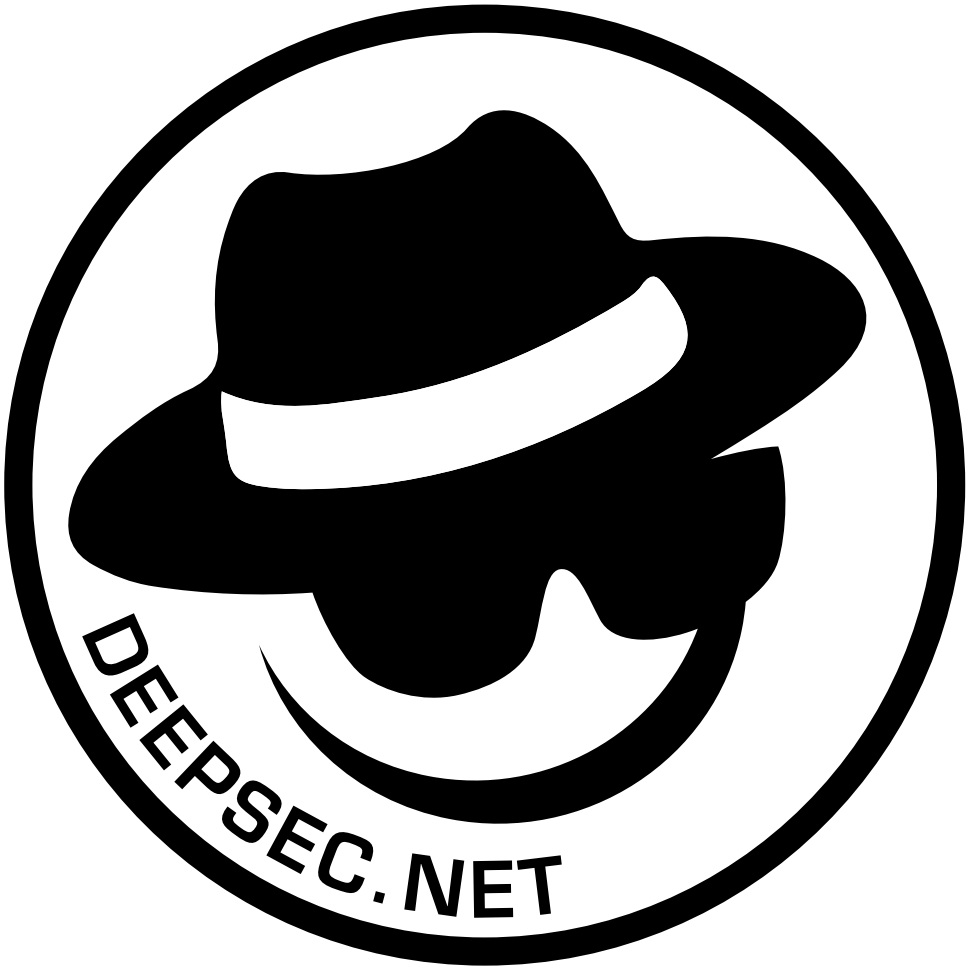


press review 2020

contents

media coverage

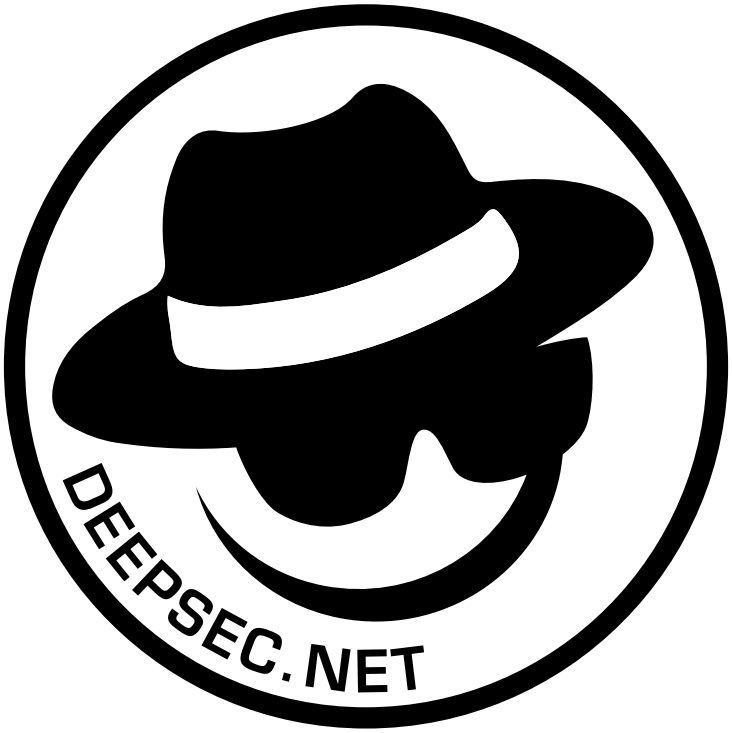
2020

contents

press releases

2020

media coverage 2020



https://www.strong-it.at/deepsec-2020-epp-edr-unhooking-their-protections/

01.12.2020

DEEPSEC 2020 – EPP/EDR UNHOOKING THEIR PROTECTIONS

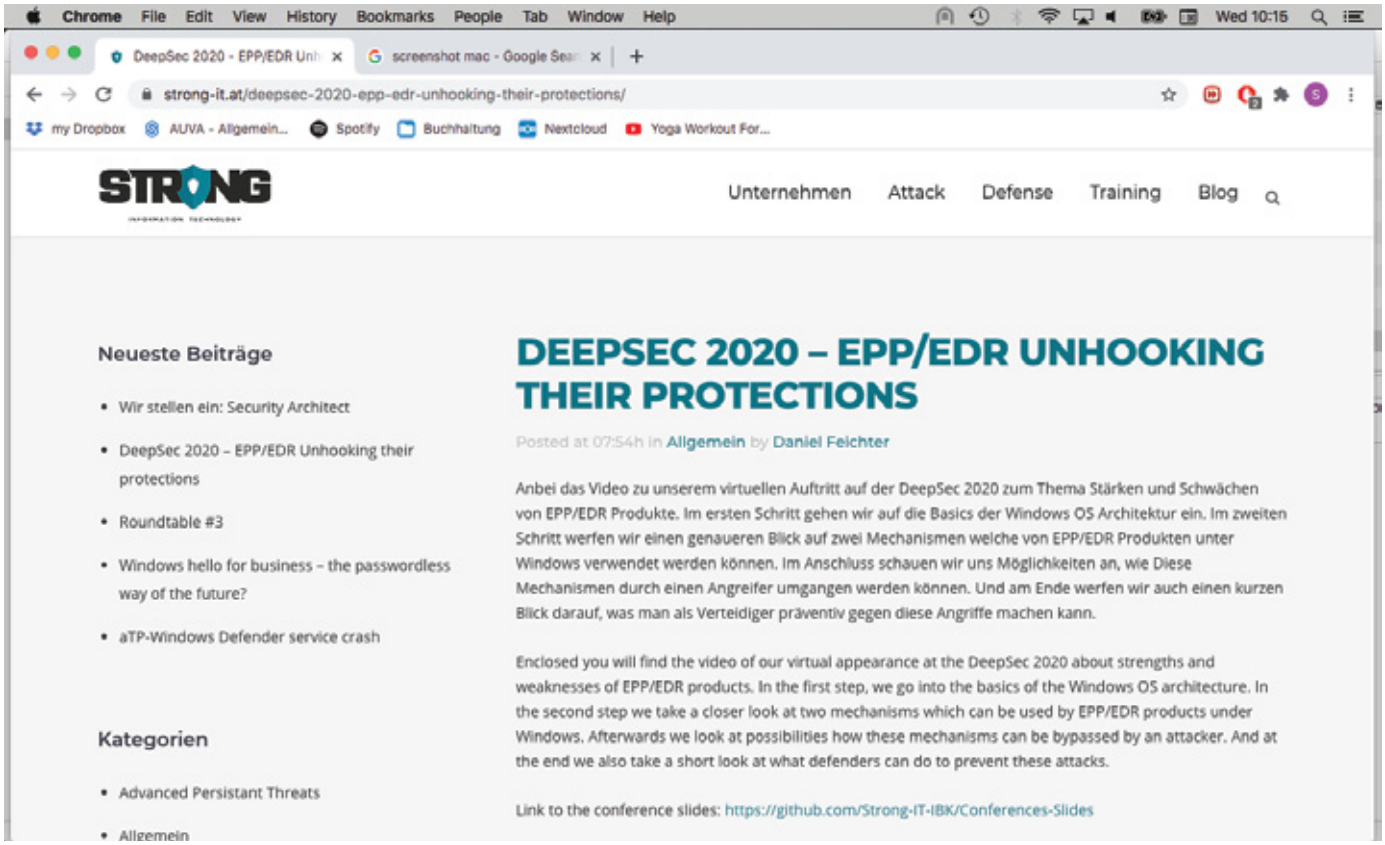
Posted at 07:54h in Allgemein by Daniel Feichter

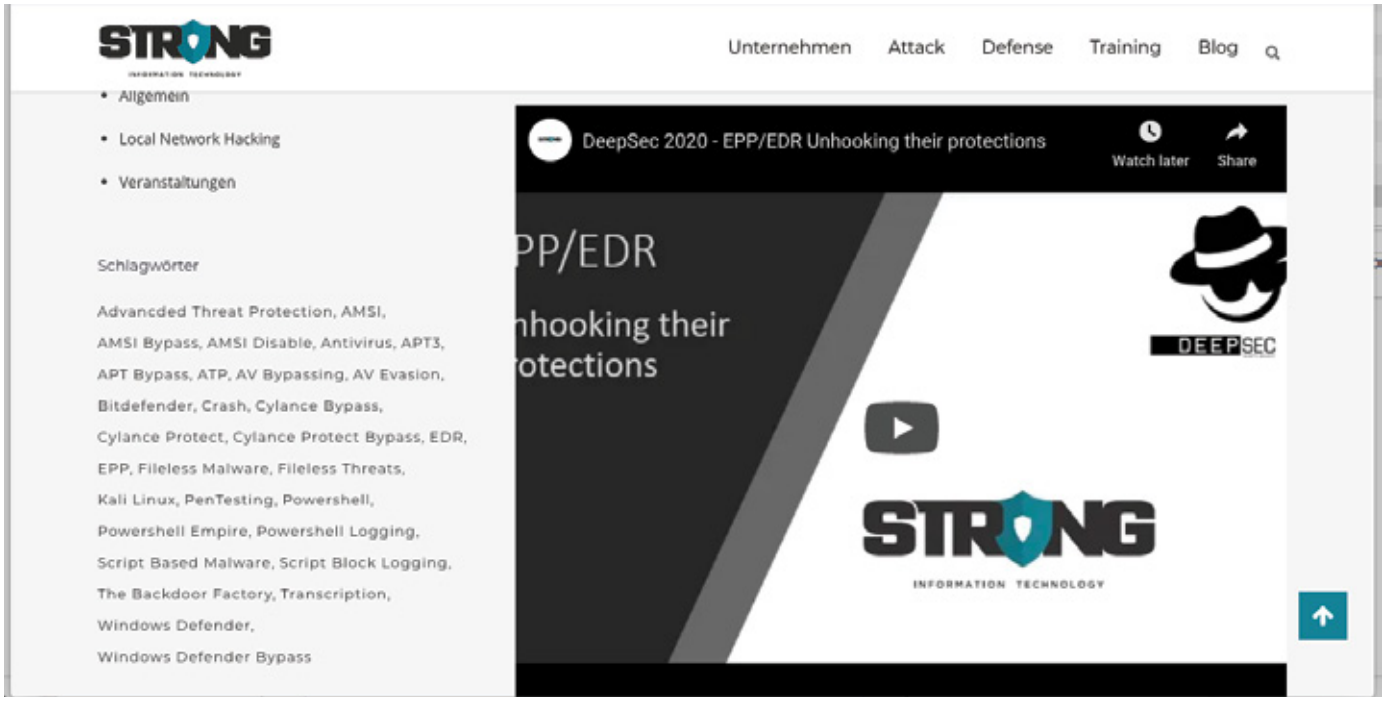
Anbei das Video zu unserem virtuellen Auftritt auf der DeepSec 2020 zum Thema Stärken und Schwächen von EPP/EDR Produkte. Im ersten Schritt gehen wir auf die Basics der Windows OS Architektur ein. Im zweiten Schritt werfen wir einen genaueren Blick auf zwei Mechanismen welche von EPP/EDR Produkten unter Windows verwendet werden können. Im Anschluss schauen wir uns Möglichkeiten an, wie Diese Mechanismen durch einen Angreifer umgangen werden können. Und am Ende werfen wir auch einen kurzen Blick darauf, was man als Verteidiger präventiv gegen diese Angriffe machen kann.

Enclosed you will find the video of our virtual appearance at the DeepSec 2020 about strengths and weaknesses of EPP/EDR products. In the first step, we go into the basics of the Windows OS architecture. In the second step we take a closer look at two mechanisms which can be used by EPP/EDR products under Windows. Afterwards we look at possibilities how these mechanisms can be bypassed by an attacker. And at the end we also take a short look at what defenders can do to prevent these attacks.

Link to the conference slides: https://github.com/Strong-IT-IBK/Conferences-Slides

https://youtu.be/a22aBofbv2g


Chrome File Edit View History Bookmarks People Tab Window Help
Wed 10:15
strong-it.at/deepsec-2020-epp-edr-unhooking-their-protections/
my Dropbox
AUVA - Allgemein...
Spotify
Buchhaltung
Nextcloud
Yoga Workout For...
STRONG
Unternehmen
Attack
Defense
Training
Blog
Neueste Beiträge
Wir stellen ein: Security Architect
DeepSec 2020 – EPP/EDR Unhooking their protections
Roundtable #3
Windows hello for business – the passwordless way of the future?
aTP-Windows Defender service crash
Kategorien
Advanced Persistant Threats
Allgemein
DEEPSEC 2020 – EPP/EDR UNHOOKING THEIR PROTECTIONS
Posted at 07:54h in Allgemein by Daniel Feichter
Anbei das Video zu unserem virtuellen Auftritt auf der DeepSec 2020 zum Thema Stärken und Schwächen von EPP/EDR Produkte. Im ersten Schritt gehen wir auf die Basics der Windows OS Architektur ein. Im zweiten Schritt werfen wir einen genaueren Blick auf zwei Mechanismen welche von EPP/EDR Produkten unter Windows verwendet werden können. Im Anschluss schauen wir uns Möglichkeiten an, wie Diese Mechanismen durch einen Angreifer umgangen werden können. Und am Ende werfen wir auch einen kurzen Blick darauf, was man als Verteidiger präventiv gegen diese Angriffe machen kann.
Enclosed you will find the video of our virtual appearance at the DeepSec 2020 about strengths and weaknesses of EPP/EDR products. In the first step, we go into the basics of the Windows OS architecture. In the second step we take a closer look at two mechanisms which can be used by EPP/EDR products under Windows. Afterwards we look at possibilities how these mechanisms can be bypassed by an attacker. And at the end we also take a short look at what defenders can do to prevent these attacks.
Link to the conference slides: https://github.com/Strong-IT-IBK/Conferences-Slides


STRONG
Unternehmen
Attack
Defense
Training
Blog
Allgemein
Local Network Hacking
Veranstaltungen
Schlagwörter
Advanced Threat Protection, AMSI, AMSI Bypass, AMSI Disable, Antivirus, APT3, APT Bypass, ATP, AV Bypassing, AV Evasion, Bitdefender, Crash, Cylance Bypass, Cylance Protect, Cylance Protect Bypass, EDR, EPP, Fileless Malware, Fileless Threats, Kali Linux, PenTesting, Powershell, Powershell Empire, Powershell Logging, Script Based Malware, Script Block Logging, The Backdoor Factory, Transcription, Windows Defender, Windows Defender Bypass
DeepSec 2020 - EPP/EDR Unhooking their protections
Watch later
Share
PP/EDR
hooking their
otections
DEEPSEC
STRONG
INFORMATION TECHNOLOGY

https://www.ardaudiothek.de/computer-kommunikation/deepsec-2020-wien-maschinelles-lernen-und-die-sicherheit/83405798

21.11.2020

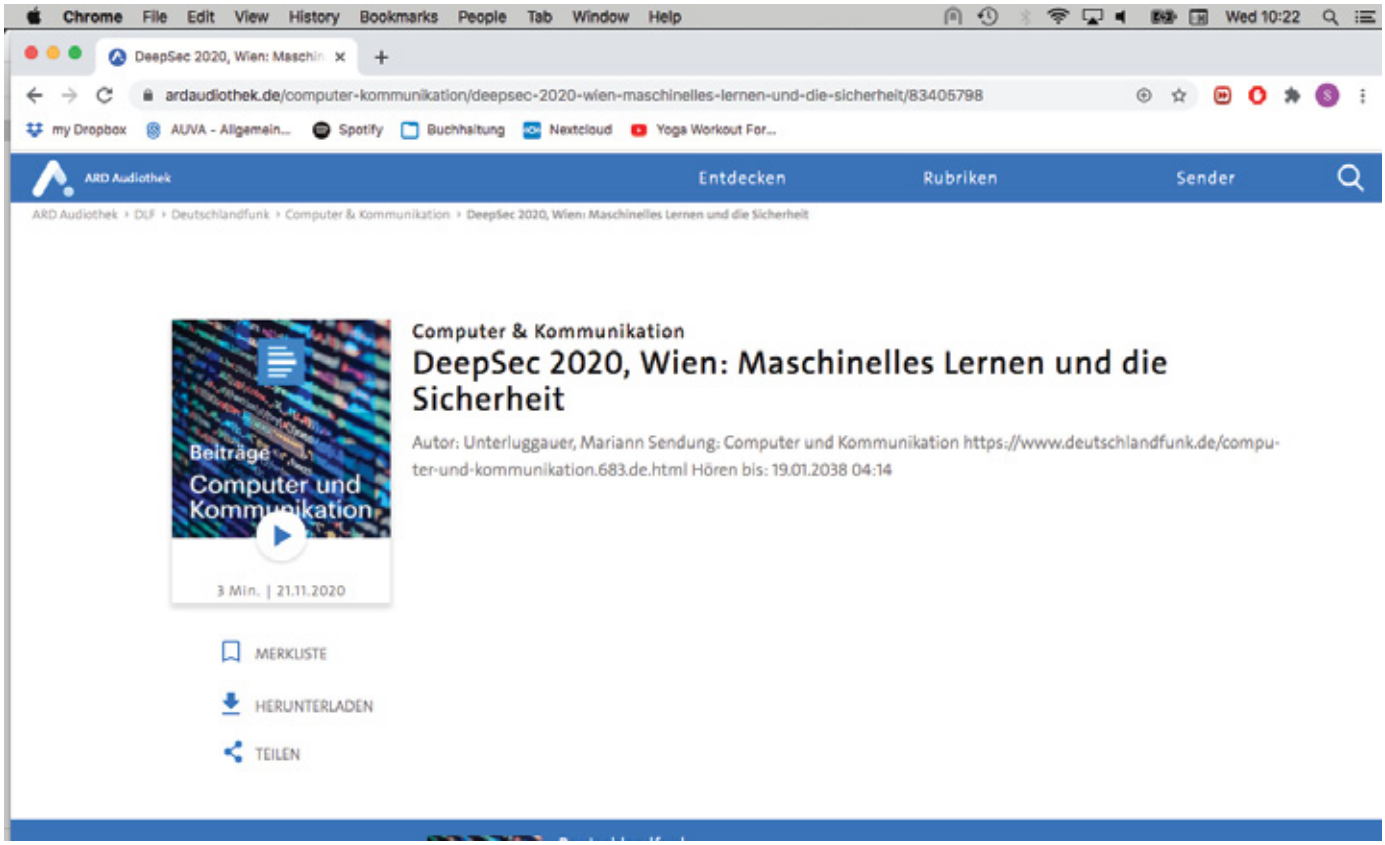
Computer & Kommunikation

DeepSec 2020, Wien: Maschinelles Lernen und die Sicherheit

Autor: Unterluggauer, Mariann Sendung: Computer und Kommunikation

https://www.deutschlandfunk.de/computer-und-kommunikation.683.de.html

Hören bis: 19.01.2038 04:14



https://www.deutschlandfunk.de/computer-und-kommunikation.683.de.html

Sendung vom 21.11.2020

Info Update 21.11.2021 [AUDIO]

Das Digitale Logbuch: Alt gegen Neu [AUDIO]

DeepSec 2020, Wien: Maschinelles Lernen und die Sicherheit [AUDIO]

Quanten-Computer: Anwendungen für den Rechner der Zunkunft [AUDIO]

Interview mit Thomas Lippert über JUWELS, den neuen Supercomputer in Jülich [AUDIO]

Computer und Kommunikation 21.11.2020, komplette Sendung [AUDIO]

Sendung vom 14.11.2020

Info-Update 14.11.2020 [AUDIO]

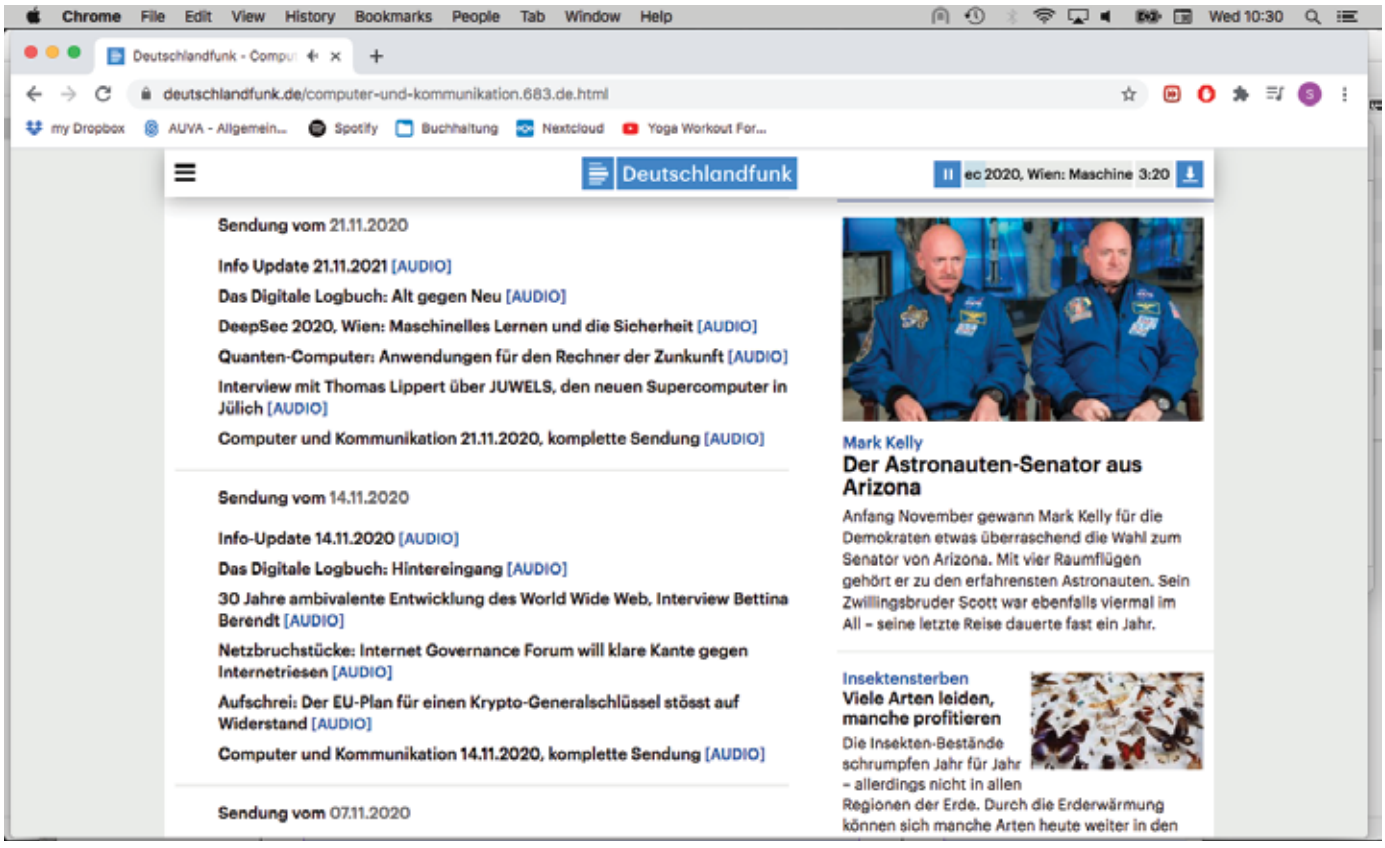
Das Digitale Logbuch: Hintereingang [AUDIO]

30 Jahre ambivalente Entwicklung des World Wide Web, Interview Bettina Berendt [AUDIO]

Netzbruchstücke: Internet Governance Forum will klare Kante gegen Internetriesen [AUDIO]

Aufschrei: Der EU-Plan für einen Krypto-Generalschlüssel stösst auf Widerstand [AUDIO]

Computer und Kommunikation 14.11.2020, komplette Sendung [AUDIO]



https://www.finanznachrichten.de/nachrichten-2020-11/51189934-sabotage-der-it-sicherheit-bedroht-heimische-wirtschaft-wirksame-ende-zu-ende-verschluesselung-ist-kritische-komponente-fuer-alltags-und-geschaeftsleb-015.htm

09.11.2020

Sabotage der IT-Sicherheit bedroht heimische Wirtschaft - Wirksame Ende-zu-Ende-Verschlüsselung ist kritische Komponente für Alltags- und Geschäftsleben

DJ Sabotage der IT-Sicherheit bedroht heimische Wirtschaft - Wirksame Ende-zu-Ende-Verschlüsselung ist kritische Komponente für Alltags- und Geschäftsleben

Wien (pts021/09.11.2020/14:30) - Vor über 300 Jahren erlebte die Kryptoanalyse, sprich die Methode zum Entschlüsseln von Geheimcodes, eine Hochzeit in Europa. In sogenannten Schwarzen Kammern oder Schwarze Kabinette (auch als cabinet noir bezeichnet) wurden in Postämtern alle Briefe von bestimmten Personen im Geheimen geöffnet, eingesehen, abgeschrieben und wieder verschlossen. Die so abgefangenen Briefe wurden dann zugestellt. Der Zweck war es, gefährliche oder schädliche Nachrichten für die damaligen Regenten zu finden. Aktivste und effizienteste Kammer Europas war die Geheime Kabinettskanzlei in Wien. Beendet wurde die Abhörpraxis erst im 19. Jahrhundert. Dieses Szenario der kaiserlichen und königlichen Höfe steht jetzt allen europäischen Unternehmen und Privatpersonen bevor. Die Ende-zu-Ende-Verschlüsselung soll per Vorschlag des EU-Ministerrats auf Drängen der Geheimdienste mit Hintertüren versehen werden.

Krieg gegen die Mathematik

Algorithmen zur Verschlüsselung und zur Verwaltung von digitalen Schlüsseln sind längst fester Bestandteil des Alltags geworden. Webseiten, Apps auf Smartphones, der virtuelle Gang zur Bank, Kommunikation mit Behörden, das Streaming von Musik oder Videos, Computerspiele, Software Upgrades, das digitale Zeitungslesen sowie Bestellungen und Abrechnungen von Unternehmen verlassen sich alle auf die Integrität und den Schutz der im Internet transportierten Inhalte.

Der Begriff Ende-zu-Ende-Verschlüsselung beschreibt dabei eine Reihe von Verfahren, bei dem nur die Kommunikationspartner selbst die Schlüssel besitzen und niemand sonst.

Spätestens seit der Dokumentation von Massenüberwachung und anderen illegalen Projekten von Geheimdiensten durch Edward Snowden haben IT-Unternehmen und Standardisierungsgremien Methoden zur Ende-zu-Ende-Verschlüsselung in viele Übertragungsprotokolle eingebaut, damit sich Firmen gegen Industriespionage und verwandte Angriffe wehren können. Der technologische Hintergrund für diese Implementationen ist Teil der Mathematik, die ganz ohne Informationstechnologie beschreibt wie Verschlüsselung, Entschlüsselung und die Schlüssel selbst aussehen.

Seit dem Kalten Krieg wurde die Mathematik der Kryptographie aktiv bekämpft. Die USA führten eine Liste mit gefährlichen Gütern, die nicht für den Export bestimmt waren. Darunter waren auch kryptografische Algorithmen. Starke Verschlüsselung war aus Angst vor der Sowjetunion selbst Unternehmen nicht zugänglich. In den 1990ern Jahren verschob sich der Krieg gegen die Kryptographie auf die Personal Computers (PCs). Bezahlbare Rechenleistung in den Händen aller wurde als existentielle Bedrohung wahrgenommen.

Den Höhepunkt dieser Auseinandersetzung mit IT-Experten und der US-amerikanischen Regierung gipfelte in dem Vorschlag über den sogenannten Clipper Chip sämtliche Sprach- und Datenübertragungen mit einer Hintertür für Behörden zu versehen. Das Projekt scheiterte aufgrund wirtschaftlicher Bedenken. Erst Präsident Clintons Executive Order 13026 nahm im Jahre 1996 kryptografische Algorithmen von der Liste der zu regulierenden Technologien. Diese Crypto Wars wiederholen sich seit dieser Zeit periodisch.

Kein Bezug zur Realität

Die Beschwörung des Bösen in allen Formen der Kryptografie hat keinen Bezug zur Realität. Der Anschlag vom 2. November 2020 in Wien war durch Fehler in der Ermittlung der Behörden möglich. Der britische investigative Journalist Duncan Campbell hielt zur DeepSec Konferenz im Jahre 2011 einen Vortrag mit dem Titel “How Terrorists Encrypt”. Er skizzierte Fälle und Verdächtige, die in den Jahren davor Ermittlungen ausgesetzt waren. Die Beispiele reichten bis zu den Attentätern vom 11. September in den USA. Keine Gruppe, kein Individuum benutzte moderne Verschlüsselung. Stattdessen wurden sehr alte Methoden wie Sprechtafeln (einfach Ersetzungen von Wörtern) zusammen mit unverschlüsselten E-Mail-Nachrichten verwendet.

Darüber hinaus wurden auch Telefonate und Treffen eingesetzt. Alle diese Methoden sind wesentlich unauffälliger und leichter anzuwenden. Je komplexer ein Kommunikationssystem ist, desto mehr Abhängigkeiten ergeben sich. Das erschwert teilweise die Verwendung und führt zu leichterer Aufklärung, weil man verschlüsselte Kommunika-

tion zwischen Endpunkten sehr leicht entdecken kann (die Tatsache, dass Verschlüsselung verwendet wird, nicht die Inhalte). Dadurch ist eine Metadatenanalyse viel leichter möglich als bei harmlosen Verabredungen zu Kaffee oder Kino.

Künstliche Schaffung eines Untergrunds

Das Fazit aus den Crypto Wars lässt sich mit einer Aussagen zusammenfassen: Wenn man Kryptographie kriminalisiert, dann besitzen nur noch Kriminelle kryptographische Mittel. Die Basis für Verschlüsselung liegt in der Mathematik. Die Umsetzung geschieht in Software. Es ist also jederzeit möglich verbotene Algorithmen auf einem universellen Computer, beispielsweise Laptop/Smartphone, zum Einsatz zu bringen. Das ist kein akademisches Beispiel. Das Los Zetas Kartell in Mexiko unterhält eine eigene Kommunikationsinfrastruktur inklusive eigenem Mobilfunknetzwerk mit Funkzellen. Mobilfunknetzwerke enthalten serienmäßig Überwachungsschnittstellen. Das ist den Experten sowie Gegenspielern bekannt. Vertrauliche Kommunikation findet daher ausschließlich über Lösungen statt, die sichere Verschlüsselung verwenden. Die Los Zetas zeigen die natürliche Reaktion, die auf Verbote und Überwachung stattfindet.

Der Vorschlag des EU-Ministerrats wird daher in letzter Konsequenz einen Untergrund schaffen, in dem die verbotenen Methoden weiter angewendet werden. Darin werden sich dann auch Unternehmen finden, die ihre Geschäftsgeheimnisse nicht mehr anders schützen können. Die Sinnhaftigkeit dieses Konzepts ist daher zu hinterfragen. Weiterhin ist nicht berücksichtigt, dass hinter den Terroranschlägen der letzten Jahrzehnte keine weltweit agierende Organisation mit Niederlassungen steckt. Es sind Ideen, die über Social Media, Unterhaltungen und Treffen weitergegeben werden. Diese stark dezentrale Struktur lässt sich durch ein Verbot der Ende-zu-Ende Verschlüsselung oder den Einbau von Hintertüren nicht behindern, aber die Arbeit von Unternehmen und der Alltag von Privatpersonen sehr wohl. Die digitale Wirtschaft, wie wir sie jetzt kennen, wäre ohne starke IT-Sicherheit nicht möglich.

Verfassungskonformität fraglich

Die Einführung von Hintertüren in verschlüsselter Kommunikation ist rechtlich sehr fraglich und gesellschaftlich bedenklich. Die Vorratsdatenspeicherung gehört ebenso zu den Maßnahmen, die ständig vorgebracht werde und wiederholt gegen geltendes Recht verstoßen. Ganz abgesehen davon betrifft eine Abschaffung sicherer Kommunikation Regierungen und Behörden gleichermaßen. Eine Schwächung von Sicherheitsmaßnahmen wird immer ausgenutzt werden.

Der Abhörskandal in Griechenland 2005 oder die kürzlich wieder diskutierten Hintertüren in Netzwerkausrüstung der US-amerikanischen Firma Juniper sind ausgewählte Beispiele dafür. Beides und vieles mehr wurde auf vergangenen DeepSec-Sicherheitskonferenzen ausgiebig diskutiert. Es bleibt zu hoffen, dass die Wirtschaft sich zukünftig trotz aller Panik legal vor digitalen Bedrohungen schützen darf. Der Wirtschaftsstandort Europa wäre es wert.

Programme und Buchung

Die DeepINTEL Security Intelligence Konferenz findet am 18. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html

Die DeepSec 2020 Konferenztage sind am 19. und 20. November. Die DeepSec Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. November statt. Aufgrund der aktuellen COVID-19-Maßnahmen sind alle Trainings und alle Vorträge virtueller Natur.

Tickets für die DeepSec Konferenz selbst und die Trainings können Sie jederzeit unter dem Link https://deepsec.net/ register.html bestellen. Ermäßigungscodes von Sponsoren stehen noch zur Verfügung. Melden Sie sich unter deepsec@deepsec.net bei Interesse. Bitte beachten Sie, dass wir aufgrund Planungssicherheit nach wie vor auf rechtzeitige Ticketbestellungen angewiesen sind.

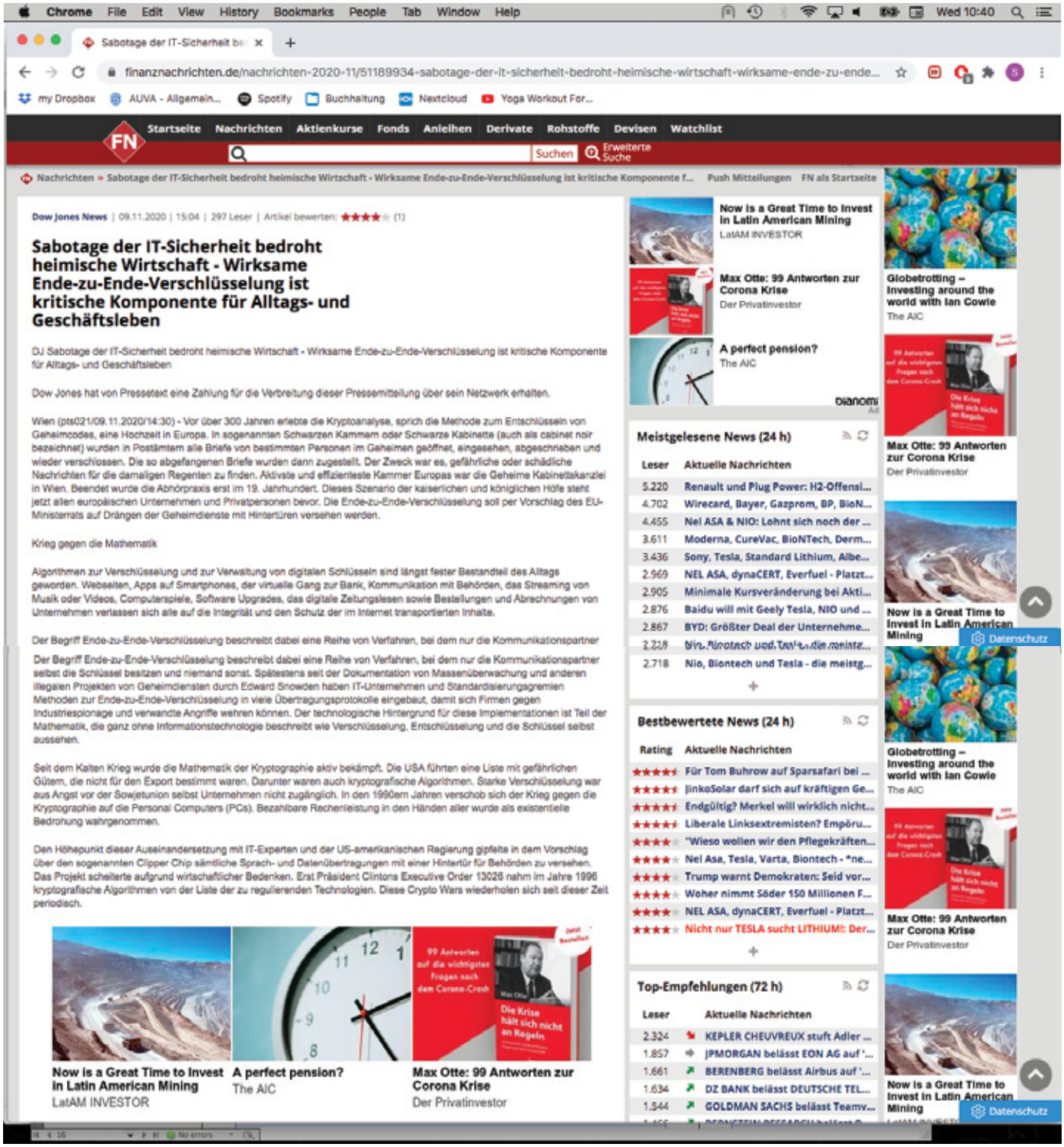
(Ende)

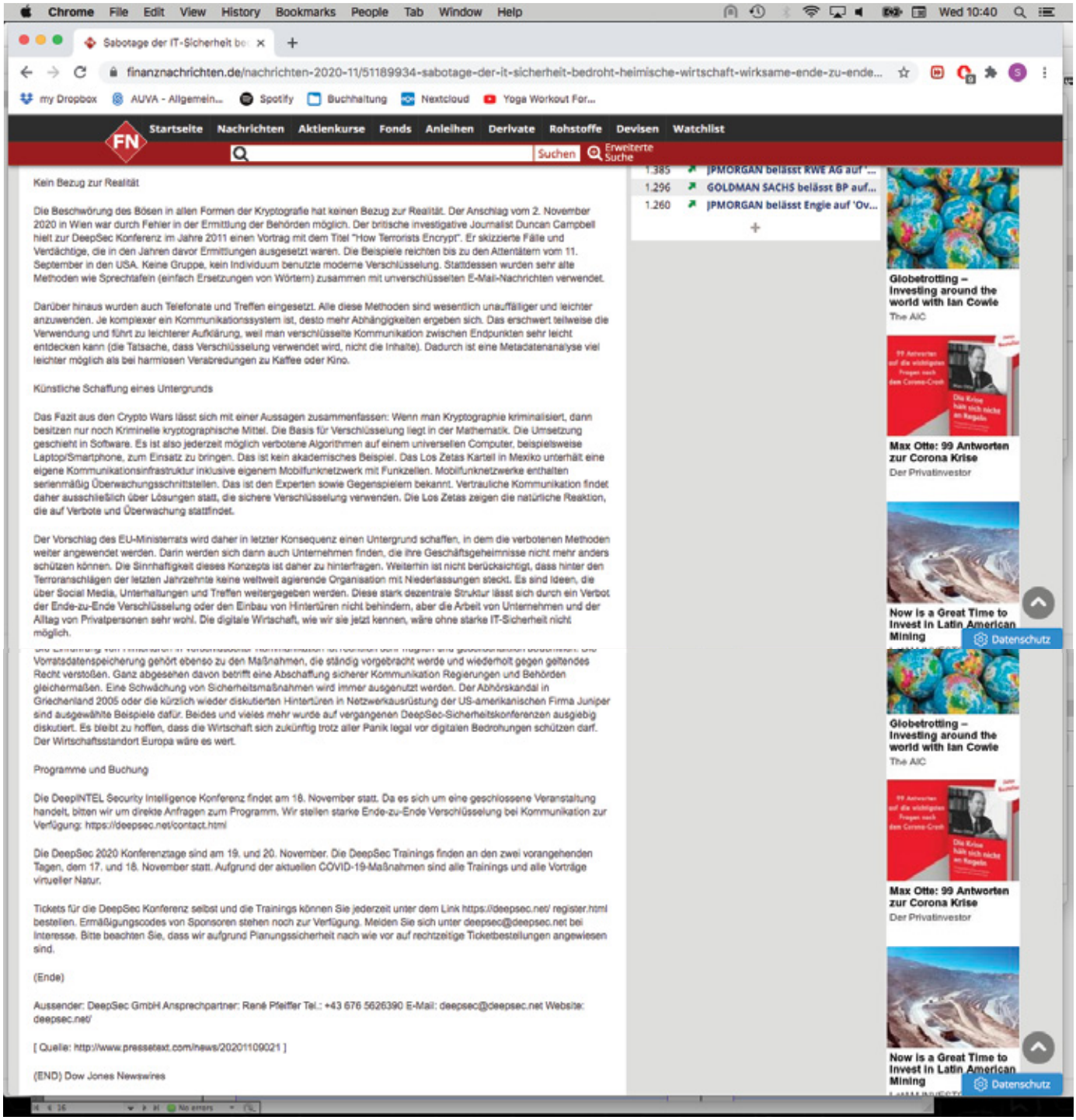
Aussender: DeepSec GmbH Ansprechpartner: René Pfeiffer Tel.: +43 676 5626390 E-Mail: deepsec@deepsec.net Website: deepsec.net/

[Quelle: http://www.pressetext.com/news/20201109021]

(END) Dow Jones Newswires

November 09, 2020 08:31 ET (13:31 GMT)


Chrome File Edit View History Bookmarks People Tab Window Help
Wed 10:40
finanznachrichten.de/nachrichten-2020-11/51189934-sabotage-der-it-sicherheit-bedroht-heimische-wirtschaft-wirksame-ende-zu-ende...
my Dropbox
AUVA - Allgemein...
Spotify
Buchhaltung
Nextcloud
Yoga Workout For...
Startseite Nachrichten Aktienkurse Fonds Anleihen Derivate Rohstoffe Devisen Watchlist
Suchen
Erweiterte Suche
Nachrichten » Sabotage der IT-Sicherheit bedroht heimische Wirtschaft - Wirksame Ende-zu-Ende-Verschlüsselung ist kritische Komponente f... Push Mitteilungen FN als Startseite
Dow Jones News | 09.11.2020 | 15:04 | 297 Leser | Artikel bewerten:
Sabotage der IT-Sicherheit bedroht heimische Wirtschaft - Wirksame Ende-zu-Ende-Verschlüsselung ist kritische Komponente für Alltags- und Geschäftsleben
DJ Sabotage der IT-Sicherheit bedroht heimische Wirtschaft - Wirksame Ende-zu-Ende-Verschlüsselung ist kritische Komponente für Alltags- und Geschäftsleben
Dow Jones hat von Pressetext eine Zahlung für die Verbreitung dieser Pressemitteilung über sein Netzwerk erhalten.
Wien (pts021/09.11.2020/14:30) - Vor über 300 Jahren erlebte die Kryptoanalyse, sprich die Methode zum Entschlüsseln von Geheimcodes, eine Hochzeit in Europa. In sogenannten Schwarzen Kammern oder Schwarze Kabinette (auch als cabinet noir bezeichnet) wurden in Postämtern alle Briefe von bestimmten Personen im Geheimen geöffnet, eingesehen, abgeschrieben und wieder verschlossen. Die so abgefangenen Briefe wurden dann zugestellt. Der Zweck war es, gefährliche oder schädliche Nachrichten für die damaligen Regenten zu finden. Aktivste und effizienteste Kammer Europas war die Geheime Kabinettskanzlei in Wien. Beendet wurde die Abhörpraxis erst im 19. Jahrhundert. Dieses Szenario der kaiserlichen und königlichen Höfe steht jetzt allen europäischen Unternehmen und Privatpersonen bevor. Die Ende-zu-Ende-Verschlüsselung soll per Vorschlag des EU-Ministerrats auf Drängen der Geheimdienste mit Hintertüren versehen werden.
Krieg gegen die Mathematik
Algorithmen zur Verschlüsselung und zur Verwaltung von digitalen Schlüsseln sind längst fester Bestandteil des Alltags geworden. Webseiten, Apps auf Smartphones, der virtuelle Gang zur Bank, Kommunikation mit Behörden, das Streaming von Musik oder Videos, Computerspiele, Software Upgrades, das digitale Zeitungslesen sowie Bestellungen und Abrechnungen von Unternehmen verlassen sich alle auf die Integrität und den Schutz der im Internet transportierten Inhalte.
Der Begriff Ende-zu-Ende-Verschlüsselung beschreibt dabei eine Reihe von Verfahren, bei dem nur die Kommunikationspartner
Now is a Great Time to Invest in Latin American Mining
LatAM INVESTOR
Max Otte: 99 Antworten zur Corona Krise
Der Privatinvestor
A perfect pension?
The AIC
Meistgelesene News (24 h)
Leser Aktuelle Nachrichten
5.220 Renault und Plug Power: H2-Offensi...
4.702 Wirecard, Bayer, Gazprom, BP, BioN...
4.455 Nel ASA & NIO: Lohnt sich noch der ...
3.611 Moderna, CureVac, BioNTech, Derm...
3.436 Sony, Tesla, Standard Lithium, Albe...
2.969 NEL ASA, dynaCERT, Everfuel - Platzt...
2.905 Minimale Kursveränderung bei Akti...
2.876 Baidu will mit Geely Tesla, NIO und ...
2.867 BYD: Größter Deal der Unternehme...
2.718 Nio, Biontech und Tesla - die meistg...
Bestbewertete News (24 h)
Rating Aktuelle Nachrichten
Für Tom Buhrow auf Sparsafari bei ...
JinkoSolar darf sich auf kräftigen Ge...
Endgültig? Merkel will wirklich nicht...
Liberale Linksextremisten? Empöru...
"Wieso wollen wir den Pflegekräften...
Nel Asa, Tesla, Varta, Biontech - *ne...
Trump warnt Demokraten: Seid vor...
Woher nimmt Söder 150 Millionen F...
NEL ASA, dynaCERT, Everfuel - Platzt...
Nicht nur TESLA sucht LITHIUM! Der...
Top-Empfehlungen (72 h)
Leser Aktuelle Nachrichten
2.324 KEPLER CHEUVREUX stuft Adler ...
1.857 JPMORGAN belässt EON AG auf '...
1.661 BERENBERG belässt Airbus auf '...
1.634 DZ BANK belässt DEUTSCHE TEL...
1.544 GOLDMAN SACHS belässt Teamv...
Globetrotting – Investing around the world with Ian Cowie
The AIC
Max Otte: 99 Antworten zur Corona Krise
Der Privatinvestor
Now is a Great Time to Invest in Latin American Mining
Datenschutz
Globetrotting – Investing around the world with Ian Cowie
The AIC
Max Otte: 99 Antworten zur Corona Krise
Der Privatinvestor
Now is a Great Time to Invest in Latin American Mining
Datenschutz
Now is a Great Time to Invest in Latin American Mining
LatAM INVESTOR
A perfect pension?
The AIC
Max Otte: 99 Antworten zur Corona Krise
Der Privatinvestor



Kein Bezug zur Realität

Die Beschwörung des Bösen in allen Formen der Kryptografie hat keinen Bezug zur Realität. Der Anschlag vom 2. November 2020 in Wien war durch Fehler in der Ermittlung der Behörden möglich. Der britische investigative Journalist Duncan Campbell hielt zur DeepSec Konferenz im Jahre 2011 einen Vortrag mit dem Titel "How Terrorists Encrypt". Er skizzierte Fälle und Verdächtige, die in den Jahren davor Ermittlungen ausgesetzt waren. Die Beispiele reichten bis zu den Attentätern vom 11. September in den USA. Keine Gruppe, kein Individuum benutzte moderne Verschlüsselung. Stattdessen wurden sehr alte Methoden wie Sprechtafeln (einfach Ersetzungen von Wörtern) zusammen mit unverschlüsselten E-Mail-Nachrichten verwendet.

Darüber hinaus wurden auch Telefonate und Treffen eingesetzt. Alle diese Methoden sind wesentlich unauffälliger und leichter anzuwenden. Je komplexer ein Kommunikationssystem ist, desto mehr Abhängigkeiten ergeben sich. Das erschwert teilweise die Verwendung und führt zu leichterer Aufklärung, weil man verschlüsselte Kommunikation zwischen Endpunkten sehr leicht entdecken kann (die Tatsache, dass Verschlüsselung verwendet wird, nicht die Inhalte). Dadurch ist eine Metadatenanalyse viel leichter möglich als bei harmlosen Verabredungen zu Kaffee oder Kino.

Künstliche Schaffung eines Untergrunds

Das Fazit aus den Crypto Wars lässt sich mit einer Aussagen zusammenfassen: Wenn man Kryptographie kriminalisiert, dann besitzen nur noch Kriminelle kryptographische Mittel. Die Basis für Verschlüsselung liegt in der Mathematik. Die Umsetzung geschieht in Software. Es ist also jederzeit möglich verbotene Algorithmen auf einem universellen Computer, beispielsweise Laptop/Smartphone, zum Einsatz zu bringen. Das ist kein akademisches Beispiel. Das Los Zetas Kartell in Mexiko unterhält eine eigene Kommunikationsinfrastruktur inklusive eigenem Mobilfunknetzwerk mit Funkzellen. Mobilfunknetzwerke enthalten serienmäßig Überwachungsschnittstellen. Das ist den Experten sowie Gegenspielern bekannt. Vertrauliche Kommunikation findet daher ausschließlich über Lösungen statt, die sichere Verschlüsselung verwenden. Die Los Zetas zeigen die natürliche Reaktion, die auf Verbote und Überwachung stattfindet.

Der Vorschlag des EU-Ministerrats wird daher in letzter Konsequenz einen Untergrund schaffen, in dem die verbotenen Methoden weiter angewendet werden. Darin werden sich dann auch Unternehmen finden, die ihre Geschäftsgeheimnisse nicht mehr anders schützen können. Die Sinnhaftigkeit dieses Konzepts ist daher zu hinterfragen. Weiterhin ist nicht berücksichtigt, dass hinter den Terroranschlägen der letzten Jahrzehnte keine weltweit agierende Organisation mit Niederlassungen steckt. Es sind Ideen, die über Social Media, Unterhaltungen und Treffen weitergegeben werden. Diese stark dezentrale Struktur lässt sich durch ein Verbot der Ende-zu-Ende Verschlüsselung oder den Einbau von Hintertüren nicht behindern, aber die Arbeit von Unternehmen und der Alltag von Privatpersonen sehr wohl. Die digitale Wirtschaft, wie wir sie jetzt kennen, wäre ohne starke IT-Sicherheit nicht möglich.

Vorratsdatenspeicherung gehört ebenso zu den Maßnahmen, die ständig vorgebracht werde und wiederholt gegen geltendes Recht verstoßen. Ganz abgesehen davon betrifft eine Abschaffung sicherer Kommunikation Regierungen und Behörden gleichermaßen. Eine Schwächung von Sicherheitsmaßnahmen wird immer ausgenutzt werden. Der Abhörskandal in Griechenland 2005 oder die kürzlich wieder diskutierten Hintertüren in Netzwerkausrüstung der US-amerikanischen Firma Juniper sind ausgewählte Beispiele dafür. Beides und vieles mehr wurde auf vergangenen DeepSec-Sicherheitskonferenzen ausgiebig diskutiert. Es bleibt zu hoffen, dass die Wirtschaft sich zukünftig trotz aller Panik legal vor digitalen Bedrohungen schützen darf. Der Wirtschaftsstandort Europa wäre es wert.

Programme und Buchung

Die DeepINTEL Security Intelligence Konferenz findet am 18. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html

Die DeepSec 2020 Konferenztage sind am 19. und 20. November. Die DeepSec Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. November statt. Aufgrund der aktuellen COVID-19-Maßnahmen sind alle Trainings und alle Vorträge virtueller Natur.

Tickets für die DeepSec Konferenz selbst und die Trainings können Sie jederzeit unter dem Link https://deepsec.net/ register.html bestellen. Ermäßigungscodes von Sponsoren stehen noch zur Verfügung. Melden Sie sich unter deepsec@deepsec.net bei Interesse. Bitte beachten Sie, dass wir aufgrund Planungssicherheit nach wie vor auf rechtzeitige Ticketbestellungen angewiesen sind.

(Ende)

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

[Quelle: http://www.pressetext.com/news/20201109021]

(END) Dow Jones Newswires

https://essentials.news/cybersecurity/general/article?url=https:%2F%2Fblog.deepsec.net%2Fdeepsec-2020-talk-journey-into-iranian-cyber-espionage-chris-kubecka%2F

26.10.2020

Cyberspace, Cyberwarfare, War, Cyber spying, Intelligence, United States

DeepSec 2020 Talk: Journey Into Iranian Cyber Espionage – Chris Kubecka

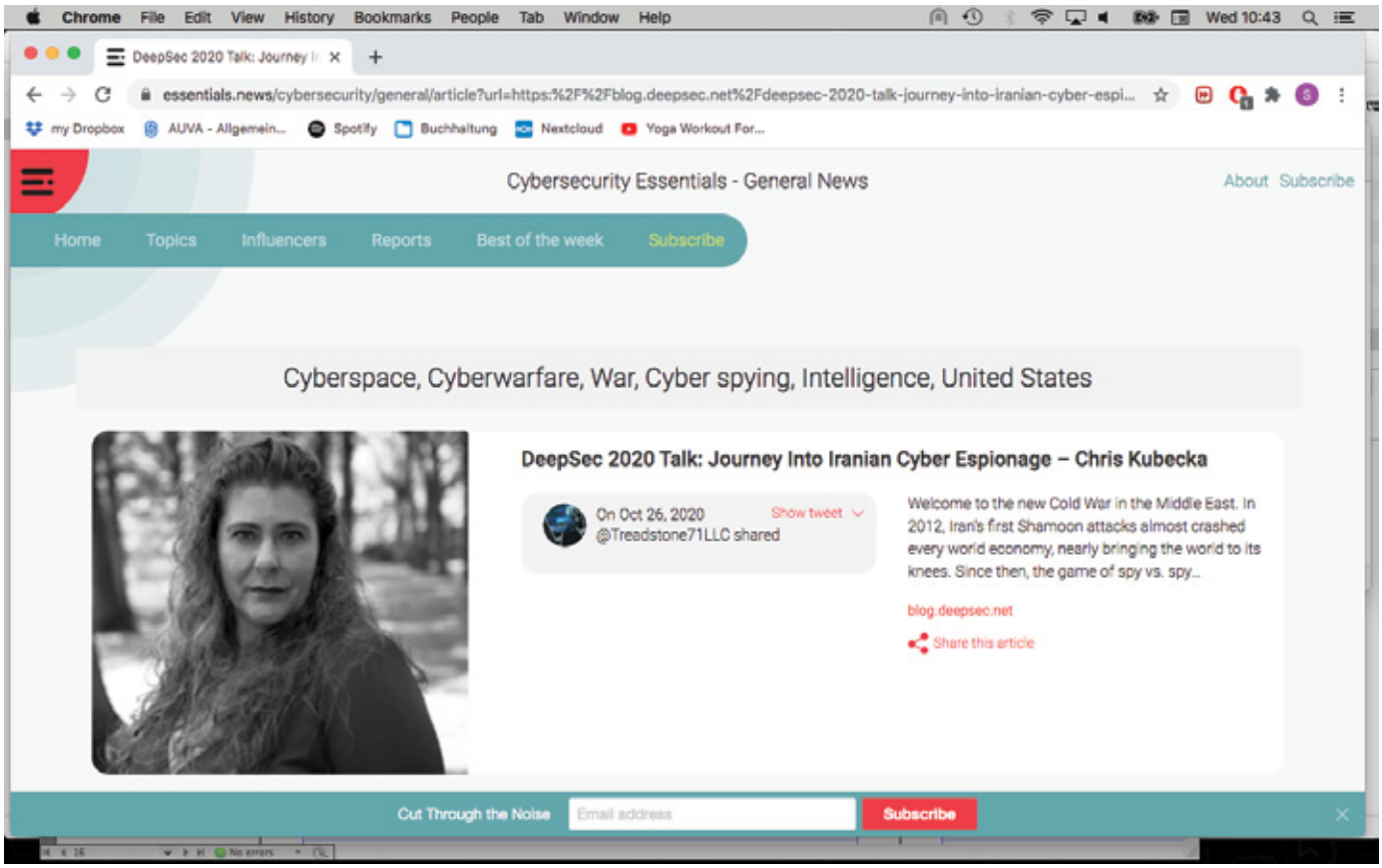
On Oct 26, 2020

@Treadstone71LLC shared

Show tweet

Welcome to the new Cold War in the Middle East. In 2012, Iran's first Shamoon attacks almost crashed every world economy, nearly bringing the world to its knees. Since then, the game of spy vs. spy…

blog.deepsec.net



https://computerwelt.at/news/deepsec-und-deepintel-konferenzen-veroeffentlichen-programm/
02.09.2020

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 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.

https://ictk.ch/inhalt/deepsec-2020-digitalisierung-ohne-informationssicherheit-hat-keine-zukunft
13.07.2020

Deepsec 2020 - Digitalisierung ohne Informationssicherheit hat keine Zukunft

Verfasst von inuit/hk am Mo, 13. Juli 2020 - 16:01

IT-Security

Konferenz

Die diesjährige Deepsec In-Depth Security Konferenz 2020 steht im Zeichen der Wissenschaft und möchte ihren Beitrag zur informationssicheren Digitalisierung liefern. Am 19. Und 20. November wird es in Wien Fachvorträge, Trainings und einen intensiven Austausch mit Experten geben. Der Zweck ist die Weiterbildung von Fachpersonen in der Informationstechnologie, um zukünftig die bestehende Hardware und Software sicher zu gestalten. Die Trainings finden am 17. und 18. November statt.

Das Angebot der Konferenz richtet sich an die Tätigkeitsbereiche Produktentwicklung, Softwareentwicklung, Geschäftsführung, Systemadministration, Forschung und Lehre. Zusätzlich wird ein Internet of Things (IoT) Hacking Village zusammen mit Partnern aufgebaut. Man kann sich direkt mit Experten austauschen und sehen, dass viele Smart Systeme alles andere als sicher sind.

Deepsec Konferenz warnt vor unsicherer Software und mangelnden Kenntnissen der Fachkräfte

Die Monate der Quarantänemaßnahmen in der Corona-Pandemie haben der Bedeutung der Informationstechnologie entschieden Nachdruck verliehen. Zwar ist das Internet schon lange in vielen Branchen integraler Bestandteil von Beruf und Alltag, aber die physischen Beschränkungen aufgrund der Covid-19-Pandemie hätten ohne moderne Telekommunikation noch wesentlich einschneidender für Behörden, die Wirtschaft und die Gesellschaft sein können. Audio-, Video- und Chat-Plattformen haben Schlimmes verhindert. Dem Ruf nach mehr Digitalisierung fehlt allerdings die wichtigste Zutat - die Informationssicherheit.

Publizierte Software ist sicher, oder?

In der Welt der Softwareentwicklung gibt es den inoffiziellen Spruch, dass ein Produkt fertig ist, wenn man es installieren kann. Der Rest ergebe sich ja dann im Betrieb. Das mag nicht die Regel sein. Einige Branchen betreiben sehr gewissenhafte Qualitätssicherung. Oft ist die Popularität der Feind der Qualität.

Die Verbreitung von Software ist leider keine geeignete Metrik für die Inhalte. Im Falle der Telekonferenzplattform Zoom konnte man auch gut erkennen, dass dieses Produkt eigentlich für einen ganz anderen Zweck bzw. eine andere Zielgruppe gedacht war. Darüber hinaus sind Fehler in Software gängig und lassen sich nur mit sorgfältigen Tests, Prozessen zum Aufspüren von Fehlfunktionen und Feedbackschleifen zurück zum Code beseitigen. Dieser Weg bedarf Zeit, die Start-ups nicht unbedingt haben. Als Folge daraus ist der Stand der Sicherheit in publizierter bzw. verfügbarer Software bestenfalls unbekannt.

Bevor ein Programm zur Verfügung stehen kann, muss es Design, Prototypen und schließlich eine Implementation geben. Erste Voraussetzung ist das sogenannte Secure Design. Werden am Anfang grundlegende Fehler gemacht, so kann die spätere Implementation daran nichts mehr ändern. Bildlich gesprochen kann ein Auto mit einer Bambuskarosserie bestimmten Herausforderungen nie genügen. Bei Software ist es genauso. Die zweite Voraussetzung ist das Secure Coding, also das Programmieren mit Methoden, die Fehler in der Software minimieren. Das ist die Theorie. Die Praxis sieht anders aus.

Secure Design und Coding sind nicht optional

Secure Design und Coding sind keine Features, welche sich leicht ein- oder ausschalten lassen. Man hat sie entweder berücksichtig, oder sie fehlen. Einen Mittelweg gibt es nicht. Darüber hinaus bietet eine sichere Software gegenüber der gleichartigen, schneller entwickelten, beliebteren und günstigeren Lösung auf den ersten Blick keine unmittelbaren Vorteile. Der Code funktioniert ja in beiden Fällen. Der Unterschied kommt erst in Ausnahmesituationen zum Vorschein. Psychologisch sind Vorteile, die man im normalen Betrieb nie sieht, sehr schwer zu bewerben. Im Falle von Zoom war es zwar einfach, auf die Verfehlungen im Bereich der sicheren Implementation hinzuweisen, aber die Schwächen waren vorher ohne kritisches Hinterfragen weltweit bei allen Installationen in täglicher Verwendung. Es wurden zu wenig Fragen gestellt. Dasselbe Problem findet sich vielfach in Wohnzimmern und Büros weltweit. Ganze Wirtschaftszweige verlassen sich auf Produkte, die sehr komplex sind, über Netzwerke wechselwirken und möglicherweise nie für die Aufgaben, die sie heute verrichten, gedacht waren. Dokumenterstellung und -verarbeitung ist ein weiteres verbreitetes Beispiel.

Solide und nachhaltige Ausbildung ist nötig

Um die Digitalisierung mit Informationssicherheit zu versehen, läuft man in ein didaktisches Dilemma. Methoden der sicheren Softwareentwicklung und des sicheren Designs kann man erst lernen, wenn man ein Grundverständnis von der Funktionsweise von Computern, gängigen Programmiersprachen (Plural, also mehr als eine),

Netzwerkprotokollen und Betriebssystemen hat. Ohne Vorwissen lassen sich die grundlegenden Prinzipien nicht erfassen. Aus diesem Grund sind Themen der IT-Security fast ausschließlich Wahlfächer, die man nach seiner Grundausbildung belegt. Die Praxis in Unternehmen bestätigt dies.

Laut Recruitern großer Tech-Firmen aus dem Silicon Valley müssen Sicherheitsspezialisten in mindesten drei verschiedenen Bereichen mehrere Jahre lang gearbeitet haben, um überhaupt für eine Stelle in der Informationssicherheit in Betracht zu kommen. Dieser Ansatz verläuft komplett diametral zur Ausrichtung vieler Ausbildungsstätten. Der viel beschworene Fachkräftemangel im Bereich der Digitalisierung hat oft Ausgebildete zum Ergebnis, die in Rekordzeit wenig gelernt haben - gesehen vom Standpunkt der Sicherheit aus. Eine erfolgreiche Digitalisierung bedingt daher eine solide und nachhaltige Ausbildung von Programmiererinnen und Programmierern sowie allen weiteren Spezialisten und Spezialistinnen im Prozess der Softwareentwicklung. Bits und Bytes ständig zu erwähnen, das Internet zu verwenden oder dauernd die Allmacht der Apps zu beschwören ist nicht ausreichend für eine sichere Zukunft. In der IT-Sicherheit ist Oberflächlichkeit keine Tugend.

Die Deepsec 2020 findet am 19. Und 20. November 2020 im Hotel „The Imperial Riding School Vienna - A Renaissance Hotel“, in der Ungargasse 60, 1030 Wien, statt.

https://deepsec.net/

Deepsec 2020 - Digitalisierung ohne Informationssicherheit hat keine Zukunft

Verfasst von **inuit/hk** am Mo, 13. Juli 2020 - 16:01

IT-Security
Konferenz

Die diesjährige Deepsec In-Depth Security Konferenz 2020 steht im Zeichen der Wissenschaft und möchte ihren Beitrag zur informationssicheren Digitalisierung liefern. Am 19. Und 20. November wird es in Wien Fachvorträge, Trainings und einen intensiven Austausch mit Experten geben. Der Zweck ist die Weiterbildung von Fachpersonen in der Informationstechnologie, um zukünftig die bestehende Hardware und Software sicher zu gestalten. Die Trainings finden am 17. und 18. November statt.

Das Angebot der Konferenz richtet sich an die Tätigkeitsbereiche Produktentwicklung, Softwareentwicklung, Geschäftsführung, Systemadministration, Forschung und Lehre. Zusätzlich wird ein Internet of Things (IoT) Hacking Village zusammen mit Partnern aufgebaut. Man kann sich direkt mit Experten austauschen und sehen, dass viele Smart Systeme alles andere als sicher sind.

Deepsec Konferenz warnt vor unsicherer Software und mangelnden Kenntnissen der Fachkräfte

Die Monate der Quarantänemaßnahmen in der Corona-Pandemie haben der Bedeutung der Informationstechnologie entschieden Nachdruck verliehen. Zwar ist das Internet schon lange in vielen Branchen integraler Bestandteil von Beruf und Alltag, aber die physischen Beschränkungen aufgrund der Covid-19-Pandemie hätten ohne moderne Telekommunikation noch wesentlich einschneidender für Behörden, die Wirtschaft und die Gesellschaft sein können. Audio-, Video- und Chat-Plattformen haben Schlimmes verhindert. Dem Ruf nach mehr Digitalisierung fehlt allerdings die wichtigste Zutat - die Informationssicherheit.

Publizierte Software ist sicher, oder?

In der Welt der Softwareentwicklung gibt es den inoffiziellen Spruch, dass ein Produkt fertig ist, wenn man es installieren kann. Der Rest ergebe sich ja dann im Betrieb. Das mag nicht die Regel sein. Einige Branchen betreiben sehr gewissenhafte Qualitätssicherung. Oft ist die Popularität der Feind der Qualität. Die Verbreitung von Software ist leider keine geeignete Metrik für die Inhalte. Im Falle der Telekonferenzplattform Zoom konnte man auch gut erkennen, dass dieses Produkt eigentlich für einen ganz anderen Zweck bzw. eine andere Zielgruppe gedacht war. Darüber hinaus sind Fehler in Software gängig und lassen sich nur mit sorgfältigen Tests, Prozessen zum Aufspüren von Fehlfunktionen und Feedbackschleifen zurück zum Code beseitigen. Dieser Weg bedarf Zeit, die Start-ups nicht unbedingt haben. Als Folge daraus ist der Stand der Sicherheit in publizierter bzw. verfügbarer Software bestenfalls unbekannt.

Bevor ein Programm zur Verfügung stehen kann, muss es Design, Prototypen und schließlich eine Implementation geben. Erste Voraussetzung ist das sogenannte Secure Design. Werden am Anfang grundlegende Fehler gemacht, so kann die spätere Implementation daran nichts mehr ändern. Bildlich gesprochen kann ein Auto mit einer Bambuskarosserie bestimmten Herausforderungen nie genügen. Bei Software ist es genauso. Die zweite Voraussetzung ist das Secure Coding, also das Programmieren mit Methoden, die Fehler in der Software minimieren. Das ist die Theorie. Die Praxis sieht anders aus.

Secure Design und Coding sind nicht optional

Secure Design und Coding sind keine Features, welche sich leicht ein- oder ausschalten lassen. Man hat sie entweder berücksichtig, oder sie fehlen. Einen Mittelweg gibt es nicht. Darüber hinaus bietet eine sichere Software gegenüber der gleichartigen, schneller entwickelten, beliebteren und günstigeren Lösung auf den ersten Blick keine unmittelbaren Vorteile. Der Code funktioniert ja in beiden Fällen. Der Unterschied kommt erst in Ausnahmesituationen zum Vorschein. Psychologisch sind Vorteile, die man im normalen Betrieb nie sieht, sehr schwer zu bewerben. Im Falle von Zoom war es zwar

le, die man im normalen Betrieb nie sieht, sehr schwer zu bewerben. Im Falle von Zoom war es zwar einfach, auf die Verfehlungen im Bereich der sicheren Implementation hinzuweisen, aber die Schwächen waren vorher ohne kritisches Hinterfragen weltweit bei allen Installationen in täglicher Verwendung. Es wurden zu wenig Fragen gestellt. Dasselbe Problem findet sich vielfach in Wohnzimmern und Büros weltweit. Ganze Wirtschaftszweige verlassen sich auf Produkte, die sehr komplex sind, über Netzwerke wechselwirken und möglicherweise nie für die Aufgaben, die sie heute verrichten, gedacht waren. Dokumenterstellung und -verarbeitung ist ein weiteres verbreitetes Beispiel.

Solide und nachhaltige Ausbildung ist nötig

Um die Digitalisierung mit Informationssicherheit zu versehen, läuft man in ein didaktisches Dilemma. Methoden der sicheren Softwareentwicklung und des sicheren Designs kann man erst lernen, wenn man ein Grundverständnis von der Funktionsweise von Computern, gängigen Programmiersprachen (Plural, also mehr als eine), Netzwerkprotokollen und Betriebssystemen hat. Ohne Vorwissen lassen sich die grundlegenden Prinzipien nicht erfassen. Aus diesem Grund sind Themen der IT-Security fast ausschließlich Wahlfächer, die man nach seiner Grundausbildung belegt. Die Praxis in Unternehmen bestätigt dies.

Laut Recruitern großer Tech-Firmen aus dem Silicon Valley müssen Sicherheitsspezialisten in mindesten drei verschiedenen Bereichen mehrere Jahre lang gearbeitet haben, um überhaupt für eine Stelle in der Informationssicherheit in Betracht zu kommen. Dieser Ansatz verläuft komplett diametral zur Ausrichtung vieler Ausbildungsstätten. Der viel beschworene Fachkräftemangel im Bereich der Digitalisierung hat oft Ausgebildete zum Ergebnis, die in Rekordzeit wenig gelernt haben - gesehen vom Standpunkt der Sicherheit aus. Eine erfolgreiche Digitalisierung bedingt daher eine solide und nachhaltige Ausbildung von Programmiererinnen und Programmierern sowie allen weiteren Spezialisten und Spezialistinnen im Prozess der Softwareentwicklung. Bits und Bytes ständig zu erwähnen, das Internet zu verwenden oder dauernd die Allmacht der Apps zu beschwören ist nicht ausreichend für eine sichere Zukunft. In der IT-Sicherheit ist Oberflächlichkeit keine Tugend.

Die Deepsec 2020 findet am 19. Und 20. November 2020 im Hotel „The Imperial Riding School Vienna - A Renaissance Hotel“, in der Ungargasse 60, 1030 Wien, statt.

https://deepsec.net/

ICT kommunikation

Kapi-Media
Ghöchstrasse 104
CH-8498 Gibswil
Tel. +41 79 437 79 33
www.ictk.ch
office@ictk.ch

Links
Newsletter
Impressum

https://reitbauer.at/elexikon/?qkeyword=DeepSec

keine Datumsangabe

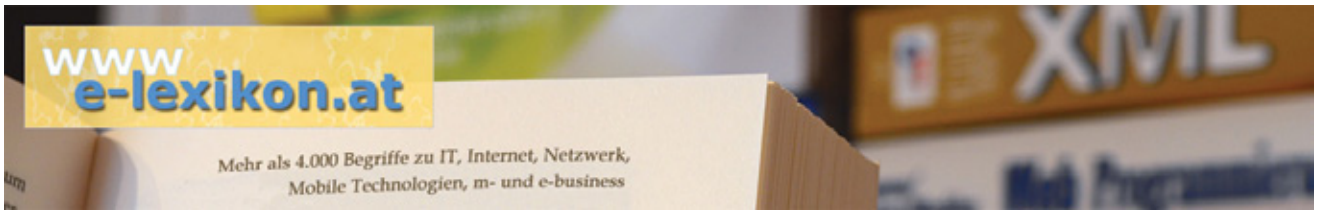
DeepSec

In-depth security conference Europe. Europäische Sicherheits-Konferenz, die einmal jährlich in Wien stattfindet.

Bei der heurigen 14. Ausgabe von 17.-20. November 2020 sind wieder zahlreiche Workshops und Vorträge zum Thema Sicherheit am Programm. Die DeepSec 2020 Konferenztage sind am 19. und 20. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. November statt. Die DeepINTEL Security Intelligence Konferenz findet am 18. November statt.

Die DeepSec In-Depth Security Konferenz will Hacker, Unternehmen aus IT und Security sowie Wissenschaftler zusammenbringen. Die Creme de la Creme der Hacker- und Security-Szene trifft sich, um ihre Erfahrungen auszutauschen und gefährliche Sicherheitslücken zu schließen.

http://www.deepsec.net



Ergebnis für **DeepSec** (1)

DeepSec

In-depth security conference Europe. Europäische Sicherheits-Konferenz, die einmal jährlich in Wien stattfindet.

Bei der heurigen 14. Ausgabe von 17.-20. November 2020 sind wieder zahlreiche Workshops und Vorträge zum Thema Sicherheit am Programm. Die DeepSec 2020 Konferenztage sind am 19. und 20. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. November statt. Die DeepINTEL Security Intelligence Konferenz findet am 18. November statt.

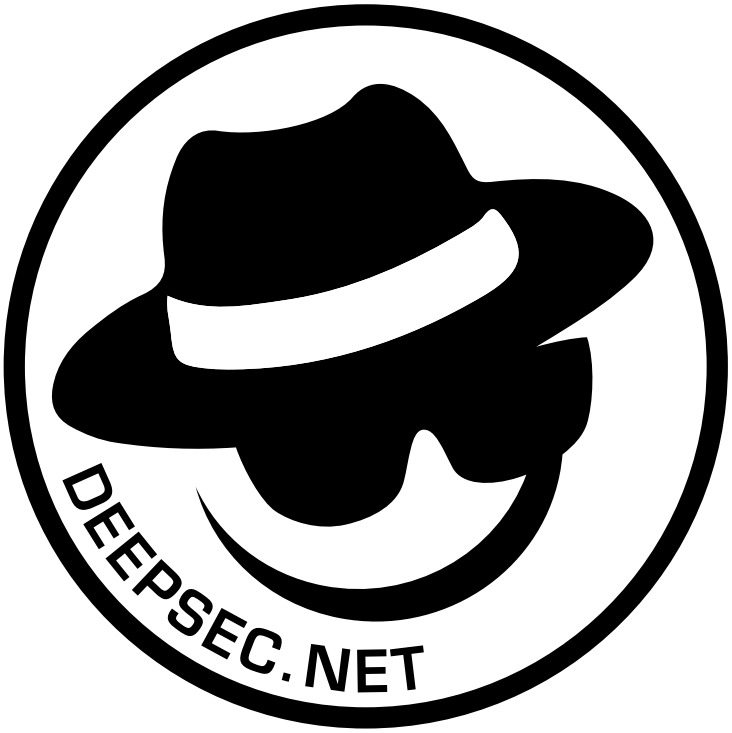
Die DeepSec In-Depth Security Konferenz will Hacker, Unternehmen aus IT und Security sowie Wissenschaftler zusammenbringen. Die Creme de la Creme der Hacker- und Security-Szene trifft sich, um ihre Erfahrungen auszutauschen und gefährliche Sicherheitslücken zu schließen.

- http://www.deepsec.net

siehe auch:

- Cloud Computing
- Hacker
- Virtualisierung
- DEFCON
- IPv6

Begriffe 1 bis 1 von 1


DEEPSEC.NET

https://www.pressetext.com/news/20201111010

pts20201111010 Technologie/Digitalisierung, Unternehmen/Wirtschaft

Präsentation neuer Wege in der Informationssicherheit

DeepSec und DeepINTEL gehen jährlich dem aktuellen Stand der Informationssicherheit auf den Grund

Wien (pts010/11.11.2020/09:05) - Das Jahr 2020 hat bisher gezeigt, dass man immer wieder mit Überraschungen und kritischen Ereignissen rechnen muss. Die Informationssicherheit hat trotzdem keine Pause. Im Gegenteil: Schwachstellen in Software, Hardware, Legislatur und Infrastruktur bedrohen permanent digitale Informationen. Damit Betroffene dennoch bessere Chancen gegen stetige Angriffe haben, werden die DeepSec- und DeepINTEL-Konferenzen dieses Jahr komplett digital via Internet stattfinden. Sicherheit gelingt nur durch gemeinsame Anstrengung. Daher wird auch in diesem November, wie jedes Jahr, ein Austauschen zwischen Expertinnen, Anwendern, Software-Entwicklerinnen, Administratoren und Verantwortlichen stattfinden!

Probleme lösen statt Verschieben

Kaum ein anderer Bereich erfindet stetig neue Begriffe wie die Informationstechnologie. Dabei schleichen sich leider oft Missverständnisse und Verschleierungen in deren Bedeutung ein. Die Worte Cloud, Virtualisierung, Sandbox oder Container sind nicht eindeutig. Es bedarf immer einer Beschreibung des Kontexts, um zu erfassen was damit eigentlich gemeint ist. Das Beiwort “Cyber” oder “Cyberspace” wird ebenso ohne Erklärungen verwendet.

William Gibson verwendete in seinen Romanen das Wort Cyberspace als Synonym für ein verbreitete verbundene digitale Technologie. Die Verwendung konkretisiert daher nichts, wodurch der Zusatz “Cyber” seine Verbreitung als allgemeine Worthülse gefunden hat. Wer zu viel “cybert”, der oder die verschiebt daher brennende Probleme samt deren Diagnose und Behebung nur ins virtuelle Nirgendwo.

Informationssicherheit muss konkret werden, weil mit abstrakten Begriffen keine Implementationen möglich sind. Die DeepSec befasst sich daher dieses Jahr ganz konkret mit Bedrohungen wie Schwachstellen gegen Cloud Plattformen, Kommunikationswege von Schadsoftware auf infizierten Systemen, der Sicherheit von Endgeräten und Angriffen auf Apps in mobilen Geräten. Diskutiert werden Details von Schwachstellen, Fehler im Design und mögliche Abhilfen. Im Spektrum der Vorträge werden auch branchenspezifische Umstände wie etwa der Umgang mit publizierten Fehlern in Produkten oder Implantate mit digitalen Funktionen diskutiert.

Welt der Metadaten

Die Welt der Daten ist beträchtlich gewachsen. Von Big Data haben mittlerweile alle schon gehört. Das wirkliche Nützliche daran ist aber Big Metadata. Daten alleine, auch in überschaubaren Mengen, bieten wenig bahnbrechende Vorteile. Erst die Verbindung zwischen verschiedenen Quellen mit passenden Beschreibungen zu den Inhalten führen zu verwertbaren Erkenntnissen. Die Vorgehensweise, Daten zuerst lange zu sammeln und im Laufe der Zeit immer stärker zu verknüpfen, ist bei bestimmten Unternehmen weit verbreitet.

Aus der Sicht der Informationssicherheit ergeben sich allerdings sehr viele Schwierigkeiten. Oft bilden sich ungewollte Ergebnisse aus Auswertungen, die Konsequenzen für die Dateneigentümerinnen und -eigentümer haben. Profile werden mittlerweile von nahezu allen Alltagsapplikationen erstellt. Das geschieht meist unbemerkt. Datensilos mit Resultaten werden erst mit Sicherheitslücken sichtbar. Genau aus diesem Grunde beschäftigen sich einige Vorträge auf der DeepSec mit Themen wie Home-Automation-Systemen oder Angriffen auf die IT von Hotels.

Spionage in der Mitte

Der Begriff der Spionage war vor Dekaden in der digitalen Welt noch sehr exotisch. Natürlich hat die Digitalisierung auch diesen Bereich stark modifiziert. Durch die zunehmende Vernetzung können auch Firmengeheimnisse leichter aus dem Home Office entwendet werden. Beispielsweise kann ein Computer im Home Office schlechter abgesichert sein, wodurch Angriffe leichter möglich sind. Schließlich besteht eine Verbindung zu firmeninternen Ressourcen, die für Angreifende interessant sein kann. Es geht dabei nicht um spektakuläre Fälle, die man sich möglicherweise wie in filmreifen Szenen vorstellt. Letztlich ist es immer ein Kopieren von Informationen, ohne aufzufallen.

Im diesjährigen DeepSec-Konferenzprogramm findet sich ein Vortrag von Chris Kubecka über Einblicke in die Welt der iranischen digitalen Spionage. Es werden dabei an echten Vorfällen die Methoden und Ereignisse illustriert, die bekannte Situationen und Technologien als Ausgangspunkt haben. Diese Veranschaulichungen sind extrem wichtig für alle, die die eigene Forschung und Entwicklung im Unternehmen vor Neugierigen beschützen müssen.

Je unspektakulärer eine Aktion, umso wirksamer kann sie sein, wenn der Kontext “Industriespionage” heisst. Aufgrund zahlreicher Unterhaltungen, die wir mit Sicherheitsexpertinnen und -experten seit 2007 geführt haben, können wir diese Präsentation ganz besonders empfehlen. Die zunehmende Vernetzung hat Spionage in die Mitte der Gesellschaft und der Wirtschaft sämtlicher Branchen gebracht.

Virtualisierung als Gelegenheit

Natürlich müssen alle Maßnahmen zum Schutz von Infrastruktur und eigener Informationstechnologie real geschehen. Die DeepSec Konferenz möchte aus diesem Grund ganz besonders in diesem Jahr neue Wege zum Austausch von Wissen und Erfahrungen bieten. Wenn Server und Dienste bereitwillig virtualisiert werden, wieso dann nicht auch der Besuch auf einer Sicherheitskonferenz? In den letzten Dekaden haben sich die am Internet teilnehmenden Systeme massiv weiterentwickelt.

Die grundlegenden Konzepte sich jedoch gleich geblieben. Es geht immer um einen Austausch von Informationen und deren Verarbeitung. Ganz analog verhält es sich zu allen, die sich in der Informationstechnologie um die Sicherheit kümmern müssen (was die Entwicklung von Software ganz speziell mit einschließt). Nutzen Sie daher das Angebot unseres Programms, welches die “in-depth” Garantie hat - Fakten, Forschung, Erfahrungsberichte, ganz ohne Selbstdarstellung und verzerrende Werbebegriffe.

Programme und Buchung

Die DeepINTEL Security Intelligence Konferenz findet am 18. November virtuell statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm.

Die DeepSec-2020-Konferenztage sind am 19. und 20. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. November, statt. Aufgrund der aktuellen COVID-19 Maßnahmen sind alle Trainings und alle Vorträge virtueller Natur.

Tickets für die DeepSec Konferenz selbst und die Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html bestellen. Ermäßigungscodes von Sponsoren stehen noch zur Verfügung. Melden Sie sich unter deepsec@deepsec.net bei Interesse. Bitte beachten Sie, dass wir aufgrund der Planungssicherheit nach wie vor auf rechtzeitige Ticketbestellungen angewiesen sind.

(Ende)

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

(/)

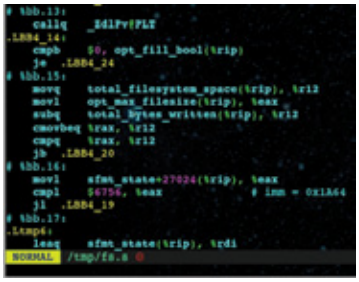
HIGHTECH

pts20201111010 Technologie/Digitalisierung, Unternehmen/Wirtschaft

Präsentation neuer Wege in der Informationssicherheit

DeepSec und DeepINTEL gehen jährlich dem aktuellen Stand der Informationssicherheit auf den Grund

Wien (pts010/11.11.2020/09:05) - **Das Jahr 2020 hat bisher gezeigt, dass man immer wieder mit Überraschungen und kritischen Ereignissen rechnen muss. Die Informationssicherheit hat trotzdem keine Pause. Im Gegenteil: Schwachstellen in Software, Hardware, Legislatur und Infrastruktur bedrohen permanent digitale Informationen. Damit Betroffene dennoch bessere Chancen gegen stetige Angriffe haben, werden die DeepSec- und DeepINTEL-Konferenzen dieses Jahr komplett digital via Internet stattfinden. Sicherheit gelingt nur durch gemeinsame Anstrengung. Daher wird auch in diesem November, wie jedes Jahr, ein Austauschen zwischen Expertinnen, Anwendern, Software-Entwicklerinnen, Administratoren und Verantwortlichen stattfinden!**



Generierter Code aus dem Alltag (Bild: DeepSec GmbH)

Probleme lösen statt Verschieben

Kaum ein anderer Bereich erfindet stetig neue Begriffe wie die Informationstechnologie. Dabei schleichen sich leider oft Missverständnisse und Verschleierungen in deren Bedeutung ein. Die Worte Cloud, Virtualisierung, Sandbox oder Container sind nicht eindeutig. Es bedarf immer einer Beschreibung des Kontexts, um zu erfassen was damit eigentlich gemeint ist. Das Beiwort "Cyber" oder "Cyberspace" wird ebenso ohne Erklärungen verwendet.

William Gibson verwendete in seinen Romanen das Wort Cyberspace als Synonym für ein verbreitete verbundene digitale Technologie. Die Verwendung konkretisiert daher nichts, wodurch der Zusatz "Cyber" seine Verbreitung als allgemeine Worthülse gefunden hat. Wer zu viel "cybert", der oder die verschiebt daher brennende Probleme samt deren Diagnose und Behebung nur ins virtuelle Nirgendwo.

Informationssicherheit muss konkret werden, weil mit abstrakten Begriffen keine Implementationen möglich sind. Die DeepSec befasst sich daher dieses Jahr ganz konkret mit Bedrohungen wie Schwachstellen gegen Cloud Plattformen, Kommunikationswege von Schadsoftware auf infizierten Systemen, der Sicherheit von Endgeräten und Angriffen auf Apps in mobilen Geräten. Diskutiert werden Details von Schwachstellen, Fehler im Design und mögliche Abhilfen. Im Spektrum der Vorträge werden auch branchenspezifische Umstände wie etwa der Umgang mit publizierten Fehlern in Produkten oder Implantate mit digitalen Funktionen diskutiert.

Welt der Metadaten

Die Welt der Daten ist beträchtlich gewachsen. Von Big Data haben mittlerweile alle schon gehört. Das wirkliche Nützliche daran ist aber Big Metadata. Daten alleine, auch in überschaubaren Mengen, bieten wenig bahnbrechende Vorteile. Erst die Verbindung zwischen verschiedenen Quellen mit passenden Beschreibungen zu den Inhalten führen zu verwertbaren Erkenntnissen. Die Vorgehensweise, Daten zuerst lange zu sammeln und im Laufe der Zeit immer stärker zu verknüpfen, ist bei bestimmten Unternehmen weit verbreitet.

Aus der Sicht der Informationssicherheit ergeben sich allerdings sehr viele Schwierigkeiten. Oft bilden sich ungewollte Ergebnisse aus Auswertungen, die Konsequenzen für die Dateneigentümerinnen und -eigentümer haben. Profile werden mittlerweile von nahezu allen Alltagsapplikationen erstellt. Das geschieht meist unbemerkt. Datensilos mit Resultaten werden erst mit Sicherheitslücken sichtbar. Genau aus diesem Grunde beschäftigen sich einige Vorträge auf der DeepSec mit Themen wie Home-Automation-Systemen oder Angriffen auf die IT von Hotels.

Spionage in der Mitte

Der Begriff der Spionage war vor Dekaden in der digitalen Welt noch sehr exotisch. Natürlich hat die Digitalisierung auch diesen Bereich stark modifiziert. Durch die zunehmende Vernetzung können auch Firmengeheimnisse leichter aus dem Home Office entwendet werden. Beispielsweise kann ein Computer im Home Office schlechter abgesichert sein, wodurch Angriffe leichter möglich sind. Schließlich besteht eine Verbindung zu firmeninternen Ressourcen, die für Angreifende interessant sein kann. Es geht dabei nicht um spektakuläre Fälle, die man sich möglicherweise wie in filmreifen Szenen vorstellt. Letztlich ist es immer ein Kopieren von Informationen, ohne aufzufallen.

Im diesjährigen DeepSec-Konferenzprogramm findet sich ein Vortrag von Chris Kubecka über Einblicke in die Welt der iranischen digitalen Spionage. Es werden dabei an echten Vorfällen die Methoden und Ereignisse illustriert, die bekannte Situationen und Technologien als Ausgangspunkt haben. Diese Veranschaulichungen sind extrem wichtig für alle, die die eigene Forschung und Entwicklung im Unternehmen vor Neugierigen beschützen müssen.

Je unspektakulärer eine Aktion, umso wirksamer kann sie sein, wenn der Kontext "Industriespionage" heisst. Aufgrund zahlreicher Unterhaltungen, die wir mit Sicherheitsexpertinnen und -experten seit 2007 geführt haben, können wir diese Präsentation ganz besonders empfehlen. Die zunehmende Vernetzung hat Spionage in die Mitte der Gesellschaft und der Wirtschaft sämtlicher Branchen gebracht.

Virtualisierung als Gelegenheit

Natürlich müssen alle Maßnahmen zum Schutz von Infrastruktur und eigener Informationstechnologie real geschehen. Die DeepSec Konferenz möchte aus diesem Grund ganz besonders in diesem Jahr neue Wege zum Austausch von Wissen und Erfahrungen bieten. Wenn Server und Dienste bereitwillig virtualisiert werden, wieso dann nicht auch der Besuch auf einer Sicherheitskonferenz? In den letzten Dekaden haben sich die am Internet teilnehmenden Systeme massiv weiterentwickelt.

Die grundlegenden Konzepte sich jedoch gleich geblieben. Es geht immer um einen Austausch von Informationen und deren Verarbeitung. Ganz analog verhält es sich zu allen, die sich in der Informationstechnologie um die Sicherheit kümmern müssen (was die Entwicklung von Software ganz speziell mit einschließt). Nutzen Sie daher das Angebot unseres Programms, welches die "in-depth" Garantie hat - Fakten, Forschung, Erfahrungsberichte, ganz ohne Selbstdarstellung und verzerrende Werbebegriffe.

Programme und Buchung

Die DeepINTEL Security Intelligence Konferenz findet am 18. November virtuell statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm.

Die DeepSec-2020-Konferenztage sind am 19. und 20. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. November, statt. Aufgrund der aktuellen COVID-19 Maßnahmen sind alle Trainings und alle Vorträge virtueller Natur.

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. Ermäßigungscodes von Sponsoren stehen noch zur Verfügung. Melden Sie sich unter deepsec@deepsec.net (mailto:deepsec@deepsec.net) bei Interesse. Bitte beachten Sie, dass wir aufgrund der Planungssicherheit nach wie vor auf rechtzeitige Ticketbestellungen angewiesen sind.

(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/20201109021

pts20201109021 Technologie/Digitalisierung, Unternehmen/Wirtschaft

Sabotage der IT-Sicherheit bedroht heimische Wirtschaft

Wirksame Ende-zu-Ende-Verschlüsselung ist kritische Komponente für Alltags- und Geschäftsleben

Wien (pts021/09.11.2020/14:30) - Vor über 300 Jahren erlebte die Kryptoanalyse, sprich die Methode zum Entschlüsseln von Geheimcodes, eine Hochzeit in Europa. In sogenannten Schwarzen Kammern oder Schwarze Kabinette (auch als cabinet noir bezeichnet) wurden in Postämtern alle Briefe von bestimmten Personen im Geheimen geöffnet, eingesehen, abgeschrieben und wieder verschlossen. Die so abgefangenen Briefe wurden dann zugestellt. Der Zweck war es, gefährliche oder schädliche Nachrichten für die damaligen Regenten zu finden. Aktivste und effizienteste Kammer Europas war die Geheime Kabinettskanzlei in Wien. Beendet wurde die Abhörpraxis erst im 19. Jahrhundert. Dieses Szenario der kaiserlichen und königlichen Höfe steht jetzt allen europäischen Unternehmen und Privatpersonen bevor. Die Ende-zu-Ende-Verschlüsselung soll per Vorschlag des EU-Ministerrats auf Drängen der Geheimdienste mit Hintertüren versehen werden.

Krieg gegen die Mathematik

Algorithmen zur Verschlüsselung und zur Verwaltung von digitalen Schlüsseln sind längst fester Bestandteil des Alltags geworden. Webseiten, Apps auf Smartphones, der virtuelle Gang zur Bank, Kommunikation mit Behörden, das Streaming von Musik oder Videos, Computerspiele, Software Upgrades, das digitale Zeitungslesen sowie Bestellungen und Abrechnungen von Unternehmen verlassen sich alle auf die Integrität und den Schutz der im Internet transportierten Inhalte.

Der Begriff Ende-zu-Ende-Verschlüsselung beschreibt dabei eine Reihe von Verfahren, bei dem nur die Kommunikationspartner selbst die Schlüssel besitzen und niemand sonst. Spätestens seit der Dokumentation von Massenüberwachung und anderen illegalen Projekten von Geheimdiensten durch Edward Snowden haben IT-Unternehmen und Standardisierungsgremien Methoden zur Ende-zu-Ende-Verschlüsselung in viele Übertragungsprotokolle eingebaut, damit sich Firmen gegen Industriespionage und verwandte Angriffe wehren können. Der technologische Hintergrund für diese Implementationen ist Teil der Mathematik, die ganz ohne Informationstechnologie beschreibt wie Verschlüsselung, Entschlüsselung und die Schlüssel selbst aussehen.

Seit dem Kalten Krieg wurde die Mathematik der Kryptographie aktiv bekämpft. Die USA führten eine Liste mit

gefährlichen Gütern, die nicht für den Export bestimmt waren. Darunter waren auch kryptografische Algorithmen. Starke Verschlüsselung war aus Angst vor der Sowjetunion selbst Unternehmen nicht zugänglich. In den 1990ern Jahren verschob sich der Krieg gegen die Kryptographie auf die Personal Computers (PCs). Bezahlbare Rechenleistung in den Händen aller wurde als existentielle Bedrohung wahrgenommen.

Den Höhepunkt dieser Auseinandersetzung mit IT-Experten und der US-amerikanischen Regierung gipfelte in dem Vorschlag über den sogenannten Clipper Chip sämtliche Sprach- und Datenübertragungen mit einer Hintertür für Behörden zu versehen. Das Projekt scheiterte aufgrund wirtschaftlicher Bedenken. Erst Präsident Clintons Executive Order 13026 nahm im Jahre 1996 kryptografische Algorithmen von der Liste der zu regulierenden Technologien. Diese Crypto Wars wiederholen sich seit dieser Zeit periodisch.

Kein Bezug zur Realität

Die Beschwörung des Bösen in allen Formen der Kryptografie hat keinen Bezug zur Realität. Der Anschlag vom 2. November 2020 in Wien war durch Fehler in der Ermittlung der Behörden möglich. Der britische investigative Journalist Duncan Campbell hielt zur DeepSec Konferenz im Jahre 2011 einen Vortrag mit dem Titel “How Terrorists Encrypt”. Er skizzierte Fälle und Verdächtige, die in den Jahren davor Ermittlungen ausgesetzt waren. Die Beispiele reichten bis zu den Attentätern vom 11. September in den USA. Keine Gruppe, kein Individuum benutzte moderne Verschlüsselung. Stattdessen wurden sehr alte Methoden wie Sprechtafeln (einfach Ersetzungen von Wörtern) zusammen mit unverschlüsselten E-Mail-Nachrichten verwendet.

Darüber hinaus wurden auch Telefonate und Treffen eingesetzt. Alle diese Methoden sind wesentlich unauffälliger und leichter anzuwenden. Je komplexer ein Kommunikationssystem ist, desto mehr Abhängigkeiten ergeben sich. Das erschwert teilweise die Verwendung und führt zu leichterer Aufklärung, weil man verschlüsselte Kommunikation zwischen Endpunkten sehr leicht entdecken kann (die Tatsache, dass Verschlüsselung verwendet wird, nicht die Inhalte). Dadurch ist eine Metadatenanalyse viel leichter möglich als bei harmlosen Verabredungen zu Kaffee oder Kino.

Künstliche Schaffung eines Untergrunds

Das Fazit aus den Crypto Wars lässt sich mit einer Aussagen zusammenfassen: Wenn man Kryptographie kriminalisiert, dann besitzen nur noch Kriminelle kryptographische Mittel. Die Basis für Verschlüsselung liegt in der Mathematik. Die Umsetzung geschieht in Software.

Es ist also jederzeit möglich verbotene Algorithmen auf einem universellen Computer, beispielsweise Laptop/Smartphone, zum Einsatz zu bringen. Das ist kein akademisches Beispiel. Das Los Zetas Kartell in Mexiko unterhält eine eigene Kommunikationsinfrastruktur inklusive eigenem Mobilfunknetzwerk mit Funkzellen. Mobilfunknetzwerke enthalten serienmäßig Überwachungsschnittstellen. Das ist den Experten sowie Gegenspielern bekannt. Vertrauliche Kommunikation findet daher ausschließlich über Lösungen statt, die sichere Verschlüsselung verwenden. Die Los Zetas zeigen die natürliche Reaktion, die auf Verbote und Überwachung stattfindet.

Der Vorschlag des EU-Ministerrats wird daher in letzter Konsequenz einen Untergrund schaffen, in dem die verbotenen Methoden weiter angewendet werden. Darin werden sich dann auch Unternehmen finden, die ihre Geschäftsgeheimnisse nicht mehr anders schützen können. Die Sinnhaftigkeit dieses Konzepts ist daher zu hinterfragen. Weiterhin ist nicht berücksichtigt, dass hinter den Terroranschlägen der letzten Jahrzehnte keine weltweit agierende Organisation mit Niederlassungen steckt. Es sind Ideen, die über Social Media, Unterhaltungen und Treffen weitergegeben werden. Diese stark dezentrale Struktur lässt sich durch ein Verbot der Ende-zu-Ende Verschlüsselung oder den Einbau von Hintertüren nicht behindern, aber die Arbeit von Unternehmen und der Alltag von Privatpersonen sehr wohl. Die digitale Wirtschaft, wie wir sie jetzt kennen, wäre ohne starke IT-Sicherheit nicht möglich.

Verfassungskonformität fraglich

Die Einführung von Hintertüren in verschlüsselter Kommunikation ist rechtlich sehr fraglich und gesellschaftlich bedenklich. Die Vorratsdatenspeicherung gehört ebenso zu den Maßnahmen, die ständig vorgebracht werde und wiederholt gegen geltendes Recht verstoßen. Ganz abgesehen davon betrifft eine Abschaffung sicherer Kommunikation Regierungen und Behörden gleichermaßen. Eine Schwächung von Sicherheitsmaßnahmen wird immer ausgenutzt werden. Der Abhörskandal in Griechenland 2005 oder die kürzlich wieder diskutierten Hintertüren in Netzwerkausrüstung der US-amerikanischen Firma Juniper sind ausgewählte Beispiele dafür. Beides und vieles mehr wurde auf vergangenen DeepSec-Sicherheitskonferenzen ausgiebig diskutiert. Es bleibt zu hoffen, dass die Wirtschaft sich zukünftig trotz aller Panik legal vor digitalen Bedrohungen schützen darf. Der Wirtschaftsstandort Europa wäre es wert.

Programme und Buchung

Die DeepINTEL Security Intelligence Konferenz findet am 18. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm.
Wir stellen starke Ende-zu-Ende Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html

Die DeepSec 2020 Konferenztage sind am 19. und 20. November. Die DeepSec Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. November statt. Aufgrund der aktuellen COVID-19-Maßnahmen sind alle Trainings und alle Vorträge virtueller Natur.

Tickets für die DeepSec Konferenz selbst und die Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html bestellen. Ermäßigungscodes von Sponsoren stehen noch zur Verfügung. Melden Sie sich unter deepsec@deepsec.net bei Interesse. Bitte beachten Sie, dass wir aufgrund Planungssicherheit nach wie vor auf rechtzeitige Ticketbestellungen angewiesen sind.

(Ende)

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

(/)

BUSINESS

pts20201109021 Technologie/Digitalisierung, Unternehmen/Wirtschaft

Sabotage der IT-Sicherheit bedroht heimische Wirtschaft

Wirksame Ende-zu-Ende-Verschlüsselung ist kritische Komponente für Alltags- und Geschäftsleben

Clipper Chip (Foto: Travis Goodspeed)

Wien (pts021/09.11.2020/14:30) - **Vor über 300 Jahren erlebte die Kryptoanalyse, sprich die Methode zum Entschlüsseln von Geheimcodes, eine Hochzeit in Europa. In sogenannten Schwarzen Kammern oder Schwarze Kabinette (auch als cabinet noir bezeichnet) wurden in Postämtern alle Briefe von bestimmten Personen im Geheimen geöffnet, eingesehen, abgeschrieben und wieder verschlossen. Die so abgefangenen Briefe wurden dann zugestellt. Der Zweck war es, gefährliche oder schädliche Nachrichten für die damaligen Regenten zu finden. Aktivste und effizienteste Kammer Europas war die Geheime Kabinettskanzlei in Wien. Beendet wurde die Abhörpraxis erst im 19. Jahrhundert. Dieses Szenario der kaiserlichen und königlichen Höfe steht jetzt allen europäischen Unternehmen und Privatpersonen bevor. Die Ende-zu-Ende-Verschlüsselung soll per Vorschlag des EU-Ministerrats auf Drängen der Geheimdienste mit Hintertüren versehen werden.**

Krieg gegen die Mathematik

Algorithmen zur Verschlüsselung und zur Verwaltung von digitalen Schlüsseln sind längst fester Bestandteil des Alltags geworden. Webseiten, Apps auf Smartphones, der virtuelle Gang zur Bank, Kommunikation mit Behörden, das Streaming von Musik oder Videos, Computerspiele, Software Upgrades, das digitale Zeitungslesen sowie Bestellungen und Abrechnungen von Unternehmen verlassen sich alle auf die Integrität und den Schutz der im Internet transportierten Inhalte.

Der Begriff Ende-zu-Ende-Verschlüsselung beschreibt dabei eine Reihe von Verfahren, bei dem nur die Kommunikationspartner selbst die Schlüssel besitzen und niemand sonst. Spätestens seit der Dokumentation von Massenüberwachung und anderen illegalen Projekten von Geheimdiensten durch Edward Snowden haben IT-Unternehmen und Standardisierungsgremien Methoden zur Ende-zu-Ende-Verschlüsselung in viele

Übertragungsprotokolle eingebaut, damit sich Firmen gegen Industriespionage und verwandte Angriffe wehren können. Der technologische Hintergrund für diese Implementationen ist Teil der Mathematik, die ganz ohne Informationstechnologie beschreibt wie Verschlüsselung, Entschlüsselung und die Schlüssel selbst aussehen.

Seit dem Kalten Krieg wurde die Mathematik der Kryptographie aktiv bekämpft. Die USA führten eine Liste mit gefährlichen Gütern, die nicht für den Export bestimmt waren. Darunter waren auch kryptografische Algorithmen. Starke Verschlüsselung war aus Angst vor der Sowjetunion selbst Unternehmen nicht zugänglich. In den 1990ern Jahren verschob sich der Krieg gegen die Kryptographie auf die Personal Computers (PCs). Bezahlbare Rechenleistung in den Händen aller wurde als existentielle Bedrohung wahrgenommen.

Den Höhepunkt dieser Auseinandersetzung mit IT-Experten und der US-amerikanischen Regierung gipfelte in dem Vorschlag über den sogenannten Clipper Chip sämtliche Sprach- und Datenübertragungen mit einer Hintertür für Behörden zu versehen. Das Projekt scheiterte aufgrund wirtschaftlicher Bedenken. Erst Präsident Clintons Executive Order 13026 nahm im Jahre 1996 kryptografische Algorithmen von der Liste der zu regulierenden Technologien. Diese Crypto Wars wiederholen sich seit dieser Zeit periodisch.

Kein Bezug zur Realität

Die Beschwörung des Bösen in allen Formen der Kryptografie hat keinen Bezug zur Realität. Der Anschlag vom 2. November 2020 in Wien war durch Fehler in der Ermittlung der Behörden möglich. Der britische investigative Journalist Duncan Campbell hielt zur DeepSec Konferenz im Jahre 2011 einen Vortrag mit dem Titel "How Terrorists Encrypt". Er skizzierte Fälle und Verdächtige, die in den Jahren davor Ermittlungen ausgesetzt waren. Die Beispiele reichten bis zu den Attentätern vom 11. September in den USA. Keine Gruppe, kein Individuum benutzte moderne Verschlüsselung. Stattdessen wurden sehr alte Methoden wie Sprechtafeln (einfach Ersetzungen von Wörtern) zusammen mit unverschlüsselten E-Mail-Nachrichten verwendet.

Darüber hinaus wurden auch Telefonate und Treffen eingesetzt. Alle diese Methoden sind wesentlich unauffälliger und leichter anzuwenden. Je komplexer ein Kommunikationssystem ist, desto mehr Abhängigkeiten ergeben sich. Das erschwert teilweise die Verwendung und führt zu leichterer Aufklärung, weil man verschlüsselte Kommunikation zwischen Endpunkten sehr leicht entdecken kann (die Tatsache, dass Verschlüsselung verwendet wird, nicht die Inhalte). Dadurch ist eine Metadatenanalyse viel leichter möglich als bei harmlosen Verabredungen zu Kaffee oder Kino.

Künstliche Schaffung eines Untergrunds

Das Fazit aus den Crypto Wars lässt sich mit einer Aussagen zusammenfassen: Wenn man Kryptographie kriminalisiert, dann besitzen nur noch Kriminelle kryptographische Mittel. Die Basis für Verschlüsselung liegt in der Mathematik. Die Umsetzung geschieht in Software. Es ist also jederzeit möglich verbotene Algorithmen auf einem universellen Computer, beispielsweise Laptop/Smartphone, zum Einsatz zu bringen. Das ist kein akademisches Beispiel. Das Los Zetas Kartell in Mexiko unterhält eine eigene Kommunikationsinfrastruktur inklusive eigenem Mobilfunknetzwerk mit Funkzellen. Mobilfunknetzwerke enthalten serienmäßig Überwachungsschnittstellen. Das ist den Experten sowie Gegenspielern bekannt. Vertrauliche Kommunikation findet daher ausschließlich über Lösungen statt, die sichere Verschlüsselung verwenden. Die Los Zetas zeigen die natürliche Reaktion, die auf Verbote und Überwachung stattfindet.

Der Vorschlag des EU-Ministerrats wird daher in letzter Konsequenz einen Untergrund schaffen, in dem die verbotenen Methoden weiter angewendet werden. Darin werden sich dann auch Unternehmen finden, die ihre Geschäftsgeheimnisse nicht mehr anders schützen können. Die Sinnhaftigkeit dieses Konzepts ist daher zu hinterfragen. Weiterhin ist nicht berücksichtigt, dass hinter den Terroranschlägen der letzten Jahrzehnte keine weltweit agierende Organisation mit Niederlassungen steckt. Es sind Ideen, die über Social Media, Unterhaltungen und Treffen weitergegeben werden. Diese stark dezentrale Struktur lässt sich durch ein Verbot

der Ende-zu-Ende Verschlüsselung oder den Einbau von Hintertüren nicht behindern, aber die Arbeit von Unternehmen und der Alltag von Privatpersonen sehr wohl. Die digitale Wirtschaft, wie wir sie jetzt kennen, wäre ohne starke IT-Sicherheit nicht möglich.

Verfassungskonformität fraglich

Die Einführung von Hintertüren in verschlüsselter Kommunikation ist rechtlich sehr fraglich und gesellschaftlich bedenklich. Die Vorratsdatenspeicherung gehört ebenso zu den Maßnahmen, die ständig vorgebracht werde und wiederholt gegen geltendes Recht verstoßen. Ganz abgesehen davon betrifft eine Abschaffung sicherer Kommunikation Regierungen und Behörden gleichermaßen. Eine Schwächung von Sicherheitsmaßnahmen wird immer ausgenutzt werden. Der Abhörskandal in Griechenland 2005 oder die kürzlich wieder diskutierten Hintertüren in Netzwerkausrüstung der US-amerikanischen Firma Juniper sind ausgewählte Beispiele dafür. Beides und vieles mehr wurde auf vergangenen DeepSec-Sicherheitskonferenzen ausgiebig diskutiert. Es bleibt zu hoffen, dass die Wirtschaft sich zukünftig trotz aller Panik legal vor digitalen Bedrohungen schützen darf. Der Wirtschaftsstandort Europa wäre es wert.

Programme und Buchung

Die DeepINTEL Security Intelligence Konferenz findet am 18. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html (https://deepsec.net/contact.html)

Die DeepSec 2020 Konferenztage sind am 19. und 20. November. Die DeepSec Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. November statt. Aufgrund der aktuellen COVID-19-Maßnahmen sind alle Trainings und alle Vorträge virtueller Natur.

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. Ermäßigungscodes von Sponsoren stehen noch zur Verfügung. Melden Sie sich unter deepsec@deepsec.net (mailto:deepsec@deepsec.net) bei Interesse. Bitte beachten Sie, dass wir aufgrund Planungssicherheit nach wie vor auf rechtzeitige Ticketbestellungen angewiesen sind.

(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/20201021013

pts20201021013 Technologie/Digitalisierung, Medien/Kommunikation

DeepSec und DeepINTEL 2020 als Hybridkonferenz

IT-Sicherheit in außergewöhnlichen Zeiten - Veranstaltungen ermöglichen virtuellen Zugriff

Wien (pts013/21.10.2020/09:45) - Von Alltag kann in der Informationssicherheit nie die Rede sein. Schwachstellen in Software, Schadsoftware, Kampagnen zum Angriff auf Unternehmen und Organisationen sowie die Verteidigung der eigenen Infrastruktur kennen keine Pause. In den vergangenen Monaten wurde die digitale Vernetzung als wichtigste Stütze der Gesellschaft und des Arbeitslebens auf die Probe gestellt. Oft wird dabei vergessen, dass nicht jede schicke App, jedes Portal und digitale Trends vertrauenswürdig sind. Die jährlichen DeepSec- und DeepINTEL-Konferenzen werden zur Sicherheit als Hybridveranstaltung ablaufen. Virtuelle Vorträge und Präsentationen in Präsenz sind für alle Teilnehmenden und Vortragenden gleichermaßen erreichbar.

Digitaler Schutz war noch nie wichtiger

Digitalisierung ist schnell ausgesprochen. Software ist noch schneller als sicher etikettiert. Leider lehren die letzten Dekaden der Sicherheitsforschung, dass Schwachstellen nur durch konsequentes Secure Design und Secure Coding reduziert werden können. Darüber hinaus müssen sichere Datenübertragung und Datenverarbeitung garantiert werden. Der Eigenwerbung zufolge erfüllen diese Kriterien sehr viele Applikationen, die man tagtäglich verwendet.

Schaut man aber hinter die Kulissen, so ergibt sich oft ein ganz anderes Bild. Transparenz ist daher kein leeres Wort in der Informationssicherheit. Die implementierten Maßnahmen zur Sicherheit - speziell von Plattformen - in Hardware sowie Software müssen fachlich hinterfragt werden können. Schnellschüsse, wie eine allmächtige App für das Smartphone oder rasch aufgebaute Webseiten, die eine mit Erfahrung aufgebaute Plattform vorgeben, rächen sich früher oder später mit ernsten Sicherheitsproblemen.

Das epidemisch grassierende Home Office bietet mannigfaltige Angriffsmöglichkeiten, weil das typische Heimnetzwerk durch viele Annehmlichkeiten wie Unterhaltung und Smart Home Technologien kaum einen nennenswerten Schutz vor Bedrohungen bieten kann. Bequemlichkeit muss nicht automatisch ein Widerspruch zur Sicherheit sein, wenn man die verwendeten Geräte und Netzwerke richtig trennt.

Social Engineering durch Falschinformationen

Außergewöhnliche Ereignisse ziehen immer kometenhaft einen Schweif von Falschinformationen nach sich, die für Betrug und Tricks ausgenutzt werden. Gerade bei der Vielzahl an Meldungen zu Gesundheitsmaßnahmen und Regelungen zum Infektionsschutz steigt die Glaubwürdigkeit von Nachrichten mit Schlagworten aus der Berichterstattung. Da die häufigsten Angriffe nach wie vor über Links zu manipulierten Webseiten oder durch sorgloses Öffnen scheinbar vertrauenswürdiger Dokumente geschehen, muss man einen kühlen Kopf bewahren. Geschürte Unsicherheit und aufgebaute Angst können sonst ausgenutzt werden.

Die Veranstaltungen im November möchten gerade im Anbetracht der jetzigen Situation das gewohnte Forum für den Austausch und Diskussionen bieten.

Virtuelle Trainings zu aktuellen Sicherheitsproblemen

Nichts geht über praktischen Erfahrungsaustausch an Beispielen zum Anfassen. Dieses Konzept steht in unseren virtuellen Trainings auch zur Verfügung. Diese werden ebenfalls im Hybridkonzept abgehalten. Teilnehmende vor Ort im Veranstaltungshotel können gemeinsam mit virtuellen Teilnehmenden Inhalte bearbeiten. Das Format bietet Raum für Diskussionen und gezielte Weiterbildung.

Im Programm findet sich dieses Jahr wieder der erfolgreiche Full Stack Security Testing Workshop von Dawid Czagan. Moderne Webapplikationen besitzen eine starke vertikale Struktur und bauen auf einer Vielzahl von Technologien auf. Entwicklerinnen und Entwickler stehen damit vor großen Herausforderungen, weil ein sehr guter Überblick über den in den Ebenen eingesetzten Code erforderlich ist.

Der Workshop behandelt alle Aspekte aktueller Webapplikationen, Angriffe gegen Datenbanksysteme (SQL und NoSQL), Übernahme von Subdomains, Attacken gegen Browser, Ausführen von eingeschleustem Code auf Systeme und vieles mehr. Im Fahrplan der DeepSec finden sich Links zu Videos, die einen genauen Überblick über den Inhalt geben.

Da die DeepSec dieses Jahr einen besonderen Fokus auf Industrial Control Systems (ICS) hat, findet auch ein Training zur Absicherung dieser Systeme statt. Tobias Zillner und Thomas Brandstetter widmen sich der Schnittstelle zwischen Information Technology (IT) und Operational Technology (OT). Das Training gibt eine Übersicht über die wichtigsten Protokolle im Industriebereich, zeigt deren Absicherung und führt durch eine Reihe von

Attacken sowie Schwachstellen. Das Wissen ist unentbehrlich für die Verteidigung von Industrieanlagen im Kontext der Digitalisierung. Die Inhalte stammen aus den Erfahrungen der Trainer die sie bei der Analyse bestehender ICS-Konfigurationen gemacht haben.

Weitere Trainings sind im Programm der DeepSec angeführt und in detaillierten Artikeln auf unserem Blog beschrieben.

Programme und Buchung

Die DeepINTEL Security Intelligence Konferenz findet am 18. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm.

Die DeepSec-2020-Konferenztage sind am 19. und 20. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. November, statt. Aufgrund der Beschränkungen für Anreise und eine stabilen Durchführung sind einige der Trainings virtueller Natur (Details entnehmen Sie bitte dem Programm bzw. fragen Sie direkt bei uns nach).

Die Konferenzen selbst werden als Hybrid-Veranstaltung ablaufen (gemischt Präsenz/virtuell, wobei alle alles sehen und hören können). Beide Veranstaltungen werden unter COVID-19 Gesundheitsmaßnahmen durchgeführt, die wir ständig aktualisiert unter diesem Link https://deepsec.net/docs/Counter_Covid-19.pdf?xfiles=on publizieren. Der Veranstaltungsort für die DeepSec und DeepINTEL 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. Fragen Sie uns oder unsere Sponsoren nach Discount Codes. Bitte beachten Sie, dass wir aufgrund Planungssicherheit auf rechtzeitige Ticketbestellungen angewiesen sind.

(Ende)

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

(/)

HIGHTECH

pts20201021013 Technologie/Digitalisierung, Medien/Kommunikation

DeepSec und DeepINTEL 2020 als Hybridkonferenz

IT-Sicherheit in außergewöhnlichen Zeiten - Veranstaltungen ermöglichen virtuellen Zugriff

Wien (pts013/21.10.2020/09:45) - **Von Alltag kann in der Informationssicherheit nie die Rede sein. Schwachstellen in Software, Schadsoftware, Kampagnen zum Angriff auf Unternehmen und Organisationen sowie die Verteidigung der eigenen Infrastruktur kennen keine Pause. In den vergangenen Monaten wurde die digitale Vernetzung als wichtigste Stütze der Gesellschaft und des Arbeitslebens auf die Probe gestellt. Oft wird dabei vergessen, dass nicht jede schicke App, jedes Portal und digitale Trends vertrauenswürdig sind. Die jährlichen DeepSec- und DeepINTEL-Konferenzen werden zur Sicherheit als Hybridveranstaltung ablaufen. Virtuelle Vorträge und Präsentationen in Präsenz sind für alle Teilnehmenden und Vortragenden gleichermaßen erreichbar.**

Digitaler Schutz war noch nie wichtiger

Digitalisierung ist schnell ausgesprochen. Software ist noch schneller als sicher etikettiert. Leider lehren die letzten Dekaden der Sicherheitsforschung, dass Schwachstellen nur durch konsequentes Secure Design und Secure Coding reduziert werden können. Darüber hinaus müssen sichere Datenübertragung und Datenverarbeitung garantiert werden. Der Eigenwerbung zufolge erfüllen diese Kriterien sehr viele Applikationen, die man tagtäglich verwendet.

Schaut man aber hinter die Kulissen, so ergibt sich oft ein ganz anderes Bild. Transparenz ist daher kein leeres Wort in der Informationssicherheit. Die implementierten Maßnahmen zur Sicherheit - speziell von Plattformen - in Hardware sowie Software müssen fachlich hinterfragt werden können. Schnellschüsse, wie eine allmächtige App für das Smartphone oder rasch aufgebaute Webseiten, die eine mit Erfahrung aufgebaute Plattform vorgeben, rächen sich früher oder später mit ernsten Sicherheitsproblemen.

Das epidemisch grassierende Home Office bietet mannigfaltige Angriffsmöglichkeiten, weil das typische Heimnetzwerk durch viele Annehmlichkeiten wie Unterhaltung und Smart Home Technologien kaum einen nennenswerten Schutz vor Bedrohungen bieten kann. Bequemlichkeit muss nicht automatisch ein Widerspruch zur Sicherheit sein, wenn man die verwendeten Geräte und Netzwerke richtig trennt.

Social Engineering durch Falschinformationen

Außergewöhnliche Ereignisse ziehen immer kometenhaft einen Schweif von Falschinformationen nach sich, die für Betrug und Tricks ausgenutzt werden. Gerade bei der Vielzahl an Meldungen zu Gesundheitsmaßnahmen und Regelungen zum Infektionsschutz steigt die Glaubwürdigkeit von Nachrichten mit Schlagworten aus der Berichterstattung. Da die häufigsten Angriffe nach wie vor über Links zu manipulierten Webseiten oder durch sorgloses Öffnen scheinbar vertrauenswürdiger Dokumente geschehen, muss man einen kühlen Kopf bewahren. Geschürte Unsicherheit und aufgebaute Angst können sonst ausgenutzt werden.

Die Veranstaltungen im November möchten gerade im Anbetracht der jetzigen Situation das gewohnte Forum für den Austausch und Diskussionen bieten.

Virtuelle Trainings zu aktuellen Sicherheitsproblemen

Nichts geht über praktischen Erfahrungsaustausch an Beispielen zum Anfassen. Dieses Konzept steht in unseren virtuellen Trainings auch zur Verfügung. Diese werden ebenfalls im Hybridkonzept abgehalten. Teilnehmende vor Ort im Veranstaltungshotel können gemeinsam mit virtuellen Teilnehmenden Inhalte bearbeiten. Das Format bietet Raum für Diskussionen und gezielte

Weiterbildung.

Im Programm findet sich dieses Jahr wieder der erfolgreiche Full Stack Security Testing Workshop von Dawid Czagan. Moderne Webapplikationen besitzen eine starke vertikale Struktur und bauen auf einer Vielzahl von Technologien auf. Entwicklerinnen und Entwickler stehen damit vor großen Herausforderungen, weil ein sehr guter Überblick über den in den Ebenen eingesetzten Code erforderlich ist.

Der Workshop behandelt alle Aspekte aktueller Webapplikationen, Angriffe gegen Datenbanksysteme (SQL und NoSQL), Übernahme von Subdomains, Attacken gegen Browser, Ausführen von eingeschleustem Code auf Systeme und vieles mehr. Im Fahrplan der DeepSec finden sich Links zu Videos, die einen genauen Überblick über den Inhalt geben.

Da die DeepSec dieses Jahr einen besonderen Fokus auf Industrial Control Systems (ICS) hat, findet auch ein Training zur Absicherung dieser Systeme statt. Tobias Zillner und Thomas Brandstetter widmen sich der Schnittstelle zwischen Information Technology (IT) und Operational Technology (OT). Das Training gibt eine Übersicht über die wichtigsten Protokolle im Industriebereich, zeigt deren Absicherung und führt durch eine Reihe von Attacken sowie Schwachstellen. Das Wissen ist unentbehrlich für die Verteidigung von Industrieanlagen im Kontext der Digitalisierung. Die Inhalte stammen aus den Erfahrungen der Trainer die sie bei der Analyse bestehender ICS-Konfigurationen gemacht haben.

Weitere Trainings sind im Programm der DeepSec angeführt und in detaillierten Artikeln auf unserem Blog beschrieben.

Programme und Buchung

Die DeepINTEL Security Intelligence Konferenz findet am 18. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm.

Die DeepSec-2020-Konferenztage sind am 19. und 20. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. November, statt. Aufgrund der Beschränkungen für Anreise und eine stabilen Durchführung sind einige der Trainings virtueller Natur (Details entnehmen Sie bitte dem Programm bzw. fragen Sie direkt bei uns nach).

Die Konferenzen selbst werden als Hybrid-Veranstaltung ablaufen (gemischt Präsenz/virtuell, wobei alle alles sehen und hören können). Beide Veranstaltungen werden unter COVID-19 Gesundheitsmaßnahmen durchgeführt, die wir ständig aktualisiert unter diesem Link https://deepsec.net/docs/Counter_Covid-19.pdf?xfiles=on (https://deepsec.net/docs/Counter_Covid-19.pdf?xfiles=on) publizieren.

Der Veranstaltungsort für die DeepSec und DeepINTEL 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. Fragen Sie uns oder unsere Sponsoren nach Discount Codes. Bitte beachten Sie, dass wir aufgrund Planungssicherheit auf rechtzeitige Ticketbestellungen angewiesen sind.

(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/20201006010

pts20201006010 Technologie/Digitalisierung, Unternehmen/Wirtschaft

Digitale Informationssicherheit hat menschliche Schwächen

DeepINTEL Security Intelligence Konferenz diskutiert strategische IT-Sicherheit in Wien

Wien (pts010/06.10.2020/08:45) - In den letzten Dekaden ist der berufliche und private Alltag immer mehr von modernen Technologien und vernetzter Kommunikation durchsetzt worden. Das hat neben vielen Annehmlichkeiten auch schwierige Herausforderungen für die Informationssicherheit hervorgebracht. Auf vielen Sicherheitskonferenzen werden daher immer komplexere technische Lösungen zelebriert. Das Problem an den Problemen, die dadurch gelöst werden sollen: Der Faktor Mensch und dessen Schwachstellen, die ganz ohne Digitalisierung auskommen. Die DeepINTEL Konferenz beschäftigt sich daher mit den Zusammenhängen und dem strategischen Hintergrund von Informationssicherheit, um Bedrohungen zu minimieren und Schutz nachhaltig verbessern zu können.

Fehler im System sind Teil des Fundaments

Immer wieder sind Berichte über Datenlecks und spektakuläre Einbrüche in den Nachrichten zu lesen. Dargestellt wird leider immer nur das Ergebnis. Natürlich ist die Spurensuche immer sehr viel zeitaufwendiger. Die unmittelbare Folge ist zuerst eine Information der Betroffenen und die Feststellung des Schadens. Die Zeit für die Aufarbeitung ist gut investiert. Eine Ermittlung der Vorgänge, die zur Überwindung der Sicherheitsmassnahmen geführt haben, kann sehr lehrreich sein. Die Verbesserung der Verteidigung basiert meist auf den Ergebnissen solcher Nachforschungen.

Fallstudien sind ein wichtiger Teil der Weiterbildung. Man lernt damit die Fehler in Infrastruktur und Systemen besser einzuschätzen. Es ist auch ein Irrglaube, dass bekannt Schwächen in Applikationen nach Publikation sofort behoben werden. Viele erfolgreiche Angriffe verwenden bekannte und gut erprobte Techniken, die für alte Schwachstellen entwickelt wurden. Sicherheitsforscher finden immer wieder anfällige Systeme auch nach Jahren. Die Gründe dafür sind vielfältig.

Bedrohungen studieren und Angreifende analysieren

Die DeepINTEL Konferenz geht noch einen Schritt weiter. Die alleinige Betrachtung von Schwachstellen und

Sicherheitstechnologie reicht . Das Wissen um die Kapazitäten der Angreifenden sind Teil der Bedrohungsanalyse, welche am Anfang einer IT Sicherheitsstrategie stehen sollte. In diesem Jahr werden die Fähigkeiten ausgewählter Gruppen diskutiert, die zu den sogenannten Advanced Persistent Threats (APTs) zählen. Diese Gruppen führen organisierte Spionage über sehr gut getarnte und logistisch vorbereitete Infrastruktur durch.

Wer sich für aktuelle Methoden und Operationen der APT Gruppen interessiert, sollte die DeepINTEL besuchen. Drei Forscher eines namhaften Sicherheitsunternehmens präsentieren Einsichten in Aktivitäten, die zur Zeit gegen Firmen und Organisationen eingesetzt werden. Im Fokus sind speziell die Änderungen in der eigenen Infrastruktur der Angreifenden und die damit einhergehende Abänderung der durchgeführten Operationen. Die Diskussion bewegt sich entlang von entdeckten und analysierten Proben von aktiver Schadsoftware und deren Kommunikation mit den Servern zur Steuerung.

Telearbeit macht Diebe

Die COVID-19 Pandemie hat zu zahlreichen Ausnahmesituationen geführt. Das Home Office war eine notwendige und für manche auch eine willkommene Abwechslung. Eine Änderung der gewohnten Umgebung bringt Gefahren mit sich. Gängige Heimnetzwerke haben weniger Sicherheitsmassnahmen Dennoch muss der Zugriff auf firmeneigene Daten und Dienste sichergestellt sein. Diese Situation hat in den vergangenen Monaten vermehrt zu Angriffen auf Teleworker geführt.

Während der DeepINTEL werden aktuelle Informationen aus Bedrohungen diskutiert, um die Methoden der Angreifenden auf Lieferketten, Betrugsversuche, Attacken auf Fernzugriffe und verwandte Themen zu analysieren. Basis der Diskussion sind auch hier Informationen aus Quellen der Bedrohungsanalyse. Die Fakten sind unverzichtbar für die gezielte und effiziente Verteidigung der eigenen Organisation, da die genauen Taktiken und Werkzeuge der Angreifenden besprochen werden.

Absicherung des menschlichen Gehirns

Menschen wechselwirken täglich miteinander. Gespräche, Telefonate, geschriebene Nachrichten, Berichte, Social Media und vieles mehr sind Teil des privaten und des geschäftlichen Alltags. Menschliche Kommunikation ist daher eine wichtige Quelle für die Informationsgewinnung. Diese Methode wird Human Intelligence (HUMINT) genannt. Sie verwendet den Kontakt zu anderen Personen, und sie ist als Methode tausende von Jahren alt.

HUMINT an sich verwendet Fragetechniken, zwischenmenschliche Kommunikation und besitzt Begriffsrahmen, die die eingesetzten Techniken beschreiben. HUMINT ist wichtig, um die Absichten und Motivationen von Angreifenden zu erfassen. Das ist ein klarer Vorteil gegenüber anderen Techniken.

Technologische Mittel zum Ausnutzen und zum Schutz von Personen im Anbetracht menschlicher Kommunikation sind nur begrenzt wirksam. Die DeepINTEL Konferenz beschäftigt sich daher eingehend mit der Fragestellung wie man das menschliche Gehirn bzw. dessen Gedanken im Lichte von HUMINT schützen kann. Schwerwiegende Angriffe werden nach wie vor durch geschickte Vernetzung, Telefonate und Kurznachrichten vorbereitet. Speziell bei rein elektronischer Kommunikation können bestehende Vertrauensverhältnisse sehr leicht untergraben oder gar Manipulierte hergestellt werden. Dies schafft ein beträchtliches Risiko für alle Abteilungen eines Unternehmens, welche intensiv mit der Außenwelt wechselwirken - beispielsweise die Personalabteilung, der Support oder der Verkauf.

Programme und Buchung

Die DeepINTEL Security Intelligence Konferenz findet am 18. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen nach dem Programm.

Die DeepSec 2020 Konferenztage sind am 19. und 20. November direkt im Anschluss. Die DeepSec Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. November statt. Aufgrund der Beschränkungen für Anreise und eine stabilen Durchführung sind einige der Trainings virtueller Natur (Details entnehmen Sie bitte dem Programm bzw. fragen Sie direkt bei uns nach). Die Konferenz selbst wird als Hybrid-Veranstaltung ablaufen (gemischt Präsenz/virtuell, wobei alle alles sehen und hören können).

Beide Veranstaltungen werden unter COVID-19 Gesundheitsmaßnahmen durchgeführt, die wir ständig aktualisiert unter diesem Link https://deepsec.net/docs/Counter_Covid-19.pdf publizieren.

Der Veranstaltungsort für die DeepSec und DeepINTEL 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.
Bitte beachten Sie, dass wir aufgrund Planungssicherheit auf rechtzeitige Ticketbestellungen angewiesen sind.

(/)

BUSINESS

pts20201006010 Technologie/Digitalisierung, Unternehmen/Wirtschaft

Digitale Informationssicherheit hat menschliche Schwächen

DeepINTEL Security Intelligence Konferenz diskutiert strategische IT-Sicherheit in Wien

Keine Tscherenkow-Strahlung, aber dennoch gefährlich (Foto: DeepSec GmbH)

Wien (pts010/06.10.2020/08:45) - **In den letzten Dekaden ist der berufliche und private Alltag immer mehr von modernen Technologien und vernetzter Kommunikation durchsetzt worden. Das hat neben vielen Annehmlichkeiten auch schwierige Herausforderungen für die Informationssicherheit hervorgebracht. Auf vielen Sicherheitskonferenzen werden daher immer komplexere technische Lösungen zelebriert. Das Problem an den Problemen, die dadurch gelöst werden sollen: Der Faktor Mensch und dessen Schwachstellen, die ganz ohne Digitalisierung auskommen. Die DeepINTEL Konferenz beschäftigt sich daher mit den Zusammenhängen und dem strategischen Hintergrund von Informationssicherheit, um Bedrohungen zu minimieren und Schutz nachhaltig verbessern zu können.**

Fehler im System sind Teil des Fundaments

Immer wieder sind Berichte über Datenlecks und spektakuläre Einbrüche in den Nachrichten zu lesen. Dargestellt wird leider immer nur das Ergebnis. Natürlich ist die Spurensuche immer sehr viel zeitaufwendiger. Die unmittelbare Folge ist zuerst eine Information der Betroffenen und die Feststellung des Schadens. Die Zeit für die Aufarbeitung ist gut investiert. Eine Ermittlung der Vorgänge, die zur Überwindung der Sicherheitsmassnahmen geführt haben, kann sehr lehrreich sein. Die Verbesserung der Verteidigung basiert meist auf den Ergebnissen solcher Nachforschungen.

Fallstudien sind ein wichtiger Teil der Weiterbildung. Man lernt damit die Fehler in Infrastruktur und Systemen besser einzuschätzen. Es ist auch ein Irrglaube, dass bekannt Schwächen in Applikationen nach Publikation sofort behoben werden. Viele erfolgreiche Angriffe verwenden bekannte und gut erprobte Techniken, die für alte Schwachstellen entwickelt wurden. Sicherheitsforscher finden immer wieder anfällige Systeme auch nach Jahren. Die Gründe dafür sind vielfältig.

Bedrohungen studieren und Angreifende analysieren

Die DeepINTEL Konferenz geht noch einen Schritt weiter. Die alleinige Betrachtung von Schwachstellen und Sicherheitstechnologie reicht . Das Wissen um die Kapazitäten der Angreifenden sind Teil der Bedrohungsanalyse, welche am Anfang einer IT Sicherheitsstrategie stehen sollte. In diesem Jahr werden die Fähigkeiten ausgewählter Gruppen diskutiert, die zu den sogenannten Advanced Persistent Threats (APTs) zählen. Diese Gruppen führen organisierte Spionage über sehr gut getarnte und logistisch vorbereitete Infrastruktur durch.

Wer sich für aktuelle Methoden und Operationen der APT Gruppen interessiert, sollte die DeepINTEL besuchen. Drei Forscher eines namhaften Sicherheitsunternehmens präsentieren Einsichten in Aktivitäten, die zur Zeit gegen Firmen und Organisationen eingesetzt werden. Im Fokus sind speziell die Änderungen in der eigenen Infrastruktur der Angreifenden und die damit einhergehende Abänderung der durchgeführten Operationen. Die Diskussion bewegt sich entlang von entdeckten und analysierten Proben von aktiver Schadsoftware und deren Kommunikation mit den Servern zur Steuerung.

Telearbeit macht Diebe

Die COVID-19 Pandemie hat zu zahlreichen Ausnahmesituationen geführt. Das Home Office war eine notwendige und für manche auch eine willkommene Abwechslung. Eine Änderung der gewohnten Umgebung bringt Gefahren mit sich. Gängige Heimnetzwerke haben weniger Sicherheitsmassnahmen Dennoch muss der Zugriff auf firmeneigene Daten und Dienste sichergestellt sein. Diese Situation hat in den vergangenen Monaten vermehrt zu Angriffen auf Teleworker geführt.

Während der DeepINTEL werden aktuelle Informationen aus Bedrohungen diskutiert, um die Methoden der Angreifenden auf Lieferketten, Betrugsversuche, Attacken auf Fernzugriffe und verwandte Themen zu analysieren. Basis der Diskussion sind auch hier Informationen aus Quellen der Bedrohungsanalyse. Die Fakten sind unverzichtbar für die gezielte und effiziente Verteidigung der eigenen Organisation, da die genauen Taktiken und Werkzeuge der Angreifenden besprochen werden.

Absicherung des menschlichen Gehirns

Menschen wechselwirken täglich miteinander. Gespräche, Telefonate, geschriebene Nachrichten, Berichte, Social Media und vieles mehr sind Teil des privaten und des geschäftlichen Alltags. Menschliche Kommunikation ist daher eine wichtige Quelle für die Informationsgewinnung. Diese Methode wird Human Intelligence (HUMINT) genannt. Sie verwendet den Kontakt zu anderen Personen, und sie ist als Methode tausende von Jahren alt. HUMINT an sich verwendet Fragetechniken, zwischenmenschliche Kommunikation und besitzt Begriffsrahmen, die die eingesetzten Techniken beschreiben. HUMINT ist wichtig, um die Absichten und Motivationen von Angreifenden zu erfassen. Das ist ein klarer Vorteil gegenüber anderen Techniken.

Technologische Mittel zum Ausnutzen und zum Schutz von Personen im Anbetracht menschlicher Kommunikation sind nur begrenzt wirksam. Die DeepINTEL Konferenz beschäftigt sich daher eingehend mit der Fragestellung wie man das menschliche Gehirn bzw. dessen Gedanken im Lichte von HUMINT schützen kann. Schwerwiegende Angriffe werden nach wie vor durch geschickte Vernetzung, Telefonate und Kurznachrichten vorbereitet. Speziell bei rein elektronischer Kommunikation können bestehende Vertrauensverhältnisse sehr leicht untergraben oder gar Manipulierte hergestellt werden. Dies schafft ein beträchtliches Risiko für alle Abteilungen eines Unternehmens, welche intensiv mit der Außenwelt wechselwirken - beispielsweise die Personalabteilung, der Support oder der Verkauf.

Programme und Buchung

Die DeepINTEL Security Intelligence Konferenz findet am 18. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen nach dem Programm.

Die DeepSec 2020 Konferenztage sind am 19. und 20. November direkt im Anschluss. Die DeepSec Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. November statt. Aufgrund der Beschränkungen für Anreise und eine stabilen Durchführung sind einige der Trainings virtueller Natur (Details entnehmen Sie bitte dem Programm bzw. fragen Sie direkt bei uns nach). Die Konferenz selbst wird als Hybrid-Veranstaltung ablaufen (gemischt Präsenz/virtuell, wobei alle alles sehen und hören können).

Beide Veranstaltungen werden unter COVID-19 Gesundheitsmaßnahmen durchgeführt, die wir ständig aktualisiert unter diesem Link https://deepsec.net/docs/Counter_Covid-19.pdf (https://deepsec.net/docs/Counter_Covid-19.pdf) publizieren.

Der Veranstaltungsort für die DeepSec und DeepINTEL 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. Bitte beachten Sie, dass wir aufgrund Planungssicherheit auf rechtzeitige Ticketbestellungen angewiesen sind.

(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/20200910011

pts20200910011 Technologie/Digitalisierung, Produkte/Innovationen

Industrielle Kontrollsysteme auf dem Prüfstand

DeepSec Konferenz veranstaltet Forum zur Absicherung von Industrial Control Systems (ICS)

Wien (pts011/10.09.2020/09:15) - Wer von Digitalisierung spricht, meint meistens vernetzte Steuerungs- und Messsysteme. Der damit verbundene Fachbegriff Industrial Control Systems (ICS) deckt einen weiten Bereich ab und reicht bis in die Industrie 4.0, in der die Informationssicherheit eine sehr große Rolle spielt. Das richtige Design und sicherer Code werden damit zu Teilen kritischer Infrastruktur. Die diesjährige DeepSec Sicherheitskonferenz bietet erstmals ein Forum - das ICS Village - an, in dem sich Entwicklerinnen und Sicherheitsexperten austauschen können, um Erfahrungen auszutauschen. Das erklärte Ziel ist es, Steuerungssysteme sicher zu gestalten, sie robust zu implementieren, richtig zu testen, und diese System angemessen zu schützen.

Dienstbare Geister der Infrastruktur

Kontrollsysteme und automatisierte Prozesssteuerung führen normalerweise ein unsichtbares Dasein. Fertigungsstraßen, Gebäudemanagement, Lichtsteuerung, Verkehrssysteme, Industrieanlagen oder Stromversorgung sind unverzichtbare Teile des operativen Geschäfts. Wenn alles funktioniert, dann sieht man nur den Produktionsbetrieb und die Ergebnisse. Erst wenn Fehlfunktionen auftreten, dann sieht man die tragende Rolle, die die Technologien einnehmen. Speziell die COVID-19 Pandemie hat gezeigt, dass Abläufe in Unternehmen und Organisationen selbst in Ausnahmesituationen funktionieren müssen. Da ICS aus tausenden von Komponenten bestehen kann, gibt es viele potentielle Fehlerquellen. Es gilt, da den Überblick zu behalten, sehr gut zu testen und Systeme zu entwickeln, die in Ausnahmesituationen zuverlässig Schaden verhindern müssen.

Die Digitalisierung hat in diesen Bereich schon lange Einzug gehalten. In Kontrollzentralen laufen schon lange alle Daten einer Anlage zentral sowie digital zusammen. Moderne Hardware und Software wird verwendet. Ohne Vernetzung geht es auch nicht. Allerdings lassen sich nicht beliebige Änderungen einführen, schnell anpassen oder bestehende Schnittstellen austauschen, da Systeme in diesem Bereich für den Betrieb über mehrere Dekaden ausgelegt sein müssen. Es gibt klare Standards für die interagierenden Systeme, um die Integration in klare Bahnen zu lenken.

OT - IT - Informationssicherheit

Operations Technology (OT) bezeichnet die Industriesteuerungsanlagen, die in der Produktion verwendet werden. Die darin verwendeten ICS-Komponenten kommen aufgrund der Entwicklungsgeschichte daher klassisch aus der nicht weltweit vernetzten Welt. Die moderne Informationstechnologie kommt hingegen kaum ohne das Internet aus. Verbindet man nun beide Welten, so kann man diese nicht einfach addieren.

Es bedarf eines sicheren Designs. Bestimmte Steuerungsanlagen wurden in der Vergangenheit mit Internetzugängen versehen und durch Filtersysteme abgesichert. Da zwecks Wartung Fernzugriffe nötig sein können, suchen Angreifende natürlich nach diesen - hoffentlich verschlossenen - Türen. Sicherheitsexperten haben in der Vergangenheit immer wieder Lücken im Fernzugriff gefunden. Beliebig Technologien kombinieren, kann also nicht der richtige Weg sein.

Das Rütteln an verschlossenen Türen ist aber nur der Anfang. Eingesetzter Code im ganzen Kontrollsystem, Verbindungen zu Messpunkten oder Kontrollsystemen, Netzwerkprotokolle, Speicherung von Daten, eingesetzte Hardware und vieles mehr sind ebenfalls potentielle Schwachstellen, die angegriffen werden können. Niemand rennt mit dem Kopf durch die Wand, was für Angriffe bedeutet, dass sie auch über Vertrauensverhältnisse und damit von innen kommen können. Es gilt also, Informationssicherheit gleich in das Design einzubauen. Hier setzt das ICS Village der DeepSec an, da es sich bei diesem Schritt um eine fachübergreifende Anstrengung handelt.

Interdisziplinäre Entwicklung

Im November werden Experten aus dem Bereich der Informationssicherheit, Forscherinnen und Unternehmen moderne Lösungsansätze für Industrial Control Systems während der DeepSec Konferenz vorstellen und diskutieren. Alle Anwendenden sind eingeladen, am ICS Village teilzunehmen und davon zu profitieren. Im Ausstellungsbereich finden sich Forschungsprojekte der FH Burgenland zur Verwaltung von IoT-Systemen. Darüber hinaus wird die Entwicklungsfirma sematicon AG vertreten sein, die einen starken Fokus auf Informationssicherheit und Kryptographie in Industrie, Elektronik sowie der IioT-Welt legt.

Vorgestellt wird unter anderem die Lösung se.MIS(TM) für die Wartungen von Industrieanlagen. Es handelt sich dabei um die Möglichkeit der kompletten Selbstverwaltung durch Anlagentechniker mit einem digitalen Wartungsbuch, welches sämtliche Änderungen und Zugriffe dokumentiert. Herkömmliche Fernzugriffsmethoden wie Virtual Private Networks (VPN) decken immer nur Teile der Anforderungen ab. se.MIS(TM) erlaubt den Betrieb mit eigener

Datenhoheit, lückenloser Protokollierung für spätere Audits und sicherem Zugang.

Nutzen Sie die Gelegenheit. Lassen Sie sich mit Expertenwissen verbinden. Die DeepSec Konferenz hat eine lange Tradition, Themen der Informationssicherheit konstruktiv und mit Schwerpunkt auf Verteidigung und Verbesserung zu behandeln. Profitieren Sie davon.

Programme und Buchung

Die DeepSec 2020-Konferenztage sind am 19. und 20. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. November, statt. Aufgrund der Beschränkungen für Anreise und eine stabilen Durchführung sind einiger der Trainings virtueller Natur (die Details entnehmen Sie bitte aus dem Programm bzw. fragen bei uns direkt nach). Die DeepINTEL Security Intelligence Konferenz findet am 18. November statt. Beide Veranstaltungen werden unter COVID-19 Gesundheitsmaßnahmen durchgeführt, die wir ständig aktualisiert unter diesem Link https://deepsec.net/docs/Counter_Covid-19.pdf publizieren.

Der Veranstaltungsort für die DeepSec und DeepINTEL 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. Bitte beachten Sie, dass wir aufgrund der Planungssicherheit auf rechtzeitige Ticketbestellungen angewiesen sind.

(Ende)

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

(/)

HIGHTECH

pts20200910011 Technologie/Digitalisierung, Produkte/Innovationen

Industrielle Kontrollsysteme auf dem Prüfstand

DeepSec Konferenz veranstaltet Forum zur Absicherung von Industrial Control Systems (ICS)

Maschinenraum eines Schiffes (Foto: Rémi Kaupp, 2007)

Wien (pts011/10.09.2020/09:15) - **Wer von Digitalisierung spricht, meint meistens vernetzte Steuerungs- und Messsysteme. Der damit verbundene Fachbegriff Industrial Control Systems (ICS) deckt einen weiten Bereich ab und reicht bis in die Industrie 4.0, in der die Informationssicherheit eine sehr große Rolle spielt. Das richtige Design und sicherer Code werden damit zu Teilen kritischer Infrastruktur. Die diesjährige DeepSec Sicherheitskonferenz bietet erstmals ein Forum - das ICS Village - an, in dem sich Entwicklerinnen und Sicherheitsexperten austauschen können, um Erfahrungen auszutauschen. Das erklärte Ziel ist es, Steuerungssysteme sicher zu gestalten, sie robust zu implementieren, richtig zu testen, und diese System angemessen zu schützen.**

Dienstbare Geister der Infrastruktur

Kontrollsysteme und automatisierte Prozesssteuerung führen normalerweise ein unsichtbares Dasein. Fertigungsstraßen, Gebäudemanagement, Lichtsteuerung, Verkehrssysteme, Industrieanlagen oder Stromversorgung sind unverzichtbare Teile des operativen Geschäfts. Wenn alles funktioniert, dann sieht man nur den Produktionsbetrieb und die Ergebnisse. Erst wenn Fehlfunktionen auftreten, dann sieht man die tragende Rolle, die die Technologien einnehmen. Speziell die COVID-19 Pandemie hat gezeigt, dass Abläufe in Unternehmen und Organisationen selbst in Ausnahmesituationen funktionieren müssen. Da ICS aus tausenden von Komponenten bestehen kann, gibt es viele potentielle Fehlerquellen. Es gilt, da den Überblick zu behalten, sehr gut zu testen und Systeme zu entwickeln, die in Ausnahmesituationen zuverlässig Schaden verhindern müssen.

Die Digitalisierung hat in diesen Bereich schon lange Einzug gehalten. In Kontrollzentralen laufen schon lange alle Daten einer Anlage zentral sowie digital zusammen. Moderne Hardware und Software wird verwendet. Ohne Vernetzung geht es auch nicht. Allerdings lassen sich nicht beliebige Änderungen einführen, schnell anpassen oder bestehende Schnittstellen austauschen, da Systeme in diesem Bereich für den Betrieb über mehrere Dekaden ausgelegt sein müssen. Es gibt klare Standards für die interagierenden Systeme, um die Integration in klare Bahnen zu lenken.

OT - IT - Informationssicherheit

Operations Technology (OT) bezeichnet die Industriesteuerungsanlagen, die in der Produktion verwendet werden. Die darin verwendeten ICS-Komponenten kommen aufgrund der Entwicklungsgeschichte daher klassisch aus der nicht weltweit vernetzten Welt. Die moderne Informationstechnologie kommt hingegen kaum ohne das Internet aus. Verbindet man nun beide Welten, so kann man diese nicht einfach addieren.

Es bedarf eines sicheren Designs. Bestimmte Steuerungsanlagen wurden in der Vergangenheit mit Internetzugängen versehen und durch Filtersysteme abgesichert. Da zwecks Wartung Fernzugriffe nötig sein können, suchen Angreifende natürlich nach diesen - hoffentlich verschlossenen - Türen. Sicherheitsexperten haben in der Vergangenheit immer wieder Lücken im Fernzugriff gefunden. Beliebig Technologien kombinieren, kann also nicht der richtige Weg sein.

Das Rütteln an verschlossenen Türen ist aber nur der Anfang. Eingesetzter Code im ganzen Kontrollsystem, Verbindungen zu Messpunkten oder Kontrollsystemen, Netzwerkprotokolle, Speicherung von Daten, eingesetzte Hardware und vieles mehr sind ebenfalls potentielle Schwachstellen, die angegriffen werden können. Niemand rennt mit dem Kopf durch die Wand, was für Angriffe bedeutet, dass sie auch über Vertrauensverhältnisse und damit von innen kommen können. Es gilt also, Informationssicherheit gleich in das Design einzubauen. Hier setzt das ICS Village der DeepSec an, da es sich bei diesem Schritt um eine fachübergreifende Anstrengung handelt.

Interdisziplinäre Entwicklung

Im November werden Experten aus dem Bereich der Informationssicherheit, Forscherinnen und Unternehmen moderne Lösungsansätze für Industrial Control Systems während der DeepSec Konferenz vorstellen und diskutieren. Alle Anwendenden sind eingeladen, am ICS Village teilzunehmen und davon zu profitieren. Im Ausstellungsbereich finden sich Forschungsprojekte der FH Burgenland zur Verwaltung von IoT-Systemen. Darüber hinaus wird die Entwicklungsfirma sematicon AG vertreten sein, die einen starken Fokus auf Informationssicherheit und Kryptographie in Industrie, Elektronik sowie der IioT-Welt legt.

Vorgestellt wird unter anderem die Lösung se.MIS(TM) für die Wartungen von Industrieanlagen. Es handelt sich dabei um die Möglichkeit der kompletten Selbstverwaltung durch Anlagentechniker mit einem digitalen Wartungsbuch, welches sämtliche Änderungen und Zugriffe dokumentiert. Herkömmliche Fernzugriffsmethoden wie Virtual Private Networks (VPN) decken immer nur Teile der Anforderungen ab. se.MIS(TM) erlaubt den Betrieb mit eigener Datenhoheit, lückenloser Protokollierung für spätere Audits und sicherem Zugang.

Nutzen Sie die Gelegenheit. Lassen Sie sich mit Expertenwissen verbinden. Die DeepSec Konferenz hat eine lange Tradition, Themen der Informationssicherheit konstruktiv und mit Schwerpunkt auf Verteidigung und Verbesserung zu behandeln. Profitieren Sie davon.

Programme und Buchung

Die DeepSec 2020-Konferenztage sind am 19. und 20. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. November, statt. Aufgrund der Beschränkungen für Anreise und eine stabilen Durchführung sind einiger der Trainings virtueller Natur (die Details entnehmen Sie bitte aus dem Programm bzw. fragen bei uns direkt nach). Die DeepINTEL Security Intelligence Konferenz findet am 18. November statt. Beide Veranstaltungen werden unter COVID-19 Gesundheitsmaßnahmen durchgeführt, die wir ständig aktualisiert unter diesem Link https://deepsec.net/docs/Counter_Covid-19.pdf (https://deepsec.net/docs/Counter_Covid-19.pdf) publizieren.

Der Veranstaltungsort für die DeepSec und DeepINTEL 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. Bitte beachten Sie, dass wir aufgrund der Planungssicherheit auf rechtzeitige Ticketbestellungen angewiesen sind.

(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/20200824013

pts20200824013 Technologie/Digitalisierung, Medien/Kommunikation

Intensivlehrgänge für krisensichere Digitalisierung in Wien

DeepSec-Sicherheitskonferenz geht thematisch in die Tiefe und betrachtet kritische Gefahren der IT

Wien (pts013/24.08.2020/10:05) - Die digitale Welt schläft bekanntlich nie. In den letzten Monaten hat sich gezeigt, dass Gesellschaft und Wirtschaft mehr denn je von global vernetzter Technologie abhängig sind. Die weltweite Verbreitung von SARS-CoV-2 hat der Telekommunikation einen enormen Schub gegeben. Das bereits bekannte Home Office, Telekonferenzsysteme und Internetapplikationen mussten physische Treffen überbrücken und den Austausch von Informationen ermöglichen. Im Zuge der sprunghaften ansteigenden Nutzung dieser Technologien wurden natürlich Sicherheitsprobleme entdeckt. Zoom ist ein prominentes Beispiel. Dabei wurde allerdings nur die Spitze des Eisbergs analysiert. Weltweit warten noch viele Schwachstellen auf ihre Entdeckung. Wer daher mehr Digitalisierung fordert, meint damit eigentlich Informationssicherheit. Genau aus diesem Grund möchte die Deep-Sec-Sicherheitskonferenz im November wie gewohnt dieses Thema in Wien, mit gesundheitlichen Schutzmaßnahmen, bearbeiten. Das vorläufige Programm der Veranstaltung wurde veröffentlicht und bietet spannende Themen.

Digitale Fundamente müssen Lasten tragen

Aufgrund der Maßnahmen gegen die Verbreitung von COVID-19 hatte Telekommunikation eine wichtige Aufgabe. Sie musste Geschäftsprozesse dort unterstützen, wo bisher Treffen im physischen Raum stattfanden. Das hat auch zu Diskussionen über die Informationssicherheit geführt, denn Firmen und Menschen haben Geheimnisse. Abseits der Pandemie hatte vorher beispielsweise kaum jemand verschlüsselte Gruppenvideokonferenzen thematisiert. Unterhaltungen in Gruppen sind technisch anspruchsvoll, weil mehrere Endpunkte sicher und in Echtzeit verbunden werden müssen. Der Zwang Onlinedienste zu verwenden, hat zu einer kritischen Hinterfragung der verwendeten Technologien geführt. Sicherheitstechnisch sucht man Fortschritt vergebens, wenn moderne Infrastruktur bei virtuellen Gesprächen die Sicherheit eines geschlossenen Raumes nicht ersetzt. Treffpunkte bzw. Besprechungsräume in der realen Welt haben lange Tradition - und bei Bedarf entsprechend ausgereifte Sicherheitskonzepte. Im Netz ist dies nach wie vor Neuland. Die im ersten Halbjahr geführten Diskussionen über die Sicherheit aufgrund der gezwungenen Nutzung haben das Bewusstsein für unsichere Lösungen im Alltag gestärkt. Sicherheitsexpertinnen und Sicherheitsexperten sind die Mängel aktueller Software jedoch nicht neu.

Die Eröffnung von Gabriele Kotsis, der neuen Präsidentin der Association for Computing Machinery (ACM), stellt daher auch gleich die Frage, ob die digitale Welt eine Ergänzung oder ein Ersatz für Bestehendes sein kann. Nicht alles lässt sich beliebig austauschen. Darüber hinaus wurde das Internet, was wir jetzt in alltäglichen Bereichen verwenden, ursprünglich als System zum Austausch von Informationen in der Forschung geboren. Mittlerweile erfüllt das Internet viel mehr Aufgaben als die Verteilung von virtuellen Artikeln. Videostreaming, Audio-Anwendungen, vernetzte Unterhaltung, Steuerungssysteme, Nachrichten, Zeitungen, Fahrzeugsteuerung, Telemetrie, Einkaufsstraßen und weit mehr. Frau Kotsis wird den Grat zwischen Ergänzung und Ersatz diskutieren und Wege in die Zukunft skizzieren.

Vorträge zur Weiterbildung

Das Programm der DeepSec bietet neben den Fachvorträgen mehrere Möglichkeiten der Weiterbildung an. Es gibt Präsentationen über die Sicherheit von mobilen Applikationen, das Sicherheitskonzept von Endgeräten und Einblicke in sichere Softwareentwicklung. Alle, die digitale Lösungen implementieren, werden von den Einsichten stark profitieren. Entgegen verbreiteter Meinung kann man Sicherheitslücken nicht erst nach Publikation einer Software finden und bekämpfen. Die Schutzmaßnahmen lassen sich sehr viel früher umsetzen, schon bei der Programmierung selbst. Moderne Entwicklungswerkzeuge bieten Wege, Schwachstellen frühzeitig zu erkennen und diese zu vermeiden.

Die Analyse von Bedrohungen ist ein weiterer Themenfokus. Verteidigung ist nur möglich, wenn man die Gegner kennt. Das Spektrum reicht dabei von digitaler Spionage, Analyse dokumentierter Angriffe bis hin zu systematischen Analyse von Gefahren, um diesen besser begegnen zu können. Dabei ist die Verwendung frei zugänglicher Informationen ein wichtiges Thema. Die Methode der Open Source Intelligence (OSINT) führt diese Informationen einer Klassifikation und Untersuchung zu, die in einem bestimmten Kontext bewertet werden. Der Unterschied zum rein strukturlosen Datensammeln ist die Bewertung und das richtige Zusammensetzen einzelner Puzzlestücke. Robert Sell von Trace Labs gibt in seinem Vortrag Einblick, wie man sich die richtige Vorgehensweise aneignet. Er hält dazu auch ein zweitägiges Training ab, in dem man sich im Details mit diesem Aspekt auseinandersetzen kann. Der Aufwand von OSINT ist im Vergleich zum Nutzen sehr gering, wenn man weiß wie man vorzugehen hat.

Trainings vor der Konferenz

Die DeepSec-Konferenz wird von zweitägigen Trainings begleitet, welche eine Vertiefung in die angebotenen Themengebiete ermöglichen.

Dawid Czagan richtet sich als Trainer an Entwicklerinnen und Entwickler, die moderne Applikationen von der Datenbank bis hin zur Weboberfläche entwickeln müssen.
Diese Art von Software ist sehr vielschichtig, weil sie von der Server Infrastruktur über das Netzwerk bis hin zum Endgerät Technologien einsetzt die gut verstanden werden müssen. Man nennt dieses Vorgehen daher “Full Stack Development”. Dawid Czagan zeigt mit Beispielen echter Anwendungen, wie man Schwachstellen findet und vermeidet.

Darüber hinaus finden sich Themen wie Open Hardware Hacking für das Testen von Sicherheitsmaßnahmen, Open-Source-Intelligence-Analyse, Management von Sicherheitsvorfällen und Absicherung von industriellen Steuerungssystemen im Programmangebot. Alle Schulungen konzentrieren sich auf ein Gebiet, welches in zwei Tagen intensiv bearbeitet wird. Speziell die Sicherheit von Industriesteueranlagen ist ein wichtiges Thema, weil sie auch die kritische Infrastruktur betreffen. Im OSINT-Kurs wird Robert Sell vermitteln, wie man Informationen bekommt, in Beziehung setzt und daraus Nutzen für die Sicherheit das eigene Unternehmens zieht. Während der Konferenz wird es dazu auch einen OSINT-Wettbewerb mit realem Szenario geben.

ICS - Weiterbildung für Industrie

Die Sicherheit von Industrial Control Systems (ICS) ist der Schwerpunkt des “ICS Village” zu diesjährigen DeepSec. Zusammen mit den Experten der Sematicon AG möchten wir allen, die diese Systeme entwickeln und implementieren, einen Austausch mit Expertinnen und Experten aus der Informationssicherheit ermöglichen. Das “ICS Village” dient als Forum, wo Teilnehmende sich direkt untereinander austauschen können. Die Motivation ist die Verbesserung von bestehenden und zukünftigen Designs. Implementationen zu attackieren ist zwar wichtig für die Aufdeckung von Schwachstellen, aber die Arbeit für die echte Informationssicherheit beginnt dann erst. Die DeepSec-Konferenz möchte damit einen wichtigen Beitrag zu sicherer Digitalisierung leisten.

Im Vordergrund steht der Austausch. Sicherheitskonferenzen haben oft den Ruf nur gut in Szene gesetzte Sicherheitslücken zu präsentieren. Die DeepSec-Konferenz geht seit ihrer Gründung immer einen Schritt weiter. Das Finden von Schwachstellen ist nur der erste Schritt. Es geht in Folge darum, wie man Abhilfe schafft, ähnliche Fehler vermeidet und digitale Lösungen sicher entwirft. Nachhaltigkeit ist das Gebot der Stunde, wenn Digitalisierung sicher und verlässlich sein muss. Aus diesem Grunde sind explizit Entwicklerinnen, Techniker, Sicherheitsforscherinnen, Anwender aus der Industrie und Forscherinnen angesprochen. Sicherheit darf nicht pausieren.

Programme und Buchung

Die DeepSec-2020-Konferenztage sind am 19. und 20. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. November, statt. Aufgrund der Beschränkungen für Anreise und eine stabilen Durchführung sind einige der Trainings virtueller Natur (die Details entnehmen Sie bitte aus dem Programm bzw. fragen bei uns direkt nach). Die DeepINTEL-Security-Intelligence-Konferenz findet am 18. November statt. Beide Veranstaltungen werden unter COVID-19-Gesundheitsmaßnahmen durchgeführt, die wir ständig aktualisiert unter diesem Link https://deepsec.net/docs/Counter_Covid-19.pdf publizieren.

Der Veranstaltungsort für die DeepSec- und DeepINTEL-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. Bitte beachten Sie, dass wir aufgrund Planungssicherheit auf rechtzeitige Ticketbestellungen angewiesen sind.

(Ende)

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

(/)

HIGHTECH

pts20200824013 Technologie/Digitalisierung, Medien/Kommunikation

Intensivlehrgänge für krisensichere Digitalisierung in Wien

DeepSec-Sicherheitskonferenz geht thematisch in die Tiefe und betrachtet kritische Gefahren der IT

Wien (pts013/24.08.2020/10:05) - Die digitale Welt schläft bekanntlich nie. In den letzten Monaten hat sich gezeigt, dass Gesellschaft und Wirtschaft mehr denn je von global vernetzter Technologie abhängig sind. Die weltweite Verbreitung von SARS-CoV-2 hat der Telekommunikation einen enormen Schub gegeben. Das bereits bekannte Home Office, Telekonferenzsysteme und Internetapplikationen mussten physische Treffen überbrücken und den Austausch von Informationen ermöglichen. Im Zuge der sprunghaften ansteigenden Nutzung dieser Technologien wurden natürlich Sicherheitsprobleme entdeckt. Zoom ist ein prominentes Beispiel. Dabei wurde allerdings nur die Spitze des Eisbergs analysiert. Weltweit warten noch viele Schwachstellen auf ihre Entdeckung. Wer daher mehr Digitalisierung fordert, meint damit eigentlich Informationssicherheit. Genau aus diesem Grund möchte die DeepSec-Sicherheitskonferenz im November wie gewohnt dieses Thema in Wien, mit gesundheitlichen Schutzmaßnahmen, bearbeiten. Das vorläufige Programm der Veranstaltung wurde veröffentlicht und bietet spannende Themen.

© Florian Stocker, Crowes Agency OG

Digitale Fundamente müssen Lasten tragen

Aufgrund der Maßnahmen gegen die Verbreitung von COVID-19 hatte Telekommunikation eine wichtige Aufgabe. Sie musste Geschäftsprozesse dort unterstützen, wo bisher Treffen im physischen Raum stattfanden. Das hat auch zu Diskussionen über die Informationssicherheit geführt, denn Firmen und Menschen haben Geheimnisse. Abseits der Pandemie hatte vorher beispielsweise kaum jemand verschlüsselte Gruppenvideokonferenzen thematisiert. Unterhaltungen in Gruppen sind technisch anspruchsvoll, weil mehrere Endpunkte sicher und in Echtzeit verbunden werden müssen. Der Zwang Onlinedienste zu verwenden, hat zu einer kritischen Hinterfragung der verwendeten Technologien geführt. Sicherheitstechnisch sucht man Fortschritt vergebens, wenn moderne Infrastruktur bei virtuellen Gesprächen die Sicherheit eines geschlossenen Raumes nicht ersetzt. Treffpunkte bzw. Besprechungsräume in der realen Welt haben lange Tradition - und bei Bedarf entsprechend ausgereifte Sicherheitskonzepte. Im Netz ist dies nach wie vor Neuland. Die im ersten Halbjahr geführten Diskussionen über die Sicherheit aufgrund der gezwungenen Nutzung haben das Bewusstsein für unsichere Lösungen im Alltag gestärkt. Sicherheitsexpertinnen und Sicherheitsexperten sind die Mängel aktueller Software jedoch nicht neu.

Die Eröffnung von Gabriele Kotsis, der neuen Präsidentin der Association for Computing Machinery (ACM), stellt daher auch gleich die Frage, ob die digitale Welt eine Ergänzung oder ein Ersatz für Bestehendes sein kann. Nicht alles lässt sich beliebig austauschen. Darüber hinaus wurde das Internet, was wir jetzt in alltäglichen Bereichen verwenden, ursprünglich als System zum Austausch von Informationen in der Forschung geboren. Mittlerweile erfüllt das Internet viel mehr Aufgaben als die Verteilung von virtuellen Artikeln. Videostreaming, Audio-Anwendungen, vernetzte Unterhaltung, Steuerungssysteme, Nachrichten, Zeitungen, Fahrzeugsteuerung, Telemetrie, Einkaufsstraßen und weit mehr. Frau Kotsis wird den Grat zwischen Ergänzung und Ersatz diskutieren und Wege in die Zukunft skizzieren.

Vorträge zur Weiterbildung

Das Programm der DeepSec bietet neben den Fachvorträgen mehrere Möglichkeiten der Weiterbildung an. Es gibt Präsentationen über die Sicherheit von mobilen Applikationen, das Sicherheitskonzept von Endgeräten und Einblicke in sichere Softwareentwicklung. Alle, die digitale Lösungen implementieren, werden von den Einsichten stark profitieren. Entgegen verbreiteter Meinung kann man Sicherheitslücken nicht erst nach Publikation einer Software finden und bekämpfen. Die Schutzmaßnahmen lassen sich sehr viel früher umsetzen, schon bei der Programmierung selbst. Moderne Entwicklungswerkzeuge bieten Wege, Schwachstellen frühzeitig zu erkennen und diese zu vermeiden.

Die Analyse von Bedrohungen ist ein weiterer Themenfokus. Verteidigung ist nur möglich, wenn man die Gegner kennt. Das Spektrum reicht dabei von digitaler Spionage, Analyse dokumentierter Angriffe bis hin zu systematischen Analyse von Gefahren, um diesen besser begegnen zu können. Dabei ist die Verwendung frei zugänglicher Informationen ein wichtiges Thema. Die Methode der Open Source Intelligence (OSINT) führt diese Informationen einer Klassifikation und Untersuchung zu, die in einem bestimmten Kontext bewertet werden. Der Unterschied zum rein strukturlosen Datensammeln ist die Bewertung und das richtige Zusammensetzen einzelner Puzzlestücke. Robert Sell von Trace Labs gibt in seinem Vortrag Einblick, wie man sich die richtige Vorgehensweise aneignet. Er hält dazu auch ein zweitägiges Training ab, in dem man sich im Details mit diesem Aspekt auseinandersetzen kann. Der Aufwand von OSINT ist im Vergleich zum Nutzen sehr gering, wenn man weiß wie man vorzugehen hat.

Trainings vor der Konferenz

Die DeepSec-Konferenz wird von zweitägigen Trainings begleitet, welche eine Vertiefung in die angebotenen Themengebiete ermöglichen. Dawid Czagan richtet sich als Trainer an Entwicklerinnen und Entwickler, die moderne Applikationen von der Datenbank bis hin zur Weboberfläche entwickeln müssen. Diese Art von Software ist sehr vielschichtig, weil sie von der Server Infrastruktur über das Netzwerk bis hin zum Endgerät Technologien einsetzt die gut verstanden werden müssen. Man nennt dieses Vorgehen daher "Full Stack Development". Dawid Czagan zeigt mit Beispielen echter Anwendungen, wie man Schwachstellen findet und vermeidet.

Darüber hinaus finden sich Themen wie Open Hardware Hacking für das Testen von Sicherheitsmaßnahmen, Open-Source-Intelligence-Analyse, Management von Sicherheitsvorfällen und Absicherung von industriellen Steuerungssystemen im Programmangebot. Alle Schulungen konzentrieren sich auf ein Gebiet, welches in zwei Tagen intensiv bearbeitet wird. Speziell die Sicherheit von Industriesteueranlagen ist ein wichtiges Thema, weil sie auch die kritische Infrastruktur betreffen. Im OSINT-Kurs wird Robert Sell vermitteln, wie man Informationen bekommt, in Beziehung setzt und daraus Nutzen für die Sicherheit das eigene Unternehmens zieht. Während der Konferenz wird es dazu auch einen OSINT-Wettbewerb mit realem Szenario geben.

ICS - Weiterbildung für Industrie

Die Sicherheit von Industrial Control Systems (ICS) ist der Schwerpunkt des "ICS Village" zu diesjährigen DeepSec. Zusammen mit den Experten der Sematicon AG möchten wir allen, die diese Systeme entwickeln und implementieren, einen Austausch mit Expertinnen und Experten aus der Informationssicherheit ermöglichen. Das "ICS Village" dient als Forum, wo Teilnehmende sich direkt untereinander austauschen können. Die Motivation ist die Verbesserung von bestehenden und zukünftigen Designs. Implementationen zu attackieren ist zwar wichtig für die Aufdeckung von Schwachstellen, aber die Arbeit für die echte Informationssicherheit beginnt dann erst. Die DeepSec-Konferenz möchte damit einen wichtigen Beitrag zu sicherer Digitalisierung leisten.

Im Vordergrund steht der Austausch. Sicherheitskonferenzen haben oft den Ruf nur gut in Szene gesetzte Sicherheitslücken zu präsentieren. Die DeepSec-Konferenz geht seit ihrer Gründung immer einen Schritt weiter. Das Finden von Schwachstellen ist nur der erste Schritt. Es geht in Folge darum, wie man Abhilfe schafft, ähnliche Fehler vermeidet und digitale Lösungen sicher entwirft. Nachhaltigkeit ist das Gebot der Stunde, wenn Digitalisierung sicher und verlässlich sein muss. Aus diesem Grunde sind explizit Entwicklerinnen, Techniker, Sicherheitsforscherinnen, Anwender aus der Industrie und Forscherinnen angesprochen. Sicherheit darf nicht pausieren.

Programme und Buchung

Die DeepSec-2020-Konferenztage sind am 19. und 20. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. November, statt. Aufgrund der Beschränkungen für Anreise und eine stabilen Durchführung sind einige der Trainings virtueller Natur (die Details entnehmen Sie bitte aus dem Programm bzw. fragen bei uns direkt nach). Die DeepINTEL-Security-Intelligence-Konferenz findet am 18. November statt. Beide Veranstaltungen werden unter COVID-19-Gesundheitsmaßnahmen durchgeführt, die wir ständig aktualisiert unter diesem Link https://deepsec.net/docs/Counter_Covid-19.pdf (https://deepsec.net/docs/Counter_Covid-19.pdf) publizieren.

Der Veranstaltungsort für die DeepSec- und DeepINTEL-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. Bitte beachten Sie, dass wir aufgrund Planungssicherheit auf rechtzeitige Ticketbestellungen angewiesen sind.

(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/20200717009

pts20200717009 Technologie/Digitalisierung, Medien/Kommunikation

Digitale Infrastruktur soll Schadsoftware integrieren

Deutsche Bundesregierung möchte Internet-Provider zur Installation von Staatstrojanern zwingen

Wien (pts009/17.07.2020/09:00) - Seit den 1990er Jahren tobt ein ständiger Kampf zwischen Behörden und Sicherheitsexperten. Eine Seite möchte digitale Infrastruktur, allen voran den Datentransport und die Kommunikation, möglichst sicher für Wirtschaft und Gesellschaft gestalten. Die andere Seite bemüht sich stets um Hintertüren zum Abfangen von Daten und Korrespondenz. Der Kampf um Zugriff auf sichere Datentransmissionen, ursprünglich als “Crypto Wars” tituliert, geht in die nächste Runde. Die deutsche Bundesregierung hat einen Gesetzesentwurf erstellt, welcher Internet-Provider und Firmen mit verwandter Tätigkeit gesetzlich zum Verteilen von Schadsoftware und Manipulation von Netzwerkverkehr zwingen soll. Künftig können also die Installation von Apps auf dem Smartphone oder automatische Software-Updates Computersysteme kompromittieren. Damit wird die Grundlage der Digitalisierung zerstört - mit weitreichenden Folgen für Gesellschaft und Wirtschaft.

Das Öl des 21. Jahrhunderts schürt Gier

Daten sind nach stark vereinfachten Slogans das Öl des 21. Jahrhunderts. Der Vergleich hinkt, denn aus Daten lässt sich keine Energie gewinnen; sie verbrauchen bloß Energie. Beim deutschen Gesetzesentwurf geht es aber nicht um den wirtschaftlichen Nutzen. Das Gegenteil ist der Fall. An der Oberfläche wird diskutiert, dass Ermittlungsbehörden Zugriff auf Kommunikation zwischen Personen und auf lokalen Geräten gespeicherte Daten benötigen. Die Dokumentation staatlicher Maßnahmen zur Spionage durch Edward Snowden hab in den letzten 7 Jahren zu weitreichenden Verbesserungen in der Informationstechnologie geführt. Die Verschlüsselung der eigenen Daten wurde in vielen Produkten nachgerüstet.

Darüber hinaus haben Unternehmen sowie Privatpersonen ihre Korrespondenz und Kommunikation zunehmend auf verschlüsselte Wege umgestellt. Kritischster Punkt bei der Implementation ist die sogenannte Ende-zu-Ende-Verschlüsselung (“E2E Encryption”). Wirklich sicher sind kryptografische Methoden nur, wenn es keine Hintertür - in Form eines Nachschlüssels - oder keine Möglichkeit zum Erraten des bzw. der Schlüssel gibt.

Die Hersteller der Smartphone-Betriebssysteme, die Methoden der Softwareentwicklung und die Internet Engineering Task Force (IETF) haben basierend auf Snowdens Enthüllungen sehr viele Verbesserungen in Protokolle und

Algorithmen eingebaut. Beispielsweise hat die IETF entgegen starkem Widerstand von Lobbyisten bei der Spezifizierung der neuen Transport Layer Security (TLS) Version 1.3 darauf geachtet, keine unsicheren Methoden mehr zuzulassen.

TLS ist die Basis für verschlüsselte Webseiten (erkennbar am HTTPS). Es ist damit die Grundlage von Telebanking, Webshops, Kommunikation mit Behörden, Portalen, E-Mail-Verkehr, Videostreaming, Telekonferenzen und vielem mehr. Alle modernen Systeme unterstützen mittlerweile Ende-zu-Ende-Verschlüsselung. Genau dies ist die Motivation für den Gesetzesvorschlag, um Hintertüren für all diese Anwendungsbereiche zu fordern.

Weltweiter Angriff gegen E2E

Deutschland ist mit dem Angriff gegen sichere Systeme nicht alleine. In den USA hat der republikanische Senator Lindsey Graham einen Gesetzesentwurf eingebracht, welcher sichere Verschlüsselung in Chatsystemen und Messengern verbietet. Das Verbot ist, wie so oft, nur indirekt ausgedrückt. Man verlangt den Zugang zu den übermittelten und gespeicherten Daten durch Dritte. Diese Formulierung ändert nicht den Zweck. Sowohl ein digitaler Angriff als auch die Bereitstellung der Daten gemäß offiziellen Anfragen sind technisch ein und dieselbe Vorgehensweise. Man schwächt tatsächlich mit diesen Gesetzen die Informationssicherheit generell. Der deutsche Gesetzesentwurf sieht beispielsweise vor, dass Schadsoftware über manipulierte Softwareupdates an Endgeräte geliefert wird.

Abgesehen von den technischen Aspekten gibt es ungelöste rechtliche Konsequenzen. Wer haftet für Schäden, die Staatstrojaner anrichten? Wer trägt die Verantwortung, wenn dieser Mechanismus von Kriminellen ausgenutzt wird? Diese Sollbruchstellen der Sicherheit würden dann für alle Bereiche gelten - vom Krankenhaus über Firmen bis hin zu Privathaushalten. Man schafft de facto Informationssicherheit national ab.

Infrastruktur, sei es digital oder analog, wird immer Teil von legalen und illegalen Aktivitäten sein. Autobahnen werden sowohl von Rettungsdiensten als auch für den Transport gestohlener Güter verwendet. Dasselbe gilt für die Stromversorgung, das Internet, die Wasserversorgung, Verkehr, Transport, Lebensmittelversorgung, das Bankenwesen oder Telefonie. Dennoch sind Kommunikationsnetzwerke im Blickpunkt.

Die aktuellen Gesetzesentwürfe zeigen, wie wenig man von der Geschichte der Überwachung und der analogen Welt versteht. Die US-Regierung hat in den 1990er Jahren die Überwachung von Mobilfunknetzen rechtlich und technisch implementiert. Der Anlass war das Vorgehen gegen organisierte Kriminalität, allen voran den Drogenschmuggel.

Der Effekt war, dass die organisierte Kriminalität auf alternative Kommunikationsmethoden ausgewichen ist. Der Schaden bleibt denen, die sich nicht selbst schützen können und Schutzbedarf haben. Im konkreten Fall wird es die eigenen Bürgerinnen, Bürger und Unternehmen treffen, die der Staat eigentlich mit gesetzlichem Auftrag schützen muss.

Einfallstor für Wirtschaftsspionage

Der systematische Einbau von Hintertüren und der Abbau von Sicherheitsmaßnahmen hat noch wesentlich weitreichendere Folgen. Die seit Jahren andauernde Diskussion über die kommende 5G-Technologie zeigt es deutlich. Der Firma Huawei wird von den USA vorgeworfen ihre 5G-Produkte mit nicht dokumentierten Zugriffsmöglichkeiten auf die Mobilfunknetzwerke auszuliefern. Im Brennpunkt ist der Vorwurf der Spionage. Im gleichen Atemzug entwerfen westliche Regierungen Gesetze, um die eigene digitale Infrastruktur zu schwächen und Dritten uneingeschränkten Zugang zu den Daten zu gewähren. Selbst die österreichische Bundesregierung hat die Prüfung des Einsatzes von staatlicher Schadsoftware zur Überwachung im Regierungsprogramm.

Und es bleibt nicht bei nur nationalen Anstrengungen. Ein Dokument aus dem EU-Ministerrat datiert mit 8. Mai 2020 beschreibt die Strategie für Europa. Dort werden verschlüsselte Datenträger, Ende-zu-Ende Verschlüsselung, plattformübergreifende Verschlüsselung, selbst entwickelte Software und verschlüsselte Internetprotokolle als kritische Barriere für Behördenermittlungen angeführt. Genau diese Komponenten sind allerdings das Fundament einer implementierten Informationssicherheit.

Der Verzicht auf grundlegenden Technologien, um Daten und Korrespondenz zu sichern, basiert auf den mathematischen Methoden der Kryptografie. Sie sind aus moderner IT Infrastruktur - sowohl bei Behörden als auch bei Unternehmen - nicht wegzudenken.

Rückkehr zur Realität

Personen benötigen Privatsphäre, daher haben sie rechtlichen Anspruch darauf. Unternehmen benötigen Rechtssicherheit für ihre Projekte, Produkte und Dienstleistungen. Das schließt jegliche Kommunikation mit ein. Fernarbeit und Telekonferenzsysteme sind durch Covid-19 Schutzmaßnahmen zu kritischen Werkzeugen geworden. Auch Betreiber von Rechenzentren dürfen nicht gezwungen werden, Hintertüren in Systeme einbauen zu müssen. Rechtlich angeordnetes Aushebeln von Sicherheitsstandards gefährdet darüber hinaus Europa als Technologiestandort.

Britische und australische Gesetze haben schon dafür gesorgt, dass man aufgrund von rechtlich vorgeschriebenen Zugriffen durch Dritte Softwareprodukte, die in diesen Ländern entwickelt wurden, nicht sicher einsetzen kann.

Die Diskussion behandelt einen wichtigen Aspekt, den Ermittlungsbehörden und Sicherheitsexperten teilen, in keinster Weise. Auch die Informationssicherheit muss sich gegen Angriffe verteidigen und muss Hinweise auf kompromittierte Systeme finden. Dennoch setzen Firmen auf starke Verschlüsselung. Das ist kein Widerspruch. Auf der diesjährigen DeepSec In-Depth Security Konferenz im November werden wieder Ansätze besprochen und Erfahrungen ausgetauscht. Kryptografie ist ein fundamentales Thema und muss ohne Hintertüren Teil sicherer Infrastruktur bleiben.

Pikantes Detail am Rande: Das deutsche Bundesland Schleswig-Holstein und die deutsche Bundeswehr möchten die Freie Software Matrix für ihre Kommunikation nutzen. Letztere möchte Matrix explizit für Nachrichten verwenden, die Verschlusssache sind. Da stellt sich die berechtigte Frage, wie der konzertierte Angriff auf IT-Sicherheit anderer Behörden ins Bild passt.

Programme und Buchung

Die DeepSec 2020 Konferenztage sind am 19. und 20. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. November, statt. Die DeepINTEL Security Intelligence Konferenz findet am 18. 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. Bitte beachten Sie, dass wir aufgrund Planungssicherheit auf rechtzeitige Ticketbestellungen angewiesen sind.
(Ende)

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

(/)

BUSINESS

pts20200717009 Technologie/Digitalisierung, Medien/Kommunikation

Digitale Infrastruktur soll Schadsoftware integrieren

Deutsche Bundesregierung möchte Internet-Provider zur Installation von Staatstrojanern zwingen

Historischer Clipper-Chip der NSA (Foto: Travis Goodspeed)

Wien (pts009/17.07.2020/09:00) - **Seit den 1990er Jahren tobt ein ständiger Kampf zwischen Behörden und Sicherheitsexperten. Eine Seite möchte digitale Infrastruktur, allen voran den Datentransport und die Kommunikation, möglichst sicher für Wirtschaft und Gesellschaft gestalten. Die andere Seite bemüht sich stets um Hintertüren zum Abfangen von Daten und Korrespondenz. Der Kampf um Zugriff auf sichere Datentransmissionen, ursprünglich als "Crypto Wars" tituliert, geht in die nächste Runde. Die deutsche Bundesregierung hat einen Gesetzesentwurf erstellt, welcher Internet-Provider und Firmen mit verwandter Tätigkeit gesetzlich zum Verteilen von Schadsoftware und Manipulation von Netzwerkverkehr zwingen soll. Künftig können also die Installation von Apps auf dem Smartphone oder automatische Software-Updates Computersysteme kompromittieren. Damit wird die Grundlage der Digitalisierung zerstört - mit weitreichenden Folgen für Gesellschaft und Wirtschaft.**

Das Öl des 21. Jahrhunderts schürt Gier

Daten sind nach stark vereinfachten Slogans das Öl des 21. Jahrhunderts. Der Vergleich hinkt, denn aus Daten lässt sich keine Energie gewinnen; sie verbrauchen bloß Energie. Beim deutschen Gesetzesentwurf geht es aber nicht um den wirtschaftlichen Nutzen. Das Gegenteil ist der Fall. An der Oberfläche wird diskutiert, dass Ermittlungsbehörden Zugriff auf Kommunikation zwischen Personen und auf lokalen Geräten gespeicherte Daten benötigen. Die Dokumentation staatlicher Maßnahmen zur Spionage durch Edward Snowden hab in den letzten 7 Jahren zu weitreichenden Verbesserungen in der Informationstechnologie geführt. Die Verschlüsselung der eigenen Daten wurde in vielen Produkten nachgerüstet.

Darüber hinaus haben Unternehmen sowie Privatpersonen ihre Korrespondenz und Kommunikation zunehmend auf verschlüsselte Wege umgestellt. Kritischster Punkt bei der Implementation ist die sogenannte Ende-zu-Ende-Verschlüsselung ("E2E Encryption"). Wirklich sicher sind kryptografische Methoden nur, wenn es keine Hintertür - in Form eines Nachschlüssels - oder keine Möglichkeit zum Erraten des bzw. der Schlüssel gibt.

Die Hersteller der Smartphone-Betriebssysteme, die Methoden der Softwareentwicklung und die Internet Engineering Task Force (IETF) haben basierend auf Snowdens Enthüllungen sehr viele Verbesserungen in Protokolle und Algorithmen eingebaut. Beispielsweise hat die IETF entgegen starkem Widerstand von Lobbyisten bei der Spezifizierung der neuen Transport Layer Security (TLS) Version 1.3 darauf geachtet, keine unsicheren Methoden mehr zuzulassen.

TLS ist die Basis für verschlüsselte Webseiten (erkennbar am HTTPS). Es ist damit die Grundlage von Telebanking, Webshops, Kommunikation mit Behörden, Portalen, E-Mail-Verkehr, Videostreaming, Telekonferenzen und vielem mehr. Alle modernen Systeme unterstützen mittlerweile Ende-zu-Ende-Verschlüsselung. Genau dies ist die Motivation für den Gesetzesvorschlag, um Hintertüren für all diese Anwendungsbereiche zu fordern.

Weltweiter Angriff gegen E2E

Deutschland ist mit dem Angriff gegen sichere Systeme nicht alleine. In den USA hat der republikanische Senator Lindsey Graham einen Gesetzesentwurf eingebracht, welcher sichere Verschlüsselung in Chatsystemen und Messengern verbietet. Das Verbot ist, wie so oft, nur indirekt ausgedrückt. Man verlangt den Zugang zu den übermittelten und gespeicherten Daten durch Dritte. Diese Formulierung ändert nicht den Zweck. Sowohl ein digitaler Angriff als auch die Bereitstellung der Daten gemäß offiziellen Anfragen sind technisch ein und dieselbe Vorgehensweise. Man schwächt tatsächlich mit diesen Gesetzen die Informationssicherheit generell. Der deutsche Gesetzesentwurf sieht beispielsweise vor, dass Schadsoftware über manipulierte Softwareupdates an Endgeräte geliefert wird.

Abgesehen von den technischen Aspekten gibt es ungelöste rechtliche Konsequenzen. Wer haftet für Schäden, die Staatstrojaner anrichten? Wer trägt die Verantwortung, wenn dieser Mechanismus von Kriminellen ausgenutzt wird? Diese Sollbruchstellen der Sicherheit würden dann für alle Bereiche gelten - vom Krankenhaus über Firmen bis hin zu Privathaushalten. Man schafft de facto Informationssicherheit national ab.

Infrastruktur, sei es digital oder analog, wird immer Teil von legalen und illegalen Aktivitäten sein. Autobahnen werden sowohl von Rettungsdiensten als auch für den Transport gestohlener Güter verwendet. Dasselbe gilt für die Stromversorgung, das Internet, die Wasserversorgung, Verkehr, Transport, Lebensmittelversorgung, das Bankenwesen oder Telefonie. Dennoch sind Kommunikationsnetzwerke im Blickpunkt.

Die aktuellen Gesetzesentwürfe zeigen, wie wenig man von der Geschichte der Überwachung und der analogen Welt versteht. Die US-Regierung hat in den 1990er Jahren die Überwachung von Mobilfunknetzen rechtlich und technisch implementiert. Der Anlass war das Vorgehen gegen organisierte Kriminalität, allen voran den Drogenschmuggel. Der Effekt war, dass die organisierte Kriminalität auf alternative Kommunikationsmethoden ausgewichen ist. Der Schaden bleibt denen, die sich nicht selbst schützen können und Schutzbedarf haben. Im konkreten Fall wird es die eigenen Bürgerinnen, Bürger und Unternehmen treffen, die der Staat eigentlich mit gesetzlichem Auftrag schützen muss.

Einfallstor für Wirtschaftsspionage

Der systematische Einbau von Hintertüren und der Abbau von Sicherheitsmaßnahmen hat noch wesentlich weitreichendere Folgen. Die seit Jahren andauernde Diskussion über die kommende 5G-Technologie zeigt es deutlich. Der Firma Huawei wird von den USA vorgeworfen ihre 5G-Produkte mit nicht dokumentierten Zugriffsmöglichkeiten auf die Mobilfunknetzwerke auszuliefern. Im Brennpunkt ist der Vorwurf der Spionage. Im gleichen Atemzug entwerfen westliche Regierungen Gesetze, um die eigene digitale Infrastruktur zu schwächen und Dritten uneingeschränkten Zugang zu den Daten zu gewähren. Selbst die österreichische Bundesregierung hat die Prüfung des Einsatzes von staatlicher Schadsoftware zur Überwachung im Regierungsprogramm.

Und es bleibt nicht bei nur nationalen Anstrengungen. Ein Dokument aus dem EU-Ministerrat datiert mit 8. Mai 2020 beschreibt die Strategie für Europa. Dort werden verschlüsselte Datenträger, Ende-zu-Ende Verschlüsselung, plattformübergreifende Verschlüsselung, selbst entwickelte Software und verschlüsselte Internetprotokolle als kritische Barriere für Behördenermittlungen angeführt. Genau diese Komponenten sind allerdings das Fundament einer implementierten Informationssicherheit.

Der Verzicht auf grundlegenden Technologien, um Daten und Korrespondenz zu sichern, basiert auf den mathematischen Methoden der Kryptografie. Sie sind aus moderner IT Infrastruktur - sowohl bei Behörden als auch bei Unternehmen - nicht wegzudenken.

Rückkehr zur Realität

Personen benötigen Privatsphäre, daher haben sie rechtlichen Anspruch darauf. Unternehmen benötigen Rechtssicherheit für ihre Projekte, Produkte und Dienstleistungen. Das schließt jegliche Kommunikation mit ein. Fernarbeit und Telekonferenzsysteme sind durch Covid-19 Schutzmaßnahmen zu kritischen Werkzeugen geworden. Auch Betreiber von Rechenzentren dürfen nicht gezwungen werden, Hintertüren in Systeme einbauen zu müssen.

Rechtlich angeordnetes Aushebeln von Sicherheitsstandards gefährdet darüber hinaus Europa als Technologiestandort. Britische und australische Gesetze haben schon dafür gesorgt, dass man aufgrund von rechtlich vorgeschriebenen Zugriffen durch Dritte Softwareprodukte, die in diesen Ländern entwickelt wurden, nicht sicher einsetzen kann.

Die Diskussion behandelt einen wichtigen Aspekt, den Ermittlungsbehörden und Sicherheitsexperten teilen, in keinster Weise. Auch die Informationssicherheit muss sich gegen Angriffe verteidigen und muss Hinweise auf kompromittierte Systeme finden. Dennoch setzen Firmen auf starke Verschlüsselung. Das ist kein Widerspruch. Auf der diesjährigen DeepSec In-Depth Security Konferenz im November werden wieder Ansätze besprochen und Erfahrungen ausgetauscht. Kryptografie ist ein fundamentales Thema und muss ohne Hintertüren Teil sicherer Infrastruktur bleiben.

Pikantes Detail am Rande: Das deutsche Bundesland Schleswig-Holstein und die deutsche Bundeswehr möchten die Freie Software Matrix für ihre Kommunikation nutzen. Letztere möchte Matrix explizit für Nachrichten verwenden, die Verschlusssache sind. Da stellt sich die berechtigte Frage, wie der konzertierte Angriff auf IT-Sicherheit anderer Behörden ins Bild passt.

Programme und Buchung

Die DeepSec 2020 Konferenztage sind am 19. und 20. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. November, statt. Die DeepINTEL Security Intelligence Konferenz findet am 18. 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. Bitte beachten Sie, dass wir aufgrund Planungssicherheit auf rechtzeitige Ticketbestellungen angewiesen sind.

(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/20200710007

pts20200710007 Technologie/Digitalisierung, Produkte/Innovationen

Digitalisierung ohne Informationssicherheit hat keine Zukunft

DeepSec Konferenz warnt vor unsicherer Software und mangelnden Kenntnissen der Fachkräfte

Wien (pts007/10.07.2020/09:05) - Die Monate, in denen wir die Auswirkungen diverser Quarantänemaßnahmen auf unseren Alltag kennenlernen durften, haben der Bedeutung der Informationstechnologie entschieden Nachdruck verliehen. Zwar ist das Internet schon lange in vielen Branchen integraler Bestandteil von Beruf und Alltag, aber die physischen Beschränkungen aufgrund der Covid-19-Pandemie hätten ohne moderne Telekommunikation noch wesentlich einschneidender für Behörden, die Wirtschaft und die Gesellschaft sein können. Audio-, Video- und Chat-Plattformen haben Schlimmes verhindert. Dem Ruf nach mehr Digitalisierung fehlt allerdings die wichtigste Zutat - die Informationssicherheit.

Publizierte Software ist sicher, oder?

In der Welt der Softwareentwicklung gibt es den inoffiziellen Spruch, dass ein Produkt fertig ist, wenn man es installieren kann. Der Rest ergebe sich ja dann im Betrieb. Das mag nicht die Regel sein. Einige Branchen betreiben sehr gewissenhafte Qualitätssicherung. Oft ist die Popularität der Feind der Qualität. Die Verbreitung von Software ist leider keine geeignete Metrik für die Inhalte. Im Falle der Telekonferenzplattform Zoom konnte man auch gut erkennen, dass dieses Produkt eigentlich für einen ganz anderen Zweck bzw. eine andere Zielgruppe gedacht war.

Darüber hinaus sind Fehler in Software gängig und lassen sich nur mit sorgfältigen Tests, Prozessen zum Aufspüren von Fehlfunktionen und Feedbackschleifen zurück zum Code beseitigen. Dieser Weg bedarf Zeit, die Startups nicht unbedingt haben. Als Folge daraus ist der Stand der Sicherheit in publizierter bzw. verfügbarer Software bestenfalls unbekannt.

Bevor ein Programm zur Verfügung stehen kann, muss es Design, Prototypen und schließlich eine Implementation geben. Erste Voraussetzung ist das sogenannte Secure Design. Werden am Anfang grundlegende Fehler gemacht, so kann die spätere Implementation daran nichts mehr ändern. Bildlich gesprochen kann ein Auto mit einer Bambuskarosserie bestimmten Herausforderungen nie genügen. Bei Software ist es genau so.

Die zweite Voraussetzung ist das Secure Coding, also das Programmieren mit Methoden, die Fehler in der Software minimieren. Das ist die Theorie. Die Praxis sieht anders aus.

Secure Design und Coding sind nicht optional

Secure Design/Coding sind keine Features, welche sich leicht ein- oder ausschalten lassen. Man hat sie entweder berücksichtig, oder sie fehlen. Einen Mittelweg gibt es nicht. Darüber hinaus bietet eine sichere Software gegenüber der gleichartigen, schneller entwickelten, beliebteren und günstigeren Lösung auf den ersten Blick keine unmittelbaren Vorteile. Der Code funktioniert ja in beiden Fällen. Der Unterschied kommt erst in Ausnahmesituationen zum Vorschein. Psychologisch sind Vorteile, die man im normalen Betrieb nie sieht, sehr schwer zu bewerben.

Im Falle von Zoom war es zwar einfach, auf die Verfehlungen im Bereich der sicheren Implementation hinzuweisen, aber die Schwächen waren vorher ohne kritisches Hinterfragen weltweit bei allen Installationen in täglicher Verwendung. Es wurden zu wenig Fragen gestellt. Dasselbe Problem findet sich vielfach in Wohnzimmern und Büros weltweit. Ganze Wirtschaftszweige verlassen sich auf Produkte, die sehr komplex sind, über Netzwerke wechselwirken und möglicherweise nie für die Aufgaben, die sie heute verrichten, gedacht waren. Dokumenterstellung und -verarbeitung ist ein weiteres verbreitetes Beispiel.

“Digitalisierung!” rufen und Ausbildung stützen!

Um die Digitalisierung mit Informationssicherheit zu versehen, läuft man in ein didaktisches Dilemma. Methoden der sicheren Softwareentwicklung und des sicheren Designs kann man erst lernen, wenn man ein Grundverständnis von der Funktionsweise von Computern, gängigen Programmiersprachen (Plural, also mehr als eine), Netzwerkprotokollen und Betriebssystemen hat. Ohne Vorwissen lassen sich die grundlegenden Prinzipien nicht erfassen. Aus diesem Grund sind Themen der IT-Security fast ausschließlich Wahlfächer, die man nach seiner Grundausbildung belegt. Die Praxis in Unternehmen bestätigt dies.

Laut Recruitern großer Tech-Firmen aus dem Silicon Valley müssen Sicherheitsspezialisten in mindesten drei verschiedenen Bereichen mehrere Jahre lang gearbeitet haben, um überhaupt für eine Stelle in der Informationssicherheit in Betracht zu kommen. Dieser Ansatz verläuft komplett diametral zur Ausrichtung vieler Ausbildungsstätten. Der viel beschworene Fachkräftemangel im Bereich der Digitalisierung hat oft Ausgebildete zum Ergebnis, die in Rekordzeit wenig gelernt haben - gesehen vom Standpunkt der Sicherheit aus.

Eine erfolgreiche Digitalisierung bedingt daher eine solide und nachhaltige Ausbildung von Programmiererinnen und Programmierern sowie allen weiteren Spezialisten und Spezialistinnen im Prozess der Softwareentwicklung. Bits und Bytes ständig zu erwähnen, das Internet zu verwenden oder dauernd die Allmacht der Apps zu beschwören ist nicht ausreichend für eine sichere Zukunft. In der IT-Sicherheit ist Oberflächlichkeit keine Tugend.

DeepSec 2020 im Zeichen der Wissenschaft

Die diesjährige DeepSec In-Depth Security Konferenz möchte ihren Beitrag an einer informationssicheren Digitalisierung stellen. Es wird Fachvorträge, Trainings und Austausch von Expertinnen und Experten geben. Der Zweck ist die Weiterbildung von Fachpersonen in der Informationstechnologie, um zukünftig die bestehende Hardware und Software sicher zu gestalten. Das Angebot richtet sich an die Tätigkeitsbereiche Produktentwicklung, Softwareentwicklung, Geschäftführung, Systemadministration, Forschung und Lehre. Zusätzlich wird ein Internet of Things (IoT) Hacking Village zusammen mit Partnern aufgebaut. Man kann sich direkt mit Expertinnen und Experten austauschen und sehen, dass viele Smart Systeme alles andere als sicher sind.

Programme und Buchungen

Die DeepSec 2020 Konferenztage sind am 19. und 20. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. November statt. Die DeepINTEL Security Intelligence Konferenz findet am 18. 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. Bitte beachten Sie, dass wir aufgrund Planungssicherheit auf rechtzeitige Ticketbestellungen angewiesen sind.
(Ende)

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

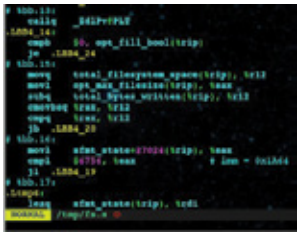
(/)

HIGHTECH

pts20200710007 Technologie/Digitalisierung, Produkte/Innovationen

Digitalisierung ohne Informationssicherheit hat keine Zukunft

DeepSec Konferenz warnt vor unsicherer Software und mangelnden Kenntnissen der Fachkräfte



Codefragment aus Secure Coding Curriculum (Copyright: René Pfeiffer)

Wien (pts007/10.07.2020/09:05) - **Die Monate, in denen wir die Auswirkungen diverser Quarantänemaßnahmen auf unseren Alltag kennenlernen durften, haben der Bedeutung der Informationstechnologie entschieden Nachdruck verliehen. Zwar ist das Internet schon lange in vielen Branchen integraler Bestandteil von Beruf und Alltag, aber die physischen Beschränkungen aufgrund der Covid-19-Pandemie hätten ohne moderne Telekommunikation noch wesentlich einschneidender für Behörden, die Wirtschaft und die Gesellschaft sein können. Audio-, Video- und Chat-Plattformen haben Schlimmes verhindert. Dem Ruf nach mehr Digitalisierung fehlt allerdings die wichtigste Zutat - die Informationssicherheit.**

Publizierte Software ist sicher, oder?

In der Welt der Softwareentwicklung gibt es den inoffiziellen Spruch, dass ein Produkt fertig ist, wenn man es installieren kann. Der Rest ergebe sich ja dann im Betrieb. Das mag nicht die Regel sein. Einige Branchen betreiben sehr gewissenhafte Qualitätssicherung. Oft ist die Popularität der Feind der Qualität. Die Verbreitung von Software ist leider keine geeignete Metrik für die Inhalte. Im Falle der Telekonferenzplattform Zoom konnte man auch gut erkennen, dass dieses Produkt eigentlich für einen ganz anderen Zweck bzw. eine andere Zielgruppe gedacht war.

Darüber hinaus sind Fehler in Software gängig und lassen sich nur mit sorgfältigen Tests, Prozessen zum Aufspüren von Fehlfunktionen und Feedbackschleifen zurück zum Code beseitigen. Dieser Weg bedarf Zeit, die Start-ups nicht unbedingt haben. Als Folge daraus ist der Stand der Sicherheit in publizierter bzw. verfügbarer Software bestenfalls unbekannt.

Bevor ein Programm zur Verfügung stehen kann, muss es Design, Prototypen und schließlich eine Implementation geben. Erste Voraussetzung ist das sogenannte Secure Design. Werden am Anfang grundlegende Fehler gemacht, so kann die spätere Implementation daran nichts mehr ändern. Bildlich gesprochen kann ein Auto mit einer Bambuskarosserie bestimmten Herausforderungen nie genügen. Bei Software ist es genau so. Die zweite Voraussetzung ist das Secure Coding, also das Programmieren mit Methoden, die Fehler in der Software minimieren. Das ist die Theorie. Die Praxis sieht anders aus.

Secure Design und Coding sind nicht optional

Secure Design/Coding sind keine Features, welche sich leicht ein- oder ausschalten lassen. Man hat sie entweder berücksichtig, oder sie fehlen. Einen Mittelweg gibt es nicht. Darüber hinaus bietet eine sichere Software gegenüber der gleichartigen, schneller entwickelten, beliebteren und günstigeren Lösung auf den ersten Blick keine unmittelbaren Vorteile. Der Code funktioniert ja in beiden Fällen. Der Unterschied kommt erst in Ausnahmesituationen zum Vorschein. Psychologisch sind Vorteile, die man im normalen Betrieb nie sieht, sehr schwer zu bewerben.

Im Falle von Zoom war es zwar einfach, auf die Verfehlungen im Bereich der sicheren Implementation hinzuweisen, aber die Schwächen waren vorher ohne kritisches Hinterfragen weltweit bei allen Installationen in täglicher Verwendung. Es wurden zu wenig Fragen gestellt. Dasselbe Problem findet sich vielfach in Wohnzimmern und Büros weltweit. Ganze Wirtschaftszweige verlassen sich auf Produkte, die sehr komplex sind, über Netzwerke wechselwirken und möglicherweise nie für die Aufgaben, die sie heute verrichten, gedacht waren. Dokumenterstellung und -verarbeitung ist ein weiteres verbreitetes Beispiel.

"Digitalisierung!" rufen und Ausbildung stützen!

Um die Digitalisierung mit Informationssicherheit zu versehen, läuft man in ein didaktisches Dilemma. Methoden der sicheren Softwareentwicklung und des sicheren Designs kann man erst lernen, wenn man ein Grundverständnis von der Funktionsweise von Computern, gängigen Programmiersprachen (Plural, also mehr als eine), Netzwerkprotokollen und Betriebssystemen hat. Ohne Vorwissen lassen sich die grundlegenden Prinzipien nicht erfassen. Aus diesem Grund sind Themen der IT-Security fast ausschließlich Wahlfächer, die man nach seiner Grundausbildung belegt. Die Praxis in Unternehmen bestätigt dies.

Laut Recruitern großer Tech-Firmen aus dem Silicon Valley müssen Sicherheitsspezialisten in mindesten drei verschiedenen Bereichen mehrere Jahre lang gearbeitet haben, um überhaupt für eine Stelle in der Informationssicherheit in Betracht zu kommen. Dieser Ansatz verläuft komplett diametral zur Ausrichtung vieler Ausbildungsstätten. Der viel beschworene Fachkräftemangel im Bereich der Digitalisierung hat oft Ausgebildete zum Ergebnis, die in Rekordzeit wenig gelernt haben - gesehen vom Standpunkt der Sicherheit aus.

Eine erfolgreiche Digitalisierung bedingt daher eine solide und nachhaltige Ausbildung von Programmiererinnen und Programmierern sowie allen weiteren Spezialisten und Spezialistinnen im Prozess der Softwareentwicklung. Bits und Bytes ständig zu erwähnen, das Internet zu verwenden oder dauernd die Allmacht der Apps zu beschwören ist nicht ausreichend für eine sichere Zukunft. In der IT-Sicherheit ist Oberflächlichkeit keine Tugend.

DeepSec 2020 im Zeichen der Wissenschaft

Die diesjährige DeepSec In-Depth Security Konferenz möchte ihren Beitrag an einer informationssicheren Digitalisierung stellen. Es wird Fachvorträge, Trainings und Austausch von Expertinnen und Experten geben. Der Zweck ist die Weiterbildung von Fachpersonen in der Informationstechnologie, um zukünftig die bestehende Hardware und Software sicher zu gestalten. Das Angebot richtet sich an die Tätigkeitsbereiche Produktentwicklung, Softwareentwicklung, Geschäftführung, Systemadministration, Forschung und Lehre. Zusätzlich wird ein Internet of Things (IoT) Hacking Village zusammen mit Partnern aufgebaut. Man kann sich direkt mit Expertinnen und Experten austauschen und sehen, dass viele Smart Systeme alles andere als sicher sind.

Programme und Buchungen

Die DeepSec 2020 Konferenztage sind am 19. und 20. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. November statt. Die DeepINTEL Security Intelligence Konferenz findet am 18. 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. Bitte beachten Sie, dass wir aufgrund Planungssicherheit auf rechtzeitige Ticketbestellungen angewiesen sind.

(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/20200513013

pts20200513013 Technologie/Digitalisierung, Medien/Kommunikation

Les applis COVID-19 dévoilent leur logiciel pendant la crise

En novembre, la conférence sur la sécurité DeepSec mettra en lumière la mascarade des logiciels

Vienne (pts013/13.05.2020/09:30) - On dit souvent, " il y a forcément une appli pour ça ! ". Cette formule toute faite est souvent prise à la légère, même en dehors du secteur informatique. La crise actuelle du COVID-19 a de nouveau désigné le code informatique comme solution universelle aux problèmes qui ne sont pas strictement liés à la technologie de l'information. La numérisation générique semble être la réponse à tous nos problèmes. Bien sûr, le traitement des données peut aider. À condition toutefois de posséder des données réelles, vérifiables et recueillies soigneusement. C'est là qu'échouent de nombreux projets.

Téléphones magiques à l'intelligence infinie

La demande d'applis n'a fait qu'augmenter ces dernières années. Ces visions n'ont rien à envier aux idées créatives des scénarios de films et de séries. Le logiciel intégré à nos petits téléphones portables doit résoudre les tâches les plus complexes et délivrer des résultats qui demandaient autrefois de longues années de travail, le tout en un simple glissement de doigts. En réalité, la plupart des applications ne font qu'effleurer la surface. On oublie volontiers un petit détail : sans connexion Internet à de gigantesques fermes de serveurs et bases de données, invisibles sur l'écran tactile, à quoi sert le code ? Les applications ne font que repousser la réalité. Si le smartphone ne chauffe pas et que la batterie tient très longtemps, la magie est alors ailleurs. L'intelligence ne représente presque rien sur l'appareil, à cause d'un manque de puissance disponible.

Il s'agit de la complexité de la construction d'une infrastructure derrière l'application que l'on voit vraiment. Sans interaction avec leurs grandes soeurs dans les centres de données, les applications sur notre téléphone diminuent rapidement. Dans ce cas de figure, les données sont non seulement le pétrole brut, mais aussi le carburant de la numérisation. L'entraînement ne fonctionne toutefois pas comme on le pense. Les utilisateurs finaux sont la source de l'or numérique. Ils ne sont pas au volant, mais plutôt au niveau de l'extraction.

Conception défectueuse en matière de sécurité

Un code moderne n'arrive pas de nulle part. Lors du développement d'applications, soit on se base sur un code existant, soit on crée ses propres bibliothèques. Même lors d'une conception mixte, il s'écoule au moins quelques mois avant de parvenir à un design testé. Si la pression est importante, le développement de logiciel emprunte volontiers des raccourcis. Pour aggraver les choses, la conception commence avec les questions du problème à résoudre et se concentre sur les fonctions dès le début. L'implémentation d'un code et d'un design sûrs est souvent laissée de côté. On voit très souvent ce genre de développements dans le domaine des appareils pour la maison connectée.

Un argument souvent avancé est celui de la publication contrôlée des applications sur les App Stores des fabricants. Naturellement, les applis y sont soumises à des tests, mais une check-list vérifiée en moins d'une minute peut difficilement déceler l'intégralité des failles de sécurité et défauts de conception. Au vu du nombre de programmes disponibles sur les stores virtuels, certaines choses passeront forcément entre les mailles du filet. La recherche de failles et de menaces prend beaucoup plus de temps. On demande souvent aux experts en sécurité si un produit en particulier est sûr. Et on attend une réponse immédiate. Ce n'est pas réaliste et cela ne fonctionne ainsi que dans les scénarios mentionnés plus tôt.

Mascarade de logiciels

En matière de numérisation, les promesses et la réalité ne se recoupent pas souvent. Ces dernières semaines, on a notamment beaucoup parlé de l'application autrichienne de traçage du coronavirus. Les débats portaient majoritairement sur la protection des données et la sûreté de l'application. En prenant du recul et en remettant en question la qualité des données que cette application est censée recueillir, le tableau change du tout au tout. Ross Anderson, un informaticien britannique de l'université de Cambridge, a analysé la précision de la plateforme smartphone dans un article intitulé " Contact Tracing in the Real World " (publié sur le blog Light Blue Touchpaper de l'institut d'informatique). Il conclut que le développement d'une application mobilise plus de ressources que ce qu'une telle application pourrait entraîner comme avantages. Bruce Schneier, un expert américain en cryptographie et en sécurité informatique, évoque sur son blog les effets des faux positifs et des faux négatifs d'une application pour le coronavirus. La seule considération de cet aspect disqualifie d'ores et déjà l'application pour une utilisation dans le monde réel. Et ceci, sans même prendre en compte la sécurité et la protection des données. L'article de Schneier " Me on COVID-19 Contact Tracing Apps " est disponible en ligne.

En outre, un smartphone est un outil probablement inadapté en cas de maladies contagieuses. Comme le GPS est trop inexact, on essaie d'utiliser le Bluetooth pour mesurer la présence et la distance. Les appareils utilisent souvent le Bluetooth LE (à basse consommation) afin de prolonger la vie de la batterie.
Mais la mesure de l'intensité du signal avec le Bluetooth LE convient tout au plus à une résolution passable lorsque les personnes sont séparées par des structures massives, en béton armé par exemple. Les matériaux comme le bois, le plâtre ou la pierre mince sont perméables à la mesure. On se heurte en plus aux réflexions qui faussent la direction et la portée. D'après les fiches techniques des fabricants de puces, la puissance de réception réelle peut être 100 fois inférieure ou supérieure à la puissance prévue. Par ailleurs, le Bluetooth LE est un système à antenne unique. Cela signifie que la direction du signal ne peut pas être établie. Pour ce faire, plusieurs antennes sont nécessaires. Les gens tiennent en outre leur smartphone de différentes façons, ce qui entraîne encore plus d'approximation. Les erreurs de localisation sont déjà si nombreuses en laboratoire que cette technologie est éliminée d'entrée. Les scénarios comprenant les transports en commun, les magasins ou les restaurants n'ont même pas été pris en considération, sans parler de la circulation dans la rue ou dans des cages d'escalier étroites (où des signaux Bluetooth LE peuvent être captés derrière toutes les portes). Les porte-clés déjà évoqués officiellement ne devraient pas non plus apporter d'amélioration significative à la situation. La physique est impitoyable sur ce point.

C'est à présent très clair. Les logiciels ne servent plus uniquement à résoudre des problèmes. On les utilise volontiers pour camoufler les questions ouvertes et pour simuler une solution. C'est une véritable mascarade que l'on retrouve à plusieurs niveaux de la société contemporaine. La tâche des expertes et experts en sécurité est de percer à jour cette mascarade. Au début de l'année, le thème " Mascarade " a donc été choisi pour la conférence DeepSec In-Depth Security de novembre - avant même la propagation du Sars-Cov-2. En matière de sécurité informatique, il s'agit toujours de jeter un oeil en coulisses. Il faut déconstruire et analyser les codes. Il faut remettre en question l'architecture des logiciels. Il faut déceler les défauts de conception.

Numérisation désillusionnée comme chantier d'amélioration

Les arguments et démarches présentés ici ne visent pas à renchérir la numérisation. L'objectif affirmé de la conférence DeepSec est de réunir les personnes en charge de différents aspects de la technologie de l'information moderne et de les inciter à échanger. Les projets évoqués d'une application de traçage coronavirus ne sont qu'un exemple. Les expertes et experts en sécurité rappellent régulièrement qu'une conception solide (sécurisée) est incontournable pour les applications. Il serait donc judicieux de consulter les spécialistes avant de s'engager dans une impasse.

Si l'approche qui la motive est réfléchie avec précision, la numérisation ne peut être que positive. N'importe quelle visite au cinéma l'illustre facilement : un film au mauvais scénario ne s'améliore pas si on le projette en haute définition ou en 3D. On ne voit alors qu'un fiasco à gros budget - c'est pareil pour le développement de logiciels. En dépit de sa thématique, la conférence DeepSec ne souhaite pas devenir une mascarade, mais plutôt donner à tous et à toutes la chance d'échanger avec des spécialistes. Il s'agit de soulever ce masque et d'examiner ce qui se cache réellement derrière une technologie. À cette fin, nous proposerons aussi des formations qui offriront sur deux jours un concentré de connaissances à manipuler et à appliquer. Les premières séances de formation sont déjà ouvertes à la réservation en ligne.

Saisissez cette opportunité pour éviter à votre produit d'échouer avant sa commercialisation. Nous tenons à préciser que cette phrase est tout particulièrement destinée aux décideurs extérieurs au marché qui souhaitent numériser les entreprises et les citoyens à d'autres niveaux. Écrire et répéter continuellement le mot numérisation ne suffit pas.

Programme et réservation

La conférence DeepSec 2020 aura lieu les 19 et 20 novembre. Les formations DeepSec auront lieu les deux jours précédents, les 17 et 18 novembre.
L'évènement DeepSec aura lieu à l'hôtel Imperial Riding School Renaissance Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Vienne.
Vous pouvez commander vos tickets pour la conférence DeepSec et pour les formations DeepSec sur https://deepsec.net/register.html

Sources des articles cités par Ross Anderson et Bruce Schneier:
https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world/
https://www.schneier.com/blog/archives/2020/05/me_on_covad-19_.html
(Ende)

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

(/)

HIGHTECH

pts20200513013 Technologie/Digitalisierung, Medien/Kommunikation

Les applis COVID-19 dévoilent leur logiciel pendant la crise

En novembre, la conférence sur la sécurité DeepSec mettra en lumière la mascarade des logiciels

Vienne (pts013/13.05.2020/09:30) - **On dit souvent, " il y a forcément une appli pour ça ! ". Cette formule toute faite est souvent prise à la légère, même en dehors du secteur informatique. La crise actuelle du COVID-19 a de nouveau désigné le code informatique comme solution universelle aux problèmes qui ne sont pas strictement liés à la technologie de l'information. La numérisation générique semble être la réponse à tous nos problèmes. Bien sûr, le traitement des données peut aider. À condition toutefois de posséder des données réelles, vérifiables et recueillies soigneusement. C'est là qu'échouent de nombreux projets.**

Communication par temps de brouillard (© Crowes Agency OG)

Téléphones magiques à l'intelligence infinie

La demande d'applis n'a fait qu'augmenter ces dernières années. Ces visions n'ont rien à envier aux idées créatives des scénarios de films et de séries. Le logiciel intégré à nos petits téléphones portables doit résoudre les tâches les plus complexes et délivrer des résultats qui demandaient autrefois de longues années de travail, le tout en un simple glissement de doigts. En réalité, la plupart des applications ne font qu'effleurer la surface. On oublie volontiers un petit détail : sans connexion Internet à de gigantesques fermes de serveurs et bases de données, invisibles sur l'écran tactile, à quoi sert le code ? Les applications ne font que repousser la réalité. Si le smartphone ne chauffe pas et que la batterie tient très longtemps, la magie est alors ailleurs. L'intelligence ne représente presque rien sur l'appareil, à cause d'un manque de puissance disponible.

Il s'agit de la complexité de la construction d'une infrastructure derrière l'application que l'on voit vraiment. Sans interaction avec leurs grandes soeurs dans les centres de données, les applications sur notre téléphone diminuent rapidement. Dans ce cas de figure, les données sont non seulement le pétrole brut, mais aussi le carburant de la numérisation. L'entraînement ne fonctionne toutefois pas comme on le pense. Les utilisateurs finaux sont la source de l'or numérique. Ils ne sont pas au volant, mais plutôt au niveau de l'extraction.

Conception défectueuse en matière de sécurité

Un code moderne n'arrive pas de nulle part. Lors du développement d'applications, soit on se base sur un code existant, soit on crée ses propres bibliothèques. Même lors d'une conception mixte, il s'écoule au moins quelques mois avant de parvenir à un design testé. Si la pression est importante, le développement de logiciel emprunte volontiers des raccourcis. Pour aggraver les choses, la conception commence avec les questions du problème à résoudre et se concentre sur les fonctions dès le début. L'implémentation d'un modèle de sécurité est souvent laissée de côté. On voit très souvent ce genre de développements dans le domaine des appareils pour la maison connectée.

Un argument souvent avancé est celui de la publication contrôlée des applications sur les App Stores des fabricants. Naturellement, les applis y sont soumises à des tests, mais une check-list vérifiée en moins d'une minute peut difficilement déceler l'intégralité des failles de sécurité et défauts de conception. Au vu du nombre de programmes disponibles sur les stores virtuels, certaines choses passeront forcément entre les mailles du filet. La recherche de failles et de menaces prend beaucoup plus de temps. On demande souvent aux experts en sécurité si un produit en particulier est sûr. Et on attend une réponse immédiate. Ce n'est pas réaliste et cela ne fonctionne ainsi que dans les scénarios mentionnés plus tôt.

Mascarade de logiciels

En matière de numérisation, les promesses et la réalité ne se recoupent pas souvent. Ces dernières semaines, on a notamment beaucoup parlé de l'application autrichienne de traçage du coronavirus. Les débats portaient majoritairement sur la protection des données et la sûreté de l'application. En prenant du recul et en remettant en question la qualité des données que cette application est censée recueillir, le tableau change du tout au tout. Ross Anderson, un informaticien britannique de l'université de Cambridge, a analysé la précision de la plateforme smartphone dans un article intitulé " Contact Tracing in the Real World " (publié sur le blog Light Blue Touchpaper de l'institut d'informatique). Il conclut que le développement d'une application mobilise plus de ressources que ce qu'une telle application pourrait entraîner comme avantages. Bruce Schneier, un expert américain en cryptographie et en sécurité informatique, évoque sur son blog les effets des faux positifs et des faux négatifs d'une application pour le coronavirus. La seule considération de cet aspect disqualifie d'ores et déjà l'application pour une utilisation dans le monde réel. Et ceci, sans même prendre en compte la sécurité et la protection des données. L'article de Schneier " Me on COVID-19 Contact Tracing Apps " est disponible en ligne.

En outre, un smartphone est un outil probablement inadapté en cas de maladies contagieuses. Comme le GPS est trop inexact, on essaie d'utiliser le Bluetooth pour mesurer la présence et la distance. Les appareils utilisent souvent le Bluetooth LE (à basse consommation) afin de prolonger la vie de la batterie. Mais la mesure de l'intensité du signal avec le Bluetooth LE convient tout au plus à une résolution passable lorsque les personnes sont séparées par des structures massives, en béton armé par exemple. Les matériaux comme le bois, le plâtre ou la pierre mince sont perméables à la mesure. On se heurte en plus aux réflexions qui faussent la direction et la portée. D'après les fiches techniques des fabricants de puces, la puissance de réception réelle peut être 100 fois inférieure ou supérieure à la puissance prévue. Par ailleurs, le Bluetooth LE est un système à antenne unique. Cela signifie que la direction du signal ne peut pas être établie. Pour ce faire, plusieurs antennes sont nécessaires. Les gens tiennent en outre leur smartphone de différentes façons, ce qui entraîne encore plus d'approximation. Les erreurs de localisation sont déjà si nombreuses en laboratoire que cette technologie est éliminée d'entrée. Les scénarios comprenant les transports en commun, les magasins ou les restaurants n'ont même pas été pris en considération, sans parler de la circulation dans la rue ou dans des cages d'escalier étroites (où des signaux Bluetooth LE peuvent être captés derrière toutes les portes). Les porte-clés déjà évoqués officiellement ne devraient pas non plus apporter d'amélioration significative à la situation. La physique est impitoyable sur ce point.

C'est à présent très clair. Les logiciels ne servent plus uniquement à résoudre des problèmes. On les utilise volontiers pour camoufler les questions ouvertes et pour simuler une solution. C'est une véritable mascarade que l'on retrouve à plusieurs niveaux de la société contemporaine. La tâche des expertes et experts en sécurité est de percer à jour cette mascarade. Au début de l'année, le thème " Mascarade " a donc été choisi pour la conférence DeepSec In-Depth Security de novembre - avant même la propagation du Sars-Cov-2. En matière de sécurité informatique, il s'agit toujours de jeter un oeil en coulisses. Il faut déconstruire et analyser les codes. Il faut remettre en question l'architecture des logiciels. Il faut déceler les défauts de conception.

Numérisation désillusionnée comme chantier d'amélioration

Les arguments et démarches présentés ici ne visent pas à renchérir la numérisation. L'objectif affirmé de la conférence DeepSec est de réunir les personnes en charge de différents aspects de la technologie de l'information moderne et de les inciter à échanger. Les projets évoqués d'une application de traçage coronavirus ne sont qu'un exemple. Les expertes et experts en sécurité rappellent régulièrement qu'une conception solide (sécurisée) est incontournable pour les applications. Il serait donc judicieux de consulter les spécialistes avant de s'engager dans une impasse.

Si l'approche qui la motive est réfléchie avec précision, la numérisation ne peut être que positive. N'importe quelle visite au cinéma l'illustre facilement : un film au mauvais scénario ne s'améliore pas si on le projette en haute définition ou en 3D. On ne voit alors qu'un fiasco à gros budget - c'est pareil pour le développement de logiciels. En dépit de sa thématique, la

conférence DeepSec ne souhaite pas devenir une mascarade, mais plutôt donner à tous et à toutes la chance d'échanger avec des spécialistes. Il s'agit de soulever ce masque et d'examiner ce qui se cache réellement derrière une technologie. À cette fin, nous proposerons aussi des formations qui offriront sur deux jours un concentré de connaissances à manipuler et à appliquer. Les premières séances de formation sont déjà ouvertes à la réservation en ligne.

Saisissez cette opportunité pour éviter à votre produit d'échouer avant sa commercialisation. Nous tenons à préciser que cette phrase est tout particulièrement destinée aux décideurs extérieurs au marché qui souhaitent numériser les entreprises et les citoyens à d'autres niveaux. Écrire et répéter continuellement le mot numérisation ne suffit pas.

Programme et réservation

La conférence DeepSec 2020 aura lieu les 19 et 20 novembre. Les formations DeepSec auront lieu les deux jours précédents, les 17 et 18 novembre.

L'évènement DeepSec aura lieu à l'hôtel Imperial Riding School Renaissance Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Vienne.

Vous pouvez commander vos tickets pour la conférence DeepSec et pour les formations DeepSec sur https://deepsec.net/register.html (https://deepsec.net/register.html)

Sources des articles cités par Ross Anderson et Bruce Schneier:

https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world/ (https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world/)

https://www.schneier.com/blog/archives/2020/05/me_on_covad-19_.html (https://www.schneier.com/blog/archives/2020/05/me_on_covad-19_.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/20200505011

pts20200505011 Technologie/Digitalisierung, Forschung/Entwicklung

Covid-19-Apps zeigen Software in der Krise

DeepSec Sicherheitskonferenz beleuchtet im November die Maskerade von Software

Wien (pts011/05.05.2020/09:30) - Es gibt in der Umgangssprache den Spruch “There’s an app for that!”. Die Floskel wird oft als Witz verstanden, selbst außerhalb der IT-Branche. Die aktuelle Covid-19-Krise hat Computer-Code wieder einmal als Universallösung für Probleme, die nicht ausschließlich mit der Informationstechnologie zusammenhängen, thematisiert. Generische Digitalisierung scheint die Antwort auf alle Probleme zu sein. Natürlich kann Datenverarbeitung helfen. Die Voraussetzung dafür ist allerdings das Vorhandensein von echten Daten, die auch nachvollziehbar und sorgfältig erhoben wurden. Genau daran scheitern viele Vorhaben.

Magische Telefone mit unendlicher Intelligenz

Der Ruf nach Apps wiederholt sich in den letzten Jahren immer wieder. Die Visionen stehen den kreativen Ideen in Drehbüchern von Spielfilmen und Serien in nichts nach. Software, die auf kleinen tragbaren Telefonen läuft, soll die komplexesten Aufgaben lösen und mit einem einfachen Wischen von Fingern Ergebnisse liefern, die man früher nur durch jahrelange Arbeit erlangen konnte. Tatsächlich kratzen die meisten Applikationen nur an der Oberfläche.

Es wird gerne ein winziges Detail vergessen: Was leistet der Code ohne Anbindung per Internet an riesige Serverfarmen und Datenbanken, die man am Touchscreen gar nicht sieht? Apps sind nur eine Verschiebung der Tatsachen. Bleibt das Smartphone kühl, und hält der Akku sehr lange, dann geschieht die Magie eigentlich ganz woanders. Smart ist am Endgerät fast nichts, mangels verfügbarer Leistung.

Es geht um die Komplexität des Aufbaus einer Infrastruktur hinter der eigentlichen App,die man sieht. Ohne Wechselwirkung mit den großen Geschwistern in Rechenzentren reduzieren sich die Anwendungen auf dem Telefon in der Hand sehr schnell. Daten sind dann bei diesem Szenario nicht nur das Rohöl, sondern sie sind auch der Treibstoff der Digitalisierung. Der Antrieb funktioniert allerdings nicht so wie man glaubt. Die Endbenutzerinnen und Endbenutzer sind die Quelle des digitalen Goldes. Sie sitzen nicht am Steuer, sondern im Bohrloch.

Fehlendes Design bei der Sicherheit

Moderner Code kann nicht aus dem Nichts entstehen. Man muss bei der Entwicklung von Applikationen entweder auf existierendem Code aufbauen oder sich die Bibliotheken erst selbst schaffen. Selbst bei einem gemischten Aufbau vergehen mindestens Monate, um halbwegs zu einem getesteten Design zu kommen. Bei großem Druck auf die Fertigstellung nimmt die Softwareentwicklung gerne Abkürzungen. Erschwerend kommt hinzu, dass das Design bei den Fragestellungen des zu lösenden Problems beginnt und sich von Anfang an auf Features konzentriert. Die Implementation von sicherem Code und sicherem Design bleibt meist zurück. Im Bereich der Smart-Home-Geräte sieht man solche Entwicklungen sehr oft.

Ein oft vorgebrachtes Argument ist die kontrollierte Publikation von Applikationen über die App Stores der Hersteller. Natürlich verlaufen dort Prüfungen, jedoch kann eine Checkliste, die in weniger als einer Minute abläuft, kaum alle Sicherheitsschwächen oder gar Designfehler aufspüren. Im Anbetracht der Vielzahl der in den virtuellen Stores verfügbaren Programme wird zwangsläufig immer etwas unauffällig durchrutschen. Das Finden von Lücken und Bedrohungen ist viel zeitaufwendiger. Sicherheitsexpertinnen werden oft gefragt, ob ein bestimmtes Produkt sicher sei. Erwartet wird eine sofortige Antwort. Das ist nicht realistisch und funktioniert so nur in den eingangs erwähnten Drehbüchern.

Software als Maskerade

Versprechung und Realität liegen bei der Digitalisierung selten nah bei einander. Speziell über die österreichische Corona Tracing App wurde in den letzten Wochen viel diskutiert. Es ging primär um Bedenken beim Thema Datenschutz und die Sicherheit der App. Geht man mehrere Schritte zurück und hinterfragt die Güte der Daten, die diese App erheben soll, so ergibt sich ein völlig anderes Bild. Ross Anderson, ein britischer Informatiker der Universität Cambridge, hat in einem Artikel mit dem Titel “Contact Tracing in the Real World” (publiziert im Blog “Light Blue Touchpaper” des Informatikinstituts) die Genauigkeit der Plattform Smartphone analysiert. Sein Fazit: Die Entwicklung einer App binde mehr Ressourcen als der Nutzen einer solchen Anwendung aufwiegen kann.

Bruce Schneier, ein US-amerikanischer Experte für Kryptographie und Computersicherheit, schreibt in seinem Blog über die Auswirkungen der positiven und negativen Falschmeldungen einer Corona-App. Die Betrachtung dieses Aspekts alleine disqualifiziert die App schon für einen Einsatz in der echten Welt. Sicherheit und Datenschutz sind in dieser Betrachtung noch nicht eingegangen. Schneiers Artikel “Me on COVID-19 Contact Tracing Apps” kann man online nachlesen.

Darüber hinaus ist ein Smartphone bei ansteckenden Krankheiten eine denkbar ungeeignete Plattform.
Da GPS zu ungenau ist, versucht man Bluetooth für die Messungen von Präsenzen und Abstand zu verwenden. Auf den Geräten kommt Bluetooth LE (Low Energy) oft zum Einsatz, um die Laufzeit der Batterien zu verlängern. Die Messung der Signalstärke bei Bluetooth LE eignet sich aber maximal für eine passable Auflösung, wenn Personen durch massive bauliche Maßnahmen, wie beispielsweise Stahlbeton, getrennt sind. Materialien wie Holz, Gips oder dünner Stein ist für die Messung durchlässig.

Zusätzlich hat man mit Reflexionen zu kämpfen, die Richtung und Reichweite verfälschen. Laut Datenblättern der Chiphersteller schwankt die Empfangsleistung teilweise um den Faktor 100. Weiterhin ist Bluetooth LE als System mit einer einzigen Antenne konzipiert. Das bedeutet, dass sich die Richtung des Signals eigentlich nicht feststellen lässt. Dazu sind mehrere Antennen notwendig. Obendrein halten Personen ihr Smartphone gerne in verschiedenen Haltung, was eine weitere Unschärfe einführt. Die Lokalisierungsfehler im Labor sind damit schon so hoch, dass diese Technologie ausscheidet. Dabei wurden Szenarien wie öffentlicher Personennahverkehr, Geschäfte oder Lokale gar nicht betrachtet, geschweige denn das Gehen auf der Straße oder in engen Treppenhäusern (wo hinter jeder Tür Bluetooth-LE-Signale messbar sind). Auch die schon öffentlich erwähnten Schlüsselanhänger dürften der Sachlage keine wesentliche Verbesserung einräumen. Die Physik ist da sehr unbarmherzig.

Der Ausflug stellt klar: Software wird leider nicht mehr nur zur Lösung von Problemen eingesetzt. Gerne verwendet man sie zur Maskierung von offenen Fragen und zum Vortäuschen von Lösungen. Es ist eine Maskerade, die wir in vielen Bereichen der modernen Gesellschaft wiederfinden. Die Aufgabe von Sicherheitsexpertinnen und -experten ist es, diese Maskerade zu durchschauen. Ganz ohne die Verbreitung von Sars-Cov-2 wurde daher Anfang des Jahres “Maskerade” als Motto für die im November stattfindende DeepSec In-Depth Security Konferenz gewählt. Bei der Informationssicherheit geht es immer um einen Blick hinter die Kulissen. Code muss dekonstruiert und analysiert werden. Softwarearchitektur muss hinterfragt werden. Schwächen im Design müssen aufgespürt werden.

Entzauberte Digitalisierung als Bauplan für Verbesserung

Die hier angeführten Argumente und Vorgehensweisen sind nicht eine Blaupause für die Verteuerung der Digitalisierung. Das erklärte Ziel der DeepSec Konferenz ist es, Menschen, die mit verschiedenen Aspekten der modernen Informationstechnologie betraut sind, an einen Tisch zu bringen und zum Austausch zu bewegen. Die erwähnten Ansätze für eine Corona-Tracing-App sind nur ein plakatives Beispiel. Sicherheitsexpertinnen und -experten mahnen regelmäßig, dass ein solides - sicheres - Design unablässig für Applikationen ist. Man ist daher gut beraten, die Fachwelt zu konsultieren, bevor man sich in eine Sackgasse redet.

Digitalisierung kann nur einen Fortschritt bringen, wenn der dahinter liegende Ansatz auch genau durchdacht ist. Jeder Gang ins Kino kann das leicht illustrieren: Kein Film mit schlechtem Drehbuch wird besser, wenn man ihn in Hochauflösung oder gar 3D dem Publikum zeigt. Man sieht dann leider nur ein teuer produziertes Fiasko - wie teilweise in der Softwareentwicklung. Die DeepSec Konferenz möchte daher trotz ihrem Motto keine Maskerade bieten, sondern allen Teilnehmerinnen und Teilnehmern die Chance geben, sich mit Fachpersonen auszutauschen. Es geht darum, hinter die Maske zu schauen und zu bewerten, was wirklich hinter einer Technologie steckt. Zu diesem Zweck werden auch Trainings angeboten, die in zwei Tagen hochkonzentriert Wissen zum Anfassen und Anwenden bieten. Die ersten Trainingseinheiten sind bereits online und können gebucht werden.

Nutzen Sie die Gelegenheit, bevor ihr Produkt versagt, noch bevor es auf dem Markt ist. Es sei darauf hingewiesen, dass dieser Satz ganz speziell für Entscheider abseits des Marktes gilt, die Unternehmen und Bürgerinnen sowie Bürger auf anderer Ebene digitalisieren möchten. Digitalisierung als Wort aufschreiben und ständig wiederholen, ist alleine zu wenig.

Programme und Buchung

Die DeepSec-2020-Konferenztage sind am 19. und 20. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. 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.

Quellen der zitierten Artikel von Ross Anderson und Bruce Schneier:
https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world/
https://www.schneier.com/blog/archives/2020/05/me_on_covad-19_.html

(Ende)

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

(/)

HIGHTECH

pts20200505011 Technologie/Digitalisierung, Forschung/Entwicklung

Covid-19-Apps zeigen Software in der Krise

DeepSec Sicherheitskonferenz beleuchtet im November die Maskerade von Software

Wien (pts011/05.05.2020/09:30) - **Es gibt in der Umgangssprache den Spruch "There's an app for that!". Die Floskel wird oft als Witz verstanden, selbst außerhalb der IT-Branche. Die aktuelle Covid-19-Krise hat Computer-Code wieder einmal als Universallösung für Probleme, die nicht ausschließlich mit der Informationstechnologie zusammenhängen, thematisiert. Generische Digitalisierung scheint die Antwort auf alle Probleme zu sein. Natürlich kann Datenverarbeitung helfen. Die Voraussetzung dafür ist allerdings das Vorhandensein von echten Daten, die auch nachvollziehbar und sorgfältig erhoben wurden. Genau daran scheitern viele Vorhaben.**

Kommunikation im Nebel (Foto: Crowes Agency)

Magische Telefone mit unendlicher Intelligenz

Der Ruf nach Apps wiederholt sich in den letzten Jahren immer wieder. Die Visionen stehen den kreativen Ideen in Drehbüchern von Spielfilmen und Serien in nichts nach. Software, die auf kleinen tragbaren Telefonen läuft, soll die komplexesten Aufgaben lösen und mit einem einfachen Wischen von Fingern Ergebnisse liefern, die man früher nur durch jahrelange Arbeit erlangen konnte. Tatsächlich kratzen die meisten Applikationen nur an der Oberfläche.

Es wird gerne ein winziges Detail vergessen: Was leistet der Code ohne Anbindung per Internet an riesige Serverfarmen und Datenbanken, die man am Touchscreen gar nicht sieht? Apps sind nur eine Verschiebung der Tatsachen. Bleibt das Smartphone kühl, und hält der Akku sehr lange, dann geschieht die Magie eigentlich ganz woanders. Smart ist am Endgerät fast nichts, mangels verfügbarer Leistung.

Es geht um die Komplexität des Aufbaus einer Infrastruktur hinter der eigentlichen App,die man sieht. Ohne Wechselwirkung mit den großen Geschwistern in Rechenzentren reduzieren sich die Anwendungen auf dem Telefon in der Hand sehr schnell. Daten sind dann bei diesem Szenario nicht nur das Rohöl, sondern sie sind auch der Treibstoff der Digitalisierung. Der Antrieb funktioniert allerdings nicht so wie man glaubt. Die Endbenutzerinnen und Endbenutzer sind die Quelle des digitalen Goldes. Sie sitzen nicht am Steuer, sondern im Bohrloch.

Fehlendes Design bei der Sicherheit

Moderner Code kann nicht aus dem Nichts entstehen. Man muss bei der Entwicklung von Applikationen entweder auf existierendem Code aufbauen oder sich die Bibliotheken erst selbst schaffen. Selbst bei einem gemischten Aufbau vergehen mindestens Monate, um halbwegs zu einem getesteten Design zu kommen. Bei großem Druck auf die Fertigstellung nimmt die Softwareentwicklung gerne Abkürzungen. Erschwerend kommt hinzu, dass das Design bei den Fragestellungen des zu lösenden Problems beginnt und sich von Anfang an auf Features konzentriert. Die Implementation von sicherem Code und sicherem Design bleibt meist zurück. Im Bereich der Smart-Home-Geräte sieht man solche Entwicklungen sehr oft.

Ein oft vorgebrachtes Argument ist die kontrollierte Publikation von Applikationen über die App Stores der Hersteller. Natürlich verlaufen dort Prüfungen, jedoch kann eine Checkliste, die in weniger als einer Minute abläuft, kaum alle Sicherheitsschwächen oder gar Designfehler aufspüren. Im Anbetracht der Vielzahl der in den virtuellen Stores verfügbaren Programme wird zwangsläufig immer etwas unauffällig durchrutschen. Das Finden von Lücken und Bedrohungen ist viel zeitaufwendiger. Sicherheitsexpertinnen werden oft gefragt, ob ein bestimmtes Produkt sicher sei. Erwartet wird eine sofortige Antwort. Das ist nicht realistisch und funktioniert so nur in den eingangs erwähnten Drehbüchern.

Software als Maskerade

Versprechung und Realität liegen bei der Digitalisierung selten nah bei einander. Speziell über die österreichische Corona Tracing App wurde in den letzten Wochen viel diskutiert. Es ging primär um Bedenken beim Thema Datenschutz und die Sicherheit der App. Geht man mehrere Schritte zurück und hinterfragt die Güte der Daten, die diese App erheben soll, so ergibt sich ein völlig anderes Bild. Ross Anderson, ein britischer Informatiker der Universität Cambridge, hat in einem Artikel mit dem Titel "Contact Tracing in the Real World" (publiziert im Blog "Light Blue Touchpaper" des Informatikinstituts) die Genauigkeit der Plattform Smartphone analysiert. Sein Fazit: Die Entwicklung einer App binde mehr Ressourcen als der Nutzen einer solchen Anwendung aufwiegen kann.

Bruce Schneier, ein US-amerikanischer Experte für Kryptographie und Computersicherheit, schreibt in seinem Blog über die Auswirkungen der positiven und negativen Falschmeldungen einer Corona-App. Die Betrachtung dieses Aspekts alleine disqualifiziert die App schon für einen Einsatz in der echten Welt. Sicherheit und Datenschutz sind in dieser Betrachtung noch nicht eingegangen. Schneiers Artikel "Me on COVID-19 Contact Tracing Apps" kann man online nachlesen.

Darüber hinaus ist ein Smartphone bei ansteckenden Krankheiten eine denkbar ungeeignete Plattform. Da GPS zu ungenau ist, versucht man Bluetooth für die Messungen von Präsenzen und Abstand zu verwenden. Auf den Geräten kommt Bluetooth LE (Low Energy) oft zum Einsatz, um die Laufzeit der Batterien zu verlängern. Die Messung der Signalstärke bei Bluetooth LE eignet sich aber maximal für eine passable Auflösung, wenn Personen durch massive bauliche Maßnahmen, wie beispielsweise Stahlbeton, getrennt sind. Materialien wie Holz, Gips oder dünner Stein ist für die Messung durchlässig.

Zusätzlich hat man mit Reflexionen zu kämpfen, die Richtung und Reichweite verfälschen. Laut Datenblättern der Chiphersteller schwankt die Empfangsleistung teilweise um den Faktor 100. Weiterhin ist Bluetooth LE als System mit einer einzigen Antenne konzipiert. Das bedeutet, dass sich die Richtung des Signals eigentlich nicht feststellen lässt. Dazu sind mehrere Antennen notwendig. Obendrein halten Personen ihr Smartphone gerne in verschiedenen Haltung, was eine weitere Unschärfe einführt. Die Lokalisierungsfehler im Labor sind damit schon so hoch, dass diese Technologie ausscheidet. Dabei wurden Szenarien wie öffentlicher Personennahverkehr, Geschäfte oder Lokale gar nicht betrachtet, geschweige denn das Gehen auf der Straße oder in engen Treppenhäusern (wo hinter jeder Tür Bluetooth-LE-Signale messbar sind). Auch die schon öffentlich erwähnten Schlüsselanhänger dürften der Sachlage keine wesentliche Verbesserung einräumen. Die Physik ist da sehr unbarmherzig.

Der Ausflug stellt klar: Software wird leider nicht mehr nur zur Lösung von Problemen eingesetzt. Gerne verwendet man sie zur Maskierung von offenen Fragen und zum Vortäuschen von Lösungen. Es ist eine Maskerade, die wir in vielen Bereichen der modernen Gesellschaft wiederfinden. Die Aufgabe von Sicherheitsexpertinnen und -experten ist es, diese Maskerade zu durchschauen. Ganz ohne die Verbreitung von Sars-Cov-2 wurde daher Anfang des Jahres "Maskerade" als Motto für die im November stattfindende DeepSec In-Depth Security Konferenz gewählt. Bei der Informationssicherheit geht es immer um einen Blick hinter die Kulissen. Code muss dekonstruiert und analysiert werden. Softwarearchitektur muss hinterfragt werden. Schwächen im Design müssen aufgespürt werden.

Entzauberte Digitalisierung als Bauplan für Verbesserung

Die hier angeführten Argumente und Vorgehensweisen sind nicht eine Blaupause für die Verteuerung der Digitalisierung. Das erklärte Ziel der DeepSec Konferenz ist es, Menschen, die mit verschiedenen Aspekten der modernen Informationstechnologie betraut sind, an einen Tisch zu bringen und zum Austausch zu bewegen. Die erwähnten Ansätze für eine Corona-Tracing-App sind nur ein plakatives Beispiel. Sicherheitsexpertinnen und -experten mahnen regelmäßig, dass ein solides - sicheres - Design unablässig für Applikationen ist. Man ist daher gut beraten, die Fachwelt zu konsultieren, bevor man sich in eine Sackgasse redet.

Digitalisierung kann nur einen Fortschritt bringen, wenn der dahinter liegende Ansatz auch genau durchdacht ist. Jeder Gang ins Kino kann das leicht illustrieren: Kein Film mit schlechtem Drehbuch wird besser, wenn man ihn in Hochauflösung oder gar 3D dem Publikum zeigt. Man sieht dann leider nur ein teuer produziertes Fiasko - wie teilweise in der Softwareentwicklung. Die DeepSec Konferenz möchte daher trotz ihrem Motto keine Maskerade bieten, sondern allen Teilnehmerinnen und Teilnehmern die Chance geben, sich mit Fachpersonen auszutauschen. Es geht darum, hinter die Maske zu schauen und zu bewerten, was wirklich hinter einer Technologie steckt. Zu diesem Zweck werden auch Trainings angeboten, die in zwei Tagen hochkonzentriert Wissen zum Anfassen und Anwenden bieten. Die ersten Trainingseinheiten sind bereits online und können gebucht werden.

Nutzen Sie die Gelegenheit, bevor ihr Produkt versagt, noch bevor es auf dem Markt ist. Es sei darauf hingewiesen, dass dieser Satz ganz speziell für Entscheider abseits des Marktes gilt, die Unternehmen und Bürgerinnen sowie Bürger auf anderer Ebene digitalisieren möchten. Digitalisierung als Wort aufschreiben und ständig wiederholen, ist alleine zu wenig.

Programme und Buchung

Die DeepSec-2020-Konferenztage sind am 19. und 20. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 17. und 18. 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.

Quellen der zitierten Artikel von Ross Anderson und Bruce Schneier:
https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world/ (https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world/)
https://www.schneier.com/blog/archives/2020/05/me_on_covad-19_.html (https://www.schneier.com/blog/archives/2020/05/me_on_covad-19_.html)

(Ende)

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