indizien für staatlich verordnete verdeckte Angriffe durch Huawei Hardware gegeben. NCSC hat seit 2010 mit Hilfe des Huawei Security Evaluation Centres (HSEC) Zugang zum Quellcode der Produkte.

Der Sinn dahinter ist eine Zertifizierung durch das NCSC bevor Technologie in sensitiven Bereichen eingesetzt werden kann. Robert Hannigan widerspricht damit direkt den Vorwürfen aus den USA und der Einschätzung von Gerhard Schindler, dem früheren Präsident des deutschen Bundesnachrichtendienstes (BND). Darüber hinaus ignorieren die Kritiker die bereits jetzt in Europa vorgeschriebenen gesetzlichen Überwachungsschnittstellen, standardisiert durch das Europäische Institut für Telekommunikationsnormen (ETSI). Diese Vorgaben gelten übrigens für alle Anbieter, die in Europa Netzwerke bauen oder bauen lassen möchten.

Intranet statt Internet

Die aktuelle Nachrichtenlage illustriert daher sehr gut was man alles in der Informationssicherheit beachten sollte. Die Absicherung der eigenen Daten ist längst nicht mehr mit einzelnen isolierten Betrachtungen getan. Die DeepSec Konferenz hat obendrein eine lange Tradition der Sicherheitsforschung im Mobilfunkbereich, angefangen von der ersten öffentlichen Publikation von Schwachstellen des A5/1 Verschlüsselungsalgorithmus (zwischen Telefon und Funkzelle) bis hin zu Sicherheitsproblemen bei Smartphones. Dieser Bereich ist nur ein Beispiel, und hat durch die rasante Verbreitung von Mobiltechnologie immens an Bedeutung gewonnen.

Um den diskutierten Killswitch in Netzwerken wieder aufzugreifen: Die Idee in einem nationalen Notfall Informationsnetzwerke zu kontrollieren ist nicht neu. Präsident Franklin D. Roosevelt hat dies im Communications Act of 1934 schon umgesetzt. Damals ging es um Medien. Im vorgeschlagenen Protecting Cyberspace as a National Asset Act of 2010 wollte man dasselbe für das Internet umsetzen, mit dem Unterschied der Abschaltung statt Kontrolle. Das vorgeschlagene Gesetz von 2010 verfiel ohne Stimmen zu bekommen, weil die technische Umsetzung nicht klar war und nach wie vor auch nicht ist. Der Gedanken mit einem simplen Schalter Kommunikationsnetzwerke nach Belieben lahmzulegen funktionierte auf der Kinoleinwand oder im Fernsehen noch gut - leider nur in der Vergangenheit, denn mittlerweile werden Informationen per Internet gestreamt.

Die Alternative ist ein strikt nationales Netzwerk. Die iranische Regierung arbeitet an einem iranischen Intranet, angespornt durch Proteste im Jahre 2009. Die chinesische Firewall versucht etwas ähnliches, allerdings durch strenge Filter gesteuert durch Redaktionen. Rußland probt derzeit ebenfalls eine Abkopplung vom Internet. Die

Kommunikationsnetzwerke sollen dann zwar noch funktionieren, aber man plant sie vom Rest der Welt zu trennen. Das ist de fakto einfach die fettarme Variante des Killswitches. Beide Ansätze demonstrieren wie enorm die Bedeutung des Internets mittlerweile geworden ist - es kann nicht mehr ignoriert werden. Das gilt für Unternehmen noch viel mehr als für Länder.

Digitaler Realismus

Realistisch betrachtet macht es wenig Sinn die eigene Bevölkerung und den Staat zunächst von einem Netzwerk abhängig zu machen, um das dann wieder abzuschalten. Die Sehnsucht nach lokalen Netzwerken beweist das. In Unternehmen ist es nicht anders. Daten müssen ausgetauscht und Kommunikation muss stattfinden. Seriöse Informationssicherheit muss daher untersuchen wie sich die Integrität der Infrastruktur und von Daten auch unter widrigen Umständen erhalten lassen. Wichtigster Punkt ist dabei das sichere Design von Applikationen von Anfang an. Dazu gab es bei den vergangenen DeepSec-Konferenzen reichlich Vorträge und Trainings als Weiterbildung für Entwicklerinnen und Planer.

Der IT-Security haftet der Ruf eines Verhinderers an. Tatsächlich ist das Gegenteil der Fall. Vergangene Sicherheitsvorfälle und publizierte Dokumente über organisierte Schwachstellen wie beispielsweise durch Edward Snowden sind und waren wesentliche Bausteine für eine Verbesserung der Sicherheit in unserem Alltag. Voraussetzung dafür ist paradoxerweise ein freier Austausch zwischen Sicherheitsforschern. Ein nationales Intranet, Verbote von kryptographischen Algorithmen, Filter für publizierte Inhalte oder ähnliche Restriktionen sind daher der maximal unsicherste Kontrapunkt zu notwendiger Sicherheit in der digitalen Welt.

Die DeepSec Konferenz möchte daher explizit nicht nur Sicherheitsexperten ansprechen. Die Durchdringung digitaler Netze erfordert für eine sinnvolle Weiterentwicklung der IT-Sicherheitsmaßnahmen die Einbindung von Unternehmen, Entwicklerinnen, der Hacker Community, Behörden, Anwendern, Infrastrukturbetreibern, Designern und interdisziplinären Wissenschaftlerinnen. Menschen in beratender Funktion sind ausdrücklich eingeladen an dem Austausch von Erfahrungen und Ideen im November in Wien teilzunehmen.

Beiträge gesucht - Call for Papers

Die DeepSec Konferenz möchte dieses Jahr das Augenmerk auf die Verbindung zwischen Geopolitik und Informationssicherheit legen. Bis zum 31. Juli 2019 werden daher Vorträge gesucht, welche sich mit Technologien beschäftigen, die beide Welten berühren. Konkret sind das die Herausforderungen für Industrie- und Steuerungssys-

teme, der Internet der Dinge, sämtliche mobil eingesetzte Kommunikationstechnologie (vom Auto bis zum Telefon), Einsatz von Algorithmen und moderne Datenhaltung. Wir erleben gerade eine beschleunigte Vermischung neuer und vorhandener Methoden. Es sind Sicherheitsforscherinnen gefragtt, die sich kreativ mit den aktuellen Möglichkeiten auseinandersetzen und Schwachstellen aufzeigen. Risiken lassen sich erst dann managen, wenn man sie kennt. Das Programmkommittee freut sich daher auf möglichst viele Einreichungen, die Trends und sogenannte Zukunftstechnologien ganz genau unter das digitale Mikroskop legen.

Die zweitägigen Trainings vor der DeepSec Konferenz sind auch Teil des Call for Papers. Trainerinnen, die ihr Wissen weitergeben möchten, sind herzlich eingeladen Kurse einzureichen. Akzeptierte Kurse werden vorzeitig bekanntgegeben, um den Teilnehmern die Planung beim Buchen zu erleichtern.

Programme und Buchung

Die DeepSec 2019-Konferenztage sind am 28. und 29. November. Parallel finden die ROOTS 2019 Vorträge in einem separaten Saal ebenso am 28. und 29. November statt. Die DeepSec Trainings finden an den zwei vorangehenden Tagen, dem 26. und 27. November statt. Die DeepINTEL Konferenz findet am 27. November statt. Das Programm senden wir auf Anfragen an deepsec@deepsec.net gerne zu. Tickets sind auf der Webseite https://deepintel.net erhältlich.

Der Veranstaltungsort für DeepSec, DeepINTEL und ROOTS 2019 ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Einreichungen können unter https://deepsec.net/cfp.html abgegeben werden. Das aktuelle Programm der Veranstaltungen wird nach dem Abschluss der Einreichungsfristen bekanntgegeben.#

Tickets für die DeepSec Konferenz sowie ROOTS 2019 und die DeepSec Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html bestellen.

HIGHTECH

pts20190218006 Technologie/Digitalisierung, Unternehmen/Wirtschaft

IT-Sicherheit steht zunehmend im Zeichen der Geopolitik

DeepSec und DeepINTEL Konferenz eröffnen Call for Papers - Einreichung für Vorträge gefragt

DeepSec Konferenz, Logo von 2017 (© Florian Stocker)

Wien (pts005/18.02.2019/08:45) - Wer den Technologie Teil des jeweiligen Lieblingsmagazins liest, kann sich vor den Versprechungen kommender Netzwerktechnologien kaum retten. Das eigene Auto wird zum Smartphone. Der sprechende Kühlschrank wird zur Therapeutin. 5G-Mobilfunknetze versprechen glasfaserschnelles Streaming von Daten auf dem geschwindigkeitsbeschränkten Elektroroller. Beim zweiten Lesen offenbahrt sich die Bedeutung des Buchstabens G in 5G - er steht für Geopolitik. Es gibt im Zuge des Netzwerkausbaus Diskussionen um versteckte Killswitches zwecks Notabschaltungen ganze Netzwerke und Hintertüren zur Belauschung der Kunden. Die im November stattfindende DeepSec-In-Depth-Security-Konferenz widmet sich den technischen Herausforderungen des Internets der Dinge, den kommenden Netzwerktechnologien und den geopolitischen Randbedingungen diktiert durch Schlüsselereignisse der letzten 6 Jahre.

5G als Fortsetzung der Handelskriege

Es gibt weltweit sehr wenige Anbieter von Mobilfunknetzwerktechnologie. Der Name Huawei wird in den letzten Monaten in der Berichterstattung recht oft erwähnt. Diskutiert werden dann selten die Vorzüge der angebotenen Produkte oder die tatsächlichen Implementationen des neuen Mobilfunkstandards 5G. Stattdessen geht es um den Vorwurf heimlich eingebauter Notabschaltungen, die auf einen Schlag das komplette Mobilfunknetz eines Betreibers lahmlegen können. Angeklagt wird auch vermeintlicher versteckter Code, der Fernzugriff und das Kopieren von Daten aus dem Netzwerk erlaubt. Gerüstet mit vielen Vorwürfen ohne konkrete Beweise wird gerade in bestimmten westlichen Ländern ein Ausschluss chinesischer Telekommunikationsausrüster öffentlich diskutiert.

Die Sorgen sind berechtigt, jedoch sind sie Sicherheitsforschern nicht fremd. Fast alle Computer, die in Europa und anderswo eingesetzt werden, stammen selten aus den Ländern, in denen sie ihre Arbeit tatsächlich verrichten. Die Chips, die Firmware und viele weitere Zutaten in Hard- und Software werden woanders gebaut. Da man in den letzten Dekaden systematisch darauf verzichtet hat, den Inhalt der Box hinter Tastatur oder Touchscreen zu hinterfragen, geschweige zu verstehen, blühen die Anschuldigungen getrieben von der Phantasie.

Die IT-Security-Forschung kann dem nur mit Fakten und solider Recherche begegnen. Robert Hannigan, der ehemalige Chef des britischen Geheimdiensts GCHQ, hat bestätigt, dass sich das britische National Cyber Security Centre (NCSC) lange Jahre mit Komponenten aus chinesischen Lieferketten beschäftigt hat. Bisher hat es laut seiner Aussage keine Indizien für staatlich verordnete verdeckte Angriffe durch Huawei Hardware gegeben. NCSC hat seit 2010 mit Hilfe des Huawei Security Evaluation Centres (HSEC) Zugang zum Quellcode der Produkte.

Der Sinn dahinter ist eine Zertifizierung durch das NCSC bevor Technologie in sensitiven Bereichen eingesetzt werden kann. Robert Hannigan widerspricht damit direkt den Vorwürfen aus den USA und der Einschätzung von Gerhard Schindler, dem früheren Präsident des deutschen Bundesnachrichtendienstes (BND). Darüber hinaus ignorieren die Kritiker die bereits jetzt in Europa vorgeschriebenen gesetzlichen Überwachungsschnittstellen, standardisiert durch das Europäische Institut für Telekommunikationsnormen (ETSI). Diese Vorgaben gelten übrigens für alle Anbieter, die in Europa Netzwerke bauen oder bauen lassen möchten.

Intranet statt Internet

Die aktuelle Nachrichtenlage illustriert daher sehr gut was man alles in der Informationssicherheit beachten sollte. Die Absicherung der eigenen Daten ist längst nicht mehr mit einzelnen isolierten Betrachtungen getan. Die DeepSec Konferenz hat obendrein eine lange Tradition der Sicherheitsforschung im Mobilfunkbereich, angefangen von der ersten öffentlichen Publikation von Schwachstellen des A5/1 Verschlüsselungsalgorithmus (zwischen Telefon und Funkzelle) bis hin zu Sicherheitsproblemen bei Smartphones. Dieser Bereich ist nur ein Beispiel, und hat durch die rasante Verbreitung von Mobiltechnologie immens an Bedeutung gewonnen.

Um den diskutierten Killswitch in Netzwerken wieder aufzugreifen: Die Idee in einem nationalen Notfall Informationsnetzwerke zu kontrollieren ist nicht neu. Präsident Franklin D. Roosevelt hat dies im Communications Act of 1934 schon umgesetzt. Damals ging es um Medien. Im vorgeschlagenen Protecting Cyberspace as a National Asset Act of 2010 wollte man dasselbe für das Internet umsetzen, mit dem Unterschied der Abschaltung statt Kontrolle. Das vorgeschlagene Gesetz von 2010 verfiel ohne Stimmen zu bekommen, weil die technische Umsetzung nicht klar war und nach wie vor auch nicht ist. Der Gedanken mit einem simplen Schalter Kommunikationsnetzwerke nach Belieben lahmzulegen funktionierte auf der Kinoleinwand oder im Fernsehen noch gut - leider nur in der Vergangenheit, denn mittlerweile werden Informationen per Internet gestreamt.

Die Alternative ist ein strikt nationales Netzwerk. Die iranische Regierung arbeitet an einem iranischen Intranet, angespornt durch Proteste im Jahre 2009. Die chinesische Firewall versucht etwas ähnliches, allerdings durch strenge Filter gesteuert durch Redaktionen. Rußland probt derzeit ebenfalls eine Abkopplung vom Internet. Die Kommunikationsnetzwerke sollen dann zwar noch funktionieren, aber man plant sie vom Rest der Welt zu trennen. Das ist de fakto einfach die fettarme Variante des Killswitches. Beide Ansätze demonstrieren wie enorm die Bedeutung des Internets mittlerweile geworden ist - es kann nicht mehr ignoriert werden. Das gilt für Unternehmen noch viel mehr als für Länder.

Digitaler Realismus

Realistisch betrachtet macht es wenig Sinn die eigene Bevölkerung und den Staat zunächst von einem Netzwerk abhängig zu machen, um das dann wieder abzuschalten. Die Sehnsucht nach lokalen Netzwerken beweist das. In Unternehmen ist es nicht anders. Daten müssen ausgetauscht und Kommunikation muss stattfinden. Seriöse Informationssicherheit muss daher untersuchen wie sich die Integrität der Infrastruktur und von Daten auch unter widrigen Umständen erhalten lassen. Wichtigster Punkt ist dabei das sichere Design von Applikationen von Anfang an. Dazu gab es bei den vergangenen DeepSec-Konferenzen reichlich Vorträge und Trainings als Weiterbildung für Entwicklerinnen und Planer.

Der IT-Security haftet der Ruf eines Verhinderers an. Tatsächlich ist das Gegenteil der Fall. Vergangene Sicherheitsvorfälle und publizierte Dokumente über organisierte Schwachstellen wie beispielsweise durch Edward Snowden sind und waren wesentliche Bausteine für eine Verbesserung der Sicherheit in unserem Alltag. Voraussetzung dafür ist paradoxerweise ein freier Austausch zwischen Sicherheitsforschern. Ein nationales Intranet, Verbote von kryptographischen Algorithmen, Filter für publizierte Inhalte oder ähnliche Restriktionen sind daher der maximal unsicherste Kontrapunkt zu notwendiger Sicherheit in der digitalen Welt.

Die DeepSec Konferenz möchte daher explizit nicht nur Sicherheitsexperten ansprechen. Die Durchdringung digitaler Netze erfordert für eine sinnvolle Weiterentwicklung der IT-Sicherheitsmaßnahmen die Einbindung von Unternehmen, Entwicklerinnen, der Hacker Community, Behörden, Anwendern, Infrastrukturbetreibern, Designern und interdisziplinären Wissenschaftlerinnen. Menschen in beratender Funktion sind ausdrücklich eingeladen an dem Austausch von Erfahrungen und Ideen im November in Wien teilzunehmen.

Beiträge gesucht - Call for Papers

Die DeepSec Konferenz möchte dieses Jahr das Augenmerk auf die Verbindung zwischen Geopolitik und Informationssicherheit legen. Bis zum 31. Juli 2019 werden daher Vorträge gesucht, welche sich mit Technologien beschäftigen, die beide Welten berühren. Konkret sind das die Herausforderungen für Industrie- und Steuerungssysteme, der Internet der Dinge, sämtliche mobil eingesetzte Kommunikationstechnologie (vom Auto bis zum Telefon), Einsatz von Algorithmen und moderne Datenhaltung. Wir erleben gerade eine beschleunigte Vermischung neuer und vorhandener Methoden. Es sind Sicherheitsforscherinnen gefragtt, die sich kreativ mit den aktuellen Möglichkeiten auseinandersetzen und Schwachstellen aufzeigen. Risiken lassen sich erst dann managen, wenn man sie kennt. Das Programmkommittee freut sich daher auf möglichst viele Einreichungen, die Trends und sogenannte Zukunftstechnologien ganz genau unter das digitale Mikroskop legen.

Die zweitägigen Trainings vor der DeepSec Konferenz sind auch Teil des Call for Papers. Trainerinnen, die ihr Wissen weitergeben möchten, sind herzlich eingeladen Kurse einzureichen. Akzeptierte Kurse werden vorzeitig bekanntgegeben, um den Teilnehmern die Planung beim Buchen zu erleichtern.

Programme und Buchung

Die DeepSec 2019-Konferenztage sind am 28. und 29. November. Parallel finden die ROOTS 2019 Vorträge in einem separaten Saal ebenso am 28. und 29. November statt. Die DeepSec Trainings finden an den zwei vorangehenden Tagen, dem 26. und 27. November statt. Die DeepINTEL Konferenz findet am 27. November statt. Das Programm senden wir auf Anfragen an

deepsec@deepsec.net (mailto:deepsec@deepsec.net) gerne zu. Tickets sind auf der Webseite https://deepintel.net (https://deepintel.net) erhältlich.

Der Veranstaltungsort für DeepSec, DeepINTEL und ROOTS 2019 ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Einreichungen können unter https://deepsec.net/cfp.html (https://deepsec.net/cfp.html) abgegeben werden. Das aktuelle Programm der Veranstaltungen wird nach dem Abschluss der Einreichungsfristen bekanntgegeben.#

Tickets für die DeepSec Konferenz sowie ROOTS 2019 und die DeepSec Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html (https://deepsec.net/register.html) bestellen.

(Ende)

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

(http://deepsec.net)

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