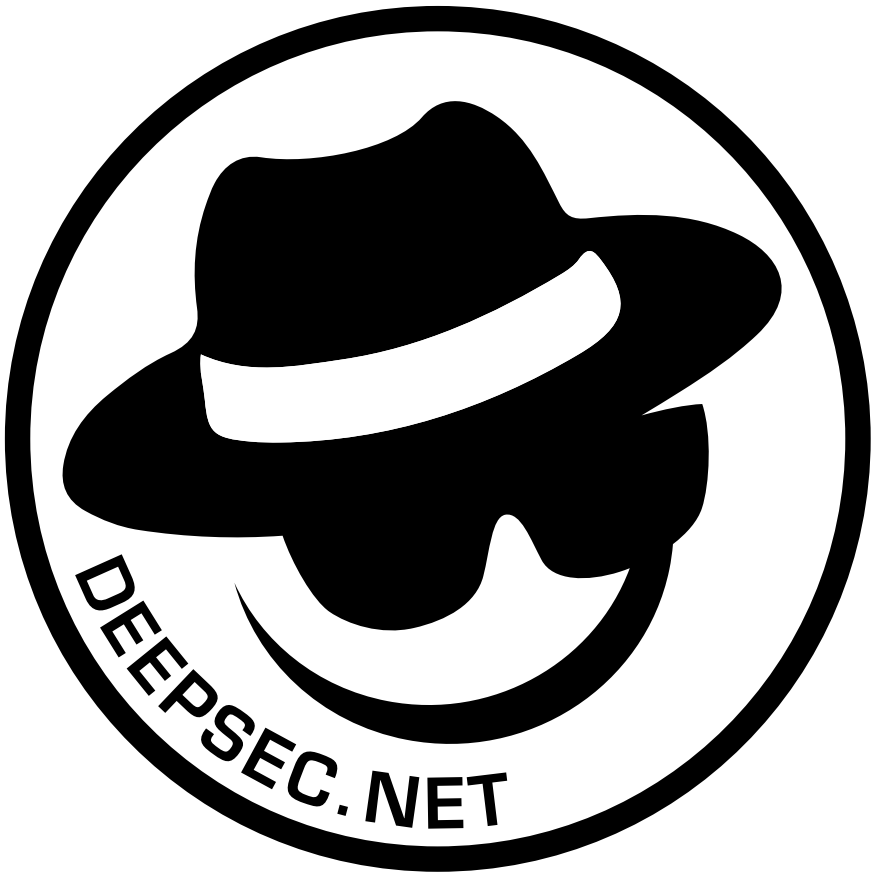


press review 2018

media coverage

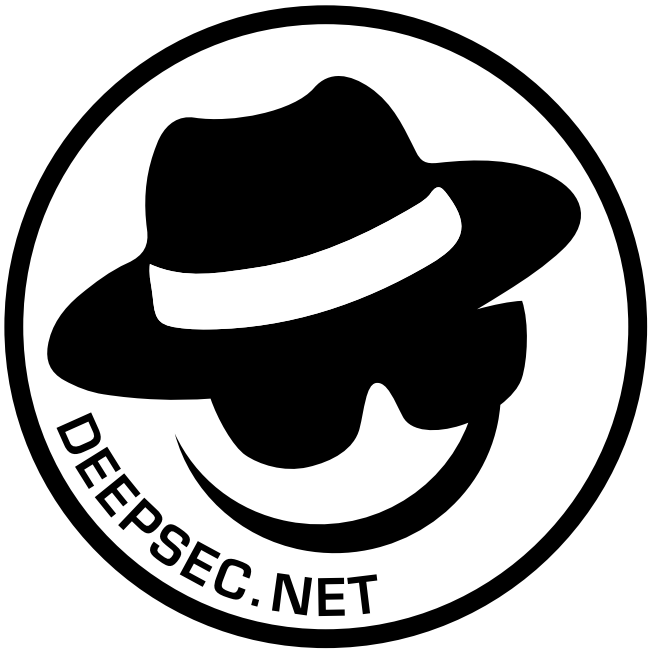
2018

contents

press releases

2018

media coverage 2018



https://sg.hu/cikkek/it-tech/134238/tarsadalmi-vita-kellene-a-bor-ala-ultetheto-chipekrol

Társadalmi vita kellene a bőr alá ültethető chipekről

13.12.2018, Berta Sandor

Jelenleg még csak a technológia iránt érdeklődő kevesek ültetnek be a bőrük alá chipet, de lehetséges, hogy elterjedt azonosítási és tárolási módszer lesz.

"Az emberek már 2004-ben is kis RFID-chipeket helyeztettek el a bőrük alatt. Így akartak bejelentkezni a számítógépekbe vagy kinyitni az autóik zárjait. A megoldásokat most már a vállalatok a dolgozóiknál alkalmazzák" - jelentette ki Ulrike Hugl, az Innsbrucki Egyetem kutatója. A szakember a DeepSec biztonsági konferencián tartott előadást a témában.
A Three Square Market nevű wisconsini vállalkozás már tavaly miniatűr chippel látta el az alkalmazottait. Az azonosítót a hüvelyk- és a mutatóujj között ültetik be a bőr alá és az emberek arra használják, hogy bejelentkezzenek az irodai számítógépeikbe, fizessenek az automatákban lévő élelmiszerekért és italokért, ajtókat nyissanak ki vagy kezeljék a fénymásolót.

A The Guardian szerint Nagy-Britanniában is egyeztetések zajlanak az érdeklődő társaságokkal. A BioTeq már 150 implantátumot ültetett be. Ezek az apró, rizsszem méretű chipek hasonlatosak azokhoz, mint amit állatokba raknak, és orvosi adatok tárolása mellett az autó integetéssel való kinyitására jók. A Biohax nevű svéd cég is szállít biochipeket, náluk egy azonosító 70 és 260 font közötti összegbe kerül. Brit jogi és pénzügyi cégek vezetőivel vannak tárgyalásban alkalmazottaik ellátására, egyikük több ezer munkavállalóval büszkélkedhet.

A munkatársakat senki sem fogja erre a lépésre kényszeríteni, az egész dolog önkéntes alapon zajlana. Hugl szerint ugyanakkor ez csupán látszat, hiszen igenis nyomás fog nehezedni a munkavállalókra és kényszert éreznek majd arra, hogy azt tegyék, amit a többiek is. A szigetországban a Confederation of British Industry (CBI) és a TUC szakszervezet figyelmeztetett a lehetséges veszélyekre. Az érdeklődő vállalatok viszont azzal érveltek, hogy a dolgozók a chipeket magáncélokra is használhatják azért, hogy kinyissák a gépkocsijaik zárjait vagy eltárolják az egészségügyi adataikat. Néhány kórház már próbaképpen eltárolta az eszközökön a betegek adatait.

Érdekes módon Jowan Österlund, a Biohax alapítója pont a biztonság növelésével érvel. "Ezek a vállalatok érzékeny adatokat kezelnek, a chipek segítenek megőrizni a korlátozások betartását." A cég eddig 4000 embert jelölt meg, többségük svéd. Jelenleg a cég a svéd állami vasúttal dolgozik együtt, hogy lehetővé tegyék, hogy az utasok ilyen formában is hordozhassák vonatjegyüket.

Hugl közölte, hogy eddig még nem folytattak társadalmi vitát erről a kérdésről, éppen ezért megtörténhet, hogy tíz év múlva mindenkibe chipet tesznek. A szakember hiányolta, hogy sok technológiai és adatvédelmi téma esetében nem kerül sor széles körű társadalmi vitára és túl kevesen foglalkoznak ezekkel a kérdésekkel. A kutató hangsúlyozta, hogy ő nem engedne chipet beültetni magába, neki ugyanis egy ilyen eljárás túl invazív lenne. Miután tudja, hogy mi mindent követnek és ellenőriznek egy ilyen eszközzel, ezért komoly aggályai lennének. Az implantátumok beépítésével kapcsolatban vannak biztonsági és egyéb aggályok is, például, mi történik, ha valaki elhagy egy vállalkozást, hiszen a belépőkódokat a chipben magával hordozza. S azt sem szabad elfelejteni, hogy egy ilyen eszközt legfeljebb kivágni lehet a bőrből, kikapcsolni nem.

English translation:

There should be a social debate about chips that can be placed under the skin

At the moment, only a few people who are interested in technology are putting chips under their skin, but it may become a common method of identification and storage.

"People have already placed small RFID chips under their skin in 2004. That's how they wanted to sign in to computers or open their car locks. The solutions are now being used by companies on their employees," said Ulrike Hugl, a researcher at the University of Innsbruck. The expert gave a lecture on the subject at the DeepSec Security Conference. The Three Square Market Wisconsin company has already provided miniature chips to its employees last year. The ID is placed under the skin between the thumb and forefinger, and people use it to sign in to their office computers, pay for food and drinks at the vending machines, open doors or handle the copier.

According to The Guardian, there are discussions with interested companies in Britain. BioTeq has already implanted 150 implants. These tiny rice-grain sized chips are similar to the ones they put into animals. The Biohax Swedish company also supplies biocides, an ID-chip sells between 70 and 260 pounds. Some british lawyers and financial executives are negotiating with their employees, one of them has thousands of employees.

None of the employees would be forced to take this step they claim, the whole thing is said to be on a voluntary basis. However, according to Hugl, this is only apparently so, because there will be social and group pressure on the workers and they will be forced to do what the others do. On the British isle, the Confederation of British Industry (CBI) and the TUC union warn about potential dangers. Interested companies however argue that employees can use their chips for private purposes too, to open their vehicle locks or store their health data. Some hospitals have already tried to store patient data on these devices.

Interestingly, Jowan Österlund, the founder of Biohax, uses security as an argument. "These companies handle sensitive data, chips can help to keep restrictions in place." The company so far has chipped 4,000 people, most of them Swedish. Currently, the company is working with the Swedish State Railways to allow passengers to carry their train tickets in this form.

Until now there has been no social debate about this issue, says Hugl. “If this goes on, we might all carry a chip-implant in ten years.” Many technological and data protection issues are not subject to a wide-ranging social debate and too few people cocern themselves with these issues. The researcher emphasizes that she would not allow a chip to be implanted under her skin, for her this procedure would be too invasive. If people would know how you can be followed and controlled with such a tool, they would have serious concerns, she claims. There are security and other concerns about installing implants as well, such as, what happens if someone leaves a business? They would still carry the access codes in their chip. And it should not be forgotten that such a device can not be turned off but cut out at most.

Társadalmi vita kellene a bőr alá ültethető chipekről

2018. december 13. 8:44, csütörtök

Jelenleg még csak a technológia iránt érdeklődő kevesek ültetnek be a bőrük alá chipet, de lehetséges, hogy elterjedt azonosítási és tárolási módszer lesz.

"Az emberek már 2004-ben is kis RFID-chipeket helyeztettek el a bőrük alatt. Így akartak bejelentkezni a számítógépekbe vagy kinyitni az autóik zárjait. A megoldásokat most már a vállalatok a dolgozóiknál alkalmazzák" - jelentette ki Ulrike Hugl, az Innsbrucki Egyetem kutatója. A szakember a DeepSec biztonsági konferencián tartott előadást (https://deepsec.net/speaker.html#PSLOT367) a témában. A Three Square Market nevű wisconsini vállalkozás már tavaly miniatűr chippel látta el (https://www.theguardian.com/money/video/2017/aug/02/olivia-solon-gets-microchipped-video) az alkalmazottait. Az azonosítót a hüvelyk- és a mutatóujj között ültetik be a bőr alá és az emberek arra használják, hogy bejelentkezzenek az irodai számítógépeikbe, fizessenek az automatákban lévő élelmiszerekért és italokért, ajtókat nyissanak ki vagy kezeljék a fénymásolót.

A The Guardian szerint (https://www.theguardian.com/technology/2018/nov/11/alarm-over-talks-to-implant-uk-employees-with-microchips) Nagy-Britanniában is egyeztetések zajlanak az érdeklődő társaságokkal. A BioTeq már 150 implantátumot ültetett be. Ezek az apró, rizsszem méretű chipek hasonlatosak azokhoz, mint amit állatokba raknak, és orvosi adatok tárolása mellett az autó integetéssel való kinyitására jók. A Biohax nevű svéd cég is szállít (https://www.telegraph.co.uk/technology/2018/11/10/major-uk-companies-preparing-microchip-employees/) biochipeket, náluk egy azonosító 70 és 260 font közötti összegbe kerül. Brit jogi és pénzügyi cégek vezetőivel vannak tárgyalásban alkalmazottaik ellátására, egyikük több ezer munkavállalóval büszkélkedhet.

További cikkek

Már több mint ezer halott kriptovaluta van

(/cikkek/it-tech/134688/mar-tobb-mint-ezer-halott-kriptovaluta-van)

Bemutatkozott az LG Q9 (/cikkek/it-tech/134671/bemutatkozott-az-lg-q9)

Őrült nagy adatlopást hajtott végre egy 20 éves fiú

(/cikkek/it-tech/134680/orult-nagy-adatlopast-hajtott-vegre-egy-20-eves-fiu)

ITunes és Airplay lesz a Samsung okostévéin

(/cikkek/it-tech/134666/itunes-es-airplay-lesz-a-samsung-okostevein)

AMD processzorra épülő Chromebook az Acertől

(/cikkek/it-tech/134664/amd-processzorra-epulo-chromebook-az-acertol)

A munkatársakat senki sem fogja erre a lépésre kényszeríteni, az egész dolog önkéntes alapon zajlana. Hugl szerint ugyanakkor ez csupán látszat, hiszen igenis nyomás fog nehezedni a munkavállalókra és kényszert éreznek majd arra, hogy azt tegyék, amit a többiek is. A szigetországban a Confederation of British Industry (CBI) és a TUC szakszervezet figyelmeztetett a lehetséges veszélyekre. Az érdeklődő vállalatok viszont azzal érveltek, hogy a dolgozók a chipeket magáncélokra is használhatják azért, hogy kinyissák a gépkocsijaik zárjait vagy eltárolják az egészségügyi adataikat. Néhány kórház már próbaképpen eltárolta az eszközökön a betegek adatait.

Érdekes módon Jowan Österlund, a Biohax alapítója pont a biztonság növelésével érvel. "Ezek a vállalatok érzékeny adatokat kezelnek, a chipek segítenek megőrizni a korlátozások betartását." A cég eddig 4000 embert jelölt meg, többségük svéd. Jelenleg a cég a svéd állami vasúttal dolgozik együtt, hogy lehetővé tegyék, hogy az utasok ilyen formában is hordozhassák vonatjegyüket.

Hugl közölte, hogy eddig még nem folytattak társadalmi vitát erről a kérdésről, éppen ezért megtörténhet, hogy tíz év múlva mindenkibe chipet tesznek. A szakember hiányolta, hogy sok technológiai és adatvédelmi téma esetében nem kerül sor széles körű társadalmi vitára és túl kevesen foglalkoznak ezekkel a kérdésekkel. A kutató hangsúlyozta, hogy ő nem engedne chipet beültetni magába, neki ugyanis egy ilyen eljárás túl invazív lenne. Miután tudja, hogy mi mindent követnek és ellenőriznek egy ilyen eszközzel, ezért komoly aggályai lennének. Az implantátumok beépítésével kapcsolatban vannak biztonsági és egyéb aggályok is, például, mi történik, ha valaki elhagy egy vállalkozást, hiszen a belépőkódokat a chipben magával hordozza. S azt sem szabad elfelejteni, hogy egy ilyen eszközt legfeljebb kivágni lehet a bőrből, kikapcsolni nem.

Belépő szintű Nokia kapta meg engedélyeit

(/cikkek/it-tech/134540/belepo-szintu-nokia-kapta-meg-engedelyeit)

Kapcsolódó cikkek és linkek

Chipeket fejlesztene a Facebook? (/cikkek/it-tech/134192/chipeket-facebook)	Fontosabb a kényelem az adatvédelemnél? (/cikkek/it-tech/134786/fontosabb-adatvedelemnel)	
Apple - búcsú a PowerVR chipektől? (/cikkek/it-tech/134221/apple-powervr)	Eszközvezérlő tetoválások jöhetnek (/cikkek/it-tech/120686/eszkozvezerlo-tetovalasok)	
2021-től nem építhetők kisebb tranzisztorok (/cikkek/it-tech/120833/2021-tranzisztorok)	Európai autóelektronikai óriáscég került kínai kézbe (/cikkek/it-tech/134663/europai-autoelektronikai-oriascegkerult-kinai-kezbe)	
Testbe építhető chip sugározhatja az adatokat (/cikkek/it-tech/111979/testbe-adatokat)	A jövő chipgyártási technológiát keresi az IBM (/cikkek/it-tech/116525/a-jovo-chipgyartasi-technologiat-keresi-az-ibm)	

Hozzászólások

https://www.fhstp.ac.at/de/newsroom/news/fh-projektvorstellungen-auf-der-deepsec-2018

FH Projektvorstellungen auf der DeepSec 2018

13.12.2018

Zuerst der erste Platz am Open Minds Award, danach eine Projektvorstellung in Seoul und jetzt auch auf der DeepSec 2018.

Die DeepSec 2018 – In-Depth Security Conference Europe – fand Ende November in Wien statt. Die zwei vorgestellten FH-Projekte SoniTalk und SoniControl werden von Matthias Zeppelzauer betreut und untersuchen die geheime Kommunikation zwischen Endgeräten: Smartphones geben mittels Ultraschallwellen Informationen weiter, dieser Informationsfluss kann unterbunden bzw. kontrolliert werden.

Unter dem Titel „Data over Sound“ erklärt Zeppelzauer die Technologie hinter den beiden Forschungsprojekten und erklärt, warum die Wahrung der Privatsphäre und ein Bewusstseni für IT-Sicherheit wichtig sind.

SoniControl und SoniTalk

Mittels Ultraschallwellen ist es möglich, zwischen mobilen Geräten unbemerkt Daten auszutauschen ohne dass es EndbenutzerInnen merken. Diese neue Technologie wird zum Beispiel verwendet, um an bestimmten Orten zielgerichtete Werbung zu schalten oder um Internetinhalte zu filtern. „SoniTalk“ versucht diese unbemerkten Verbindungen zu enttarnen und zu blockieren, sodass NutzerInnen wieder volle Kontrolle über persönliche Daten erhalten und diese nicht für Werbezwecke missbraucht werden.

Weiterführende Links

Project Introduction: Data over Sound – Risks and Chances of an emerging Communication Channel

Infos zum Projekt SoniControl

Zur Website DeepSec 2018

13.12.2018

FH Projektvorstellungen auf der DeepSec 2018

#forschung
(https://www.fhstp.ac.at/de/newsroom/@@newsroom_filter/422a632f72d9464da33bac0bc140a3


(https://www.fhstp.ac.at/de/newsroom/news/fh-projektvorstellungen-auf-der-deepsec-2018/@@display-file/image/Gebaeude_Panorama_Nacht_c_Fotostudio_Kraus.jpg)

Zuerst der erste Platz am Open Minds Award, danach eine Projektvorstellung in Seoul und jetzt auch auf der DeepSec 2018.

Die DeepSec 2018 (https://www.deepsec.net) – In-Depth Security Conference Europe – fand Ende November in Wien statt. Die zwei vorgestellten FH-Projekte SoniTalk und SoniControl werden von Matthias Zeppelzauer betreut und untersuchen die geheime Kommunikation zwischen Endgeräten: Smartphones geben mittels Ultraschallwellen Informationen weiter, dieser Informationsfluss kann unterbunden bzw. kontrolliert werden.

Unter dem Titel „Data over Sound“ erklärt Zeppelzauer die Technologie hinter den beiden Forschungsprojekten und erklärt, warum die Wahrung der Privatsphäre und ein Bewusstseni für IT-Sicherheit wichtig sind.

SoniControl und SoniTalk

Mittels Ultraschallwellen ist es möglich, zwischen mobilen Geräten unbemerkt Daten auszutauschen ohne dass es EndbenutzerInnen merken. Diese neue Technologie wird zum Beispiel verwendet, um an bestimmten Orten zielgerichtete Werbung zu schalten oder um Internetinhalte zu filtern. „SoniTalk“ versucht diese unbemerkten Verbindungen zu enttarnen und zu blockieren, sodass NutzerInnen wieder volle Kontrolle über persönliche Daten erhalten und diese nicht für Werbezwecke missbraucht werden.

Weiterführende Links

- Project Introduction (https://www.deepsec.net/speaker.html#PSLOT398): Data over Sound – Risks and Chances of an emerging Communication Channel
- Infos zum Projekt SoniControl (https://sonicontrol.fhstp.ac.at/)
- Zur Website DeepSec 2018 (https://www.deepsec.net/)

Jetzt teilen:

Facebook (https://www.facebook.com/sharer/sharer.php?app_id=111123232258315&u=https%3A%2F%2Fwww.fhstp.ac.at%2Fde%2Fnewsroom%2Fnews%2projektvorstellungen-auf-der-deepsec-2018)
Twitter (https://twitter.com/intent/tweet?text=&url=https%3A%2F%2Fwww.fhstp.ac.at%2Fde%2Fnewsroom%2Fnews%2Ffh-projektvorstellungen-auf-der-deepsec-2018&via=fh_stpoelten&hashtags=fhstp)
WhatsApp (whatsapp://send?text=https%3A%2F%2Fwww.fhstp.ac.at%2Fde%2Fnewsroom%2Fnews%2Ffh-projektvorstellungen-auf-der-deepsec-2018)
LinkedIn (https://www.linkedin.com/shareArticle?mini=true&url=https%3A%2F%2Fwww.fhstp.ac2018&title=FH%20Projektvorstellungen%20auf%20der%20DeepSec%202018&summary=Zuerst%projektvorstellungen-auf-der-deepsec-2018)
Xing (https://www.xing.com/spi/shares/new?url=https%3A%2F%2Fwww.fhstp.ac.at%2Fde%2Fnewsroom%2Fnews%2Ffh-projektvorstellungen-auf-der-deepsec-2018)

https://www.golem.de/news/sicherheit-welche-gefahren-durch-drohnen-drohen-1812-138091.html

Welche Gefahren durch Drohnen drohen

Deepsec 2018 - Flugobjekte mit biologischen Kampfstoffen, Motorsäge oder Pistole: 140 Risiken durch Drohnen hat der Sicherheitsexterte Dominique Brack gesammelt. Die geplanten Angriffe sind dabei gar nicht die schlimmsten.

Ein Interview von Jan Weisensee veröffentlicht am 6. Dezember 2018, 11:00 Uhr

Der für das Schweizer Telekommunikationsunternehmen Swisscom tätige Sicherheitsexperte Dominique Brack analysiert zusammen mit anderen Anbietern kritischer Infrastrukturen mögliche Angriffsszenarien mit kommerziell erhältlichen Drohnen. Auf der Sicherheitskonferenz Deepsec in Wien hat er seine Ergebnisse vorgestellt.

Golem.de: Herr Brack, Sie beschäftigen sich mit Gefahren durch den Einsatz ziviler Drohnen. Welches ist der beängstigendste Drohnenangriff, den Sie sich realistisch vorstellen können?

Dominique Brack: Es gibt natürlich sehr viele komplexe Angriffe, die zum Beispiel dazu führen können, dass der Betrieb eines Kernkraftwerks erheblich gestört werden kann. In Venezuela wurde vermeintlich ein Anschlag auf den Präsidenten durch eine Drohne mit Sprengstoff registriert. Das FBI Hostage Rescue Team wurde durch einen Drohnenschwarm behindert, gelenkt durch jene Kriminellen, die das Team observierte. In Syrien setzte die Terrormiliz IS mit Sprengstoff bestückte Drohnen ein. Daraufhin hat DJI weite Teile Syriens und des Iraks per Softwareupdate zu No-Fly-Zones erklärt, in denen DJI-Drohnen nicht fliegen. Am wahrscheinlichsten sind aber immer noch unabsichtliche Drohneneinsätze, also jemand fliegt irgendwo hinein, wo es nicht geplant war, eine Drohne stürzt bei einem Sportevent ab. Das sind die Szenarien, die am ehesten eintreffen.

Golem.de: Während Ihres Vortrags auf der Deepsec-Konferenz in Wien haben Sie einen kleinen Film laufen lassen, der eine Drohne zeigt, die frontal mit einer Flugzeugtragfläche kollidiert. Ist Ihnen ein solcher Fall schon einmal untergekommen?

Brack: Das war ein Test der University of Dayton. Das Video zeigt die Auswirkungen des Einschlags einer Drohne auf die Konstruktion eines Flugzeugflügels. Mit rund 380 Kilometern pro Stunde wurde die Drohne zum Aufschlag gebracht, und das hat natürlich die Tragfläche durchschlagen. Drohnen erzeugen bei der Flugsicherheit ähnliche Schäden wie Vögel, das heißt an den Scheiben, Propellern oder Tragflächen von Flugzeugen. Aber es gibt

natürlich auch die Gefahr, dass Flugzeuge nicht landen dürfen, wenn sich eine Drohne in der Kontrollzone des Flughafens befindet. Das war zum Beispiel in Dubai der Fall, wo der Flugbetrieb vier Stunden lang gestört war. Die Kosten wurden auf 98.368 US-Dollar pro Minute geschätzt, denn die Flieger müssen in eine Warteschleife oder auf einen anderen Flughafen ausweichen. Also im Prinzip ist so ein Vorfall eine ökonomische Denial-of-Service-Attacke.

Golem.de: Sie arbeiten eigentlich für ein Telekommunikationsunternehmen. Wie kommen Sie dazu, sich mit den Gefahren durch Drohnen zu beschäftigen?

Brack: Als Telko-Unternehmen sind wir auch Teil der kritischen Infrastruktur unseres Landes. In diesem Bereich arbeiten wir mit den anderen Betreibern solcher Infrastrukturen, wie Banken, Kommunikation, Energie, Abfallwesen, öffentliche Sicherheit et cetera zusammen und im Rahmen dieser Zusammenarbeit wurden die Risiken durch Drohnen angesprochen und entsprechend ausgearbeitet.

Golem.de: Werden die Erkenntnisse, die Sie aus Ihrer Arbeit gewinnen, durch Ihren Arbeitgeber direkt vermarktet?

Brack: Jein. Also wir arbeiten viel im Bereich der strategischen Sicherheit und das stellen wir natürlich auch der Allgemeinheit zur Verfügung. Wenn wir aber einen konkreten Auftrag erhalten, beispielsweise von einem Spital oder einem großen Rockkonzert, dann werden wir als Consultants eingesetzt und dann ist das natürlich ein kommerzielles Engagement.

Golem.de: Sie haben einen Risikokatalog für kommerzielle Drohnen mit verschiedenen Angriffsszenarien entwickelt.

Brack: Genau. Der Katalog enthält zurzeit rund 140 individuelle Risiken und wächst auch ständig. Diese Risiken haben wir evaluiert und strukturiert, um Methodik in das Thema Drohnen zu bringen. Dabei handelt es sich um Risiken, die sich bereits materialisiert haben beziehungsweise wirklich ausgeführt wurden. Es gibt zum Beispiel ein Proof-of-Concept, bei dem mit einer Drohne eine Pistole abgefeuert wurde, das klappt gut. Oder sogar solche mit angehängter Motorsäge, mit denen man Bäume und Eiszapfen geschnitten hat. Aus solchen Anwendungsfällen haben wir die Risiken entsprechend abgeleitet. Das sind Anwendungsfälle, die existieren, die lediglich bisher noch nicht missbraucht wurden, zum Beispiel als offensive Angriffe gegen Institutionen, Organisationen oder die Öffentlichkeit.

Golem.de: Beispiel Pistole: Arbeiten Sie auch mit militärischen Akteuren zusammen?

Brack: Was dort vermutlich eher relevant ist, sind Risiken durch Drohnen mit Payload, also etwas, das abgeworfen wird. Da gibt es ja bereits viele Erkenntnisse aus unseren Gefängnissen, wo mit Hilfe von Drohnen Waren geschmuggelt werden, etwa Drogen, Geld, Handys oder SIM-Karten. Es gibt auch Drohnen, die an der mexikanischen Grenze Drogen schmuggeln, das wird also effektiv als Mittel eingesetzt.

Golem.de: Welche weiteren real existierenden Angriffe kennen Sie aus Ihrer Arbeit?

Brack: Definitiv kennen wir den Einsatz gegen Personen, wo wirklich aktiv ein Schaden angerichtet werden soll. Die Drohnen werden zum Beispiel mutwillig in ein Fenster geflogen, in ein Auto oder in eine Menschenmenge. Was wir auch oft erleben, sind Verletzungen der Privatsphäre, bei denen es um das Ausspähen etwa von VIP-Properties geht.

Golem.de: Wie sieht es beim nachrichtendienstlichen Ausspähen aus?

Brack: Das ist definitiv ein Problem. Die Drohne ist ein fliegendes IoT-Device. Sie ist eine Verlängerung sämtlicher Spähmöglichkeiten, die es heute gibt: im Sinne der Distanz, der Zeit und der Höhe. Wenn ich mit Access Points hacke, dann fliege ich den Access Point einfach in ein Kraftwerk, in die Hochsicherheitszone oder eine militärische Kaserne rein und kann dort auch landen. Bestehende Risiken werden eigentlich verstärkt mit der Drohne.

Golem.de: Wie können sich Betroffene vor diesen Gefahren schützen?

Brack: Einerseits ist die normale Vorsicht angebracht. Wer zum Schutz einen Zaun baut, sollte vielleicht auch einmal in den Himmel schauen. Gefährlich ist es, sich durch Zäune und Zugangskontrollen am Boden in falscher Sicherheit zu wiegen. Andererseits schützen auch Vorsichtsmaßnahmen wie ein Schutz gegen Einsicht von außen, wenn man ein Meeting hat, auf dem etwa interne Geschäftszahlen oder andere klassifizierte Informationen präsentiert werden. Darüber hinaus ist es sehr schwierig, sich als Privater gegen solche Bedrohungen zu wehren, denn eine Drohne kann sehr hoch fliegen, ist daher fast unsichtbar und kaum zu hören.

Golem.de: Wie sieht es mit aktiven Abwehrmaßnahmen aus?

Brack: Es gibt zwar Drohenerkennungslösungen, aber bei der aktiven Abwehr ist das Problem, dass die effektivste Lösung - das Jamming - für Privatpersonen gar nicht erlaubt ist. Ich denke, das wird sich in den nächsten Jahren

auch nicht ändern. Dass man einfach mal schnell einen Jammer [Störsender, Anm. d. Red.] aufstellt und damit alle Frequenzen stört, das gibt es leider nur im Actionfilm. In Wirklichkeit ist die Technik absolut verboten und darf nur von Polizei und Militär eingesetzt werden. Die Polizei wiederum setzt das nur bei großen Events wie zum Beispiel dem World Economic Forum ein, wo sie etwas schützen muss. Für Private gibt es fast keine aktiven Abwehrmöglichkeiten. Zumindest in der Schweiz geht beispielsweise Herunterschießen gar nicht. Schon die Drohne mit dem Gartenschlauch abzuspritzen oder mit Steinen danach zu werfen, ist rechtlich problematisch. Man kann eine Drohne natürlich melden, wenn man den Piloten identifiziert hat, aber ansonsten ist es sehr schwierig, sich aktiv zu wehren. Da hinkt das Gesetz der Technik weit hinterher.

Golem.de: Was müsste der Gesetzgeber tun, um die Situation zu verbessern?

Brack: Ich denke, es werden bereits sehr viele Schritte unternommen, um die Öffentlichkeit zu schützen, zum Beispiel durch Gewichtsbeschränkungen, so typischerweise um die 250 Gramm. Also was gilt noch als Spielzeugdrohne, die man ja gerne mit seinen Kindern fliegen möchte, und was nicht. Außerdem darf man über eine bestimmte Höhe nicht aufsteigen und es gibt Apps, die einem anzeigen, ob zum Beispiel ein Flughafen in der Nähe ist. Es wird schon viel unternommen, einige Länder sind sehr streng, da gibt es komplette Flugverbote oder man muss sich lizenzieren oder die Drohne registrieren. Beides wird sicherlich irgendwann flächendeckend eingeführt, damit der Drohneneinsatz auch versicherungstechnisch geklärt ist. Das Problem ist natürlich: Gesetze haben noch nie Kriminelle von ihrem Tun abgehalten. Daher muss ich mir als Unternehmen oder als Anbieter kritischer Infrastrukturen überlegen, wie man sich darüber hinaus noch gegen dedizierte und gegebenenfalls verheerenden Drohnenangriffe schützen muss.

Golem.de: Wäre es nicht sinnvoll, hier das Jamming zu erlauben?

Brack: Ich denke nicht, denn das ist viel zu gefährlich. Wir haben Szenarien entwickelt, in denen zum Beispiel in einem Fußballstadion das Wi-Fi oder 5G gejammt werden, aber auf diese Netze sind ja auch Notfallorganisationen wie Sanitäter oder Polizei angewiesen. Was ich mir dagegen gut vorstellen könnte, und daran arbeiten wir gerade zusammen mit der Schweizer Polizei und dem Militär, wäre die Einführung von lizenzierten Jammern in einer Public-Private-Partnership. Ich könnte mir ein gemeinsames digitales Lagebild vorstellen, das eine Drohnenpräsenz in forensischer Qualität aufzeichnet und diese Information live mit der Polizei teilt. So könnte man sagen, liebe Polizei, hier ist der Beweis, die Drohne ist dort, könnt ihr uns helfen. Dann könnte die Polizei den Knopf zum Jamming drücken. Denn für diese Art von Bedrohungen braucht es definitiv Lösungen, ohne Jamming generell zu erlauben.

Ein ähnliches Problem besteht mit Rettungshelikoptern. Wenn jemand eine Drohne an einem Ort legal fliegen lässt, zum Beispiel auf einem Feld, und zu diesem Zeitpunkt auf einer nahegelegenen Straße ein Unfall passiert. Dann kommt der Rettungshelikopter, um die Verletzten ins Spital zu bringen. Wenn dann dort eine Drohne herumfliegt - und wir hatten in der Schweiz mehrere solcher Fälle -, darf der Rettungshelikopter nicht abfliegen. Die Polizei musste erst um mehrere Häuser herumrennen und versuchen, den Drohnenpiloten zu identifizieren, der einfach zu einem digitalen Gaffer geworden ist.

Golem.de: Wie reagieren neue Kunden und Betroffene auf Ihre Warnungen?

Brack: Ich habe jetzt viel mit großen Events zu tun, wie die Jugendolympiade 2020 und verschiedene Musik- und Filmfestivals. Viele von denen sind gewohnt, Risikoanalysen über Flucht- und Zutrittswege und Gefahrenszenarien zu machen. Aber die spezifische Gefahr durch Drohnen sind ganz neu.

Golem.de: Wie werden sich Drohnen in den kommenden fünf Jahren technologisch entwickeln?

Brack: Drohnen werden sicher viel autonomer werden. Es gibt ja heute bereits spezialisierte Drohnen für die Fotografie, die einem automatisch folgen, zum Beispiel wenn man Mountainbike fährt. In Zukunft werden Drohnen automatisch Anweisungen wie "fliege mit der Wärmbildkamera um mein Haus" ausführen. Auch für die Verteilung von Medikamenten in schwer zugänglichen Regionen oder sogar das Abwerfen eines Rettungsrings in Seenot sind kommende Anwendungsfälle.

Diese Automatisierung kann auf der anderen Seite auch die Risiken minimieren, denn in solchen Fällen ist vorprogrammiert, was eine Drohne darf und was nicht. Auch technologisch wird es noch Veränderungen geben. Die Motoren werden effizienter, die Flugdauer länger und auch beim Leichtbau und vielleicht bei der Solartechnologie wird es Entwicklungen geben. Aber es gibt natürlich auch eine physikalisch bedingte Effizienzgrenze bei dem, was eine Drohne kann. In manchen Szenarien wie etwa bei einem Langdistanz- oder Schwerlastflug ist es oft einfacher, einen klassischen Helikopter einzusetzen.

Golem.de: Herr Brack, wir danken Ihnen für das Gespräch.

Sicherheit: Welche Gefahren durch Drohnen drohen

Deepsec 2018

Flugobjekte mit biologischen Kampfstoffen, Motorsäge oder Pistole: 140 Risiken durch Drohnen hat der Sicherheitsexterte Dominique Brack gesammelt. Die geplanten Angriffe sind dabei gar nicht die schlimmsten.

Ein Interview von Jan Weisensee veröffentlicht am

6. Dezember 2018, 11:00 Uhr

(Bild: Dominique Brack)

Zivile Drohnen können mit allerhand Payload bestückt werden.

Der für das Schweizer Telekommunikationsunternehmen Swisscom tätige Sicherheitsexperte Dominique Brack analysiert zusammen mit anderen Anbietern kritischer Infrastrukturen mögliche Angriffsszenarien mit kommerziell erhältlichen Drohnen. Auf der Sicherheitskonferenz Deepsec in Wien hat er seine Ergebnisse vorgestellt.

Inhalt:

Golem.de: Herr Brack, Sie beschäftigen sich mit Gefahren durch den Einsatz ziviler Drohnen. Welches ist der beängstigendste Drohnenangriff, den Sie sich realistisch vorstellen können?
Dominique Brack: Es gibt natürlich sehr viele komplexe Angriffe, die zum Beispiel dazu führen können, dass der Betrieb eines Kernkraftwerks erheblich gestört werden kann. In Venezuela wurde vermeintlich ein Anschlag auf den Präsidenten durch eine Drohne mit Sprengstoff registriert. Das FBI Hostage Rescue Team wurde durch einen Drohnenschwarm behindert, gelenkt durch jene Kriminellen, die das Team observierte. In Syrien setzte die Terrormiliz IS mit Sprengstoff bestückte Drohnen ein. Daraufhin hat DJI weite Teile Syriens und des Iraks per Softwareupdate zu No-Fly-Zones erklärt, in denen DJI-Drohnen nicht fliegen. Am wahrscheinlichsten sind aber immer noch unabsichtliche Drohneneinsätze, also jemand fliegt irgendwo hinein, wo es nicht geplant war, eine Drohne stürzt bei einem Sportevent ab. Das sind die Szenarien, die am ehesten eintreffen.
Golem.de: Während Ihres Vortrags auf der Deepsec-Konferenz in Wien haben Sie einen kleinen Film laufen lassen, der eine Drohne zeigt, die frontal mit einer Flugzeugtragfläche kollidiert. Ist Ihnen ein solcher Fall schon einmal untergekommen?

Brack: Das war ein Test der University of Dayton. Das Video zeigt die Auswirkungen des Einschlags einer Drohne auf die Konstruktion eines Flugzeugflügels. Mit rund 380 Kilometern pro Stunde wurde die Drohne zum Aufschlag gebracht, und das hat natürlich die Tragfläche durchschlagen. Drohnen erzeugen bei der Flugsicherheit ähnliche Schäden wie Vögel, das heißt an den Scheiben, Propellern oder Tragflächen von Flugzeugen. Aber es gibt natürlich auch die Gefahr, dass Flugzeuge nicht landen dürfen, wenn sich eine Drohne in der Kontrollzone des Flughafens befindet. Das war zum Beispiel in Dubai der Fall, wo der Flugbetrieb vier Stunden lang gestört war. Die Kosten wurden auf 98.368 US-Dollar pro Minute geschätzt, denn die Flieger müssen in eine Warteschleife oder auf einen anderen Flughafen ausweichen. Also im Prinzip ist so ein Vorfall eine ökonomische Denial-of-Service-Attacke.
Golem.de: Sie arbeiten eigentlich für ein Telekommunikationsunternehmen. Wie kommen Sie dazu, sich mit den Gefahren durch Drohnen zu beschäftigen?
Brack: Als Telko-Unternehmen sind wir auch Teil der kritischen Infrastruktur unseres Landes. In diesem Bereich arbeiten wir mit den anderen Betreibern solcher Infrastrukturen, wie Banken, Kommunikation, Energie, Abfallwesen, öffentliche Sicherheit et cetera zusammen und im Rahmen dieser Zusammenarbeit wurden die Risiken durch Drohnen angesprochen und entsprechend ausgearbeitet.
Golem.de: Werden die Erkenntnisse, die Sie aus Ihrer Arbeit gewinnen, durch Ihren Arbeitgeber direkt vermarktet?
Brack: Jein. Also wir arbeiten viel im Bereich der strategischen Sicherheit und das stellen wir natürlich auch der Allgemeinheit zur Verfügung. Wenn wir aber einen konkreten Auftrag erhalten, beispielsweise von einem Spital oder einem großen Rockkonzert, dann werden wir als Consultants eingesetzt und dann ist das natürlich ein kommerzielles Engagement.

Allgemeine Risiken durch zivile Drohnen (Quelle: Dominique Brack)

Golem.de: Sie haben einen Risikokatalog für kommerzielle Drohnen mit verschiedenen Angriffsszenarien entwickelt.
Brack: Genau. Der Katalog enthält zurzeit rund 140 individuelle Risiken und wächst auch ständig. Diese Risiken haben wir evaluiert und strukturiert, um Methodik in das Thema Drohnen zu bringen. Dabei handelt es sich um Risiken, die sich bereits materialisiert haben beziehungsweise wirklich ausgeführt wurden. Es gibt zum Beispiel ein Proof-of-Concept, bei dem mit einer Drohne eine Pistole abgefeuert wurde, das klappt gut. Oder sogar solche mit angehängter Motorsäge, mit denen man Bäume und Eiszapfen geschnitten hat. Aus solchen Anwendungsfällen haben wir die Risiken entsprechend abgeleitet. Das sind Anwendungsfälle, die existieren, die lediglich bisher noch nicht missbraucht wurden, zum Beispiel als offensive Angriffe gegen Institutionen, Organisationen oder die Öffentlichkeit.

Video: DJI Zenmuse XT2 (4:09)

Golem.de: Beispiel Pistole: Arbeiten Sie auch mit militärischen Akteuren zusammen?
Brack: Was dort vermutlich eher relevant ist, sind Risiken durch Drohnen mit Payload, also etwas, das abgeworfen wird. Da gibt es ja bereits viele Erkenntnisse aus unseren Gefängnissen, wo mit Hilfe von Drohnen Waren geschmuggelt werden, etwa Drogen, Geld, Handys oder SIM-Karten. Es gibt auch Drohnen, die an der mexikanischen Grenze Drogen schmuggeln, das wird also effektiv als Mittel eingesetzt.
Golem.de: Welche weiteren real existierenden Angriffe kennen Sie aus Ihrer Arbeit?
Brack: Definitiv kennen wir den Einsatz gegen Personen, wo wirklich aktiv ein Schaden angerichtet werden soll. Die Drohnen werden zum Beispiel mutwillig in ein Fenster geflogen, in ein Auto oder in eine Menschenmenge. Was wir auch oft erleben, sind Verletzungen der Privatsphäre, bei denen es um das Ausspähen etwa von VIP-Properties geht.
Golem.de: Wie sieht es beim nachrichtendienstlichen Ausspähen aus?
Brack: Das ist definitiv ein Problem. Die Drohne ist ein fliegendes IoT-Device. Sie ist eine Verlängerung sämtlicher Spähmöglichkeiten, die es heute gibt: im Sinne der Distanz, der Zeit und der Höhe. Wenn ich mit Access Points hacke, dann fliege ich den Access Point einfach in ein Kraftwerk, in die Hochsicherheitszone oder eine militärische Kaserne rein und kann dort auch landen. Bestehende Risiken werden eigentlich verstärkt mit der Drohne.

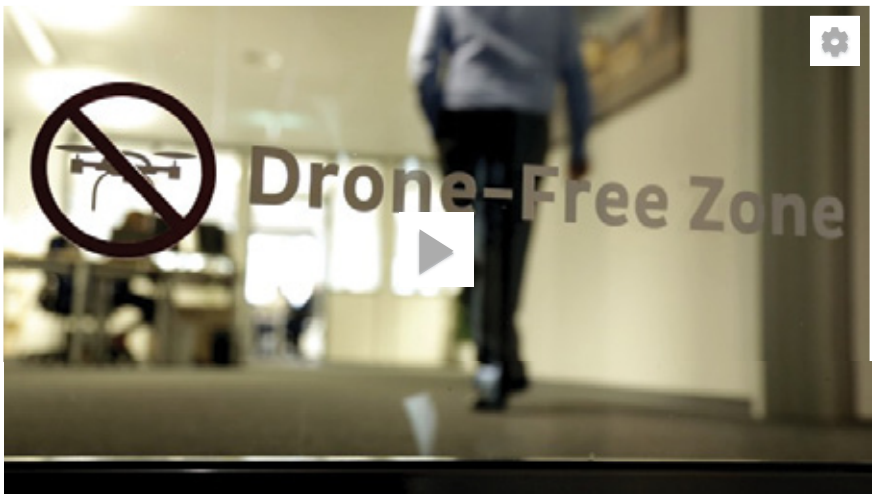
Wie kann man sich schützen?

Golem.de: Wie können sich Betroffene vor diesen Gefahren schützen?

Brack: Einerseits ist die normale Vorsicht angebracht. Wer zum Schutz einen Zaun baut, sollte vielleicht auch einmal in den Himmel schauen. Gefährlich ist es, sich durch Zäune und Zugangskontrollen am Boden in falscher Sicherheit zu wiegen. Andererseits schützen auch Vorsichtsmaßnahmen wie ein Schutz gegen Einsicht von außen, wenn man ein Meeting hat, auf dem etwa interne Geschäftszahlen oder andere klassifizierte Informationen präsentiert werden. Darüber hinaus ist es sehr schwierig, sich als Privater gegen solche Bedrohungen zu wehren, denn eine Drohne kann sehr hoch fliegen, ist daher fast unsichtbar und kaum zu hören.

Golem.de: Wie sieht es mit aktiven Abwehrmaßnahmen aus?

Brack: Es gibt zwar Drohenerkennungslösungen, aber bei der aktiven Abwehr ist das Problem, dass die effektivste Lösung - das Jamming - für Privatpersonen gar nicht erlaubt ist. Ich denke, das wird sich in den nächsten Jahren auch nicht ändern. Dass man einfach mal schnell einen Jammer [Störsender, Anm. d. Red.] aufstellt und damit alle Frequenzen stört, das gibt es leider nur im Actionfilm. In Wirklichkeit ist die Technik absolut verboten und darf nur von Polizei und Militär eingesetzt werden. Die Polizei wiederum setzt das nur bei großen Events wie zum Beispiel dem World Economic Forum ein, wo sie etwas schützen muss. Für Private gibt es fast keine aktiven Abwehrmöglichkeiten. Zumindest in der Schweiz geht beispielsweise Herunterschießen gar nicht. Schon die Drohne mit dem Gartenschlauch abzuspritzen oder mit Steinen danach zu werfen, ist rechtlich problematisch. Man kann eine Drohne natürlich melden, wenn man den Piloten identifiziert hat, aber ansonsten ist es sehr schwierig, sich aktiv zu wehren. Da hinkt das Gesetz der Technik weit hinterher.



Video: Dedrone - Bericht (1:47)

Golem.de: Was müsste der Gesetzgeber tun, um die Situation zu verbessern?

Brack: Ich denke, es werden bereits sehr viele Schritte unternommen, um die Öffentlichkeit zu schützen, zum Beispiel durch Gewichtsbeschränkungen, so typischerweise um die 250 Gramm. Also was gilt noch als Spielzeugdrohne, die man ja gerne mit seinen Kindern fliegen möchte, und was nicht. Außerdem darf man über eine bestimmte Höhe nicht aufsteigen und es gibt Apps, die einem anzeigen, ob zum Beispiel ein Flughafen in der Nähe ist. Es wird schon viel unternommen, einige Länder sind sehr streng, da gibt es komplette Flugverbote oder man muss sich lizenzieren oder die Drohne registrieren. Beides wird sicherlich irgendwann flächendeckend eingeführt, damit der Drohneneinsatz auch versicherungstechnisch geklärt ist. Das Problem ist natürlich: Gesetze haben noch nie Kriminelle von ihrem Tun abgehalten. Daher muss ich mir als Unternehmen oder als Anbieter kritischer Infrastrukturen überlegen, wie man sich darüber hinaus noch gegen dedizierte und gegebenenfalls verheerenden Drohnenangriffe schützen muss.

Golem.de: Wäre es nicht sinnvoll, hier das Jamming zu erlauben?

Brack: Ich denke nicht, denn das ist viel zu gefährlich. Wir haben Szenarien entwickelt, in denen zum Beispiel in einem Fußballstadion das Wi-Fi oder 5G gejammt werden, aber auf diese Netze sind ja auch Notfallorganisationen wie Sanitäter oder Polizei angewiesen. Was ich mir dagegen gut vorstellen könnte, und daran arbeiten wir gerade zusammen mit der Schweizer Polizei und dem Militär, wäre die Einführung von lizenzierten Jammern in einer Public-Private-Partnership. Ich könnte mir ein gemeinsames digitales Lagebild vorstellen, das eine Drohnenpräsenz in forensischer Qualität aufzeichnet und diese Information live mit der Polizei teilt. So könnte man sagen, liebe Polizei, hier ist der Beweis, die Drohne ist dort, könnt ihr uns helfen. Dann könnte die Polizei den Knopf zum Jamming drücken. Denn für diese Art von Bedrohungen braucht es definitiv Lösungen, ohne Jamming generell zu erlauben.

Ein ähnliches Problem besteht mit Rettungshelikoptern. Wenn jemand eine Drohne an einem Ort legal fliegen lässt, zum Beispiel auf einem Feld, und zu diesem Zeitpunkt auf einer nahegelegenen Straße ein Unfall passiert. Dann kommt der Rettungshelikopter, um die Verletzten ins Spital zu bringen. Wenn dann dort eine Drohne herumfliegt - und wir hatten in der Schweiz mehrere solcher Fälle -, darf der Rettungshelikopter nicht abfliegen. Die Polizei musste erst um mehrere Häuser herumrennen und versuchen, den Drohnenpiloten zu identifizieren, der einfach zu einem digitalen Gaffer geworden ist.

Golem.de: Wie reagieren neue Kunden und Betroffene auf Ihre Warnungen?

Brack: Ich habe jetzt viel mit großen Events zu tun, wie die Jugendolympiade 2020 und verschiedene Musik- und Filmfestivals. Viele von denen sind gewohnt, Risikoanalysen über Flucht- und Zutrittswege und Gefahrenszenarien zu machen. Aber die spezifische Gefahr durch Drohnen sind ganz neu.

Golem.de: Wie werden sich Drohnen in den kommenden fünf Jahren technologisch entwickeln?

Brack: Drohnen werden sicher viel autonomer werden. Es gibt ja heute bereits spezialisierte Drohnen für die Fotografie, die einem automatisch folgen, zum Beispiel wenn man Mountainbike fährt. In Zukunft werden Drohnen automatisch Anweisungen wie "fliege mit der Wärmbildkamera um mein Haus" ausführen. Auch für die Verteilung von Medikamenten in schwer zugänglichen Regionen oder sogar das Abwerfen eines Rettungsrings in Seenot sind kommende Anwendungsfälle.

Diese Automatisierung kann auf der anderen Seite auch die Risiken minimieren, denn in solchen Fällen ist vorprogrammiert, was eine Drohne darf und was nicht. Auch technologisch wird es noch Veränderungen geben. Die Motoren werden effizienter, die Flugdauer länger und auch beim Leichtbau und vielleicht bei der Solartechnologie wird es Entwicklungen geben. Aber es gibt natürlich auch eine physikalisch bedingte Effizienzgrenze bei dem, was eine Drohne kann. In manchen Szenarien wie etwa bei einem Langdistanz- oder Schwerlastflug ist es oft einfacher, einen klassischen Helikopter einzusetzen.

Golem.de: Herr Brack, wir danken Ihnen für das Gespräch. ■

https://futurezone.at/science/ein-chip-unter-der-haut-ist-mir-zu-invasiv/400340710

„Ein Chip unter der Haut ist mir zu invasiv“

05.12.2018, Barbara Wimmer

Erste Firmen lassen ihren Mitarbeitern Chips einpflanzen. Die Wissenschaftlerin Ulrike Hugl warnt, dass dieser Trend bald Alltag sein könnte.

Was vor 15 Jahren als Spaß unter IT-Nerds begonnen hat, kommt jetzt immer mehr im Alltag an: das Einpflanzen von Chips unter die Haut. „Menschen haben sich bereits 2004 zum Spaß kleine RFID-Chips einpflanzen lassen, um sich damit am Computer einzuloggen oder ihr Auto aufzusperren. Jetzt setzen es Firmen bei ihren Mitarbeitern ein“, erzählt Ulrike Hugl, Forscherin an der Universität Innsbruck, im Gespräch mit dem KURIER. Sie hielt auf der Sicherheitskonferenz DeepSec einen Vortrag zum Thema „RFID-Chip im Körper“.

Das Technik-Unternehmen „Three Square Market“ (32M) in Wisconsin in den USA hatte seine Mitarbeiter schon vor eineinhalb Jahren mit einem Mini-Chip ausgestattet, der zwischen Daumen und Zeigefinger unter der Haut implantiert wurde. Der Chip wird seither von den Mitarbeitern dazu genutzt, um sich in die Büro-Computer einzuloggen, für Essen und Trinken aus den Automaten zu zahlen, Türen zu öffnen und den Kopierer zu bedienen.

Großflächiger Einsatz in England

Vor kurzem wurde via Guardian bekannt, dass auch in Großbritannien bereits Gespräche mit interessierten Firmen laufen, dieses Modell großflächig zu kopieren. Die Chips dafür stammen von der schwedischen Firma Biohax. „Die Firmen stammen aus dem Finanz- und Rechtsbereich und sind nicht klein. Ein Unternehmen soll mehrere hunderttausend Angestellte haben“, sagt Hugl. Das Einsetzen eines Biochips kostet dabei etwa 170 Euro pro Stück.
Die Mitarbeiter sollen nicht dazu gezwungen werden, sondern das Ganze soll auf Freiwilligkeit beruhen, heißt es seitens der Unternehmen. Für Hugl ist das allerdings mehr Schein als Sein: „Natürlich entsteht da ein Druck auf die Mitarbeiter. Es entsteht soziale Kontrolle und ein Gruppenzwang, das tun zu müssen, was die anderen machen.“

Breite Kritik

Für die Forscherin sei das in etwa vergleichbar mit „Sozial Freezing“: „Unternehmen haben angekündigt, die Kosten für das Einfrieren von Eizellen von Mitarbeiterinnen zu übernehmen. Natürlich ist dadurch ein Druck auf die Mitarbeiterinnen entstanden, nicht mehr selbst zu entscheiden, wann sie Kinder bekommen. Ich frage mich da: Wie weit dürfen Firmen gehen?“

In Großbritannien warnten der Firmenverband CBI (Confederation of British Industry) sowie die Gewerkschaft TUC vor solchen Entwicklungen. „In Österreich würden derartige Vorhaben auf großen Widerstand der Gewerkschaften und Arbeitnehmervertretungen stoßen. Ohne Betriebsrat ginge das nicht“, meint Hugl. „Allerdings kann ich es mir als Option vorstellen, wenn die Mitarbeiter das aktiv vorantreiben.“

Die Firmen argumentierten damit, dass Mitarbeiter den Chip auch privat nutzen dürften, um etwa Autos aufzusperren oder um ihre Gesundheitsdaten darauf zu speichern. Dieser Ansatz wurde auch bereits von einigen Spitälern ausprobiert, um darauf Patientendaten zu speichern.

Fehlende Diskussion in der Gesellschaft

„Ich könnte mir vorstellen, dass die technologische Entwicklung weiter voranschreitet und wir keine kritische Diskussion darüber in der Gesellschaft haben. Dann kann es passieren, dass sich niemand etwas dabei denkt und sich in zehn Jahren alle einen Chip einpflanzen lassen“, warnt Hugl. Die Wissenschaftlerin bemängelt, dass wie bei vielen Technologie- und Datenschutz-Themen eine „breite Diskussion“ in der Gesellschaft fehle und sich zu wenig Menschen damit befassen.

Hugl selbst würde sich nie so einen Chip einpflanzen lassen. „Ein Chip unter der Haut ist mir zu invasiv“, sagt sie. „Nachdem ich weiß, was da alles getrackt, gemonitored und gedatamined wird, hätte ich meine größten Bedenken. Ich meide generell Technologien, die Daten über mich sammeln“, so die Forscherin. „Aus dem Bereich Wirtschaftskriminalität wissen wir, dass sich Angreifer anpassen an Technologien oder sie so nutzen, dass sie zu ihrem Vorteil sind. Eine Zutrittskarte kann ich jemandem physisch wegnehmen. Das Implantat kann ich allerdings nur herausschneiden“, fährt die Expertin fort.

Schnelle Entwicklung möglich

Der Chip ist zudem in der Lage, genau zu tracken wann ein Mitarbeiter kommt und geht. Außerdem stellt sich die Frage, was mit dem Chip passiert, wenn ein Mitarbeiter das Unternehmen wieder verlässt. „Was bedeutet das für den Körper?“, fragt sich Hugl, die davor warnt, dass das, was vor 15 Jahren als Versuche begonnen hat, plötzlich relativ rasch zu einer Massenanwendung werden könnte. Laut Amal Gfraafstra, der mit Digiwell selbst kleine Chips zum Implantieren vertreibt, seien es längst nicht mehr nur "IT-Nerds", die sich Chips einpflanzen würden. Es sei bereits das "Tattoo der Neuzeit".

„Manchmal vergehen da nur ein paar Jahre dazwischen. Viel hängt davon ab, wie man etwas vermarktet“, warnt Hugl, die fürchtet, dass wir von der Entwicklung „einfach überrollt“ werden könnten. Die Wissenschaftlerin wünscht sich daher einen breiten Diskurs über diese Themen – und zwar bevor sich plötzlich jeder einen Chip einpflanzen lässt, ohne davor nachzudenken.

SCIENCE 05.12.2018

„Ein Chip unter der Haut ist mir zu invasiv"

Bei Messen lassen sich NFC-Besucher freiwillig Chips einsetzen © Bild: APA/AFP/JONATHAN NACKSTRAND / JONATHAN NACKSTRAND

Erste Firmen lassen ihren Mitarbeitern Chips einpflanzen. Die Wissenschaftlerin Ulrike Hugl warnt, dass dieser Trend bald Alltag sein könnte.

Was vor 15 Jahren als Spaß unter IT-Nerds begonnen hat, kommt jetzt immer mehr im Alltag an: das Einpflanzen von Chips unter die Haut. „Menschen haben sich bereits 2004 zum Spaß kleine RFID-Chips einpflanzen lassen, um sich damit am Computer einzuloggen oder ihr Auto aufzusperren. Jetzt setzen es Firmen bei ihren Mitarbeitern ein", erzählt Ulrike Hugl, Forscherin an der Universität Innsbruck, im Gespräch mit dem KURIER. Sie hielt auf der Sicherheitskonferenz DeepSec einen Vortrag zum Thema „RFID-Chip im Körper".

Das Technik-Unternehmen „Three Square Market" (32M) in Wisconsin in den USA hatte seine Mitarbeiter schon vor eineinhalb Jahren mit einem Mini-Chip ausgestattet, der zwischen Daumen und Zeigefinger unter der Haut implantiert wurde. Der Chip wird seither von den Mitarbeitern dazu genutzt, um sich in die Büro-Computer einzuloggen, für Essen und Trinken aus den Automaten zu zahlen, Türen zu öffnen und den Kopierer zu bedienen.

DIGITAL LIFE

US-Firma lässt ihren Mitarbeitern Chips einpflanzen

Erste Firmen in Europa und den USA setzen auf NFC-Implantate bei ihren Angestellten. Sie sollen damit die Bürotüren aufsperren können. Experten warnen vor den Folgen.

Großflächiger Einsatz in England

Vor kurzem wurde via Guardian bekannt, dass auch in Großbritannien bereits Gespräche mit interessierten Firmen laufen, dieses Modell großflächig zu kopieren. Die Chips dafür stammen von der schwedischen Firma Biohax. „Die Firmen stammen aus dem Finanz- und Rechtsbereich und sind nicht klein. Ein Unternehmen soll mehrere hunderttausend Angestellte haben", sagt Hugl. Das Einsetzen eines Biochips kostet dabei etwa 170 Euro pro Stück.

Die Mitarbeiter sollen nicht dazu gezwungen werden, sondern das Ganze soll auf Freiwilligkeit beruhen, heißt es seitens der Unternehmen. Für Hugl ist das allerdings mehr Schein als Sein: „Natürlich entsteht da ein Druck auf die Mitarbeiter. Es entsteht soziale Kontrolle und ein Gruppenzwang, das tun zu müssen, was die anderen machen."

Breite Kritik

Für die Forscherin sei das in etwa vergleichbar mit „Sozial Freezing": „Unternehmen haben angekündigt, die Kosten für das Einfrieren von Eizellen von Mitarbeiterinnen zu übernehmen. Natürlich ist dadurch ein Druck auf die Mitarbeiterinnen entstanden, nicht mehr selbst zu entscheiden, wann sie Kinder bekommen. Ich frage mich da: Wie weit dürfen Firmen gehen?"

In Großbritannien warnten der Firmenverband CBI (Confederation of British Industry) sowie die Gewerkschaft TUC vor solchen Entwicklungen. „In Österreich würden derartige Vorhaben auf großen Widerstand der Gewerkschaften und Arbeitnehmervertretungen stoßen. Ohne Betriebsrat ginge das nicht", meint Hugl. „Allerdings kann ich es mir als Option vorstellen, wenn die Mitarbeiter das aktiv vorantreiben."

Die Firmen argumentierten damit, dass Mitarbeiter den Chip auch privat nutzen dürften, um etwa Autos aufzusperren oder um ihre Gesundheitsdaten darauf zu speichern. Dieser Ansatz wurde auch bereits von einigen Spitälern ausprobiert, um darauf Patientendaten zu speichern.

Ulrike Hugl auf der DeepSec in Wien © Bild: Joanna Pianka

Fehlende Diskussion in der Gesellschaft

„Ich könnte mir vorstellen, dass die technologische Entwicklung weiter voranschreitet und wir keine kritische Diskussion darüber in der Gesellschaft haben. Dann kann es passieren, dass sich niemand etwas dabei denkt und sich in zehn Jahren alle einen Chip einpflanzen lassen", warnt Hugl. Die Wissenschaftlerin bemängelt, dass wie bei vielen Technologie- und Datenschutz-Themen eine „breite Diskussion" in der Gesellschaft fehle und sich zu wenig Menschen damit befassen.

Hugl selbst würde sich nie so einen Chip einpflanzen lassen. „Ein Chip unter der Haut ist mir zu invasiv", sagt sie. „Nachdem ich weiß, was da alles getrackt, gemonitored und gedatamined wird, hätte ich meine größten Bedenken. Ich meide generell Technologien, die Daten über mich sammeln", so die Forscherin. „Aus dem Bereich Wirtschaftskriminalität wissen wir, dass sich Angreifer anpassen an Technologien oder sie so nutzen, dass sie zu ihrem Vorteil sind. Eine Zutrittskarte kann ich jemandem physisch wegnehmen. Das Implantat kann ich allerdings nur herausschneiden", fährt die Expertin fort.

SCIENCE

"Ein Chip unter der Haut ist das Tattoo der Neuzeit"

Technik, die unter die Haut geht: Auf der CeBIT haben sich hunderte Menschen einen Chip in den Handrücken einsetzen lassen. Die futurezone hat sich den Trend angesehen.

Schnelle Entwicklung möglich

Der Chip ist zudem in der Lage, genau zu tracken wann ein Mitarbeiter kommt und geht. Außerdem stellt sich die Frage, was mit dem Chip passiert, wenn ein Mitarbeiter das Unternehmen wieder verlässt. „Was bedeutet das für den Körper?", fragt sich Hugl, die davor warnt, dass das, was vor 15 Jahren als Versuche begonnen hat, plötzlich relativ rasch zu einer Massenanwendung werden könnte. Laut Amal Gfraafstra, der mit Digiwell selbst kleine Chips zum Implantieren vertreibt, seien es längst nicht mehr nur "IT-Nerds", die sich Chips einpflanzen würden. Es sei bereits das "Tattoo der Neuzeit".

„Manchmal vergehen da nur ein paar Jahre dazwischen. Viel hängt davon ab, wie man etwas vermarktet", warnt Hugl, die fürchtet, dass wir von der Entwicklung „einfach überrollt" werden könnten. Die Wissenschaftlerin wünscht sich daher einen breiten Diskurs über diese Themen – und zwar bevor sich plötzlich jeder einen Chip einpflanzen lässt, ohne davor nachzudenken.

(futurezone) | Stand: 05.12.2018, 6:00 | Autor: BARBARA WIMMER

https://www.golem.de/news/cybercrime-profiling-der-typische-onlinekriminelle-ist-ein-34-jaehriger-mann-1812-138014.html

CYBERCRIME PROFILING:

Der typische Onlinekriminelle ist ein 34-jähriger Mann

Deepsec 2018 - Forscher aus Österreich versuchen herauszufinden, welcher Typ Mensch hinter der steigenden Onlinekriminalität steckt. Dabei identifizieren sie Tätergruppen und können diese bestimmten Straftatbeständen zuordnen.

Artikel veröffentlicht am 3. Dezember 2018, 10:16 Uhr, Jan Weisensee

Seit 13 Jahren erforscht Edith Huber die Onlinekriminalität im Nachbarland Österreich. Die Soziologin der Universität Krems interessiert sich dabei besonders für die sich wandelnde Definition von Cybercrime sowie für die Eigenschaften von Tätern und Opfern.

Ihren Forschungsergebnissen zufolge, die Huber gemeinsam mit der Soziologin Bettina Pospisil auf der diesjährigen Deepsec-Konferenz in Wien vorgestellt hat, ist der durchschnittliche Cyberkriminelle rund 34 Jahre alt, männlich und alleinstehend. Anders als klischeehafte Darstellungen es oft nahelegen, sind die meisten Täter dagegen keine IT-Profis mit Universitätsabschluss in Informatik. Bei der Mehrheit der untersuchten Cybercrime-Fälle handelt es sich um Identitätsdiebstahl und Racheakte (Revenge-Crime), die sich mit eher simplen Techniken durchführen lassen. Oft bedürfe es gar keines besonderen technischen Könnens, um die untersuchten Angriffe durchzuführen.

Für ihre Arbeit haben sich die Forscherinnen ihrem Vortrag auf der Deepsec zufolge durch Tausende Akten von am Gericht in Wien anhängenden Cybercrime-Fällen gearbeitet.

Schlecht geschützte Konten und schwache Passwörter

"Privatpersonen werden häufig Opfer von Tätern, die sich unerlaubt Zugriff auf Online-Bezahlsysteme verschaffen, beispielsweise in Form von illegalen Überweisungen, Kreditkartenmissbrauch, illegalem Zugang auf Online-Shoppingportale und so weiter", erklärt Huber. Dies sei oft technisch einfach zu bewerkstelligen, da viele Opfer ihre Zugangsdaten nur schlecht schützten oder leicht erratbare Passwörter verwendeten. Diese Vorgehensweise werde auch häufig bei Racheakten angewendet. Zumeist würden Zugangsdaten zu Social-Media-Plattformen wie Facebook, Instagram oder zu E-Mail-Konten gestohlen, mit deren Hilfe anschließend Fotos, Videos oder andere private

Informationen gestreut werden können. "Viele Delikte, die früher im Bereich des Stalkings zu subsumieren waren, werden nun über diese Schiene ausgetragen."

"Analysiert man die letzten zehn bis 15 Jahre, kann man massiv den Einfluss der Digitalisierung auf die Onlinekriminalität erkennen", sagt Huber. "Durch Breitbandinitiativen und die stetige Ausweitung der Nutzung mobiler internetfähiger Geräte sowie der Verwendung von Smartphones steigt zudem die Zahl potenzieller Opfer."

Auch Unternehmen werden Opfer

Auch bei Angriffen auf Unternehmen und kritische Infrastrukturen haben sich die Angriffsmethoden laut Huber geändert. Zwar gehe es auch hier sehr häufig um Identitätsdiebstahl, der objektive Schaden dürfte in einem professionellen Umfeld aber oft ungleich höher ausfallen. "Mehr als 60 Prozent der Opfer im Unternehmensbereich fallen in die Kategorien Bank- und Finanzdienstleister", erklärt Huber. "Firmen und kritische Infrastrukturen werden zudem häufiger Opfer sogenannter Core-Cybercrime, also jenen Cybercrime-Delikten, die ausschließlich online existieren." Hierbei spiele vor allem die Zunahme von Malware-, Ransomware- und Social-Engeneering-Attacken eine Rolle.

Dem österreichischen Bundeskriminalamt zufolge steigt die Zahl angezeigter Cybercrime-Fälle stetig - von rund 2.900 im Jahr 2007 auf fast 17.000 im Jahr 2017. Die Aufklärungsrate kann diesem hohen Aufkommen offenbar nicht folgen: Wie die beiden Forscherinnen ermittelt haben, sind zumindest am Wiener Gericht fast 93 Prozent der untersuchten Fälle ungelöst.

Cybercrime Profiling: Der typische Onlinekriminelle ist ein 34-jähriger Mann

Deepsec 2018

Forscher aus Österreich versuchen herauszufinden, welcher Typ Mensch hinter der steigenden Onlinekriminalität steckt. Dabei identifizieren sie Tätergruppen und können diese bestimmten Straftatbeständen zuordnen.

Artikelveröffentlicht am3. Dezember 2018, 10:16 Uhr, Jan Weisensee

(Bild: Maxpixel/CC0 1.0)

Durchschnittliche Onlinekriminelle sind Männer Mitte 30.

Seit 13 Jahren erforscht Edith Huber die Onlinekriminalität im Nachbarland Österreich. Die Soziologin der Universität Krems interessiert sich dabei besonders für die sich wandelnde Definition von Cybercrime sowie für die Eigenschaften von Tätern und Opfern.

Ihren Forschungsergebnissen zufolge, die Huber gemeinsam mit der Soziologin Bettina Pospisil auf der diesjährigen Deepsec-Konferenz in Wien vorgestellt hat, ist der durchschnittliche Cyberkriminelle rund 34 Jahre alt, männlich und alleinstehend.

Anders als klischeehafte Darstellungen es oft nahelegen, sind die meisten Täter dagegen keine IT-Profis mit Universitätsabschluss in Informatik. Bei der Mehrheit der untersuchten Cybercrime-Fälle handelt es sich um Identitätsdiebstahl und Racheakte (Revenge-Crime), die sich mit eher simplen Techniken durchführen lassen. Oft bedürfe es gar keines besonderen technischen Könnens, um die untersuchten Angriffe durchzuführen.

Für ihre Arbeit haben sich die Forscherinnen ihrem Vortrag auf der Deepsec zufolge durch Tausende Akten von am Gericht in Wien anhängenden Cybercrime-Fällen gearbeitet.

Schlecht geschützte Konten und schwache Passwörter

"*Privatpersonen werden häufig Opfer von Tätern, die sich unerlaubt Zugriff auf Online-Bezahlsysteme verschaffen, beispielsweise in Form von illegalen Überweisungen, Kreditkartenmissbrauch, illegalem Zugang auf Online-Shoppingportale und so weiter*", erklärt Huber. Dies sei oft technisch einfach zu bewerkstelligen, da viele Opfer ihre Zugangsdaten nur schlecht schützten oder leicht erratbare Passwörter verwendeten. Diese Vorgehensweise werde auch häufig bei Racheakten angewendet. Zumeist würden Zugangsdaten zu Social-Media-Plattformen wie Facebook, Instagram oder zu E-Mail-Konten gestohlen, mit deren Hilfe anschließend Fotos, Videos oder andere private Informationen gestreut werden können. "*Viele Delikte, die früher im Bereich des Stalkings zu subsumieren waren, werden nun über diese Schiene ausgetragen.*"

"*Analysiert man die letzten zehn bis 15 Jahre, kann man massiv den Einfluss der Digitalisierung auf die Onlinekriminalität erkennen*", sagt Huber. "*Durch Breitbandinitiativen und die stetige Ausweitung der Nutzung mobiler internetfähiger Geräte sowie der Verwendung von Smartphones steigt zudem die Zahl potenzieller Opfer.*"

Auch Unternehmen werden Opfer

Auch bei Angriffen auf Unternehmen und kritische Infrastrukturen haben sich die Angriffsmethoden laut Huber geändert. Zwar gehe es auch hier sehr häufig um Identitätsdiebstahl, der objektive Schaden dürfte in einem professionellen Umfeld aber oft ungleich höher ausfallen. "*Mehr als 60 Prozent der Opfer im Unternehmensbereich fallen in die Kategorien Bank- und Finanzdienstleister*", erklärt Huber. "*Firmen und kritische Infrastrukturen werden zudem häufiger Opfer sogenannter Core-Cybercrime, also jenen Cybercrime-Delikten, die ausschließlich online existieren.*" Hierbei spiele vor allem die Zunahme von Malware-, Ransomware- und Social-Engeneering-Attacken eine Rolle.

Dem österreichischen Bundeskriminalamt zufolge steigt die Zahl angezeigter Cybercrime-Fälle stetig - von rund 2.900 im Jahr 2007 auf fast 17.000 im Jahr 2017. Die Aufklärungsrate kann diesem hohen Aufkommen offenbar nicht folgen: Wie die beiden Forscherinnen ermittelt haben, sind zumindest am Wiener Gericht fast 93 Prozent der untersuchten Fälle ungelöst. ▪

Themenseiten:

Cybercrime, Malware, Passwort, Ransomware, Virus, Internet, Security

Zu den Kommentaren springen

Kurier

Cybersicherheits-Experte warnt vor der zunehmenden Vernetzung von Dingen

Kurier, 30.11.2018

Smart. Der niederländische Cybersecurity-Experte Peter Zinn warnte auf der Sicherheitskonferenz DeepSec in Wien vor potenziellen Gefahren, die durch neue Technologien auf die Gesellschaft zukommen. Die zunehmende Vernetzung würde uns als Gesellschaft etwa, anders als von Gadget-Herstellern propagiert, nicht schlauer machen. „Smart ist das neue dumm“, sagte Zinn. Er spricht damit etwa Gadgets an wie smarte Uhren, Thermostate oder aber auch vernetzte Autos oder Städte. „Es wird das nächste größere Desaster, wenn wir so weiter machen wie bisher.“ Der Grund für seine harten Worte: Derzeit wird Sicherheit nicht mitgedacht und alle vernetzten Geräte sind leicht angreifbar für Hacker. „Das liegt daran, dass die Gadgets meistens billig sein müssen, klein und leicht benutzbar. Für Verschlüsselung ist hier kein Platz mehr. Diese Anforderungen sind falsch und wir brauchen hier rasch ein Umdenken“, warnt der Experte.

Problemlösung

Die meisten Konsumenten würden derzeit für Sicherheitsfeatures nicht mehr Geld zahlen, weil sie den Wert nicht erkennen. „Dieses Problem kennen auch viele Internet Service Provider“, meint Zinn, der als unabhängiger Berater auch Städte auf ihrem Weg zur Smart City begleitet.„Wenn ich mit Verantwortlichen von Städten zusammensitze und ihnen erkläre, dass wir mehr Sicherheit brauchen, verstehen das die meisten. Sicherheit kostet allerdings etwas extra. Auch das verstehen sie.“ Für Zinn ist ein Umdenken bei den Entscheidungsträgern daher nicht unrealistisch. Er hofft zudem, dass es noch möglich ist, den Markt mit Regulierungen in die richtige Richtung zu lenken. Konsumenten selbst, so Zinn, können hier wenig tun. „Der wichtigste Ratschlag ist, auf sichere Passwörter zu setzen.“

– BARBARA WIMMER

Vier Grad weniger durch grünes Bauen

Greenpass. Ein Wiener Start-up berechnet, wie Bäume und Pflanzen in der Stadt für niedrigere Temperaturen sorgen

VON **MARTIN STEPANEK**

Der Klimawandel, der sich in den vergangenen Jahren durch anhaltende Hitzewellen sowie extreme Unwetter mit Überschwemmungen bemerkbar machte, trifft Städte besonders hart. Denn durch die enorme Gebäudemasse und die mit Asphalt und Beton versiegelten Böden heizen sich urbane Zentren exorbitant auf. Bei Starkregen können die Wassermassen nicht in der Erde versickern, sondern schießen unkontrolliert die Straßen entlang und sorgen so für Überflutungen. Zudem sind überproportional viele Menschen betroffen. Schon heute leben laut einem Bericht der EU-Kommission mehr als 85 Prozent der Weltbevölkerung in städtischen Regionen.

Am Computer planen

Das Problem am Schopf packen will die Wiener Jungfirma Greenpass. Sie hat eine Planungssoftware entwickelt, mit der die positiven Auswirkungen von begrünten Flächen in der Stadt berechnet werden. Indem auch die Kostenfaktoren aufgeschlüsselt und optimiert werden, will man Architekten und Bauträger zu einer grüneren Bauweise animieren.

Als Vorzeigebeispiel von begrüntem Wohnraum in der Stadt dient der 2014 eingeweihte Hochhauskomplex „Bosco Verticale“ (dt. senkrechter Wald) in Mailand

„Messungen zeigen, dass die Temperatur in begrünten Stadtteilen um bis zu vier Grad geringer als in der unmittelbaren Umgebung ist. Bei der gefühlten Temperatur holt man etwa im Schatten von Bäumen sogar bis zu 15 Grad heraus“, sagt Greenpass-Gründer Florian Kraus im KURIER-Gespräch. Pflanzen werden bei großer Hitze zu natürlichen Klimaanlagen, indem sie zu „schwitzen“ beginnen und Wasser über ihre Blätter verdunsten. Neben dieser Verdunstungskälte schützen Bäume und Pflanzen Gebäude und Straßen vor direkter Sonnenstrahlung. Begrünte Dächer haben zusätzlich den Effekt, dass sie Regen und Feuchtigkeit speichern und längerfristig wieder an die Umgebung abgeben können.

Weltpremiere

„Die positiven Effekte von Grünflächen auf das Mikroklima von Städten waren auch bisher schon bekannt. Durch unsere Software ist dies aber erstmals schnell und einfach quantifizierbar bzw. kann so in die Planung einfließen“, erklärt Kraus. Um spürbare Effekte zu erzielen, müsse man auch nicht zwangsläufig mehr Geld in die Hand nehmen. „Konventionell werden 0,5 bis drei Prozent der Gesamtbaukosten für die Gestaltung von Grünelementen verwendet. Unsere Simulation zeigt per Knopfdruck, wie dieses Geld optimal eingesetzt werden kann, also wo Bäume platziert oder Flächen begrünt werden sollten.“

Ikea überzeugt

Die erst im Juni 2018 gegründete Firma, die acht Jahre Entwicklungs- und Forschungsarbeit – etwa an der Universität für Bodenkultur – vorweist, konnte bereits erste Erfolge feiern. So griffen die Planer von Ikea für die geplante Filiale am Westbahnhof in Wien auf die Expertise von Greenpass zurück. Das Start-up berechnete, dass ein Planungsentwurf mit zahlreichen Grünelementen in der Fassade zu einer Temperaturverringerung von bis zu zwei Grad in der Umgebung führt. Ein zuvor ins Auge gefasster Glas-Kubus, der im Sommer die Hitzeentwicklung verstärkt hätte, wurde verworfen. Mit an Bord ist die Firma und ihre Software auch beim Wiener Stadtentwicklungsprojekt „Eurogate II“ und der „Biotope City“ am Wienerberg. Weitere Projekte werden in Graz, Klagenfurt und Krems realisiert.

Investoren gesucht

Mit einer Finanzierungsrunde, die über die Crowdfunding-Plattform Green Rocket läuft, soll die bereits vorbereitete Expansion nach Deutschland, Italien, Frankreich und Großbritannien vorangetrieben werden. Diese verspricht Investoren aktuell bis zu 7,5 Prozent Zinsen. In den ersten zehn Tagen konnte Greenpass bereits knapp 150.000 Euro aufstellen.

„Angesichts der Klimakrise braucht es Maßnahmen, um unsere Städte lebenswerter und kühler zu machen. Alles, was wir jetzt bauen, wird uns die nächsten 100 Jahre begleiten – im Guten wie im Schlechten“, sagt Kraus.

KONFERENZ

Cybersicherheits-Experte warnt vor der zunehmenden Vernetzung von Dingen

Smart. Der niederländische Cybersecurity-Experte Peter Zinn warnte auf der Sicherheitskonferenz DeepSec in Wien vor potenziellen Gefahren, die durch neue Technologien auf die Gesellschaft zukommen. Die zunehmende Vernetzung würde uns als Gesellschaft etwa, anders als von Gadget-Herstellern propagiert, nicht schlauer machen. „Smart ist das neue dumm“, sagte Zinn. Er spricht damit etwa Gadgets an wie smarte Uhren, Thermostate oder aber auch vernetzte Autos oder Städte. „Es wird das nächste größere Desaster, wenn wir so weitermachen wie bisher.“ Der Grund für seine harten Worte: Derzeit wird Sicherheit nicht mitgedacht und alle vernetzten Geräte sind leicht angreifbar für Hacker. „Das liegt daran, dass die Gadgets meistens billig sein müssen, klein und leicht benutzbar. Für Verschlüsselung ist hier kein Platz mehr. Diese Anforderungen sind falsch und wir brauchen hier rasch ein Umdenken“, warnt der Experte.

Problemlösung

Die meisten Konsumenten würden derzeit für Sicherheitsfeatures nicht mehr Geld zahlen, weil sie den Wert nicht erkennen. „Dieses Problem kennen auch viele Internet Service Provider“, meint Zinn, der als unabhängiger Berater auch Städte auf ihrem Weg zur Smart City begleitet. „Wenn ich mit Verantwortlichen von Städten zusammensitze und ihnen erkläre, dass wir mehr Sicherheit brauchen, verstehen das die meisten. Sicherheit kostet allerdings etwas extra. Auch das verstehen sie.“ Für Zinn ist ein Umdenken bei den Entscheidungsträgern daher nicht unrealistisch. Er hofft zudem, dass es noch möglich ist, den Markt mit Regulierungen in die richtige Richtung zu lenken. Konsumenten selbst, so Zinn, können hier wenig tun. „Der wichtigste Ratschlag ist, auf sichere Passwörter zu setzen.“

– BARBARA WIMMER

https://blog.rootshell.be/2018/11/30/deepsec-2018-wrap-up/

DeepSec 2018 Wrap-Up

November 30, 2018, Xavier Mertens

I'm writing this quick wrap-up in Vienna, Austria where I attended my first DeepSec conference. This event was already on my schedule for a while but I never had a chance to come. This year, I submitted a training and I was accepted! Good opportunity to visit the beautiful city of Vienna! Like many security conferences, the event started with a set of trainings on Tuesday and Wednesday. My training topic was about using OSSEC for threat hunting.

On Thursday and Friday, regular talks were scheduled and split across three tracks. Two tracks for regular presentations and the third one called "Roots", more dedicated to academic researches and papers. There was a good balance between offensive and defensive presentations.

The keynote speaker was Peter Zinn and he presented a very entertaining keynote called "We're all gonna die". Basically, the main idea was to review how our world is changing in many points and new threats are coming: the climate change, magnetic fields, Donald Trump, etc. But also from an information technology point of view. Peter revealed that we have to face 4 types of "cyber-zombies":

People
Inequality
Operational technology and IOT
Artificial Intelligence (here is a funny video that demonstrate how AI may fail)
Later, we will face the "IoP" of "Internet of People". IT will be present inside our bodies (RFID implants, sensors, contact lenses, …) and we'll have to deal with them. Nice keynote!

Here is a quick recap of the talk that I attended. Fernando Arnaboldi and "Uncovering Vulnerabilities in Secure Coding Guidelines". The idea behind this talk was to demonstrate that, even if you follow all well-known development guidelines (like OWASP, CWE or NIST), you can fail. He gave several snippets of code as examples. Personally, I liked the mention to the new KPI: "the WTF's/minute".

Then, Werner Schober presented the "Internet of Dildos". Always entertaining to have a talk focusing on "exotic" IoT devices. He explained the different vulnerabilities that he found in a sex-toy and the associated mobile app &

website in Germany. Basically, he explained how it was possible to access all (hot) pictures uploaded by the users, how to enable (make vibrate) any device connected in the world or, worse, access to personal data of the consumers…

Then, Eric Leblond talked about the new features that are constantly added to the Suricata IDS with a focus on eBPF filters. I already saw Eric's presentation a few month ago but he added more stuff like a crazy idea to use BCC ("BPF Code Compiler") to generate BFP filters from C code directly present in a Python script!

Joe Slowik came to speak about ICS attacks. More and more ICS attacks are reported in the news because there is some kind of aura of sophistication around them. Joe started with a recap of the major ICS attacks that industries faced in the last years. But, many attacks are successful because the IT components used to control the ICS components are vulnerable and the same tools are abuse to compromize them (like Mimikatz, PsExec, etc). Note that the talk was a mix of offensive & defensive.

Benjamin Ridgway (from the Microsoft Incident Response Center) came to speak about incident handling. The abstract was not clear and a lot of people expected a talk explaining how to select and use the right tools to perform incident management but it was completely different and not technical. Benjamin explained how to implement your IH process with a focus on the following points:

Human psychological response to stressful and/or dangerous situations
Strategies for effectively managing human factors during a crisis
Polices and structures that set up incident response teams for success
Tools for building a healthy and happy incident response team
It was an excellent presentation, one of my preferred!

Then, Dr. Silke Holtmanns from Nokia Bell Las came to speak about new attack vectors for mobile core networks. The problem for people that are not in the field of mobile networks is the complexity of terms and abbreviations used. It's crazy! But Silke explained very well the basic: how roaming is used, how billing profile are managed. Of course, the idea was then to explain some attacks. I like the one focusing on how to change a billing plan when you're abroad to reduce the roaming costs. Very didactic!

The new speaker was Mark Baenziger which is doing incident handling. He explained the challenges that incident handlers might face when handling personal data (and so, how to protect their privacy). He explained how, in some

case, security teams failed to achieve this properly.

The last slot was assigned to Paula de la Hoz Garrido (she's studying in Spain). She explained her project of network monitoring tools bundled on a Raspberry Pi. Interesting but the practical part was missing (how to build the project on the Pi. The talk was more a review of tools that are used to capture/process packets.

The second day started with a nice talk called "Everything is connected: how to hack Bank Account using Instagram". The idea was to abuse phone services provided by some banks to allow their customers to perform a lot of basic operations (through IVR). Aleksandr Kolchanov explained the attacks he performed against an Ukrainian bank. Some services are available only based on the caller-ID. This information can be easily spoofed using only services (ex: spooftel.com). Funny but crazy!

Then, I switched to the "Roots" room to attend a talk about using data over sound. More precisely, ultrasonic sounds. Matthias Zeppelzauer explained the research he made about this technology which is used more then we could expect! It's possible to collect interesting informations (ex: how people watch television programs) or to deliver ads to people entering a shop. He also presented the project "SoniControl" which is some kind of an ultrasonic firewall to protect the privacy of users.

My next choice was "RFID Chip Inside the Body: Reflecting the Current State of Usage, Triggers, and Ethical Issues" presented by Ulrike Hugl. RFID implants in human bodies are not new but what's the status today? Are people ready to have such kind of hardware under their skin? There is not massive deployment but some companies try to convince their users to use this technology. But it remains usually tests or funny projects.

Finally, my last choice was "Global Deep Scans – Measuring Vulnerability Levels across Organizations, Industries, and Countries" by Luca Melette & Fabian Bräunlein. I was curious when I read the abstract. The idea behind this research was to scan the Internet, to classify scanned IP addresses by location and business. Then, they used an algorithm to compute an "hackability" level. Indeed, from a defender perspective, it's interesting to learn how your competitor are safe. From an attacker point of view, it's nice to know which are the most juicy targets. The result of their research is available here.

This was a very quick wrap-up of my first DeepSec (and I hope not the last one!). The conference size is nice, not too many attendees (my rough estimation is ~200 people) and properly managed by the crew. Thanks to them!

孫子兵法 /dev/random

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

Search ...

DeepSec 2018 Wrap-Up

November 30, 2018 Event, Security Leave a comment

I'm writing this quick wrap-up in Vienna, Austria where I attended my first DeepSec conference. This event was already on my schedule for a while but I never had a chance to come. This year, I submitted a training and I was accepted! Good opportunity to visit the beautiful city of Vienna! Like many security conferences, the event started with a set of trainings on Tuesday and Wednesday. My training topic was about using OSSEC for threat hunting.

Stay in Touch

Upcoming Events

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

On Thursday and Friday, regular talks were scheduled and split across three tracks. Two tracks for regular presentations and the third one called "Roots", more dedicated to academic researches and papers. There was a good balance between offensive and defensive presentations.

The keynote speaker was Peter Zinn and he presented a very entertaining keynote called "*We're all gonna die*". Basically, the main idea was to review how our world is changing in many points and new threats are coming: the climate change, magnetic fields, Donald Trump, etc. But also from an information technology point of view. Peter revealed that we have to face 4 types of "cyber-zombies":

- People
- Inequality
- Operational technology and IOT
- Artificial Intelligence (here is a funny video that demonstrate how AI may fail)

Later, we will face the "IoP" of "Internet of People". IT will be present inside our bodies (RFID implants, sensors, contact lenses, ...) and we'll have to deal with them. Nice keynote!

Here is a quick recap of the talk that I attended. Fernando Arnaboldi and "*Uncovering Vulnerabilities in Secure Coding Guidelines*". The idea behind this talk was to demonstrate that, even if you follow all well-known development guidelines (like OWASP, CWE or NIST), you can fail. He gave several snippets of code as

Recent Articles

- [SANS ISC] Malicious Script Leaking Data via FTP
- [SANS ISC] Using OSSEC Active-Response as a DFIR Framework
- "Hunting with OSSEC" at BruCON Spring Training
- [SANS ISC] Restricting PowerShell Capabilities with NetSh
- [SANS ISC] Phishing Attack Through Non-Delivery Notification

examples. Personally, I liked the mention to the new KPI: "the WTF's/minute".

Then, Werner Schober presented the "*Internet of Dildos*". Always entertaining to have a talk focusing on "exotic" IoT devices. He explained the different vulnerabilities that he found in a sex-toy and the associated mobile app & website in Germany. Basically, he explained how it was possible to access all (hot) pictures uploaded by the users, how to enable (make vibrate) any device connected in the world or, worse, access to personal data of the consumers...

Then, Eric Leblond talked about the new features that are constantly added to the Suricata IDS with a focus on eBPF filters. I already saw Eric's presentation a few month ago but he added more stuff like a crazy idea to use BCC ("BPF Code Compiler") to generate BFP filters from C code directly present in a Python script!

Joe Slowik came to speak about ICS attacks. More and more ICS attacks are reported in the news because there is some kind of aura of sophistication around them. Joe started with a recap of the major ICS attacks that industries faced in the last years. But, many attacks are successful because the IT components used to control the ICS components are vulnerable and the same tools are abuse to compromize them (like Mimikatz, PsExec, etc). Note that the talk was a mix of offensive & defensive.

Benjamin Ridgway (from the Microsoft Incident Response Center) came to speak about incident

Popular Articles

- Show me your SSID's, I'll Tell Who You Are!
  32,023 views
- Keep an Eye on SSH Forwarding!
  28,138 views
- Sending Windows Event Logs to Logstash
  25,636 views
- Check Point Firewall Logs and Logstash (ELK) Integration
  20,874 views
- Socat, Another Network Swiss Army Knife
  18,146 views
- Vulnerability Scanner within Nmap
  17,384 views
- Forensics: Reconstructing Data from Pcap Files

handling. The abstract was not clear and a lot of people expected a talk explaining how to select and use the right tools to perform incident management but it was completely different and not technical. Benjamin explained how to implement your IH process with a focus on the following points:

- Human psychological response to stressful and/or dangerous situations
- Strategies for effectively managing human factors during a crisis
- Polices and structures that set up incident response teams for success
- Tools for building a healthy and happy incident response team

It was an excellent presentation, one of my preferred!

Then, Dr. Silke Holtmanns from Nokia Bell Las came to speak about new attack vectors for mobile core networks. The problem for people that are not in the field of mobile networks is the complexity of terms and abbreviations used. It's crazy! But Silke explained very well the basic: how roaming is used, how billing profile are managed. Of course, the idea was then to explain some attacks. I like the one focusing on how to change a billing plan when you're abroad to reduce the roaming costs. Very didactic!

The new speaker was Mark Baenziger which is doing incident handling. He explained the challenges that incident handlers might face when handling personal data (and so, how to

17,315 views
- dns2tcp: How to bypass firewalls or captive portals?

16,847 views
- Post-BruCON Experience – Running a Wall of Sheep in the Wild

15,062 views
- Bash: History to Syslog

11,194 views

Recent Tweets

Interesting PDF delivered via Google Drive. It contains a fake Google CAPTCHA. When you click on it, you're redirec... twitter.com/i/web/status/10829...

protect their privacy). He explained how, in some case, security teams failed to achieve this properly.

The last slot was assigned to Paula de la Hoz Garrido (she's studying in Spain). She explained her project of network monitoring tools bundled on a Raspberry Pi. Interesting but the practical part was missing (how to build the project on the Pi. The talk was more a review of tools that are used to capture/process packets.

The second day started with a nice talk called "*Everything is connected: how to hack Bank Account using Instagram*". The idea was to abuse phone services provided by some banks to allow their customers to perform a lot of basic operations (through IVR). Aleksandr Kolchanov explained the attacks he performed against an Ukrainian bank. Some services are available only based on the caller-ID. This information can be easily spoofed using only services (ex: spooftel.com). Funny but crazy!

Then, I switched to the "Roots" room to attend a talk about using data over sound. More precisely, ultrasonic sounds. Matthias Zeppelzauer explained the research he made about this technology which is used more then we could expect! It's possible to collect interesting informations (ex: how people watch television programs) or to deliver ads to people entering a shop. He also presented the project "SoniControl" which is some kind of an ultrasonic firewall to protect the privacy of users.

Yesterday at 12:16

Want! twitter.com/Optimus__Prime/sta...

Yesterday at 11:40

So, in March at #RSA, @NSAGov will demonstrate its #GHIDRA framework that many people will install on their systems... twitter.com/i/web/status/10826...

January 8, 2019 13:31

When you finished to resolve all dependencies

My next choice was "*RFID Chip Inside the Body: Reflecting the Current State of Usage, Triggers, and Ethical Issues*" presented by Ulrike Hugl. RFID implants in human bodies are not new but what's the status today? Are people ready to have such kind of hardware under their skin? There is not massive deployment but some companies try to convince their users to use this technology. But it remains usually tests or funny projects.

Finally, my last choice was "*Global Deep Scans – Measuring Vulnerability Levels across Organizations, Industries, and Countries*" by Luca Melette & Fabian Bräunlein. I was curious when I read the abstract. The idea behind this research was to scan the Internet, to classify scanned IP addresses by location and business. Then, they used an algorithm to compute an "hackability" level. Indeed, from a defender perspective, it's interesting to learn how your competitor are safe. From an attacker point of view, it's nice to know which are the most juicy targets. The result of their research is available here.

This was a very quick wrap-up of my first DeepSec (and I hope not the last one!). The conference size is nice, not too many attendees (my rough estimation is ~200 people) and properly managed by the crew. Thanks to them!

Conference DeepSec Event Security Vienna

« [SANS ISC] More obfuscated shell scripts: Fake MacOS Flash update

Botconf 2018 Wrap-Up Day #1 »

to install a Python3 module on an air-gapped system... pic.twitter.com/sL17xfA4S5

January 8, 2019 10:31

<sarcasm> First good resolution for this year: Upgrade all your passwords and replace the ending '2018' with '2019'! </sarcasm>

January 7, 2019 13:38

Time Machine

Select Month

https://wien.wirtschaftszeit.at/wirtschaftskalender-detail/kal/tx_cal_phpicalendar/deepsec-in-depth-security-konferenz-insecurity-of-things-iot/2018/11/29

DeepSec In-Depth Security Konferenz: Insecurity of Things (IoT)
29. Nov 2018 - 30. Nov 2018

Die DeepSec In-Depth Security Konferenz widmet sich in diesem Jahr dem Thema Insecurity of Things (IoT) und Komponenten alltäglicher Infrastruktur. Die stetig voranschreitende Vernetzung eröffnet Angreifern völlig neue Wege - schneller, als Entwickler und Hersteller Fehler beheben können. Statt Secure Design bei Produkten und Code einzusetzen, integriert man Machine Learning und Künstliche Intelligenz - leider implementiert durch passende Statistik und den Algorithmus der Woche aus dem Tagesmenü des Entwicklungsbaukastens. Die Vorträge auf der DeepSec Konferenz werden daher die vermeintlichen Techniken der Zukunft auf den Prüfstand stellen. Mobilfunknetzwerke, das Internet der Dinge, Kollaborationsplattformen in der Cloud, Customer Relationship Management Systeme und der Faktor Mensch stehen im Fadenkreuz.
Smart is the new Cyber

Die Informationstechnologie hat den berechtigten Ruf ständig neue Begriffe und Akronyme zu erfinden um Lösungen für technische Probleme vorzugaukeln. Meist handelt es sich um ein reines Versteckspiel, sehr gut illustriert durch die Schlagworte Cyber, Cloud und Virtual. Hinter den Kulissen sind einige Begriffe berechtigt, aber kaum jemand prüft was sich hinter einem Produkt wirklich versteckt. Bestes Beispiel ist der Trend nun alles Smart zu machen, ganz egal ob Sicherheit ein Designkriterium war oder nicht. Die Stromversorgung soll zum Smart Grid werden, Fragenkataloge werden zum Smart Assistant, etc.

Ein Blick ins Innere offenbart Komponenten, die oft ohne ein Konzept von Sicherheit irgendwie miteinander verbunden werden. Das beste Beispiel sind Smartphones, die zum Universalschlüssel mutiert sind. Auf einem einzigen Gerät befindet sich eine Vielzahl von Zugängen, die bestimmte Apps benötigen. Damit werden diese Gegenstände automatisch zu einem begehrten Angriffsziel. Im Workshop Mobile App Attacks 2.0 wird gezeigt, wie man Apps und die Smartphone Plattform als Basis für erfolgreiche Angriffe verwendet. Und auch ein Workshop zum Thema Mobilfunksicherheit ist Teil des Programms. Der Trainer David Burgess ist ein Veteran auf diesem Gebiet und hat schon 2009 auf der DeepSec schwere Sicherheitslücken in Mobilfunknetzen entdeckt und dokumentiert. Dieses Jahr ist er wieder auf der DeepSec und kann auch etwas zu den neuen Standards sagen.

Unsicherheit der Dinge überall

Sicherheitslücken von Gegenständen aus dem Internet of Things (IoT) werden in Vorträgen und Workshops ebenso vorgestellt und analysiert. Johannes Pohl zeigt in seinem Training vor, wie man die Kommunikation von IoT Geräten analysiert. Diese Arbeit dient als Basis für daraus abgeleitete Angriffe. Wenige Hersteller sind wirklich in der Lage eine sichere Kommunikation als Protokoll zu entwerfen und zu implementieren, unabhängig ob das Protokoll neu erdacht ist oder auf etablierten Standards beruht.

Werner Schober, Sicherheitsforscher der Firma SEC Consult, stellt in seinem Vortrag Schwachstellen von "smartem" Sexspielzeug vor. Was wie ein schlechter Scherz klingt, ist leider keiner. Alle IoT-Geräte jeder Branche sind eine Gefahr. Da in Casinos schon über ein vernetztes Aquarium eingebrochen wurde, spielt der ursprüngliche Zweck des Gerät keine Rolle. Speziell bei Sexspielzeugen ist zusätzlich die Disziplin regelmäßiger Updates der Firmware betreffend sicher geringer als beim "smarten" Fernseher. Damit werden diese Gegenstände automatisch zu einem Risiko für Sicherheit und Privatsphäre zugleich. Im Alltag lassen sich mittlerweile zahllose weitere Dinge aufzählen, die für Angriffe auf Informationssysteme verwendet werden können.

Faktor Mensch

Egal welche Technologie man einsetzt, der Faktor Mensch bleibt wichtiger Teil der Informationssicherheit. Auch der menschliche Körper wird vernetzt. Ulrike Hugl von der Universität Innsbruck thematisiert implantierte RFID (radio-frequency identification) Chips. Mit solchen Fremdkörpern ist man dann selbst Teil von Fragen über Datensicherheit und Angriffen durch Dritte, denn RFID Komponenten tragen Daten und können ausgelesen werden. Behandelt werden Verbreitung, Nutzung und ethische Fragestellungen.

Darüber hinaus gibt es Vorträge zum Thema Bedrohungsanalyse, die ein wichtiger Teil der digitalen Verteidigung ist. Sie wird oft durch automatische Prozesse durchgeführt. Im Vortrag wird die Grenze zu den Fähigkeiten menschlicher Experten gezogen und wie man diese durch automatisierte Systeme unterstützen kann. Stefan Schumacher beleuchtet in seiner Präsentation wie sich das menschliche Gehirn manipulieren lässt und wie man mit Methoden die auf diesem Wissen basieren Social Engineering Angriffe umsetzen kann. Die meisten erfolgreichen Attacken verwenden immer eine Komponente, die den Faktor Mensch berührt.

Interdisziplinär und Verbindung zur Forschung

Die Informationssicherheit kommt aktuell nicht nur mit Technik alleine weiter. Sicherheitsprobleme müssen immer in einem interdisziplinären Team untersucht und gelöst werden. Das bedeutet, dass die DeepSec In-Depth Security Konferenz für ein Spektrum aus Forschung, Lehre, Industrie, Behörden und Unternehmen gedacht ist. Genau wie im letzten Jahr haben Besucherinnen und Besucher auch die Möglichkeit Vorträge des parallel stattfindenden

Reversing and Offensive-oriented Trends Symposiums zu besuchen.

ROOTS ist ein akademischer Workshop, welcher parallel ort- und zeitgleich mit der DeepSec stattfindet. Der Anspruch ist es, zu zeigen, dass durch die Kombination von Wissenschaft und Informationstechnologie, und durch die Kombination von professionellem Insiderwissen, akademischer Forschung und praktischen Ansätzen, moderne digitale Infrastruktur besser als je zuvor verteidigt werden kann. Nutzen Sie die Gelegenheit.

Programm und Buchung

Die DeepSec Konferenztage sind am 29. und 30. November. Die Trainings finden an den zwei vorangehenden Tagen, dem 27. und 28. November, statt. Der Veranstaltungsort ist Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Sie finden das aktuelle Programm unter dem Link: deepsec.net/schedule.html

Tickets für die Konferenz und die Trainings können Sie unter dem Link deepsec.net/register.html bestellen.

WIRTSCHAFTS|zeit

Wirtschaftskalender

< Zurück zur Übersicht

DeepSec In-Depth Security Konferenz: Insecurity of Things (IoT)
29. Nov 2018 - 30. Nov 2018

Ort:
Imperial Riding School Renaissance Vienna Hotel
Ungargasse 60, 1030 Wien

Details

Die DeepSec In-Depth Security Konferenz widmet sich in diesem Jahr dem Thema Insecurity of Things (IoT) und Komponenten alltäglicher Infrastruktur. Die stetig voranschreitende Vernetzung eröffnet Angreifern völlig neue Wege - schneller, als Entwickler und Hersteller Fehler beheben können. Statt Secure Design bei Produkten und Code einzusetzen, integriert man Machine Learning und Künstliche Intelligenz - leider implementiert durch passende Statistik und den Algorithmus der Woche aus dem Tagesmenü des Entwicklungsbaukastens. Die Vorträge auf der DeepSec Konferenz werden daher die vermeintlichen Techniken der Zukunft auf den Prüfstand stellen. Mobilfunknetzwerke, das Internet der Dinge, Kollaborationsplattformen in der Cloud, Customer Relationship Management Systeme und der Faktor Mensch stehen im Fadenkreuz.
Smart is the new Cyber

Die Informationstechnologie hat den berechtigten Ruf ständig neue Begriffe und Akronyme zu erfinden um Lösungen für technische Probleme vorzugaukeln. Meist handelt es sich um ein reines Versteckspiel, sehr gut illustriert durch die Schlagworte Cyber, Cloud und Virtual. Hinter den Kulissen sind einige Begriffe berechtigt, aber kaum jemand prüft was sich hinter einem Produkt wirklich versteckt. Bestes Beispiel ist der Trend nun alles Smart zu machen, ganz egal ob Sicherheit ein Designkriterium war oder nicht. Die Stromversorgung soll zum Smart Grid werden, Fragenkataloge werden zum Smart Assistant, etc.

Ein Blick ins Innere offenbart Komponenten, die oft ohne ein Konzept von Sicherheit irgendwie miteinander verbunden werden. Das beste Beispiel sind Smartphones, die zum Universalschlüssel mutiert sind. Auf einem einzigen Gerät befindet sich eine Vielzahl von Zugängen, die bestimmte Apps benötigen. Damit werden diese Gegenstände automatisch zu einem begehrten Angriffsziel. Im Workshop Mobile App Attacks 2.0 wird gezeigt, wie man Apps und die Smartphone Plattform als Basis für erfolgreiche Angriffe verwendet. Und auch ein Workshop zum Thema Mobilfunksicherheit ist Teil des Programms. Der Trainer David Burgess ist ein Veteran auf diesem Gebiet und hat schon 2009 auf der DeepSec schwere Sicherheitslücken in Mobilfunknetzen entdeckt und dokumentiert. Dieses Jahr ist er wieder auf der DeepSec und kann auch etwas zu den neuen Standards sagen.

Unsicherheit der Dinge überall
Sicherheitslücken von Gegenständen aus dem Internet of Things (IoT) werden in Vorträgen und Workshops ebenso vorgestellt und analysiert. Johannes Pohl zeigt in seinem Training vor, wie man die Kommunikation von IoT Geräten analysiert. Diese Arbeit dient als Basis für daraus abgeleitete Angriffe. Wenige Hersteller sind wirklich in der Lage eine sichere Kommunikation als Protokoll zu entwerfen und zu implementieren, unabhängig ob das Protokoll neu erdacht ist oder auf etablierten Standards beruht.

Werner Schober, Sicherheitsforscher der Firma SEC Consult, stellt in seinem Vortrag Schwachstellen von "smartem" Sexspielzeug vor. Was wie ein schlechter Scherz klingt, ist leider keiner. Alle IoT-Geräte jeder Branche sind eine Gefahr. Da in Casinos schon über ein vernetztes Aquarium eingebrochen wurde, spielt der ursprüngliche Zweck des Gerät keine Rolle. Speziell bei Sexspielzeugen ist zusätzlich die Disziplin regelmäßiger Updates der Firmware betreffend sicher geringer als beim "smarten" Fernseher. Damit werden diese Gegenstände automatisch zu einem Risiko für Sicherheit und Privatsphäre zugleich. Im Alltag lassen sich mittlerweile zahllose weitere Dinge aufzählen, die für Angriffe auf Informationssysteme verwendet werden können.

Faktor Mensch
Egal welche Technologie man einsetzt, der Faktor Mensch bleibt wichtiger Teil der Informationssicherheit. Auch der menschliche Körper wird vernetzt. Ulrike Hugl von der Universität Innsbruck thematisiert implantierte RFID (radio-frequency identification) Chips. Mit solchen Fremdkörpern ist man dann selbst Teil von Fragen über Datensicherheit und Angriffen durch Dritte, denn RFID Komponenten tragen Daten und können ausgelesen werden. Behandelt werden Verbreitung, Nutzung und ethische Fragestellungen.

Darüber hinaus gibt es Vorträge zum Thema Bedrohungsanalyse, die ein wichtiger Teil der digitalen Verteidigung ist. Sie wird oft durch automatische Prozesse durchgeführt. Im Vortrag wird die Grenze zu den Fähigkeiten menschlicher Experten gezogen und wie man diese durch automatisierte Systeme unterstützen kann. Stefan Schumacher beleuchtet in seiner Präsentation wie sich das menschliche Gehirn manipulieren lässt und wie man mit Methoden die auf diesem Wissen basieren Social Engineering Angriffe umsetzen kann. Die meisten erfolgreichen Attacken verwenden immer eine Komponente, die den Faktor Mensch berührt.

Interdisziplinär und Verbindung zur Forschung
Die Informationssicherheit kommt aktuell nicht nur mit Technik alleine weiter. Sicherheitsprobleme müssen immer in einem interdisziplinären Team untersucht und gelöst werden. Das bedeutet, dass die DeepSec In-Depth Security Konferenz für ein Spektrum aus Forschung, Lehre, Industrie, Behörden und Unternehmen gedacht ist. Genau wie im letzten Jahr haben Besucherinnen und Besucher auch die Möglichkeit Vorträge des parallel stattfindenden Reversing and Offensive-oriented Trends Symposiums zu besuchen.

ROOTS ist ein akademischer Workshop, welcher parallel ort- und zeitgleich mit der DeepSec stattfindet. Der Anspruch ist es, zu zeigen, dass durch die Kombination von Wissenschaft und Informationstechnologie, und durch die Kombination von professionellem Insiderwissen, akademischer Forschung und praktischen Ansätzen, moderne digitale Infrastruktur besser als je zuvor verteidigt werden kann.
Nutzen Sie die Gelegenheit.

Programm und Buchung
Die DeepSec Konferenztage sind am 29. und 30. November. Die Trainings finden an den zwei vorangehenden Tagen, dem 27. und 28. November, statt. Der Veranstaltungsort ist Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Sie finden das aktuelle Programm unter dem Link: deepsec.net/schedule.html

Tickets für die Konferenz und die Trainings können Sie unter dem Link deepsec.net/register.html bestellen.

Organisator:
DeepSec GmbH
Bräuhausgasse 32, 1050 Wien

Details

< Zurück zur Übersicht

https://futurezone.at/digital-life/sicherheitsexperte-smart-ist-das-neue-dumm/400339486

Sicherheitsexperte: „Smart ist das neue dumm“

29.11.2018, Barbara Wimmer

Cybersicherheitsexperte Peter Zinn warnt auf der Sicherheitskonferenz DeepSec vor Gefahren, die durch neuen Technologien auf uns zukommen.

Die zunehmende Vernetzung würde uns als Gesellschaft, anders als von Gadget-Herstellern propagiert, nicht schlauer machen. „Smart ist das neue dumm“, sagt Zinn am Donnerstag auf der DeepSec in Wien. Er spricht damit etwa Gadgets an wie smarte Uhren, Thermostate oder aber auch vernetzte Autos oder Städte. „Es wird das nächste größere Desaster, wenn wir so weitermachen wie bisher.“

Der Grund für seine harten Worte: Derzeit wird Sicherheit nicht mitgedacht und alle vernetzten Geräte sind leicht angreifbar für Hacker. „Das liegt daran, dass die Gadgets meistens billig sein müssen, klein und leicht benutzbar. Für Verschlüsselung ist hier kein Platz mehr. Diese Anforderungen sind falsch und wir brauchen hier rasch ein Umdenken“, warnt der Experte. Die meisten Konsumenten würden derzeit für Sicherheitsfeatures nicht mehr Geld zahlen, weil sie den Wert nicht erkennen.

Smart Citys hören zu

„Dieses Problem kennen auch viele Internet Service Provider“, meint Zinn, der als unabhängiger Berater auch Städte auf ihrem Weg zur Smart City begleitet. „Wenn ich mit Verantwortlichen von Städten zusammensitze und ihnen erkläre, dass wir mehr Sicherheit brauchen, verstehen das die meisten. Sie hören zu. Sicherheit kostet allerdings etwas extra. Auch das verstehen sie. Auch mit einer minimalen Zeitverzögerung muss man rechnen, wenn man Sicherheit von Anfang an einplant, aber es zahlt sich aus“, so Zinn im Gespräch mit der futurezone. Für Zinn ist ein Umdenken bei den Entscheidungsträgern daher noch möglich. Er hofft zudem, dass man den Markt mit Regulierungen noch in die richtige Richtung lenken kann.

Obwohl Zinns Vortrag auf der DeepSec „We’re All Gonna Die“ („Wir werden alle sterben“) hieß, glaubt er nicht dass zuvor viele Menschen sterben müssen, bevor sich etwas beim Internet der Dinge ändert. Diese These hatten australische Sicherheitsforscher aufgestellt, die etwa auf die Automobilbranche im Zeitalter vor der Einführung von Airbags verwiesen haben. „Vielleicht braucht man Sicherheitsvorfälle, bevor Firmen wirklich Geld für Sicherheit in die Hand nehmen, aber wir schaffen es auch ohne dass dabei jemand stirbt“, sagt der Sicherheitsberater. „Wahrscheinlich würde es aber helfen.“

IT im Körper

Eine Weiterentwicklung von IoT sei als nächster Schritt das „Internet of People“, also das Internet, das Menschen in ihren Körpern tragen werden. Sei es eine Kontaktlinse mit verbessertem Sehvermögen, Gehirnimplantate, oder vernetzte Herzschrittmacher. „Mit IT können wir unser Leben verbessern“, meint der Experte, der selbst nicht davor zurückschrecken würde, sich Implantate einsetzen zu lassen, obwohl er auch die Gefahren kennt. So mussten sich im vergangenen Jahr zahlreiche Menschen mit Herzschrittmachern im Spital einem Update unterziehen, um sich vor potenziellen Angriffen zu schützen, die den Tod herbeiführen könnten.

„Derartige Daten werden allerdings auch für Versicherungen interessant. Ich glaube daher, dass wir hier einen Kampf zwischen der Möglichkeit, länger zu leben und unserer Privatsphäre erleben werden“, sagt Zinn. „Während wir uns hin zu mehr Sicherheit bewegen, glaube ich, dass das Konzept der Privatsphäre in 50 Jahren überholt sein könnte. Wie man an China sieht, braucht man Privatsphäre nicht zum Überleben“, so der Experte.

KI als Waffe

Neben dem Internet der Dinge und dem Internet of People sieht Zinn auch noch Kriege von künstlicher Intelligenz (KI) auf uns als Gesellschaft zukommen. „Da gab es diesen einen Vorfall: Ein AP-Twitter-Account wurde gehackt und eine Falschnachricht von Obamas Tod verbreitet. Daraufhin fielen die künstlich gesteuerten Aktienkurse so schnell, dass es zu spät war, um es zu stoppen. Solche Dinge werden künftig als Waffe verwendet“, erklärt der Experte. „Man kann KI für sehr präzise Attacken verwenden und bis man rausgefunden hat, was passiert ist, kann es schon zu spät sein.“

Die schlechte Nachricht kommt nun zum Schluss: Die Gesellschaft ist abhängig von Politik, Beratern und Sicherheitsforschern, um diese Gefahren zu minimieren. Konsumenten selbst, so Zinn, können hier wenig tun. „Für Kunden habe ich nur den Ratschlag, gute Passwörter zu wählen.“ Bei vielen sei hierfür die Motivation groß, aber nicht das Wissen. „Ein gutes Passwort kann auch aus einem Satz mit vier Wörtern bestehen“, so Zinn. „Es müssen nicht immer zahlreiche Sonderzeichen sein.“ Die Sicherheitsbranche, die noch bis Freitagabend auf der DeepSec-Konferenz tagt, ruft er zum Handeln auf: „Nicht viele Menschen verstehen, worum es geht. Es liegt an uns, an euch, die Welt sicherer zu machen.“

DIGITAL LIFE 29.11.2018

Sicherheitsexperte: „Smart ist das neue dumm"

© Bild: Getty Images/iStockphoto / Comomolas/iStockphoto.com

Cybersicherheitsexperte Peter Zinn warnt auf der Sicherheitskonferenz DeepSec vor Gefahren, die durch neuen Technologien auf uns zukommen.

Die zunehmende Vernetzung würde uns als Gesellschaft, anders als von Gadget-Herstellern propagiert, nicht schlauer machen. „Smart ist das neue dumm", sagt Zinn am Donnerstag auf der DeepSec in Wien. Er spricht damit etwa Gadgets an wie smarte Uhren, Thermostate oder aber auch vernetzte Autos oder Städte. „Es wird das nächste größere Desaster, wenn wir so weitermachen wie bisher."

Der Grund für seine harten Worte: Derzeit wird Sicherheit nicht mitgedacht und alle vernetzten Geräte sind leicht angreifbar für Hacker. „Das liegt daran, dass die Gadgets meistens billig sein müssen, klein und leicht benutzbar. Für Verschlüsselung ist hier kein Platz mehr. Diese Anforderungen sind falsch und wir brauchen hier rasch ein Umdenken", warnt der Experte. Die meisten Konsumenten würden derzeit für Sicherheitsfeatures nicht mehr Geld zahlen, weil sie den Wert nicht erkennen.

Peter Zinn auf der DeepSec in Wien © Bild: Joanna Pianka

Smart Citys hören zu

„Dieses Problem kennen auch viele Internet Service Provider", meint Zinn, der als unabhängiger Berater auch Städte auf ihrem Weg zur Smart City begleitet. „Wenn ich mit Verantwortlichen von Städten zusammensitze und ihnen erkläre, dass wir mehr Sicherheit brauchen, verstehen das die meisten. Sie hören zu. Sicherheit kostet allerdings etwas extra. Auch das verstehen sie. Auch mit einer minimalen Zeitverzögerung muss man rechnen, wenn man Sicherheit von Anfang an einplant, aber es zahlt sich aus", so Zinn im Gespräch mit der futurezone. Für Zinn ist ein Umdenken bei den Entscheidungsträgern daher noch möglich. Er hofft zudem, dass man den Markt mit Regulierungen noch in die richtige Richtung lenken kann.

Obwohl Zinns Vortrag auf der DeepSec „We're All Gonna Die" („Wir werden alle sterben") hieß, glaubt er nicht dass zuvor viele Menschen sterben müssen, bevor sich etwas beim Internet der Dinge ändert. Diese These hatten australische Sicherheitsforscher aufgestellt, die etwa auf die Automobilbranche im Zeitalter vor der Einführung von Airbags verwiesen haben. „Vielleicht braucht man Sicherheitsvorfälle, bevor Firmen wirklich Geld für Sicherheit in die Hand nehmen, aber wir schaffen es auch ohne dass dabei jemand stirbt", sagt der Sicherheitsberater. „Wahrscheinlich würde es aber helfen."

IT im Körper

Eine Weiterentwicklung von IoT sei als nächster Schritt das „Internet of People", also das Internet, das Menschen in ihren Körpern tragen werden. Sei es eine Kontaktlinse mit verbessertem Sehvermögen, Gehirnimplantate, oder vernetzte Herzschrittmacher. „Mit IT können wir unser Leben verbessern", meint der Experte, der selbst nicht davor zurückschrecken würde, sich Implantate einsetzen zu lassen, obwohl er auch die Gefahren kennt. So mussten sich im vergangenen Jahr zahlreiche Menschen mit Herzschrittmachern im Spital einem Update unterziehen, um sich vor potenziellen Angriffen zu schützen, die den Tod herbeiführen könnten.

„Derartige Daten werden allerdings auch für Versicherungen interessant. Ich glaube daher, dass wir hier einen Kampf zwischen der Möglichkeit, länger zu leben und unserer Privatsphäre erleben werden", sagt Zinn. „Während wir uns hin zu mehr Sicherheit bewegen, glaube ich, dass das Konzept der Privatsphäre in 50 Jahren überholt sein könnte. Wie man an China sieht, braucht man Privatsphäre nicht zum Überleben", so der Experte.

DIGITAL LIFE

Hacker steuern Herzschrittmacher, Hersteller verweigert Update

Sicherheitsforscher zeigen auf der Black Hat, wie sie einen Herzschrittmacher aus der Ferne beeinflussen können. Die Hersteller-Firma spricht von "geringem Risiko".

KI als Waffe

Neben dem Internet der Dinge und dem Internet of People sieht Zinn auch noch Kriege von künstlicher Intelligenz (KI) auf uns als Gesellschaft zukommen. „Da gab es diesen einen Vorfall: Ein AP-Twitter-Account wurde gehackt und eine Falschnachricht von Obamas Tod verbreitet. Daraufhin fielen die künstlich gesteuerten Aktienkurse so schnell, dass es zu spät war, um es zu stoppen. Solche Dinge werden künftig als Waffe verwendet", erklärt der Experte. „Man kann KI für sehr präzise Attacken verwenden und bis man rausgefunden hat, was passiert ist, kann es schon zu spät sein."

Die schlechte Nachricht kommt nun zum Schluss: Die Gesellschaft ist abhängig von Politik, Beratern und Sicherheitsforschern, um diese Gefahren zu minimieren. Konsumenten selbst, so Zinn, können hier wenig tun. „Für Kunden habe ich nur den Ratschlag, gute Passwörter zu wählen." Bei vielen sei hierfür die Motivation groß, aber nicht das Wissen. „Ein gutes Passwort kann auch aus einem Satz mit vier Wörtern bestehen", so Zinn. „Es müssen nicht immer zahlreiche Sonderzeichen sein." Die Sicherheitsbranche, die noch bis Freitagabend auf der DeepSec-Konferenz tagt, ruft er zum Handeln auf: „Nicht viele Menschen verstehen, worum es geht. Es liegt an uns, an euch, die Welt sicherer zu machen."

BARBARA WIMMER
(futurezone) | Stand: 29.11.2018, 16:39 | Autor:

https://www.mkcybersecurity.com/deepsec-2018-training-advanced-penetration-testing-in-the-real-world-davy-douhine-guillaume-lopes-%E2%80%A2/

DEEPSEC 2018 TRAINING: ADVANCED PENETRATION TESTING IN THE REAL WORLD – DAVY DOUHINE & GUILLAUME LOPES

17.11.2018

Guillaume and Davy, senior pentesters, will share many techniques, tips and tricks with pentesters, red teamers, bug bounty researchers or even defenders during a 2-day 100% “hands-on” workshop. This is the very training you’d like to have instead of wasting your precious time trying and failing while pentesting.

The main topics of the training are:

- Buffer overflow 101: Find and exploit buffer overflows yourself and bypass OS protections. (A lot of pentesters don’t even know how it works. So let’s have a look under the hood);
- Web exploitation: Manually find and exploit web app vulnerabilities using Burpsuite. (Yes, running WebInspect, AppScan, Acunetix or Netsparker is fine but you can do a lot more by hand);
- Passwords: Optimize the way you attack offline and online passwords. (0day is fun, but the way attackers gain access most of the time is simply by using login/pass words);

We asked Davy and Guillaume a few more questions about their training.

Please tell us the top 5 facts about your training.

It’s an hands-on training! Less talk and more exercises.

The goal is to learn techniques that you can apply in real use cases.

Know how hackers perform their attacks.

A variety of subjects are reviewed!

Learn the basics in order to be able to dig deeper into new subjects.

How did you come up with it? Was there something like an initial spark that set your mind on creating this talk / course?

Performing penetration tests (or pentests in short) is our daily job, but it is also a real hobby for us. We like learn-

ing new techniques, developing custom scripts or tools and also participating in Capture The Flag (CTF) sessions. After several years of pentest jobs, we found that clients are still amazed by the vulnerabilities we exploit and the techniques we use. This is not black magic! So, the idea of the course is to demystify the penetration test and show the participants how pentests are performed in the real world. In addition, we also wanted to avoid giving a training with just a list of tools and their description.

Why do you think this is an important topic?
Attacks are performed everyday against many companies and lead to data information leakage containing personal, but sometimes also financial information (i.e credit cards). Knowing the techniques allows one to understand the attacks, and, at the same time, to implement the protections to prevent them.

Is there something you want everybody to know – some good advice for our readers maybe?
Information security is evolving very fast and it is difficult to keep up to date on any and every subject. The training could be interesting for people having experience in penetration testing on a specific area (web app, mobile, etc.), or even for people who'd never performed pentests before and are willing to learn. Also, people having defensive experience could be interested to learn how hackers work.

A prediction for the future – what do you think will be the next innovations or future downfalls when it comes to your field of expertise / the topic of your training in particular?
For many years, some have been predicting the end of pentest, arguing that it will be replaced by bug-bounties or automated security audits. Clearly that has not happened yet, the demand is stronger than ever. Artificial intelligence will surely put us out of work one day, but we're not sure our generation will see that day.

Founder of RandoriSec, a security focused IT firm, Davy Douhine is working in the ITSec field since almost fifteen years. He has mainly worked for financial, banks and defence key accounts doing pentests and trainings to help them to improve their security.

Guillaume Lopes is working in the pentest field since about 10 years. He has written many ITSec articles and has attended many security conferences.

Source: https://blog.deepsec.net/deepsec-2018-training-advanced-penetration-testing-in-the-real-world-davy-douhine-guillaume-lopes/

DEEPSEC 2018 TRAINING: ADVANCED PENETRATION TESTING IN THE REAL WORLD – DAVY DOUHINE & GUILLAUME LOPES •

() November 17, 2018

Guillaume and Davy, senior pentesters, will share many techniques, tips and tricks with pentesters, red teamers, bug bounty researchers or even defenders during a 2-day 100% "hands-on" workshop. This is the very training you'd like to have instead of wasting your precious time trying and failing while pentesting.

The main topics of the training are:

- Buffer overflow 101: Find and exploit buffer overflows yourself and bypass OS protections. (A lot of pentesters don't even know how it works. So let's have a look under the hood);
- Web exploitation: Manually find and exploit web app vulnerabilities using Burpsuite. (Yes, running WebInspect, AppScan, Acunetix or Netsparker is fine but you can do a lot more by hand);
- Passwords: Optimize the way you attack offline and online passwords. (0day is fun, but the way attackers gain access most of the time is simply by using login/passwords);

We asked Davy and Guillaume a few more questions about their training.

Please tell us the top 5 facts about your training.

1. It's an hands-on training! Less talk and more exercises.
2. The goal is to learn techniques that you can apply in real use cases.
3. Know how hackers perform their attacks.
4. A variety of subjects are reviewed!
5. Learn the basics in order to be able to dig deeper into new subjects.

How did you come up with it? Was there something like an initial spark that set your mind on creating this talk / course?

Performing penetration tests (or pentests in short) is our daily job, but it is also a real hobby for us. We like learning new techniques, developing custom scripts or tools and also participating in Capture The Flag (CTF) sessions. After several years of pentest jobs, we found that clients are still amazed by the vulnerabilities we exploit and the techniques we use. This is not black magic! So, the idea of the course is to demystify the penetration test and show the participants how pentests are performed in the real world. In addition, we also wanted to avoid giving a training with just a list of tools and their description.

Why do you think this is an important topic?

Attacks are perform everyday against many companies and lead to data information leakage containing personal, but sometimes also financial information (i.e credit cards). Knowing the techniques allows one to understand the attacks, and, at the same time, to implement the protections to prevent them.

Is there something you want everybody to know – some good advice for our readers maybe?

Information security is evolving very fast and it is difficult to keep up to date on any and every subject. The training could be interesting for people having experience in penetration testing on a specific area (web app, mobile, etc.), or even for people who'd never performed pentests before and are willing to learn. Also, people having defensive experience could be interested to learn how hackers work.

A prediction for the future – what do you think will be the next innovations or future downfalls when it comes to your field of expertise / the topic of your training in particular?

For many years, some have been predicting the end of pentest, arguing that it will be replaced by bug-bounties or automated security audits. Clearly that has not happened yet, the demand is stronger than ever. Artificial intelligence will surely put us out of work one day, but we're not sure our generation will see that day.

Founder of RandoriSec, a security focused IT firm, Davy Douhine is working in the ITSec field since almost fifteen years. He has mainly worked for financial, banks and defence key accounts doing pentests and trainings to help them to improve their security.

Guillaume Lopes is working in the pentest field since about 10 years. He has written many ITSec articles and has attended many security conferences.

Tags: , , , , , , , , , ,

This entry was posted on September 24, 2018 at 08:45. You can follow any responses to this entry through the RSS 2.0 feed. You can leave a response, or from your own site.

Source

> DeepSec 2018 Training: Advanced Penetration Testing in the Real World – Davy Douhine & Guillaume Lopes (https://blog.deepsec.net/deepsec-2018-training-advanced-penetration-testing-in-the-real-world-davy-douhine-guillaume-lopes/)

Share this:

https://computerwelt.at/news/topmeldung/deepsec-konferenz-geheimdienste-wollen-informationssicherheit-abschaffen/

DeepSec: Geheimdienste wollen Informationssicherheit abschaffen

11.09.2018, Klaus Lorbeer

Seit es Sicherheitsmaßnahmen gibt, wird über ihren Nutzen und ihre Stärke diskutiert. Bei digitaler Kommunikation kommt stets das Thema der Hintertüren auf. Hochqualitative Schlösser sind in der analogen Welt erwünscht, um Werte vor Diebstahl zu schützen. In der digitalen Welt soll das anders werden.

Die „Five Eyes" (sprich die Geheimdienste der Vereinigten Staaten, Großbritanniens, Australiens, Neuseelands und Kanada) möchten alle Staaten der Welt bei verschlüsselter Kommunikation zum Einbau von Nachschlüsseln, also Hintertüren, zwingen. Dazu fand Ende August in Australien ein Treffen der Five Eyes Innenminister statt. Dieser Vorschlag birgt schwerwiegende Nachteile für die Wirtschaft und die nationale Sicherheit jedes Staates.

Messenger statt Mobilfunk

Als die Mobiltelefone ihren Siegeszug antraten, gab es nur unverschlüsselte Kurznachrichten (auch bekannt als SMS, Short Message Service). Vor der Ära der Smartphones haben einige Hersteller eigene proprietäre Formate entwickelt, um den Inhalt der Nachrichten zu schützen. In den letzten Jahren gab es einen Schwenk in Richtung Messenger Apps, die das Internet für die Nachrichtenübertragung nutzen. Damit konnten und können Entwicklerinnen offene Standards mit starker Verschlüsselung einsetzen, die nicht den gesetzlich vorgeschriebenen Schnittstellen zur Telekommunikationsüberwachung in den Mobilfunknetzwerken unterliegen.

Diese Telekommunikationsüberwachung (international auch „Lawful Interception" genannt) ist fester Bestandteil der Netzwerkinfrastuktur und erfasst ständig Ortsdaten, Logins, Betriebszeiten, Adressen, Mobilfunkidentifikationen sowie weitere Daten. Moderne Messenger setzen daher meist das Prinzip der Ende-zu-Ende-Verschlüsselung ein, wo nur die kommunizierenden Endgeräte die Schlüssel zur Nachricht besitzen. Das Netzwerk kennt diese nicht und kann den Inhalt der Nachrichten nicht sehen. Dies ist nur über mobilen Datenzugang, sprich Internetzugriff, möglich.

Die Gefahren dieser Schnittstellen wurden durch die publizierten Dokumente von Edward Snowden im Jahre 2013 und die Abhöraffäre in Athen in den Jahren 2004 und 2005 illustriert. Bereits 2015 hielt James Bamford, US-amerikanischer Journalist und Nachrichtendienstexperte, den Eröffnungsvortrag zur DeepSec-Konferenz und erläuterte

darin wie die Mobiltelefone der griechische Regierung über rechtlich geforderte Hintertüren von Unbekannten abgehört wurden. Kostas Tsalikidis, der zuständige Netzwerkverantwortliche, beging Tage nach Bekanntwerden der Abhörkonfigurationen Selbstmord. Die Täter der Abhöraktion wurden trotz größter langwieriger Ermittlungen nie ausfindig gemacht.

Mathematik ist in Australien nicht rechtskräftig

Sicherheitsforscher und Ingenieure sind sich der Gefahren schlecht implementierter und unsicherer Kommunikation sehr wohl bewusst. Aus diesem Grunde wird spätestens seit den Snowden Enthüllungen starke Kryptographie und sichere Kommunikation von Technologiefirmen und Entwicklerinnen forciert. Das Institute of Electrical and Electronics Engineers (IEEE) und die Internet Engineering Task Force (IETF) haben in allen Standards der letzten Jahre Protokolle standardisiert, die weder Hintertüren noch absichtlich geschwächte Algorithmen enthalten. Das moderne Internet, und damit unsere heutige Kommunikationsgesellschaft, basiert auf diesen Standards.

Die Techniker versuchen damit, das Pendant zu sicheren Brücken zu schaffen, die ja auch keine Sollbruchstelle haben dürfen. Infrastruktur muss verlässlich sein. Man darf dabei nicht vergessen, dass nicht nur Telefonate und Nachrichten von den gesetzlichen Schwachstellen betroffen sind. Forderungen nach Nachschlüsseln betreffen Finanztransaktionen, das komplette World Wide Web, sämtliche Anwendungen auf Smartphones, das Internet-der-Dinge, alle Smart-Technologien, kurzum alle Unternehmen und Märkte weltweit.

Der ehemalige australische Premierminister Malcolm Turnbull hat den Forderungen, weltweit immer und überall sämtliche Kommunikation mitlesen zu können, höchste Priorität gegeben. Er sagt im Juli diesen Jahres, dass das Gesetzbuch Australiens über der Mathematik stehe. Damit bezog er sich auf die Kritik von Forschern der Kryptographie, die ein Teilgebiet der Mathematik ist. Diese Logik ist fragwürdig, betonen die DeepSec-Konferenz-Veranstalter, denn niemand hat bisher die Gravitation für illegal erklärt, um Arbeitsunfälle zu verhindern oder leichter Berge besteigen zu können. Die Frage ist einzig und alleine, ob man echte Sicherheit haben möchte oder nicht. Der Brandschutz ist eine gute Analogie. Niemand möchte Schutzvorkehrungen gegen Brände, die nicht immer funktionieren. Genauso möchte auch niemand elektronische Zahlungsmittel nutzen, die bis auf Widerruf sicher sind.

Nationale Sicherheit schafft sich international ab

Die Forderung der Five Eyes lässt sich auch umformulieren. Da die Dienste ebenso die Mathematik zum Schutz ihrer Länder einsetzen, müssten sie sich selbst schwächen. Das betrifft dann insbesondere Wirtschaftsspionage, die sehr oft Ländergrenzen überquert. Eine komplette Zerstörung bzw. die Sabotage von wichtigen Komponenten

der Informationssicherheit ist ein kurzsichtiger Reflex, sind die Experten der DeepSec-Konferenz überzeugt. Es gehe nicht nur um die Vorzeigefirmen im Silicon Valley. Hintertüren und Nachschlüssel belasteten jedwede Kommunikation über Geschäftsgeheimnisse bis hin zur sicheren elektronische Kommunikation von Rechtsanwälten mit der Justiz und Behörden.

Man darf dabei nicht vergessen, dass diese Forderung nicht nur von den Five Eyes gestellt werden wird, sollte es zu einer Umsetzung durch Regierungen kommen. Die Vereinten Nationen führen momentan eine Liste von 206 Mitgliedsstaaten. Die Forderungen der Five Eyes werden dann von den „206 Eyes" auch gestellt werden. Politisch Verantwortliche sind sehr gut beraten, die Warnungen von Experten nicht zu ignorieren. Stimmt man der Forderung nach Hintertüren zu, so müssen die Geheimdienste der Five Eyes dann auch den Diensten Europas, Russlands, Chinas und Nordkoreas jeweils ihre eigene nationale Kommunikation offenlegen, denn die Mathematik der Sicherheit oder Unsicherheit gilt für alle gleichermaßen. Die Forderung hat daher mit der Realität rein gar nichts zu tun, mit Informationssicherheit schon gar nicht.

Lösungen nicht im Monolog möglich

Sicherheitsforscher sitzen im selben Boot wie die Behörden. Auch sie müssen Angreifer finden und müssen mit oder gegen Schutzmaßnahmen arbeiten. Dennoch rücken IEEE, IETF und alle technischen Organisationen nicht von der Forderung nach starker Sicherheit ab. Da die Five-Eyes-Forderungen explizit legislative Maßnahmen ansprechen, ist das ein wertvolles Kompliment für die Techniker. Das bedeutet, dass die technische Umsetzung nur sehr schwer oder mit den derzeit verfügbaren Mitteln nicht angreifbar ist.

Die Implementation von Sicherheit ist immer ein Ergebnis interdisziplinärer Zusammenarbeit. Genau aus diesem Grund möchte die DeepSec-Konferenz jährlich Vertreter aus Forschung, Behörden, Wirtschaft und der internationalen Hacker-Community an einen Tisch bringen. Eine vernetzte Welt benötigt vernetztes Denken. Insellösungen oder kurzfristige Maßnahmen sind nicht zukunftsgerichtet. Daher hat die diesjährige DeepSec-Konferenz ihren Schwerpunkt auf Infrastruktur, Internet der Dinge, Mobilität (sei es Funk, Gerät oder Transport) und auch Kryptographie gelegt. Spezialisten aus vier Kontinenten tauschen sich im November in Wien aus, um Bedrohungen der Zukunft zu begegnen.

Details und Programm der DeepSec-Konferenz

Die DeepSec-Konferenztage sind am 29. und 30. November. Die Trainings finden an den zwei vorangehenden Tagen, dem 27. und 28. November statt. Der Veranstaltungsort ist das Hotel The Imperial Riding School Vienna – A Renaissance Hotel in der Ungargasse 60, 1030 Wien.

Das aktuelle Programm kann unter dem Link https://deepsec.net/schedule.html eingesehen werden. Tickets für die Konferenz und die Trainings können Interessierte unter dem Link https://deepsec.net/register.html bestellen.

James Bamford hat in der Publikation „In-Depth Security – Proceedings of the DeepSec Conferences Volume 2“ seinen Vortrag als Artikel mit dem Titel „A Death in Athens – The Inherent Vulnerability of „Lawful Intercept““ zusammengefasst. Das Buch ist im Handel erhältlich oder kann direkt über die DeepSec GmbH bezogen werden. Nachfolgend Bamfords Vortrag auf Video:

Link:
A Death in Athens: The inherent Vulnerability of “Lawful Intercept” Programs – James Bamford from Deepsec Conference on Vimeo.

11. September 2018 Klaus Lorbeer/pi

DeepSec: Geheimdienste wollen Informationssicherheit abschaffen

Seit es Sicherheitsmaßnahmen gibt, wird über ihren Nutzen und ihre Stärke diskutiert. Bei digitaler Kommunikation kommt stets das Thema der Hintertüren auf. Hochqualitative Schlösser sind in der analogen Welt erwünscht, um Werte vor Diebstahl zu schützen. In der digitalen Welt soll das anders werden.

Die DeepSec-Konferenz findet in Wien am 29. und 30. November statt. (c) DeepSec GmbH

Die „Five Eyes" (sprich die Geheimdienste der Vereinigten Staaten, Großbritanniens, Australiens, Neuseelands und Kanada) möchten alle Staaten der Welt bei verschlüsselter Kommunikation zum Einbau von Nachschlüsseln, also Hintertüren, zwingen. Dazu fand Ende August in Australien ein Treffen der Five Eyes Innenminister statt. Dieser Vorschlag birgt schwerwiegende Nachteile für die Wirtschaft und die nationale Sicherheit jedes Staates.

Messenger statt Mobilfunk

Als die Mobiltelefone ihren Siegeszug antraten, gab es nur unverschlüsselte Kurznachrichten (auch bekannt als SMS, Short Message Service). Vor der Ära der Smartphones haben einige Hersteller eigene proprietäre Formate entwickelt, um den Inhalt der Nachrichten zu schützen. In den letzten Jahren gab es einen Schwenk in Richtung Messenger Apps, die das Internet für die Nachrichtenübertragung nutzen. Damit konnten und können Entwicklerinnen offene Standards mit starker Verschlüsselung einsetzen, die nicht den gesetzlich vorgeschriebenen Schnittstellen zur Telekommunikationsüberwachung in den Mobilfunknetzwerken unterliegen.

Diese Telekommunikationsüberwachung (international auch „Lawful Interception" genannt) ist fester Bestandteil der Netzwerkinfrastuktur und erfasst ständig Ortsdaten, Logins, Betriebszeiten, Adressen, Mobilfunkidentifikationen sowie weitere Daten. Moderne Messenger setzen daher meist das Prinzip der Ende-zu-Ende-Verschlüsselung ein, wo nur die kommunizierenden Endgeräte die Schlüssel zur Nachricht besitzen. Das Netzwerk kennt diese nicht und kann den Inhalt der Nachrichten nicht sehen.

Die Gefahren dieser Schnittstellen wurden durch die publizierten Dokumente von Edward Snowden im Jahre 2013 und die Abhöraffäre in Athen in den Jahren 2004 und 2005 illustriert. Bereits 2015 hielt James Bamford, US-amerikanischer Journalist und Nachrichtendienstexperte, den Eröffnungsvortrag zur DeepSec-Konferenz und erläuterte darin wie die Mobiltelefone der griechische Regierung über rechtlich geforderte Hintertüren von Unbekannten abgehört wurden. Kostas Tsalikidis, der zuständige Netzwerkverantwortliche, beging Tage nach Bekanntwerden der Abhörkonfigurationen Selbstmord. Die Täter der Abhöraktion wurden trotz größter langwieriger Ermittlungen nie ausfindig gemacht.

Mathematik ist in Australien nicht rechtskräftig

Sicherheitsforscher und Ingenieure sind sich der Gefahren schlecht implementierter und unsicherer Kommunikation sehr wohl bewusst. Aus diesem Grunde wird spätestens seit den Snowden Enthüllungen starke Kryptographie und sichere Kommunikation von Technologiefirmen und Entwicklerinnen forciert. Das Institute of Electrical and Electronics Engineers (IEEE) und die Internet Engineering Task Force (IETF) haben in allen Standards der letzten Jahre Protokolle standardisiert, die weder Hintertüren noch absichtlich geschwächte Algorithmen enthalten. Das moderne Internet, und damit unsere heutige Kommunikationsgesellschaft, basiert auf diesen Standards.

Die Techniker versuchen damit, das Pendant zu sicheren Brücken zu schaffen, die ja auch keine Sollbruchstelle haben dürfen. Infrastruktur muss verlässlich sein. Man darf dabei nicht vergessen, dass nicht nur Telefonate und Nachrichten von den gesetzlichen Schwachstellen betroffen sind. Forderungen nach Nachschlüsseln betreffen Finanztransaktionen, das komplette World Wide Web, sämtliche Anwendungen auf Smartphones, das Internet-der-Dinge, alle Smart-Technologien, kurzum alle Unternehmen und Märkte weltweit.

Der ehemalige australische Premierminister Malcolm Turnbull hat den Forderungen, weltweit immer und überall sämtliche Kommunikation mitlesen zu können, höchste Priorität gegeben. Er sagt im Juli diesen Jahres, dass das Gesetzbuch Australiens über der Mathematik stehe. Damit bezog er sich auf die Kritik von Forschern der Kryptographie, die ein Teilgebiet der Mathematik ist. Diese Logik ist fragwürdig, betonen die DeepSec-Konferenz-Veranstalter, denn niemand hat bisher die Gravitation für illegal erklärt, um Arbeitsunfälle zu verhindern oder leichter Berge besteigen zu können. Die Frage ist einzig und alleine, ob man echte Sicherheit haben möchte oder nicht. Der Brandschutz ist eine gute Analogie. Niemand möchte Schutzvorkehrungen gegen Brände, die nicht immer funktionieren. Genauso möchte auch niemand elektronische Zahlungsmittel nutzen, die bis auf Widerruf sicher sind.

Nationale Sicherheit schafft sich international ab

Die Forderung der Five Eyes lässt sich auch umformulieren. Da die Dienste ebenso die Mathematik zum Schutz ihrer Länder einsetzen, müssten sie sich selbst schwächen. Das betrifft dann insbesondere Wirtschaftsspionage, die sehr oft Ländergrenzen überquert. Eine komplette Zerstörung bzw. die Sabotage von wichtigen Komponenten der Informationssicherheit ist ein kurzsichtiger Reflex, sind die Experten der DeepSec-Konferenz überzeugt. Es gehe nicht nur um die Vorzeigefirmen im Silicon Valley. Hintertüren und Nachschlüssel belasteten jedwede Kommunikation über Geschäftsgeheimnisse bis hin zur sicheren

Man darf dabei nicht vergessen, dass diese Forderung nicht nur von den Five Eyes gestellt werden wird, sollte es zu einer Umsetzung durch Regierungen kommen. Die Vereinten Nationen führen momentan eine Liste von 206 Mitgliedsstaaten. Die Forderungen der Five Eyes werden dann von den „206 Eyes" auch gestellt werden. Politisch Verantwortliche sind sehr gut beraten, die Warnungen von Experten nicht zu ignorieren. Stimmt man der Forderung nach Hintertüren zu, so müssen die Geheimdienste der Five Eyes dann auch den Diensten Europas, Russlands, Chinas und Nordkoreas jeweils ihre eigene nationale Kommunikation offenlegen, denn die Mathematik der Sicherheit oder Unsicherheit gilt für alle gleichermaßen. Die Forderung hat daher mit der Realität rein gar nichts zu tun, mit Informationssicherheit schon gar nicht.

Lösungen nicht im Monolog möglich

Sicherheitsforscher sitzen im selben Boot wie die Behörden. Auch sie müssen Angreifer finden und müssen mit oder gegen Schutzmaßnahmen arbeiten. Dennoch rücken IEEE, IETF und alle technischen Organisationen nicht von der Forderung nach starker Sicherheit ab. Da die Five-Eyes-Forderungen explizit legislative Maßnahmen ansprechen, ist das ein wertvolles Kompliment für die Techniker. Das bedeutet, dass die technische Umsetzung nur sehr schwer oder mit den derzeit verfügbaren Mitteln nicht angreifbar ist.

Die Implementation von Sicherheit ist immer ein Ergebnis interdisziplinärer Zusammenarbeit. Genau aus diesem Grund möchte die DeepSec-Konferenz jährlich Vertreter aus Forschung, Behörden, Wirtschaft und der internationalen Hacker-Community an einen Tisch bringen. Eine vernetzte Welt benötigt vernetztes Denken. Insellösungen oder kurzfristige Maßnahmen sind nicht zukunftsgerichtet. Daher hat die diesjährige DeepSec-Konferenz ihren Schwerpunkt auf Infrastruktur, Internet der Dinge, Mobilität (sei es Funk, Gerät oder Transport) und auch Kryptographie gelegt. Spezialisten aus vier Kontinenten tauschen sich im November in Wien aus, um Bedrohungen der Zukunft zu begegnen.

Details und Programm der DeepSec-Konferenz

Die DeepSec-Konferenztage sind am 29. und 30. November. Die Trainings finden an den zwei vorangehenden Tagen, dem 27. und 28. November statt. Der Veranstaltungsort ist das Hotel The Imperial Riding School Vienna – A Renaissance Hotel in der Ungargasse 60, 1030 Wien.

Das aktuelle Programm kann unter dem Link **https://deepsec.net/schedule.html** eingesehen werden. Tickets für die Konferenz und die Trainings können Interessierte unter dem Link **https://deepsec.net/register.html** bestellen.

James Bamford hat in der Publikation „In-Depth Security – Proceedings of the DeepSec Conferences Volume 2" seinen Vortrag als Artikel mit dem Titel „A Death in Athens – The Inherent Vulnerability of „Lawful Intercept"" zusammengefasst. Das Buch ist im Handel erhältlich oder kann direkt über die DeepSec GmbH bezogen werden. Nachfolgend Bamfords Vortrag auf Video:

A Death in Athens: The inherent Vulnerability of "Lawful Intercept" Programs - James Bamford

from Deepsec Conference

39:23

A Death in Athens: The inherent Vulnerability of "Lawful Intercept" Programs – James Bamford from Deepsec Conference on Vimeo.

GEHEIMDIENSTE KONFERENZ SECURITY ÜBERWACHUNG WIEN

MEHR ARTIKEL

NEWS

Computer schreibt Songs wie ein Popstar

NEWS

CES: IBM zeigt erste integrierte Quanten-Computer für den kommerziellen Einsatz

KNOWHOW

Wi-Fi Mesh: Was Sie über Mesh-Netzwerke in Unternehmen wissen sollten

NEWS

„Schluss mit den KI-Mythen"

NEWS

Gerd Ingo Janitschek neuer Geschäftsführer von docu tools

NEWS

Anstieg File-basierter Angriffe

https://computerwelt.at/news/deepsec-konferenz-bietet-weiterbildung-fuer-sicherheitsforscher-an/

DeepSec-Konferenz bietet Weiterbildung für Sicherheitsforscher

09.09.2018, Klaus Lorbeer

Die DeepSec In-Depth Security Konferenz bietet neben Vorträgen zum Versagen von Sicherheitsmaßnahmen dieses Jahr einen Workshop für das Finden von Schwachstellen an.

Das Testen von Software im Rahmen der Qualitätssicherung reicht in der modernen, vernetzen Welt leider nicht mehr aus. Die Vorsilbe „Smart“ ändert nichts an bestehenden Schwächen. Der Kurs auf der DeepSec InDepth Security Konferenz für das Finden von Schwachstellen richtet sich daher an Fachkräfte, die bereits in der Entwicklung arbeiten, und Sicherheitsexperten, um gezielt die Entwicklung sicherer Produkte in Industrie und Unternehmen zu stärken.

Komplexe Technologien und ihre Fehleranfälligkeit

Moderne Produkte kommen nicht erst seit der Geburt des Internet-der-Dinge nicht ohne Software aus. Fügt man Vernetzung und eine hohe Komplexität der Einzelteile hinzu, so ist dies ein Erfolgsrezept für Fehler. Natürlich gibt es oft eine Qualitätssicherung und Prüfungen auf die wichtigsten Funktionen, jedoch ist die Folge von schwerwiegenden Fehlfunktionen durch den Umfang der Codezeilen eine Frage der Statistik. Wie können sich Hersteller und Entwickler helfen? Zieht man die mathematische Spieltheorie zu Rate, so ist die Antwort: Kopfgeld für Fehler – Bug Bounties als Belohnung.

Organisierte Jagd nach Softwarefehlern

Die Bug-Bounty-Programme wurden vor einigen Jahren als feste Institution ins Leben gerufen, um einerseits Sicherheitsforschern und -forscherinnen die Möglichkeit zu geben, ihre Arbeit beim Finden und Suchen von Fehlern zu würdigen. Auf der anderen Seite regelt ein solches Programm automatisch den Ablauf wie kritische Fehler gemeldet, dokumentiert, reproduziert und seitens der zuständigen Entwickler und Entwicklerinnen behoben werden. Es gibt leider immer noch sehr viele Hersteller, die nicht auf gemeldete Fehler reagieren und keine Updates zur Verfügung stellen. Das Anbieten von Bug Bounties spricht daher für das Engagement eines Unternehmens und sichert die Qualität der eigenen Produkte. Obendrein erfährt man dann vom Versagen des eigenen Produkts nicht aus der Presse oder aus dem Internet.

Der große Vorteil ist die gute Qualität der Fehlerberichte. Fehler-in-Software-finden ist das tägliche Brot der Softwa-

reentwicklung, aber kritische Schwachstellen, die ein Sicherheitsproblem darstellen, erkennt man oft nicht sofort. Die Informationssicherheit ist ein interdisziplinärer Bereich der Informatik, welche Fähigkeiten in Softwareentwicklung, Mathematik, Reverse Engineering (sprich die Nachkonstruktion einer Applikation oder eines Protokolls) und viel Geduld erfordert. Dazu ist fundiertes Wissen, ausreichend Erfahrung und eine gezielte Ausbildung erforderlich, die nicht alle im Entwicklungsteam besitzen.

Die Bug-Bounty-Programme werden sehr gut angenommen. HackerOne, eine Plattform zur koordinierten Publikation von Schwachstellen, führt Buch über die Ausschüttungen an Entdeckern von Fehlern. Derzeit wurden in Summe über 20 Millionen US-Dollar an Forscher von verschiedenen Firmen ausgezahlt. Das erklärte Ziel ist das Erreichen von 100 Millionen US-Dollar bis 2020.

Ausbildung zum Bug-Bounty-Hunter

Dies diesjährige DeepSec-Sicherheitskonferenz hat einen zweitägigen Kurs zum Thema Bug Hunting. Der Trainer Dawid Czagan, selbst unter den Top 10 der Bug-Hunter-Liste von HackerOne, hat ein Curriculum ausgearbeitet, das Fortgeschrittenen mit Kenntnissen von Praktiken der Softwareentwicklung die Ansätze und Denkweise von Sicherheitsexperten beibringt. Teilnehmer lernen wie die vielen Teile von modernen Anwendungen wechselwirken, wo man in Protokolle zur Analyse einsteigt und worauf man achten muss. Da viele Arbeiten mittlerweile über Weboberflächen stattfinden, sei es sichtbar für den Benutzer oder unsichtbar hinter den Kulissen, wird die Webtechnologie der Fokus des Kurses sein. Dabei geht es nicht nur um die Kopfgeldjagd.

Der Workshop besteht nicht nur aus trockener Theorie. Dawid Czagan hat Fallbeispiele aus produktiven Umgebungen vorbereitet, um die verschiedenen Klassen von Fehler zu illustrieren. Der komplette Kurs ist eine Mischung aus kurzem Vortrag zur Erklärung gefolgt von praktischen Übungen, um das neu erworbene Wissen zu festigen. Die vermittelten Fähigkeiten sind eine wertvolle Ergänzung für jede Qualitätssicherung und eine gefragte Weiterbildung für Entwickler und Entwicklerinnen. Die Veranstaltung richtet sich gezielt an Sicherheitsforscher, Penetration Tester, Consultants, Projektleiter/Entwickler aus der Softwareentwicklung und IT-Architekten, die grundlegende Designs entwerfen, auf dem Anwendungen und Systeme aufbauen.

Die Angreifer haben diese Mittel schon. Es wird Zeit, dass Sie aufholen. Vernetzte Systeme schlafen nie.

Programm und Buchung

Die DeepSec-Konferenztage finden am 29. und 30. November, die Trainings an den zwei vorangehenden Tagen, dem 27. und 28. November, statt.

Der Veranstaltungsort ist das Hotel „The Imperial Riding School Vienna – A Renaissance Hotel“ in der Ungargasse 60, 1030 Wien.

Interessierte finden das aktuelle Programm hier. Tickets für die Konferenz und die Trainings können unter https://deepsec.net/register.html bestellt werden.

Das Blog der Konferenz mit Informationen und Hintergründen zu den Vorträgen und dem Workshop gibt es unter https://blog.deepsec.net.

9. September 2018 Klaus Lorbeer/pi

DeepSec-Konferenz bietet Weiterbildung für Sicherheitsforscher

Die DeepSec In-Depth Security Konferenz bietet neben Vorträgen zum Versagen von Sicherheitsmaßnahmen dieses Jahr einen Workshop für das Finden von Schwachstellen an.

Die DeepSec-Konferenz 2018 findet vom 29.-30. November 2018 im Imperial Riding School Renaissance Vienna Hotel statt. (c) DeepSec

Das Testen von Software im Rahmen der Qualitätssicherung reicht in der modernen, vernetzen Welt leider nicht mehr aus. Die Vorsilbe „Smart" ändert nichts an bestehenden Schwächen. Der Kurs auf der DeepSec InDepth Security Konferenz für das Finden von Schwachstellen richtet sich daher an Fachkräfte, die bereits in der Entwicklung arbeiten, und Sicherheitsexperten, um gezielt die Entwicklung sicherer Produkte in Industrie und Unternehmen zu stärken.

Komplexe Technologien und ihre Fehleranfälligkeit

Moderne Produkte kommen nicht erst seit der Geburt des Internet-der-Dinge nicht ohne Software aus. Fügt man Vernetzung und eine hohe Komplexität der Einzelteile hinzu, so ist dies ein Erfolgsrezept für Fehler. Natürlich gibt es oft eine Qualitätssicherung und Prüfungen auf die wichtigsten Funktionen, jedoch ist die Folge von schwerwiegenden Fehlfunktionen durch den Umfang der Codezeilen eine Frage der Statistik. Wie können sich Hersteller und Entwickler helfen? Zieht man die mathematische Spieltheorie zu Rate, so ist die Antwort: Kopfgeld für Fehler – Bug Bounties als Belohnung.

Organisierte Jagd nach Softwarefehlern

Die Bug-Bounty-Programme wurden vor einigen Jahren als feste Institution ins Leben gerufen, um einerseits Sicherheitsforschern und -forscherinnen die Möglichkeit zu geben, ihre Arbeit beim Finden und Suchen von Fehlern zu würdigen. Auf der anderen Seite regelt ein solches Programm automatisch den Ablauf wie kritische Fehler gemeldet, dokumentiert, reproduziert und seitens der zuständigen Entwickler und Entwicklerinnen behoben werden. Es gibt leider immer noch sehr viele Hersteller, die nicht auf gemeldete Fehler reagieren und keine Updates zur Verfügung stellen. Das Anbieten von Bug Bounties spricht daher für das Engagement eines Unternehmens und sichert die Qualität der eigenen Produkte. Obendrein erfährt man dann vom Versagen des eigenen Produkts nicht aus der Presse oder aus dem Internet.

Der große Vorteil ist die gute Qualität der Fehlerberichte. Fehler-in-Software-finden ist das tägliche Brot der Softwareentwicklung, aber kritische Schwachstellen, die ein Sicherheitsproblem darstellen, erkennt man oft nicht sofort. Die Informationssicherheit ist ein interdisziplinärer Bereich der Informatik, welche Fähigkeiten in Softwareentwicklung, Mathematik, Reverse Engineering (sprich die Nachkonstruktion einer Applikation oder eines Protokolls) und viel Geduld erfordert. Dazu ist fundiertes Wissen, ausreichend Erfahrung und eine gezielte Ausbildung erforderlich, die nicht alle im Entwicklungsteam besitzen.

Die Bug-Bounty-Programme werden sehr gut angenommen. HackerOne, eine Plattform zur koordinierten Publikation von Schwachstellen, führt Buch über die Ausschüttungen an Entdeckern von Fehlern. Derzeit wurden in Summe über 20 Millionen US-Dollar an Forscher von verschiedenen Firmen ausgezahlt. Das erklärte Ziel ist das Erreichen von 100 Millionen US-Dollar bis 2020.

Ausbildung zum Bug-Bounty-Hunter

Dies diesjährige DeepSec-Sicherheitskonferenz hat einen zweitägigen Kurs zum Thema Bug Hunting. Der Trainer Dawid Czagan, selbst unter den Top 10 der Bug-Hunter-Liste von HackerOne, hat ein Curriculum ausgearbeitet, das Fortgeschrittenen mit Kenntnissen von Praktiken der Softwareentwicklung die Ansätze und Denkweise von Sicherheitsexperten beibringt. Teilnehmer lernen wie die vielen Teile von modernen Anwendungen wechselwirken, wo man in Protokolle zur Analyse einsteigt und worauf man achten muss. Da viele Arbeiten mittlerweile über Weboberflächen stattfinden, sei es sichtbar für den Benutzer oder unsichtbar hinter den Kulissen, wird die Webtechnologie der Fokus des Kurses sein. Dabei geht es nicht nur um die Kopfgeldjagd.

Der Workshop besteht nicht nur aus trockener Theorie. Dawid Czagan hat Fallbeispiele aus produktiven Umgebungen vorbereitet, um die verschiedenen Klassen von Fehler zu illustrieren. Der komplette Kurs ist eine Mischung aus kurzem Vortrag zur Erklärung gefolgt von praktischen Übungen, um das neu erworbene Wissen zu festigen. Die vermittelten Fähigkeiten sind eine wertvolle Ergänzung für jede Qualitätssicherung und eine gefragte Weiterbildung für Entwickler und Entwicklerinnen. Die Veranstaltung richtet sich gezielt an Sicherheitsforscher, Penetration Tester, Consultants, Projektleiter/Entwickler aus der Softwareentwicklung und IT-Architekten, die grundlegende Designs entwerfen, auf dem Anwendungen und Systeme aufbauen.

Die Angreifer haben diese Mittel schon. Es wird Zeit, dass Sie aufholen. Vernetzte Systeme schlafen nie.

Programm und Buchung

Die DeepSec-Konferenztage finden am 29. und 30. November, die Trainings an den zwei vorangehenden Tagen, dem 27. und 28. November, statt. Der Veranstaltungsort ist das Hotel „The Imperial Riding School Vienna – A Renaissance Hotel“ in der Ungargasse 60, 1030 Wien.

Interessierte finden das aktuelle Programm **hier**. Tickets für die Konferenz und die Trainings können unter **https://deepsec.net/register.html** bestellt werden.

Das Blog der Konferenz mit Informationen und Hintergründen zu den Vorträgen und dem Workshop gibt es unter **https://blog.deepsec.net.**

https://digitalguardian.com/blog/call-papers-inside-track

CALL FOR PAPERS: THE INSIDE TRACK

09.03.2018, Dr. Jessica Barker

Get advice from organisers and reviewers of cyber security conferences on how to write winning conference submissions.

I enjoy speaking at conferences, and my career has benefitted from it. I have gone from being a pretty nervous public speaker, to one who barely notices nerves in the lead up to a talk, even when stepping on stage to speak to thousands of people. I often have conversations with people who say they would love to do the same, but for one reason or another, haven't made the leap to giving their first talk. I have encouraged some of those people to make the jump and they have all gone on to get the 'speaking bug'.

So, I recently did a twitter poll, asking why people who want to speak at conferences, don't go on to do so. With over 6,000 votes, the poll had a much greater response than I expected, which indicates that there is a great desire among people to speak at conferences, but a variety of factors get in their way.

Now, I'm not saying that everyone should speak at conferences, but if you want to, then let's try to make it happen. There are so many events and conferences out there, from small local get-togethers to huge conferences that draw international audiences, so finding the right place for your first talk is the first step. Remember that lots of the established conferences, like besides, usually have rookie and lightening tracks that are a great first stepping-stone for new speakers.

Returning to the poll for a minute, the four options I gave as answers were based on the reasons most people have given me for not speaking at conferences. It's frustrating that you can only provide four poll answers on twitter, as I had to omit two other pretty likely reasons for not speaking at conferences: employers that don't allow it and your submission to the call for papers not being accepted. For people who are submitting to conferences and not having their submission accepted, or who don't know where to start with a cfp, I've asked organisers and reviewers of some fantastic cyber security conferences for their advice on writing a submission.

Advice From Conference Organisers:

Daniel Cuthbert
Blackhat Review Board

Biggest advice I can give anyone is to stop, read and think 'does this make sense? does it articulate what I'm trying to say?'

Too often I see submissions that have been submitted without being QA'd by a colleague/friend/loved one. If you look at any large conference, the number of submissions are often high, so you need your submission to be as clear as possible about what it is you are going to present, why this excites the hell out of you and why it should everyone else and also give a sense to the review board that you've taken effort in creating the submission.

Loved ones can be brutal, especially those not in this field. Ask them to read it and honestly reply back if they understood it. If they didn't, then you know you need to work on it. I'm more than happy to help anyone get their submission ready, you just need to ask.

Lance Spitzner
Director, SANS Security Awareness
SANS European Security Awareness Summit and US Security Awareness Summit

- Focus on the meat of your talk. Far too often submissions try to be fun / catchy with cool title and lots of fancy ‘cyber bingo’ words in the submission. Instead, focus on the value. What are people going to learn from your talk, what will they be able to do differently as a result, how will they be able to apply your lessons learned. The more value your talk provides, the more likely you will be accepted.

- People love real world stories, both success and failure. Academic theory is great, but the best talks have real world stories to back-up their lessons learned.

René Pfeiffer,

Managing Director, DeepSec GmbH

- Everything you submit must be ready for publication
- Make sure the title expresses what you want to say.
- Mark any content intended for organisers only appropriately
- Provide a small and larger abstract - text-only, no formatting
- Make sure a wide(r) audience can understand what the point of the presentation is
- It's not a film production. Don't add special effects and show. Facts and didactics plus some training on presentation will do nicely.

Check out more of René's advice here.

Per Thorshiem

Founder of Password Con and Password Consulting

Well, there's always the standard recommendations: describe the problem/challenge, your approach, your solution and alternatives that might exist. Key takeaways from your talk will be XYZ-something. Then there's the standard recommendation of presenting real-world scenarios, obviously something you've experienced yourself, instead of pure hypothetical work. Depending on the type of conference of course.

Previous talks/cons you've done, feedback received, links to online slides/recordings can be a plus, but don't overdo it. Then there's the fact most cons ask for original content. It's almost as if they want all 0-days in every single talk. Such talks may be cool & impressive, but if the problem described has already been fixed with a patch, it is nothing but a «LOOK AT ME I AM SO L33T!» talk, promoting your own value & services. So I am fond of talks that describes problems and challenges that looks at the root causes, and tries to do something about them, which is why I do PasswordsCon).

Adrian @Alien8

CEO Cortex Insight

Co-founder, co-organiser & Event Director of 44CON

Main thing I see when I review — the biggest sin is not explaining what the purpose of the talk is and what the take-aways are.

The reviewers won't necessarily read your talk (you might not have written it yet!) but they need to see that you understand this

Also submit early. That helps a lot :)

For more information on how to get a submission accepted at 44CON, there is a great blog post here.

Steve Quinn

Atlantic Security Conference Board Member

For me when looking at submissions I look for topics that I think would be relevant for our community. I always want to bring content that I feel our local community will find relevant and useful. My suggestion would be research and understand your target audience and try to present something they will want to spend time viewing.

Robin @DigiNinja

Co-founder of SteelCon

Submit something interesting regardless of the technical level. If I had the choice of fun to listen to or highly technical I'd go for the fun talk most of the time. People want to be entertained.

Think of the audience, if it is a general, all welcome conference, then a general talk that most people will want to watch will get more bums on seats than something very specialised which may show off a super cool technique but will leave most people stood around in the lobby waiting for the next talk.

Thank you to all of the organisers above, who have provided an insight into what they see, and what they're looking for. The three top tips, which I have pulled out from all of the comments above, are:

1. Put yourself in the audience's shoes: what fits this conference and what will people enjoy listening to? Try to appeal to a wide audience
2. Don't worry too much about being l33t, by no means do you need to be dropping 0 days to give a good talk
3. Spend time clearly articulating what your talk is about and, crucially, what the audience will take away from it; check with friends and family that what you have written makes sense

While I have pulled out these three general pointers, the various comments above show that individual conferences have different approaches and priorities. So, look at the conference you are interested in speaking at, and consider what you can offer that will be of particular interest to them. Check out their previous talks, read their website to see what they are looking for and even try reaching out to the organisers if you have specific questions or want some guidance.

A final piece of advice is to look to your local infosec meet-ups as a great place to give your first talk, or to test out a new talk and get some honest feedback. There are so many DC groups all over the world, and you will generally find a friendly and welcoming group of people who will be happy to listen to whatever you want to talk about and give you feedback.

CALL FOR PAPERS: THE INSIDE TRACK

Dr. Jessica Barker (https://digitalguardian.com/author/dr-jessica-barker)
Last Updated: Friday March 9, 2018

Get advice from organisers and reviewers of cyber security conferences on how to write winning conference submissions.

I enjoy speaking at conferences, and my career has benefitted from it. I have gone from being a pretty nervous public speaker, to one who barely notices nerves in the lead up to a talk, even when stepping

on stage to speak to thousands of people. I often have conversations with people who say they would love to do the same, but for one reason or another, haven't made the leap to giving their first talk. I have encouraged some of those people to make the jump and they have all gone on to get the 'speaking bug'.

So, I recently did a twitter poll, asking why people who want to speak at conferences, don't go on to do so. With over 6,000 votes, the poll had a much greater response than I expected, which indicates that there is a great desire among people to speak at conferences, but a variety of factors get in their way.

Now, I'm not saying that everyone **should** speak at conferences, but if you want to, then let's try to make it happen. There are so many events and conferences out there, from small local get-togethers to huge conferences that draw international audiences, so finding the right place for your first talk is the first step. Remember that lots of the established conferences, like besides, usually have rookie and lightening tracks that are a great first

stepping-stone for new speakers.

Returning to the poll for a minute, the four options I gave as answers were based on the reasons most people have given me for not speaking at conferences. It's frustrating that you can only provide four poll answers on twitter, as I had to omit two other pretty likely reasons for not speaking at conferences: employers that don't allow it and your submission to the call for papers not being accepted. For people who are submitting to conferences and not having their submission accepted, or who don't know where to start with a cfp, I've asked organisers and reviewers of some fantastic cyber security conferences for their advice on writing a submission.

Advice From Conference Organisers:

Daniel Cuthbert
Blackhat (http://www.blackhat.com) Review Board

> Biggest advice I can give anyone is to stop, read and think 'does this make sense? does it articulate what I'm trying to say?'
>
> Too often I see submissions that have been submitted without being QA'd by a colleague/friend/loved one. If you look at any large conference, the number of submissions are often high, so you need your submission to be as clear as possible about what it is you are going to present, why this excites the hell out of you and why it should everyone else and also give a sense to the review board that you've taken effort in creating the submission.
>
> Loved ones can be brutal, especially those not in this field. Ask them to read it and honestly

reply back if they understood it. If they didn't, then you know you need to work on it. I'm more than happy to help anyone get their submission ready, you just need to ask.

Lance Spitzner
Director, SANS Security Awareness (https://securingthehuman.sans.org)
SANS European Security Awareness Summit (https://www.sans.org/event/european-security-awareness-summit-2017) and US Security Awareness Summit (https://www.sans.org/event/security-awareness-summit-2017)

- Focus on the meat of your talk. Far too often submissions try to be fun / catchy with cool title and lots of fancy 'cyber bingo' words in the submission. Instead, focus on the value. What are people going to learn from your talk, what will they be able to do differently as a result, how will they be able to apply your lessons learned. The more value your talk provides, the more likely you will be accepted.

- People love real world stories, both success and failure. Academic theory is great, but the best talks have real world stories to back-up their lessons learned.

René Pfeiffer,
Managing Director, DeepSec GmbH (https://deepsec.net)

- Everything you submit must be ready for publication

- Make sure the title expresses what you want

to say.

- Mark any content intended for organisers only appropriately

- Provide a small and larger abstract - text-only, no formatting

- Make sure a wide(r) audience can understand what the point of the presentation is

- It's not a film production. Don't add special effects and show. Facts and didactics plus some training on presentation will do nicely.

Check out more of René's advice here (http://blog.deepsec.net/tips-for-conference-speakers/).

Per Thorshiem
Founder of Password Con (https://passwordscon.org) and Password Consulting (https://password.consulting)

Well, there's always the standard recommendations: describe the problem/challenge, your approach, your solution and alternatives that might exist. Key takeaways from your talk will be XYZ-something. Then there's the standard recommendation of presenting real-world scenarios, obviously something you've experienced yourself, instead of pure hypothetical work. Depending on the type of conference of course.

Previous talks/cons you've done, feedback received, links to online slides/recordings can be a plus, but don't overdo it. Then there's the

> fact most cons ask for original content. It's almost as if they want all 0-days in every single talk. Such talks may be cool & impressive, but if the problem described has already been fixed with a patch, it is nothing but a «LOOK AT ME I AM SO L33T!» talk, promoting your own value & services. So I am fond of talks that describes problems and challenges that looks at the root causes, and tries to do something about them, which is why I do PasswordsCon).

Adrian @Alien8
CEO Cortex Insight (https://cortexinsight.com)
Co-founder, co-organiser & Event Director of 44CON (https://44con.com)

> Main thing I see when I review — the biggest sin is not explaining what the purpose of the talk is and what the takeaways are.
>
> The reviewers won't necessarily read your talk (you might not have written it yet!) but they need to see that you understand this
> Also submit early. That helps a lot :)

For more information on how to get a submission accepted at 44CON, there is a great blog post here (https://44con.com/2017/02/07/how-to-game-the-44con-cfp/).

Steve Quinn
Atlantic Security Conference (https://atlseccon.com)
Board Member

> For me when looking at submissions I look for topics that I think would be relevant for our community. I always want to bring content that

> I feel our local community will find relevant and useful. My suggestion would be research and understand your target audience and try to present something they will want to spend time viewing.

Robin @DigiNinja
Co-founder of SteelCon (https://www.steelcon.info)

> Submit something interesting regardless of the technical level. If I had the choice of fun to listen to or highly technical I'd go for the fun talk most of the time. People want to be entertained. Think of the audience, if it is a general, all welcome conference, then a general talk that most people will want to watch will get more bums on seats than something very specialised which may show off a super cool technique but will leave most people stood around in the lobby waiting for the next talk.

Thank you to all of the organisers above, who have provided an insight into what they see, and what they're looking for. The three top tips, which I have pulled out from all of the comments above, are:

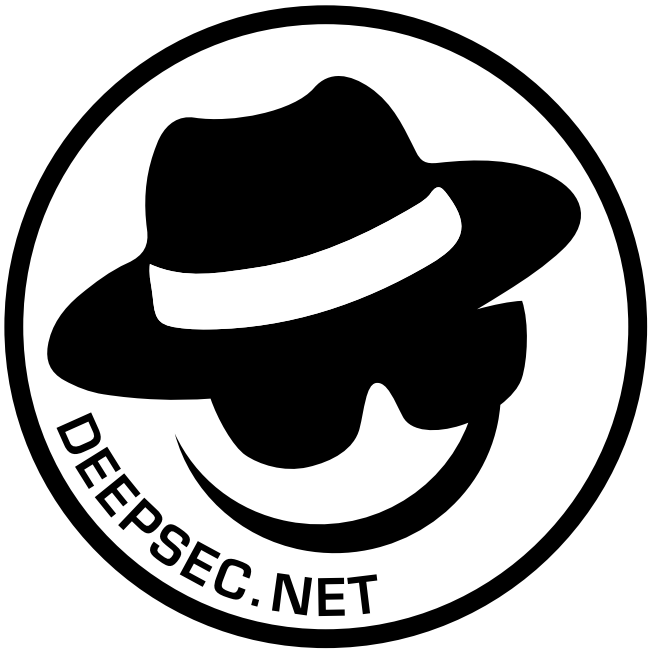
> 1. Put yourself in the audience's shoes: what fits this conference and what will people enjoy listening to? Try to appeal to a wide audience
> 2. Don't worry too much about being l33t, by no means do you need to be dropping 0 days to give a good talk
> 3. Spend time clearly articulating what your talk is about and, crucially, what the audience will take away from it; check with friends and family

that what you have written makes sense

While I have pulled out these three general pointers, the various comments above show that individual conferences have different approaches and priorities. So, look at the conference you are interested in speaking at, and consider what you can offer that will be of particular interest to them. Check out their previous talks, read their website to see what they are looking for and even try reaching out to the organisers if you have specific questions or want some guidance.

A final piece of advice is to look to your local infosec meet-ups as a great place to give your first talk, or to test out a new talk and get some honest feedback. There are so many DC groups (https://defcongroups.org/dcpages.html) all over the world, and you will generally find a friendly and welcoming group of people who will be happy to listen to whatever you want to talk about and give you feedback.

press releases 2018



https://www.pressetext.com/news/20181112011

IT-Sicherheitsindustrie stellt sich Herausforderungen der digitalen Endzeitstimmung

DeepSec- und DeepINTEL-Konferenz bieten über 50 Vorträge und Trainings im November an

Wien (pts011/12.11.2018/09:15) - Die zunehmende Verbreitung der Vernetzung, das Wachstum des Internets und die zunehmende Anzahl von miniaturisierten Computern im Alltag haben nicht nur den Komfort sondern auch die Gefahren erhöht. Neben dem Internet der Dinge (Internet of Things) haben auch Virtualisierungstechnologien die Anzahl der Computer nicht verringert, sondern massiv gesteigert. Konsolidierung ist veraltet. Eine natürliche Konsequenz der Datenexplosion sind Sicherheitslücken, die alleine aufgrund der numerischen Masse von Netzknoten, Rechnern und Speicher vermehrt auftreten. Regulationen alleine werden dieses Problem nicht in den Griff bekommen. Die DeepSec Konferenz setzt in diesem Jahr daher auf fachliche Kompetenz statt auf leere Gebote.

Eröffnung der Endzeit

Der unabhängige IT-Spezialist Peter Zinn wird mit seinem Vortrag "We're all gonna die" die DeepSec Konferenz eröffnen. Er wird in seiner Präsentation die Utopien thematisieren, die die digitale Informationsverarbeitung und das Internet in ihren jungen Jahren versprochen haben. Schon in der Science-Fiction-Literatur kamen Szenarien vor, die uns allen das Leben erleichtern und viel Arbeit abnehmen sollten, um sich dadurch auf andere Tätigkeiten konzentrieren zu können. Beim heutigen Studium der Nachrichten kann man allerdings sehr viel über die dunklen Seiten der Technologien lesen. Datenlecks, Manipulation von Information, Verzicht auf Fakten, Gedankenströmungen statt einem Strom von Gedanken und unüberlegte Reflexreaktionen bestimmen die digitale Welt. Peter Zinn wird Utopie mit Dystopie vergleichen und Schlussfolgerungen für unsere Zukunft ziehen.

Man darf dabei nicht vergessen, dass die Sicherheitsforschung eigentlich sehr große Sprünge gemacht und den Stand der Technik stark verbessert hat. Verschlüsselte Kommunikation ist mittlerweile wesentlich verbreiteter als noch vor 10 oder 20 Jahren, auch aufgrund der Sensibilisierung vor der zunehmenden Überwachung und deren Missbrauch. Softwareentwicklerinnen haben aktuell mehr Wissen um sicher Programmieren zu können. Das Testen von IT-Systemen auf Sicherheitsschwachstellen ist zur Standardprozedur geworden. All diese Errungenschaften werden gerne im Anblick der Datenlecks und Datenpannen in den Schlagzeilen vergessen.

Kombination mit ROOTS 2018 und DeepINTEL

Auch in diesem Jahr ist die Kombination der DeepSec Konferenz mit wissenschaftlicher Forschung und strategischer Überlegung zu Informationssicherheit Teil des Programms. Das Reversing and Offensive-Oriented Trends

Symposium 2018 (ROOTS) findet nun zum zweiten Mal parallel zur DeepSec am selben Veranstaltungsort statt. Es werden wissenschaftliche Publikationen zum Thema offensiver Sicherheit in Vorträgen vorgestellt. Die dazugehörigen Forschungsartikel werden im Rahmen eines Bandes über die Organisation Association for Computing Machinery (ACM) publiziert. Im ROOTS-Programm enthalten sind eine Analyse der Swift Programmiersprache, der Einfluss von Benutzeroberflächen auf die Sicherheit, Werkzeuge zur Identifikation von ausführbarem Code und Hilfsmittel zur Analyse von Applikationen auf der GNU/Linux Plattform.

Ohne Strategie stolpert man blind in die Zukunft. Aus diesem Grunde findet erstmals einen Tag vor der DeepSec die DeepINTEL Security Intelligence Konferenz statt. Sie beschäftigt sich mit strategischen Fragen im Umgang mit Bedrohungen, Schutz von kritischer Infrastruktur, Aufklärung der gegnerischen Fähigkeiten und Methoden zur Ausrichtung einer modernen Verteidigung. Im Fokus stehen aktuell Human Intelligence (HUMINT), Drohnenabwehr, strategisches Risikomanagement, Einblicke in Dark Markets und strategische Aufklärung von Bedrohungen. Weiterhin werden Auswirkungen von Angriffen auf Kommunikation am Beispiel staatlicher Verfolgung von Journalisten in bestimmten Ländern besprochen. Die DeepINTEL ist eine nichtöffentliche Konferenz. Alle Inhalte werden nur den Anwesenden zur Verfügung gestellt und nicht publiziert. Das Programm ist auf Anfrage (per E-Mail oder Anruf) verfügbar.

Sicherheit durch ständiges Training

Der praktische Teil darf natürlich nicht fehlen. Wie jedes Jahr finden in den zwei Tagen vor der DeepSec Konferenz hochqualitative Trainings von Experten statt. Christian Wojnar bietet Expertise bei der Analyse von Schadsoftware im Workshop "Malware Analysis Intro" an. Das ist nicht nur für Entwickler von Antivirussoftware interessant. Schadsoftware spielt bei allen Sicherheitsvorfällen eine Rolle. Das Wissen um deren Eigenschaften ist daher Grundkompetenz für Systemadministration und Softwareentwicklung.

Dawid Czagan, einer der Top 10-Bug Hunter weltweit, lehrt wie man Fehler in modernen Applikationen findet. Ein seinem Training geht es um die vielen Schichten heutiger Web-Applikationen angefangen vom Web Browser, über die Applikation auf dem Server selbst, bis hin zu den Datenbanksystemen im Hintergrund. Aufgrund der Verbreitung von Webtechnologie in allen Bereichen gilt auch dieses Wissen mittlerweile zur Basisausbildung aller Entwicklerinnen und IT Mitarbeitern. Dawids Training trägt den Titel "Mastering Web Attacks with Full-Stack Exploitation" und hat noch freie Plätze.

Enterprise-Resource-Planning (ERP) Systeme sind in allen Unternehmen vertreten. Oft befinden sie sich im internen Netzwerk und stellen das Herz jeder Unternehmung dar. Die SAP-Plattform ist der prominenteste Vertreter von

EPR-Systemen. Pablo Artuso führt in seinem Workshop vor wie man die Sicherheit von SAP-Systemen evaluiert, wie man sie angreift und wie man sie verteidigen kann. Die Teilnehmer werden direkt an SAP-Installationen Übungen durchführen, also komplett mit praktischen Beispielen an echten Systemen lernen. Die Wichtigkeit der in diesem Training vermittelten Inhalte lassen sich kaum stärker betonen. Wenn Eindringlinge an ERP-Systeme kommen, dann geht es um sehr viel, unter Umständen die Existenz des Unternehmens. Die Schulung ist eine gute Methode Schaden zu verhindern oder zumindest zu verringern, der sich nicht mehr beheben lässt.

Mit Faktencheck in die Zukunft

Alle, die mit Digitalisierung eine Zukunft ohne Existenzbedrohung erreichen möchten, werden sich mit dem Themenkomplex Informationssicherheit auseinandersetzen müssen. Es gibt keine Abkürzungen. Hektisches Auslagern von Daten und Diensten ist letztlich nur ein anderes Wort für Kompetenzkonkurs. Das kann sich niemand mehr leisten. Moderne IT-Infrastruktur und eigene Applikationen können sehr wohl auf neuen Technologien aufbauen. Es muss nur sichergestellt sein, dass die strategische und taktische IT-Security Bestandteil aller Überlegungen ist. Für diese Entscheidungsprozesse müssen die eigenen Abläufe, die eingesetzten Applikationen, alle Aspekte der Datenhaltung und Sicherheitsprüfungen bekannt und geplant sein. Wer da den Anschluss verliert, wird früher oder später ein Sicherheitsproblem haben.

Der Austausch mit Expertinnen und Sicherheitsforschern ist der erste Schritt. Wir laden Sie daher herzlich ein unsere Veranstaltungen zu besuchen und sich für die Zukunft zu rüsten, die bereits morgen beginnt.

Programme und Buchung

Die DeepSec-Konferenztage sind am 29. und 30. November. Parallel finden die ROOTS 2018-Vorträge in einem separaten Saal ebenso am 29. und 30. November statt. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 27. und 28. November statt.

Die DeepINTEL Konferenz findet am 28. November statt. Das Programm senden wir auf Anfragen an deepsec@deepsec.net gerne zu. Tickets sind auf der Webseite https://deepintel.net erhältlich.

Der Veranstaltungsort für DeepSec, DeepINTEL und ROOTS 2018 ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Sie finden das aktuelle Programm unter dem Link: https://deepsec.net/schedule.html

DeepSec 2018/09

Tickets für die DeepSec Konferenz sowie ROOTS 2018 und die DeepSec-Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html bestellen.

Aussender: DeepSec GmbH

Ansprechpartner: René Pfeiffer

Tel.: +43 676 5626390

E-Mail: deepsec@deepsec.net

Website: deepsec.net

pts20181112011 Computer/Telekommunikation, Unternehmen/Finanzen

IT-Sicherheitsindustrie stellt sich Herausforderungen der digitalen Endzeitstimmung

DeepSec- und DeepINTEL-Konferenz bieten über 50 Vorträge und Trainings im November an

DeepSec, Logo (Copyright: Florian Stocker, 2016)

Wien (pts011/12.11.2018/09:15) - **Die zunehmende Verbreitung der Vernetzung, das Wachstum des Internets und die zunehmende Anzahl von miniaturisierten Computern im Alltag haben nicht nur den Komfort sondern auch die Gefahren erhöht. Neben dem Internet der Dinge (Internet of Things) haben auch Virtualisierungstechnologien die Anzahl der Computer nicht verringert, sondern massiv gesteigert. Konsolidierung ist veraltet. Eine natürliche Konsequenz der Datenexplosion sind Sicherheitslücken, die alleine aufgrund der numerischen Masse von Netzknoten, Rechnern und Speicher vermehrt auftreten. Regulationen alleine werden dieses Problem nicht in den Griff bekommen. Die DeepSec Konferenz setzt in diesem Jahr daher auf fachliche Kompetenz statt auf leere Gebote.**

Eröffnung der Endzeit

Der unabhängige IT-Spezialist Peter Zinn wird mit seinem Vortrag "We're all gonna die" die DeepSec Konferenz eröffnen. Er wird in seiner Präsentation die Utopien thematisieren, die die digitale Informationsverarbeitung und das Internet in ihren jungen Jahren versprochen haben. Schon in der Science-Fiction-Literatur kamen Szenarien vor, die uns allen das Leben erleichtern und viel Arbeit abnehmen sollten, um sich dadurch auf andere Tätigkeiten konzentrieren zu können. Beim heutigen Studium der Nachrichten kann man allerdings sehr viel über die dunklen Seiten der Technologien lesen. Datenlecks, Manipulation von Information, Verzicht auf Fakten, Gedankenströmungen statt einem Strom von Gedanken und unüberlegte Reflexreaktionen bestimmen die digitale Welt. Peter Zinn wird Utopie mit Dystopie vergleichen und Schlussfolgerungen für unsere Zukunft ziehen.

Man darf dabei nicht vergessen, dass die Sicherheitsforschung eigentlich sehr große Sprünge gemacht und den Stand der Technik stark verbessert hat. Verschlüsselte Kommunikation ist mittlerweile wesentlich verbreiteter als noch vor 10 oder 20 Jahren, auch aufgrund der Sensibilisierung vor der zunehmenden Überwachung und deren Missbrauch. Softwareentwicklerinnen haben aktuell mehr Wissen um sicher Programmieren zu können. Das Testen von IT-Systemen auf Sicherheitsschwachstellen ist zur Standardprozedur geworden. All diese Errungenschaften werden gerne im Anblick der Datenlecks und Datenpannen in den Schlagzeilen vergessen.

Kombination mit ROOTS 2018 und DeepINTEL

Auch in diesem Jahr ist die Kombination der DeepSec Konferenz mit wissenschaftlicher Forschung und strategischer Überlegung zu Informationssicherheit Teil des Programms. Das Reversing and Offensive-Oriented Trends Symposium 2018 (ROOTS) findet nun zum zweiten Mal parallel zur DeepSec am selben Veranstaltungsort statt. Es werden wissenschaftliche Publikationen zum Thema offensiver Sicherheit in Vorträgen vorgestellt. Die dazugehörigen Forschungsartikel werden im Rahmen eines Bandes über die Organisation Association for Computing Machinery (ACM) publiziert. Im ROOTS-Programm enthalten sind eine Analyse der Swift Programmiersprache, der Einfluss von Benutzeroberflächen auf die Sicherheit, Werkzeuge zur Identifikation von ausführbarem Code und Hilfsmittel zur Analyse von Applikationen auf der GNU/Linux Plattform.

Ohne Strategie stolpert man blind in die Zukunft. Aus diesem Grunde findet erstmals einen Tag vor der DeepSec die DeepINTEL Security Intelligence Konferenz statt. Sie beschäftigt sich mit strategischen Fragen im Umgang mit Bedrohungen, Schutz von kritischer Infrastruktur, Aufklärung der gegnerischen Fähigkeiten und Methoden zur Ausrichtung einer modernen Verteidigung. Im Fokus stehen aktuell Human Intelligence (HUMINT), Drohnenabwehr, strategisches Risikomanagement, Einblicke in Dark Markets und strategische Aufklärung von Bedrohungen. Weiterhin werden Auswirkungen von Angriffen auf Kommunikation am Beispiel staatlicher Verfolgung von Journalisten in bestimmten Ländern besprochen. Die DeepINTEL ist eine nichtöffentliche Konferenz. Alle Inhalte werden nur den Anwesenden zur Verfügung gestellt und nicht publiziert. Das Programm ist auf Anfrage (per E-Mail oder Anruf) verfügbar.

Sicherheit durch ständiges Training

Der praktische Teil darf natürlich nicht fehlen. Wie jedes Jahr finden in den zwei Tagen vor der DeepSec Konferenz hochqualitative Trainings von Experten statt. Christian Wojnar bietet Expertise bei der Analyse von Schadsoftware im Workshop "Malware Analysis Intro" an. Das ist nicht nur für Entwickler von Antivirussoftware interessant. Schadsoftware spielt bei allen Sicherheitsvorfällen eine Rolle. Das Wissen um deren Eigenschaften ist daher Grundkompetenz für Systemadministration und Softwareentwicklung.

Dawid Czagan, einer der Top 10-Bug Hunter weltweit, lehrt wie man Fehler in modernen Applikationen findet. Ein seinem Training geht es um die vielen Schichten heutiger Web-Applikationen angefangen vom Web Browser, über die Applikation auf dem Server selbst, bis hin zu den Datenbanksystemen im Hintergrund. Aufgrund der Verbreitung von Webtechnologie in allen Bereichen gilt auch dieses Wissen mittlerweile zur Basisausbildung aller Entwicklerinnen und IT Mitarbeitern. Dawids Training trägt den Titel "Mastering Web Attacks with Full-Stack Exploitation" und hat noch freie Plätze.

Enterprise-Resource-Planning (ERP) Systeme sind in allen Unternehmen vertreten. Oft befinden sie sich im internen Netzwerk und stellen das Herz jeder Unternehmung dar. Die SAP-Plattform ist der prominenteste Vertreter von EPR-Systemen. Pablo Artuso führt in seinem Workshop vor wie man die Sicherheit von SAP-Systemen evaluiert, wie man sie angreift und wie man sie verteidigen kann. Die Teilnehmer werden direkt an SAP-Installationen Übungen durchführen, also komplett mit praktischen Beispielen an echten Systemen lernen. Die Wichtigkeit der in diesem Training vermittelten Inhalte lassen sich kaum stärker betonen. Wenn Eindringlinge an ERP-Systeme kommen, dann geht es um sehr viel, unter Umständen die Existenz des Unternehmens. Die Schulung ist eine gute Methode Schaden zu verhindern oder zumindest zu verringern, der sich nicht mehr beheben lässt.

Mit Faktencheck in die Zukunft

Alle, die mit Digitalisierung eine Zukunft ohne Existenzbedrohung erreichen möchten, werden sich mit dem Themenkomplex Informationssicherheit auseinandersetzen müssen. Es gibt keine Abkürzungen. Hektisches Auslagern von Daten und Diensten ist letztlich nur ein anderes Wort für Kompetenzkonkurs. Das kann sich niemand mehr leisten. Moderne IT-Infrastruktur und eigene Applikationen können sehr wohl auf neuen Technologien aufbauen. Es muss nur sichergestellt sein, dass die strategische und taktische IT-Security Bestandteil aller Überlegungen ist. Für diese Entscheidungsprozesse müssen die eigenen Abläufe, die eingesetzten Applikationen, alle Aspekte der Datenhaltung und Sicherheitsprüfungen bekannt und geplant sein. Wer da den Anschluss verliert, wird früher oder später ein Sicherheitsproblem haben.

Der Austausch mit Expertinnen und Sicherheitsforschern ist der erste Schritt. Wir laden Sie daher herzlich ein unsere Veranstaltungen zu besuchen und sich für die Zukunft zu rüsten, die bereits morgen beginnt.

Programme und Buchung

Die DeepSec-Konferenztage sind am 29. und 30. November. Parallel finden die ROOTS 2018-Vorträge in einem separaten Saal ebenso am 29. und 30. November statt. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 27. und 28. November statt.

Die DeepINTEL Konferenz findet am 28. November statt. Das Programm senden wir auf Anfragen an deepsec@deepsec.net gerne zu. Tickets sind auf der Webseite https://deepintel.net erhältlich.

Der Veranstaltungsort für DeepSec, DeepINTEL und ROOTS 2018 ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Sie finden das aktuelle Programm unter dem Link: https://deepsec.net/schedule.html

Tickets für die DeepSec Konferenz sowie ROOTS 2018 und die DeepSec-Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html bestellen.

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

https://www.pressetext.com/news/20181017010

Moderne IT benötigt kurze Wege zur Kompetenz

DeepSec Konferenz und Fachgruppe UBIT verbinden Informationssicherheit mit Wirtschaft

Wien (pts010/17.10.2018/09:15) - Kein Unternehmen kommt ohne moderne Datenhaltung und Kommunikation aus. Damit sind diese aber nicht nur mit dem Internet, sondern auch mit Bedrohungen für digitale Infrastruktur verbunden. Es gibt viele Wege, sich zu schützen. Die DeepSec IT Sicherheitskonferenz und die Wiener Fachgruppe für Unternehmensberatung, Buchhaltung und IT (UBIT) bieten den besten Weg, um Bedrohungen zu minimieren - lokale Kompetenz, erstklassige Expertise und aktuelles Wissen. Es ist dabei nebensächlich, ob es um Webapplikationen, Telefonie, Datenhaltung, Anschaffung von Geräten oder die Inbetriebnahme von Software geht. Der gemeinsame Nenner ist der richtige Umgang mit und die richtige Kombination von Technologien. Darüber hinaus gilt es, rechtliche Vorgaben einzuhalten. Es war nie egal, wo Firmendaten verarbeitet werden. Durch die steigende Vernetzung ist es jetzt die zentrale Frage, die über das Geschäft entscheidet. Die DeepSec Konferenz bietet dazu dieses Jahr wieder zweitägige Trainings an. Die UBIT unterstützt mit erstklassigen Expertinnen und Experten, die mit dem neuesten Stand der Technik vertraut sind.

Digitale Kompetenz als Schlüsselfaktor für Unternehmen

Aufgrund der immer weiter voranschreitenden Digitalisierung, darunter auch Entwicklungen wie das Internet of Things oder Industrie 4.0, nimmt die Informationstechnologie einen immer wichtigeren Stellenwert ein. Kaum ein Unternehmen kommt mehr ohne irgendeine Art von IT aus, für immer mehr wird sie sogar zur kritischen Infrastruktur. Das bedeutet auch, dass die digitale Infrastruktur und deren Sicherheit bzw. Stabilität auf der Agenda eines jeden Unternehmens ganz oben stehen muss. "Die richtige IT bietet enorme unternehmerische Vorteile. Komplexere IT-Systeme, zunehmender Einsatz von mobilen Geräten, dezentrale Speicherungen via Cloud-Dienste, eine immer dichtere Vernetzung mit anderen Geräten - all das erfordert jedoch eine professionelle Pflege der Systeme", so Martin Puaschitz, Obmann der Wiener Fachgruppe für Unternehmensberatung, Buchhaltung und IT (UBIT).

Zum Einen geht es dabei um die richtige Verwendung der Technologien, stellt doch vor allem der Faktor Mensch das größte Risiko dar. Eine Umfrage der Fachgruppe UBIT Wien zeigt, dass menschliches Fehlverhalten und mangelndes Verständnis im Umgang mit IT-Systemen zu den Hauptgründen für IT-Probleme in Unternehmen zählen. Erst danach folgen Viren und Schadsoftware als Fehlerursache, wobei sich auch dieses Problem oftmals auf den falschen Umgang der NutzerInnen zurückführen lässt. Die häufigsten Folgen solcher Probleme stellen mit Umsatzverlusten, entgangenen Gewinnen durch Hinderung an der unternehmerischen Tätigkeit und anfallenden

Kosten für die Anschaffung neuer Hard- und Software unmittelbare finanzielle Schäden dar.

Zum Anderen geht es um die Verwendung der richtigen Technologien bzw. darum, das Verständnis dafür zu schärfen. Viele Unternehmen setzen beispielsweise auf Cloud-Anbieter und wissen dabei gar nicht, wo anschließend die Unternehmensdaten gespeichert werden. Je nach Lage und der dort herrschenden Rechtslage, kann das im Ernstfall gravierende Auswirkungen haben, zudem kann das auch den Vorgaben der neuen EU-Datenschutz-Grundverordnung widersprechen. Um hier das Bewusstsein zu schärfen und den Cloud-Usern eine Orientierung zu geben, wurde von der Wirtschaftskammer Wien die Austrian Cloud-Initiativen ins Leben gerufen. Mit dieser Initiative können sich Cloud-Dienstleister, die ihre Server in Österreich haben, entsprechend zertifizieren lassen. Der Nutzer bekommt dadurch eine Garantie, dass seine Daten im Land gespeichert und verarbeitet werden. Das digitale Know-how über die richtigen Technologien sowie die korrekte Anwendung sind somit von wesentlicher Bedeutung.

Digitales Know-how als kritischer Faktor für Wirtschaftsstandort

Das Problem dabei ist, dass dieses digitale Know-how, vor allem fachliche Expertise, zunehmend zur Mangelware wird. Keine Neuigkeit, jedoch nimmt dieser Mangel nun bedrohliche Ausmaße an. Allen voran für ein Land wie Österreich, welches bis dato vor allem durch sein Know-how bekannt und geschätzt wurde. Das könnte sich bald rasch ändern. Die verstärkte Digitalisierung erfordert auch entsprechende Arbeitskräfte, in qualitativer wie auch quantitativer Hinsicht. "Die Folge: Aktuell fehlen österreichweit mindestens 10.000 IT-Kräfte, Tendenz stark steigend. Laut der EU-Kommission wird es bis 2020 europaweit sogar eine Lücke von rund einer Million Arbeitskräfte in der IT-Branche geben", weiß Puaschitz. Fehlende Arbeitskräfte mit entsprechendem Know-how führen unweigerlich zu einem höheren Sicherheitsrisiko, welches wiederum durch den Anstieg von Cybercrime-Attacken weiter multipliziert wird. Zudem bedroht diese Entwicklung auch den Wirtschaftsstandort generell.

Aktuell erwirtschaftet die Branche der Informations- und Kommunikationstechnologie (IKT) rund 8,6 Prozent der österreichischen Wertschöpfung, indirekte Effekte nicht miteingerechnet. "Die Branche ist somit eine wichtige Säule für den österreichischen Wirtschaftsstandort. Die Sicherstellung von ausreichend qualifizierten Arbeitskräften muss ganz oben auf der politischen und wirtschaftlichen Agenda stehen, sonst droht uns ein nachhaltiger Rückstand", findet Puaschitz klare Worte.

Ausbildung als Sicherheitsmaßnahme

"Moderne Wohnzimmer haben mehr Webserver als Firmen vor 15 Jahren", merkt René Pfeiffer, Geschäftführer der DeepSec Konferenz an. Alles möchte heutzutage smart sein. Das bedeutet starke Vernetzung auch in kleinen

Bereichen. Sicherheitstechnisch ist man gut beraten, Fehler zu finden, bevor es die Angreiferinnen tun. Der zweitägige Workshop "Mastering Web Attacks with Full-Stack Exploitation" bietet einen sehr guten Einstieg. Webtechnologie ist allgegenwärtig. Wer sich mit Schwachstellen darin beschäftigt, hat die Chance, Fehler zu finden, bevor sie ausgenutzt werden. Der Trainer Dawid Czagan gehört zu den weltweit Top 10 Bug Huntern, die Schwachstellen finden und Betroffenen melden.

Netzwerke ziehen sich durch Alltag und Arbeitswelt wie viele rote Fäden. Vernetzung ist eine Kerntechnologie, ohne die Angreifer nicht operieren können. Paul Coggins bietet zwei Tage lang Expertise für Verteidigerinnen und Sicherheitstester an. Sein Workshop "Fundamentals of Routing and Switching for Blue and Red Team" ist nicht nur für Netzwerkdienstleister wie Internetanbieter oder Mobilfunkfirmen interessant. Netzwerke sind überall. Jedes Unternehmen hat viele davon. Das Training kann daher den Blick auf die eigenen Infrastruktur schärfen, denn diese ist alles andere als statisch - und Verbesserungen in puncto Informationssicherheit haben noch nie geschadet.

Programme und Buchung

Die DeepSec-Konferenztage sind am 29. und 30. November. Die Trainings finden an den zwei vorangehenden Tagen, dem 27. und 28. November, statt. Vertreter der Wiener Fachgruppe für Unternehmensberatung, Buchhaltung und IT (UBIT) werden vor Ort anwesend sein. Der Veranstaltungsort ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Sie finden das aktuelle Programm unter dem Link: https://deepsec.net/schedule.html

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

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

pts20181017010 Computer/Telekommunikation, Unternehmen/Finanzen

Moderne IT benötigt kurze Wege zur Kompetenz

DeepSec Konferenz und Fachgruppe UBIT verbinden Informationssicherheit mit Wirtschaft

Wien (pts010/17.10.2018/09:15) - **Kein Unternehmen kommt ohne moderne Datenhaltung und Kommunikation aus. Damit sind diese aber nicht nur mit dem Internet, sondern auch mit Bedrohungen für digitale Infrastruktur verbunden. Es gibt viele Wege, sich zu schützen. Die DeepSec IT Sicherheitskonferenz und die Wiener Fachgruppe für Unternehmensberatung, Buchhaltung und IT (UBIT) bieten den besten Weg, um Bedrohungen zu minimieren - lokale Kompetenz, erstklassige Expertise und aktuelles Wissen. Es ist dabei nebensächlich, ob es um Webapplikationen, Telefonie, Datenhaltung, Anschaffung von Geräten oder die Inbetriebnahme von Software geht. Der gemeinsame Nenner ist der richtige Umgang mit und die richtige Kombination von Technologien. Darüber hinaus gilt es, rechtliche Vorgaben einzuhalten. Es war nie egal, wo Firmendaten verarbeitet werden. Durch die steigende Vernetzung ist es jetzt die zentrale Frage, die über das Geschäft entscheidet. Die DeepSec Konferenz bietet dazu dieses Jahr wieder zweitägige Trainings an. Die UBIT unterstützt mit erstklassigen Expertinnen und Experten, die mit dem neuesten Stand der Technik vertraut sind.**

Digitale Kompetenz als Schlüsselfaktor für Unternehmen

Aufgrund der immer weiter voranschreitenden Digitalisierung, darunter auch Entwicklungen wie das Internet of Things oder Industrie 4.0, nimmt die Informationstechnologie einen immer wichtigeren Stellenwert ein. Kaum ein Unternehmen kommt mehr ohne irgendeine Art von IT aus, für immer mehr wird sie sogar zur kritischen Infrastruktur. Das bedeutet auch, dass die digitale Infrastruktur und deren Sicherheit bzw. Stabilität auf der Agenda eines jeden Unternehmens ganz oben stehen muss. "Die richtige IT bietet enorme unternehmerische Vorteile. Komplexere IT-Systeme, zunehmender Einsatz von mobilen Geräten, dezentrale Speicherungen via Cloud-Dienste, eine immer dichtere Vernetzung mit anderen Geräten - all das erfordert jedoch eine professionelle Pflege der Systeme", so Martin Puaschitz, Obmann der Wiener Fachgruppe für Unternehmensberatung, Buchhaltung und IT (UBIT).

Zum einen geht es dabei um die richtige Verwendung der Technologien, stellt doch vor allem der Faktor Mensch das größte Risiko dar. Eine Umfrage der Fachgruppe UBIT Wien zeigt, dass menschliches Fehlverhalten und mangelndes Verständnis im Umgang mit IT-Systemen zu den Hauptgründen für IT-Probleme in Unternehmen zählen. Erst danach folgen Viren und Schadsoftware als Fehlerursache, wobei sich auch dieses Problem oftmals auf den falschen Umgang der NutzerInnen zurückführen lässt. Die häufigsten Folgen solcher Probleme stellen mit Umsatzverlusten, entgangenen Gewinnen durch Hinderung an der unternehmerischen Tätigkeit und anfallenden Kosten für die Anschaffung neuer Hard- und Software unmittelbare finanzielle Schäden dar.

Zum anderen geht es um die Verwendung der richtigen Technologien bzw. darum, das Verständnis dafür zu schärfen. Viele Unternehmen setzen beispielsweise auf Cloud-Anbieter und wissen dabei gar nicht, wo anschließend die Unternehmensdaten gespeichert werden. Je nach Lage und der dort herrschenden Rechtslage, kann das im Ernstfall gravierende Auswirkungen haben, zudem kann das auch den Vorgaben der neuen EU-Datenschutz-Grundverordnung widersprechen. Um hier das Bewusstsein zu schärfen und den Cloud-Usern eine Orientierung zu geben, wurde von der Wirtschaftskammer Wien die Austrian Cloud-

Initiativen ins Leben gerufen. Mit dieser Initiative können sich Cloud-Dienstleister, die ihre Server in Österreich haben, entsprechend zertifizieren lassen. Der Nutzer bekommt dadurch eine Garantie, dass seine Daten im Land gespeichert und verarbeitet werden. Das digitale Know-how über die richtigen Technologien sowie die korrekte Anwendung sind somit von wesentlicher Bedeutung.

Digitales Know-how als kritische Faktoren für Wirtschaftsstandort

Das Problem dabei ist, dass dieses digitale Know-how, vor allem fachliche Expertise, zunehmend zur Mangelware wird. Keine Neuigkeit, jedoch nimmt dieser Mangel nun bedrohliche Ausmaße an. Allen voran für ein Land wie Österreich, welches bis dato vor allem durch sein Know-how bekannt und geschätzt wurde. Das könnte sich bald rasch ändern. Die verstärkte Digitalisierung erfordert auch entsprechende Arbeitskräfte, in qualitativer wie auch quantitativer Hinsicht. "Die Folge: Aktuell fehlen österreichweit mindestens 10.000 IT-Kräfte, Tendenz stark steigend. Laut der EU-Kommission wird es bis 2020 europaweit sogar eine Lücke von rund einer Million Arbeitskräfte in der IT-Branche geben", weiß Puaschitz. Fehlende Arbeitskräfte mit entsprechendem Know-how führen unweigerlich zu einem höheren Sicherheitsrisiko, welches wiederum durch den Anstieg von Cybercrime-Attacken weiter multipliziert wird. Zudem bedroht diese Entwicklung auch den Wirtschaftsstandort generell.

Aktuell erwirtschaftet die Branche der Informations- und Kommunikationstechnologie (IKT) rund 8,6 Prozent der österreichischen Wertschöpfung, indirekte Effekte nicht miteingerechnet. "Die Branche ist somit eine wichtige Säule für den österreichischen Wirtschaftsstandort. Die Sicherstellung von ausreichend qualifizierten Arbeitskräften muss ganz oben auf der politischen und wirtschaftlichen Agenda stehen, sonst droht uns ein nachhaltiger Rückstand", findet Puaschitz klare Worte.

Ausbildung als Sicherheitsmaßnahme

"Moderne Wohnzimmer haben mehr Webserver als Firmen vor 15 Jahren", merkt René Pfeiffer, Geschäftführer der DeepSec Konferenz an. Alles möchte heutzutage smart sein. Das bedeutet starke Vernetzung auch in kleinen Bereichen. Sicherheitstechnisch ist man gut beraten, Fehler zu finden, bevor es die Angreiferinnen tun. Der zweitägige Workshop "Mastering Web Attacks with Full-Stack Exploitation" bietet einen sehr guten Einstieg. Webtechnologie ist allgegenwärtig. Wer sich mit Schwachstellen darin beschäftigt, hat die Chance, Fehler zu finden, bevor sie ausgenutzt werden. Der Trainer Dawid Czagan gehört zu den weltweit Top 10 Bug Huntern, die Schwachstellen finden und Betroffenen melden.

Netzwerke ziehen sich durch Alltag und Arbeitswelt wie viele rote Fäden. Vernetzung ist eine Kerntechnologie, ohne die Angreifer nicht operieren können. Paul Coggins bietet zwei Tage lang Expertise für Verteidigerinnen und Sicherheitstester an. Sein Workshop "Fundamentals of Routing and Switching for Blue and Red Team" ist nicht nur für Netzwerkdienstleister wie Internetanbieter oder Mobilfunkfirmen interessant. Netzwerke sind überall. Jedes Unternehmen hat viele davon. Das Training kann daher den Blick auf die eigenen Infrastruktur schärfen, denn diese ist alles andere als statisch - und Verbesserungen in puncto Informationssicherheit haben noch nie geschadet.

Programme und Buchung

Die DeepSec-Konferenztage sind am 29. und 30. November. Die Trainings finden an den zwei vorangehenden Tagen, dem 27. und 28. November, statt. Vertreter der Wiener Fachgruppe für Unternehmensberatung, Buchhaltung und IT (UBIT) werden vor Ort anwesend sein. Der Veranstaltungsort ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Sie finden das aktuelle Programm unter dem Link: https://deepsec.net/schedule.html

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

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

Website: deepsec.net/

https://www.pressetext.com/news/20181009009

Systemische Fehler als Sicherheitslücken

DeepSec und Privacy Week beleuchten Konsequenzen von Hintertüren in der IT

Wien (pts009/09.10.2018/09:15) - Seit die Menschheit Nachrichten verschickt, versucht man, diese abzufangen. Die moderne Kommunikationsgesellschaft schreibt mehr auf kleine, digitale Zettel als man mitlesen kann. Geschützt wird alles mit den Methoden der Mathematik - Verschlüsselung ist im Internet allgegenwärtig. Der Stand der Sicherheitstechnik ist die sogenannte Ende-zu-Ende-Verschlüsselung, bei der nur die Kommunikationspartner Zugang zu den Gesprächsinhalten oder Nachrichten haben. Dritte können nicht mitlesen, ganz unabhängig von der Situation. Dieser Umstand führt seit Einführung der Technologie zu einem Kampf zwischen Sicherheitsforscherinnen, Datenschützern und Ermittlerinnen.

Geschlossene Türen mit Pferden einrennen

Bei Ende-zu-Ende-Verschlüsselung verbleiben die Schlüssel zu den Nachrichten, sowie die Inhalte selbst, auf den bei der Konversation beteiligten Endgeräten. Das ist das gewünschte Ziel, da diese Art der Kommunikation in Netzwerken Anwendung findet, die nicht vertrauenswürdig oder öffentlich sind, wie beispielsweise das Internet. Es gibt in diesen Umgebungen keine andere Möglichkeit zur sicheren Kommunikation. Die Ende-zu-Ende-Verschlüsselung ist alternativlos. Das wird auch durch die Geschichte belegt. Rechtliche Regelungen, die Anbieter von Kommunikationsdiensten verpflichten Regierungsbehörden Zugriff auf die Kommunikation der Nutzer zu gewähren, führten in den 1990er Jahren zur Entwicklung der Pretty Good Privacy (PGP) Software. Die damaligen Auseinandersetzungen tragen im englischsprachigen Raum daher die Bezeichnung Crypto Wars.

Man begegnet den Hürden der Mathematik mit Mitteln aus der Antike. Hintertüren oder trojanische Pferde, sprich eingeschleuste Software zum Lesen der Nachrichten vor Verschlüsselung, sollen auf den Endgeräten direkt eingesetzt werden, um an der Quelle mitlesen zu können. Sicherheitstechnisch stellen jedoch Hintertüren eine Schwachstelle in Hardware oder Software dar. Für den Einsatz der trojanischen Pferde muss eine Schwachstelle vorhanden sein, um die Applikation unbemerkt installieren zu können. Beide Ansätze stehen der Informationssicherheit diametral entgegen.

Eingebauter Missbrauch

Selbst wenn der Einsatz der sogenannten Staatstrojaner seitens der Behörden nur für die Ausforschung von Drogendelikten oder ähnlich schweren Fällen vorgesehen sein sollte, so ist es denkbar, dass eine solche Abhör-

software entkommt und einem anderen Zweck zugeführt wird. Die Abhöraffäre in Griechenland im Jahre 2004 ist ein reales Beispiel. Damals wurden über die gesetzlich vorgeschriebenen Abhörschnittstellen im Mobilfunknetzwerk Telefonate und Nachrichten von griechischen Regierungs- und Behördenmitgliedern mitgeschnitten. Die Angreifern nutzten die bereits vorhandenen Schnittstellen aus. Kostas Tsalikidis, der Netzwerkplanungsmanager des Mobilfunkoperators, wurde zwei Tage nach Bekanntwerden der Lücke tot in seiner Wohnung aufgefunden. Die Täter des Abhörskandals wurden trotz jahrelanger Ermittlungen nie gefunden.

Zwar sind bei Software keine fest eingebauten Schnittstellen zur Überwachung per se aktiv oder vorgesehen, es gibt jedoch Voraussetzungen, die erfüllt sein müssen. Mit einem Staatstrojaner, manchmal auch Bundestrojaner genannt, nutzt der Staat aktiv Schwachstellen in Computerprogrammen oder Apps in Smartphones aus, um Einzelpersonen zu überwachen. Oft kauft er diese Schwachstellen sogar selbst für Steuergelder auf dem Schwarzmarkt ein und informiert die Entwicklerfirmen bewusst nicht über die ihm dann bekannten Fehler, um die Lücken möglichst lange für eigene Zwecke offen zu halten. Dabei wird die Sicherheit aller Menschen und Computersysteme aufs Spiel gesetzt. Im August 2018 wurde seitens der Abteilung Cyber- und IT-Sicherheit im Bundesinnenministerium auf einer Tagung bestätigt, dass das Wissen um unbekannte Sicherheitslücken bis zu einem gewissen Anteil vor der Öffentlichkeit zurückgehalten wird, um digitale Systeme anzugreifen.

Lücken schließen statt darauf aufzubauen

Die DeepSec Sicherheitskonferenz beschäftigt sich seit dem ersten Tag mit dem Thema Sicherheitslücken. Es wurden in den vergangenen Jahren die Sicherheit von Mobilfunknetzen, Internet Infrastruktur, mobilen Geräten, Applikationen aller Art, Softwarekomponenten von Betriebssystemen und vieles mehr eingehend analysiert. Schwachstellen eignen sich nicht als Fundament, auf dem man ein Haus sicher bauen kann.

Sicherheitsforscherinnen weltweit sind sich einig, dass ausschließlich die Publikation von Fehlern (in Zusammenarbeit mit daran interessierten Herstellern) zu deren Behebung führt. In Zeiten der Diskussion um Wahlkampfmanipulation, Bedrohungen für kritischer Infrastrukturen, steigende Vernetzung in sensitiven Wirtschaftsbranchen und militärische Nutzung von Software ist ein möglichst hohes Maß an Informationssicherheit bedeutender denn je. Daher gibt es auf der DeepSec Konferenz im November diesen Jahres wieder Präsentationen und Trainings zu diesem Thema.

Besonders empfohlen sind die Vorträge, die sich gezielt mit den Tätern auseinandersetzen. Edith Huber und Bettina Pospisil präsentieren die Ergebnisse ihrer Recherche zu Profilen von Tätern und Opfern im Bereich Cybercrime. Dr. Silke Holtmanns thematisiert in ihrem Vortrag den Stand der Technik in Bezug auf Sicherheit in Mobilfunknetzen

sowie die Herausforderungen für 5G. Mark Baenziger nimmt die Spannungen zwischen Überwachern und Überwachten zum Anlass, um die Tätigkeiten in einem IT Security Team unter beiden Gesichtspunkten zu beleuchten.

Privacy Week: Vorträge zum Thema

Zum Themenkomplex Staatstrojaner gibt es auf der PrivacyWeek gleich zwei Vorträge. Andre Meister, langjähriger Redakteur bei netzpolitik.org, gibt in seinem Vortrag einen Überblick zum Stand der Technik welche bei Staatstrojanern eingesetzt wird, zu den sie vermeintlich regelnden Gesetzen und den zahlreichen Problemen bei deren Umsetzung. Seine Präsentation trägt den Titel des Themas - "Staatstrojaner".

Lukas Gahleitner von Amnesty International Österreich hält einen Vortrag mit dem Titel "Menschenrechtliche Schutzpflichten von Staaten oder Was haben Seeminen vor der albanischen Küste mit dem Staatstrojaner zu tun?", der die völkerrechtliche Dimension des Themas veranschaulicht. Letztlich sind Sicherheitslücken eine Gefahr für Infrastruktur und die eigenen Bürgerinnen. Was ist also zu tun, wenn ein Staat von Schwachstellen weiß? Lukas Gahleitner hat diesbezüglich Vorschläge und stellt diese zur Diskussion.

Programme und Buchung

Die DeepSec Konferenztage sind am 29. und 30. November. Die Trainings finden an den zwei vorangehenden Tagen, dem 27. und 28. November statt. Der Veranstaltungsort ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.
Sie finden das aktuelle Programm unter dem Link: https://deepsec.net/schedule.html

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

Die Privacy Week findet vom 22. bis 28. Oktober 2018 im Volkskundemuseum im 8. Bezirk in Wien statt. Das Programm findet sich unter https://fahrplan.privacyweek.at . DieTickets für die Privacy Week können Sie online unter diesem Link https://privacyweek.at/tickets bestellen.

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

pts20181009009 Computer/Telekommunikation, Unternehmen/Finanzen

Systemische Fehler als Sicherheitslücken

DeepSec und Privacy Week beleuchten Konsequenzen von Hintertüren in der IT

Geschlossene Türen mit Pferden einrennen (© Florian Stocker)

Wien (pts009/09.10.2018/09:15) - **Seit die Menschheit Nachrichten verschickt, versucht man, diese abzufangen. Die moderne Kommunikationsgesellschaft schreibt mehr auf kleine, digitale Zettel als man mitlesen kann. Geschützt wird alles mit den Methoden der Mathematik - Verschlüsselung ist im Internet allgegenwärtig. Der Stand der Sicherheitstechnik ist die sogenannte Ende-zu-Ende-Verschlüsselung, bei der nur die Kommunikationspartner Zugang zu den Gesprächsinhalten oder Nachrichten haben. Dritte können nicht mitlesen, ganz unabhängig von der Situation. Dieser Umstand führt seit Einführung der Technologie zu einem Kampf zwischen Sicherheitsforscherinnen, Datenschützern und Ermittlerinnen.**

Geschlossene Türen mit Pferden einrennen

Bei Ende-zu-Ende-Verschlüsselung verbleiben die Schlüssel zu den Nachrichten, sowie die Inhalte selbst, auf den bei der Konversation beteiligten Endgeräten. Das ist das gewünschte Ziel, da diese Art der Kommunikation in Netzwerken Anwendung findet, die nicht vertrauenswürdig oder öffentlich sind, wie beispielsweise das Internet. Es gibt in diesen Umgebungen keine andere Möglichkeit zur sicheren Kommunikation. Die Ende-zu-Ende-Verschlüsselung ist alternativlos. Das wird auch durch die Geschichte belegt. Rechtliche Regelungen, die Anbieter von Kommunikationsdiensten verpflichten Regierungsbehörden Zugriff auf die Kommunikation der Nutzer zu gewähren, führten in den 1990er Jahren zur Entwicklung der Pretty Good Privacy (PGP) Software. Die damaligen Auseinandersetzungen tragen im englischsprachigen Raum daher die Bezeichnung Crypto Wars.

Man begegnet den Hürden der Mathematik mit Mitteln aus der Antike. Hintertüren oder trojanische Pferde, sprich eingeschleuste Software zum Lesen der Nachrichten vor Verschlüsselung, sollen auf den Endgeräten direkt eingesetzt werden, um an der Quelle mitlesen zu können. Sicherheitstechnisch stellen jedoch Hintertüren eine Schwachstelle in Hardware oder Software dar. Für den Einsatz der trojanischen Pferde muss eine Schwachstelle vorhanden sein, um die Applikation unbemerkt installieren zu können. Beide Ansätze stehen der Informationssicherheit diametral entgegen.

Eingebauter Missbrauch

Selbst wenn der Einsatz der sogenannten Staatstrojaner seitens der Behörden nur für die Ausforschung von Drogendelikten oder ähnlich schweren Fällen vorgesehen sein sollte, so ist es denkbar, dass eine solche Abhörsoftware entkommt und einem anderen Zweck zugeführt wird. Die Abhöraffäre in Griechenland im

Jahre 2004 ist ein reales Beispiel. Damals wurden über die gesetzlich vorgeschriebenen Abhörschnittstellen im Mobilfunknetzwerk Telefonate und Nachrichten von griechischen Regierungs- und Behördenmitgliedern mitgeschnitten. Die Angreifern nutzten die bereits vorhandenen Schnittstellen aus. Kostas Tsalikidis, der Netzwerkplanungsmanager des Mobilfunkoperators, wurde zwei Tage nach Bekanntwerden der Lücke tot in seiner Wohnung aufgefunden. Die Täter des Abhörskandals wurden trotz jahrelanger Ermittlungen nie gefunden.

Zwar sind bei Software keine fest eingebauten Schnittstellen zur Überwachung per se aktiv oder vorgesehen, es gibt jedoch Voraussetzungen, die erfüllt sein müssen. Mit einem Staatstrojaner, manchmal auch Bundestrojaner genannt, nutzt der Staat aktiv Schwachstellen in Computerprogrammen oder Apps in Smartphones aus, um Einzelpersonen zu überwachen. Oft kauft er diese Schwachstellen sogar selbst für Steuergelder auf dem Schwarzmarkt ein und informiert die Entwicklerfirmen bewusst nicht über die ihm dann bekannten Fehler, um die Lücken möglichst lange für eigene Zwecke offen zu halten. Dabei wird die Sicherheit aller Menschen und Computersysteme aufs Spiel gesetzt. Im August 2018 wurde seitens der Abteilung Cyber- und IT-Sicherheit im Bundesinnenministerium auf einer Tagung bestätigt, dass das Wissen um unbekannte Sicherheitslücken bis zu einem gewissen Anteil vor der Öffentlichkeit zurückgehalten wird, um digitale Systeme anzugreifen.

Lücken schließen statt darauf aufzubauen

Die DeepSec Sicherheitskonferenz beschäftigt sich seit dem ersten Tag mit dem Thema Sicherheitslücken. Es wurden in den vergangenen Jahren die Sicherheit von Mobilfunknetzen, Internet Infrastruktur, mobilen Geräten, Applikationen aller Art, Softwarekomponenten von Betriebssystemen und vieles mehr eingehend analysiert. Schwachstellen eignen sich nicht als Fundament, auf dem man ein Haus sicher bauen kann.

Sicherheitsforscherinnen weltweit sind sich einig, dass ausschließlich die Publikation von Fehlern (in Zusammenarbeit mit daran interessierten Herstellern) zu deren Behebung führt. In Zeiten der Diskussion um Wahlkampfmanipulation, Bedrohungen für kritischer Infrastrukturen, steigende Vernetzung in sensitiven Wirtschaftsbranchen und militärische Nutzung von Software ist ein möglichst hohes Maß an Informationssicherheit bedeutender denn je. Daher gibt es auf der DeepSec Konferenz im November diesen Jahres wieder Präsentationen und Trainings zu diesem Thema.

Besonders empfohlen sind die Vorträge, die sich gezielt mit den Tätern auseinandersetzen. Edith Huber und Bettina Pospisil präsentieren die Ergebnisse ihrer Recherche zu Profilen von Tätern und Opfern im Bereich Cybercrime. Dr. Silke Holtmanns thematisiert in ihrem Vortrag den Stand der Technik in Bezug auf Sicherheit in Mobilfunknetzen sowie die Herausforderungen für 5G. Mark Baenziger nimmt die Spannungen zwischen Überwachern und Überwachten zum Anlass, um die Tätigkeiten in einem IT Security Team unter beiden Gesichtspunkten zu beleuchten.

Privacy Week: Vorträge zum Thema

Zum Themenkomplex Staatstrojaner gibt es auf der PrivacyWeek gleich zwei Vorträge. Andre Meister, langjähriger Redakteur bei netzpolitik.org, gibt in seinem Vortrag einen Überblick zum Stand der Technik welche bei Staatstrojanern eingesetzt wird, zu den sie vermeintlich regelnden Gesetzen und den zahlreichen Problemen bei deren Umsetzung. Seine Präsentation trägt den Titel des Themas - "Staatstrojaner".

Lukas Gahleitner von Amnesty International Österreich hält einen Vortrag mit dem Titel "Menschenrechtliche Schutzpflichten von Staaten oder Was haben Seeminen vor der albanischen Küste mit dem Staatstrojaner zu tun?", der die völkerrechtliche Dimension des Themas veranschaulicht. Letztlich sind Sicherheitslücken eine Gefahr für Infrastruktur und die eigenen Bürgerinnen. Was ist also zu tun, wenn ein Staat von Schwachstellen weiß? Lukas Gahleitner hat diesbezüglich Vorschläge und stellt diese zur Diskussion.

Programme und Buchung

Die DeepSec Konferenztage sind am 29. und 30. November. Die Trainings finden an den zwei vorangehenden Tagen, dem 27. und 28. November statt. Der Veranstaltungsort ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.
Sie finden das aktuelle Programm unter dem Link: https://deepsec.net/schedule.html

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

Die Privacy Week findet vom 22. bis 28. Oktober 2018 im Volkskundemuseum im 8. Bezirk in Wien statt. Das Programm findet sich unter https://fahrplan.privacyweek.at . DieTickets für die Privacy Week können Sie online unter diesem Link https://privacyweek.at/tickets bestellen.

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

https://www.pressetext.com/news/20180925007

Wissen schützt: Begriffsverwirrung um Sicherheit und Datenschutz

DeepSec Konferenz und Privacy Week bündeln Kräfte zur Weiterbildung von Fachpersonal

Wien (pts007/25.09.2018/09:05) - Datenschutz und Informationssicherheit werden gerne in einem Atemzug genannt. Manchmal werden auch die gängigen Anglizismen Privacy und Security verwendet. Der Unterschied zwischen den beiden Begriffen ist oft nicht deutlich verständlich, besonders, wenn man Publikationen liest oder politischen Diskussionen folgt, in der beide Worte gerne synonym verwendet werden. Es kommt dann meist "irgendwas mit Schutz und Privatsphäre, möglichst digital" heraus. Die unvermeidliche Folge ist dann ein hochgefährliches Halbwissen, welches zu Sicherheitslücken führt. Privatsphäre und Geheimnisse sind schützenswert, sie sind jedoch nicht völlig gleich. Die DeepSec Konferenz und die Privacy Week möchten daher im Oktober und November diesen Jahres Aufklärungsarbeit durch Vorträge und Workshops leisten.

Informationssicherheit als Fundament

Ohne Grundmauern bleibt bei Gebäuden kein Stein auf dem anderen. Die Informationssicherheit ist daher immer die grundlegende Komponente, wenn es um Sicherheit oder Schutz geht. Darauf baut alles andere auf. Das oberste Ziel ist, Daten vor unbefugtem Zugriff zu bewahren, und die Integrität der Daten zu gewährleisten. Damit ist Schutz vor Manipulation, digitaler Diebstahl (sprich das Kopieren von Daten) oder der Missbrauch von Systemen der Informationsverarbeitung automatisch enthalten.

Die Tücke liegt in der praktischen Umsetzung, da der moderne Alltag zu Hause und in der Arbeitswelt stark vernetzt und vom ständigen Zugriff auf Daten lebt. Baut man Schleusen und Schranken ein, so muss man sich sehr gut überlegen wie man das im produktiven Betrieb umsetzen kann. Es ist kein unlösbares Problem, es bedarf nur guter Planung. Um die simple Analogie zur Datenautobahn zu strapazieren: Im Straßenverkehr hat man es ja auch geschafft. Vordergründig ist immer eine intelligente Architektur, gepaart mit Expertinnen, die interdisziplinär arbeiten. Dabei muss man auch wissen, wer wie zu welchem Zweck Daten verarbeitet. Wer Vorschriften und Sicherheitsmaßnahmen implementiert, ohne zu wissen, was dies für jeden einzelnen Arbeitsplatz bedeutet, der setzt die Grundlage für eine endlose Serie von Ausnahmen und Sonderregelungen, letztlich also Sicherheitslücken.

Datenschutz involviert Bürger mit Rechten

Sobald personenbezogene Daten ins Spiel kommen, wird es - im wahrsten Sinne des Wortes - persönlich. Bürgerinnen haben Rechte, die ihnen die Verfassung zugesteht. Damit kommt die Privatsphäre ins Spiel. Zusätzlich

wird der Fokus geändert. Die Informationssicherheit schützt Daten und Systeme generell. Beim Datenschutz ist der Schutz persönlicher Daten im Vordergrund. Dazu gehören auch Logiken, um aus Daten Profile zu erstellen, die wiederum einzelnen Personen zugeordnet werden können.

An diesem Punkt gibt es Unterschieden zwischen den beiden Disziplinen. Informationssicherheit muss zuweilen feststellen, wie ein fehlgeschlagener Loginversuch oder ein Zugriff auf Daten geschehen konnte. Dazu müssen zwangsläufig Protokolle geschrieben und personenbezogene Informationen verarbeitet werden. Jeder Systemadministrator hat schon zu Diagnosezwecken Logdateien durchsucht. Man sieht dort automatisch Zeitstempel, eindeutige Kennungen oder Namen, abhängig vom verwendeten System. Natürlich gilt der Schutz auf für diese Daten, und genau da beginnen die inhaltlichen Abstimmungen, die zwischen beiden Disziplinen notwendig sind. Die DeepSec Konferenz und die Privacy Week möchten daher Datenschützerinnen und Informationsschützer an einen Tisch bringen, um Wissen und Erfahrungen auszutauschen.

Vortrag auf der Privacy Week 2018

René Pfeiffer, Geschäftsführer der DeepSec GmbH, wird auf der Privacy Week einen Vortrag mit dem Titel "Das Verhältnis zwischen Privacy und Security" halten. Datenschutz bedient sich der Datensicherheit, um die gesteckten Ziele - den Schutz privater Daten - umzusetzen. Umgekehrt muss Datensicherheit nicht automatisch mit persönlichen Daten zu tun haben. Betriebssysteme und Applikationen dürfen sich jederzeit auch selbst ohne die Präsenz von Anwenderinnen schützen. Abhängig vom Kontext kommt Informationssicherheit allerdings durchaus mit Profilen und Persönlichkeiten in Berührung. Die unsägliche Biometrie für Logins ist ein (schlechtes) Beispiel, da man körperliche Merkmale nicht ändern kann; dasselbe gilt für die Analyse von Verhalten, um die Benutzung von Konten durch Menschen zu prüfen, oder simple Nachrichten mit Namen, Telefonnummern oder ähnlichem. Überwachung ist oft ein Problem für den Datenschutz, ist aber fallweise eine Komponente von Datensicherheit. Wieder hängt es stark vom Kontext ab.

Der Vortrag möchte daher nicht relativieren, sondern Klarheit in die Verwirrung bringen. Die Gemeinsamkeiten sowie Unterschiede zwischen den beiden Disziplinen müssen verstanden werden bevor man eine Umsetzung von Maßnahmen wagt. Der Inhalt des Vortrags soll beim semantischen Navigieren helfen und dem Publikum die Chance geben, Scharlatanerie von echtem Schutz zu unterscheiden. Man wird nach der Präsentation klar erkennen, dass Daten definitiv nicht das Rohöl des 21. Jahrhunderts sind. Gründerinnen und Mitarbeiter von Start-Ups sind explizit eingeladen, um sich weiterzubilden.

Präsentationen auf der DeepSec Konferenz

Der Vortrag "Blinding the Watchers: The Growing Tension between Privacy Concerns and Information Security" von Mark Baenziger beleuchtet das Spannungsfeld von Informationssicherheit und Privatsphäre. An Beispielen wird erläutert wie Sicherheitsbeauftragte Datenschutzmassnahmen bei Untersuchungen von Vorfällen deaktiviert haben. Der Fokus der Präsentation liegt auf den Mechanismen, die IT Sicherheitsabteilungen einsetzen, um ihre Ziele zu erreichen. Die Werkzeuge, die Angriffe und Betrugsversuche aufklären, müssen zwangsläufig auf Daten zugreifen, die personenbezogen sein können. Es werden Wege aufgezeigt wie man alternative Analyseansätze verwenden kann. Schließlich gelten rechtliche Vorgaben sowohl für Sicherheit von Infrastruktur, Geschäftsdaten und persönlichen Daten. Compliance kann man nicht nach Belieben ignorieren. Beschäftigen Sie sich mit den Lösungen bevor die Probleme auftreten. Zur DeepSec Konferenz sind zahlreiche Experten vor Ort, die Sie während der Veranstaltung ansprechen können.

Programme und Buchung

Die DeepSec-Konferenztage sind am 29. und 30. November. Die Trainings finden an den zwei vorangehenden Tagen, dem 27. und 28. November statt. Der Veranstaltungsort ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.
Sie finden das aktuelle Programm unter dem Link: https://deepsec.net/schedule.html

Tickets für die DeepSec Konferenz und die Trainings können Sie jederzeit unter dem Link https://deepsec.net/register.html bestellen.
Die Privacy Week findet vom 22. bis 28. Oktober 2018 im Volkskundemuseum im 8. Bezirk in Wien statt. Das Programm findet sich unter https://fahrplan.privacyweek.at . DieTickets für die Privacy Week können Sie online unter diesem Link https://privacyweek.at/tickets bestellen.

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

pts20180925007 Computer/Telekommunikation, Handel/Dienstleistungen

Wissen schützt: Begriffsverwirrung um Sicherheit und Datenschutz

DeepSec Konferenz und Privacy Week bündeln Kräfte zur Weiterbildung von Fachpersonal

Wien (pts007/25.09.2018/09:05) - **Datenschutz und Informationssicherheit werden gerne in einem Atemzug genannt. Manchmal werden auch die gängigen Anglizismen Privacy und Security verwendet. Der Unterschied zwischen den beiden Begriffen ist oft nicht deutlich verständlich, besonders, wenn man Publikationen liest oder politischen Diskussionen folgt, in der beide Worte gerne synonym verwendet werden. Es kommt dann meist "irgendwas mit Schutz und Privatsphäre, möglichst digital" heraus. Die unvermeidliche Folge ist dann ein hochgefährliches Halbwissen, welches zu Sicherheitslücken führt. Privatsphäre und Geheimnisse sind schützenswert, sie sind jedoch nicht völlig gleich. Die DeepSec Konferenz und die Privacy Week möchten daher im Oktober und November diesen Jahres Aufklärungsarbeit durch Vorträge und Workshops leisten.**

Informationssicherheit als Fundament

Ohne Grundmauern bleibt bei Gebäuden kein Stein auf dem anderen. Die Informationssicherheit ist daher immer die grundlegende Komponente, wenn es um Sicherheit oder Schutz geht. Darauf baut alles andere auf. Das oberste Ziel ist, Daten vor unbefugtem Zugriff zu bewahren, und die Integrität der Daten zu gewährleisten. Damit ist Schutz vor Manipulation, digitaler Diebstahl (sprich das Kopieren von Daten) oder der Missbrauch von Systemen der Informationsverarbeitung automatisch enthalten.

Die Tücke liegt in der praktischen Umsetzung, da der moderne Alltag zu Hause und in der Arbeitswelt stark vernetzt und vom ständigen Zugriff auf Daten lebt. Baut man Schleusen und Schranken ein, so muss man sich sehr gut überlegen wie man das im produktiven Betrieb umsetzen kann. Es ist kein unlösbares Problem, es bedarf nur guter Planung. Um die simple Analogie zur Datenautobahn zu strapazieren: Im Straßenverkehr hat man es ja auch geschafft. Vordergründig ist immer eine intelligente Architektur, gepaart mit Expertinnen, die interdisziplinär arbeiten. Dabei muss man auch wissen, wer wie zu welchem Zweck Daten verarbeitet. Wer Vorschriften und Sicherheitsmaßnahmen implementiert, ohne zu wissen, was dies für jeden einzelnen Arbeitsplatz bedeutet, der setzt die Grundlage für eine endlose Serie von Ausnahmen und Sonderregelungen, letztlich also Sicherheitslücken.

Datenschutz involviert Bürger mit Rechten

Sobald personenbezogene Daten ins Spiel kommen, wird es - im wahrsten Sinne des Wortes - persönlich. Bürgerinnen haben Rechte, die ihnen die Verfassung zugesteht. Damit kommt die Privatsphäre ins Spiel. Zusätzlich wird der Fokus geändert. Die Informationssicherheit schützt Daten und Systeme generell. Beim Datenschutz ist der Schutz persönlicher Daten im Vordergrund. Dazu gehören auch Logiken, um aus Daten Profile zu erstellen, die wiederum einzelnen Personen zugeordnet werden können.

An diesem Punkt gibt es Unterschieden zwischen den beiden Disziplinen. Informationssicherheit muss zuweilen feststellen, wie ein fehlgeschlagener Loginversuch oder ein Zugriff auf Daten geschehen konnte. Dazu müssen zwangsläufig Protokolle geschrieben und personenbezogene Informationen verarbeitet werden. Jeder Systemadministrator hat schon zu Diagnosezwecken Logdateien durchsucht. Man sieht dort automatisch Zeitstempel, eindeutige Kennungen oder Namen, abhängig vom verwendeten System. Natürlich gilt der Schutz auf für diese Daten, und genau da beginnen die inhaltlichen Abstimmungen, die zwischen beiden Disziplinen notwendig sind. Die DeepSec Konferenz und die Privacy Week möchten daher Datenschützerinnen und Informationsschützer an einen Tisch bringen, um Wissen und Erfahrungen auszutauschen.

Vortrag auf der Privacy Week 2018

René Pfeiffer, Geschäftsführer der DeepSec GmbH, wird auf der Privacy Week einen Vortrag mit dem Titel "Das Verhältnis zwischen Privacy und Security" halten. Datenschutz bedient sich der Datensicherheit, um die gesteckten Ziele - den Schutz privater Daten - umzusetzen. Umgekehrt muss Datensicherheit nicht automatisch mit persönlichen Daten zu tun haben. Betriebssysteme und Applikationen dürfen sich jederzeit auch selbst ohne die Präsenz von Anwenderinnen schützen. Abhängig vom Kontext kommt Informationssicherheit allerdings durchaus mit Profilen und Persönlichkeiten in Berührung. Die unsägliche Biometrie für Logins ist ein (schlechtes) Beispiel, da man körperliche Merkmale nicht ändern kann; dasselbe gilt für die Analyse von Verhalten, um die Benutzung von Konten durch Menschen zu prüfen, oder simple Nachrichten mit Namen, Telefonnummern oder ähnlichem. Überwachung ist oft ein Problem für den Datenschutz, ist aber fallweise eine Komponente von Datensicherheit. Wieder hängt es stark vom Kontext ab.

Der Vortrag möchte daher nicht relativieren, sondern Klarheit in die Verwirrung bringen. Die Gemeinsamkeiten sowie Unterschiede zwischen den beiden Disziplinen müssen verstanden werden bevor man eine Umsetzung von Maßnahmen wagt. Der Inhalt des Vortrags soll beim semantischen Navigieren helfen und dem Publikum die Chance geben, Scharlatanerie von echtem Schutz zu unterscheiden. Man wird nach der Präsentation klar erkennen, dass Daten definitiv nicht das Rohöl des 21. Jahrhunderts sind. Gründerinnen und Mitarbeiter von Start-Ups sind explizit eingeladen, um sich weiterzubilden.

Präsentationen auf der DeepSec Konferenz

Der Vortrag "Blinding the Watchers: The Growing Tension between Privacy Concerns and Information Security" von Mark Baenziger beleuchtet das Spannungsfeld von Informationssicherheit und Privatsphäre. An Beispielen wird erläutert wie Sicherheitsbeauftragte Datenschutzmassnahmen bei Untersuchungen von Vorfällen deaktiviert haben. Der Fokus der Präsentation liegt auf den Mechanismen, die IT Sicherheitsabteilungen einsetzen, um ihre Ziele zu erreichen. Die Werkzeuge, die Angriffe und Betrugsversuche aufklären, müssen zwangsläufig auf Daten zugreifen, die personenbezogen sein können. Es werden Wege aufgezeigt wie man alternative Analyseansätze verwenden kann. Schließlich gelten rechtliche Vorgaben sowohl für Sicherheit von Infrastruktur, Geschäftsdaten und persönlichen Daten. Compliance kann man nicht nach Belieben ignorieren. Beschäftigen Sie sich mit den Lösungen bevor die Probleme auftreten. Zur DeepSec Konferenz sind zahlreiche Experten vor Ort, die Sie während der Veranstaltung ansprechen können.

Programme und Buchung

Die DeepSec-Konferenztage sind am 29. und 30. November. Die Trainings finden an den zwei vorangehenden Tagen, dem 27. und 28. November statt. Der Veranstaltungsort ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.
Sie finden das aktuelle Programm unter dem Link: https://deepsec.net/schedule.html

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

Die Privacy Week findet vom 22. bis 28. Oktober 2018 im Volkskundemuseum im 8. Bezirk in Wien statt. Das Programm findet sich unter https://fahrplan.privacyweek.at . DieTickets für die Privacy Week können Sie online unter diesem Link https://privacyweek.at/tickets bestellen.

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

https://www.pressetext.com/news/20180911014

Geheimdienste wollen Informationssicherheit abschaffen

DeepSec Konferenz kritisiert offenen Angriff auf sichere Ende-zu-Ende-Verschlüsselung

Wien (pts014/11.09.2018/09:25) - Seit es Sicherheitsmaßnahmen gibt, existiert die Diskussionen um ihre Nutzen und um ihre Stärke. Bei digitaler Kommunikation kommt immer wieder das Thema der Hintertüren auf. Hochqualitative Schlösser sind in der analogen Welt erwünscht, um Werte vor Diebstahl zu schützen. In der digitalen Welt soll das nun anders werden. Die Five Eyes (sprich die Geheimdienste der Vereinigten Staaten, des Vereinigten Königreichs, Australiens, Neuseelands und Kanada) möchten nun alle Staaten der Welt bei verschlüsselter Kommunikation zum Einbau von Nachschlüsseln, also Hintertüren, zwingen. Dazu fand Ende August in Australien ein Treffen der Five Eyes Innenminister statt. Dieser Vorschlag birgt schwerwiegende Nachteile für die Wirtschaft und die nationale Sicherheit jedes Staates.

Messenger statt Mobilfunk

Als die Mobiltelefone ihren Siegeszug antraten, gab es nur unverschlüsselte Kurznachrichten (auch bekannt als SMS, Short Message Service). Vor der Ära der Smartphones haben einige Hersteller eigene proprietäre Formate entwickelt, um den Inhalt der Nachrichten zu schützen. In den letzten Jahren gab es einen Schwenk in Richtung Messenger Apps, die das Internet für die Nachrichtenübertragung nutzen. Damit konnten und können Entwicklerinnen offene Standards mit starker Verschlüsselung einsetzen, die nicht den gesetzlich vorgeschriebenen Schnittstellen zur Telekommunikationsüberwachung in den Mobilfunknetzwerken unterliegen.

Diese Telekommunikationsüberwachung (international auch Lawful Interception genannt) ist fester Bestandteil der Netzwerkinfrastuktur und erfasst ständig Ortsdaten, Logins, Betriebszeiten, Adressen, Mobilfunkidentifikationen sowie weitere Daten. Moderne Messenger setzen daher meist das Prinzip der Ende-zu-Ende-Verschlüsselung ein, wo nur die kommunizierenden Endgeräte die Schlüssel zur Nachricht besitzen. Das Netzwerk kennt diese nicht und kann den Inhalt der Nachrichten nicht sehen. Dies ist nur über mobilen Datenzugang, sprich Internetzugriff, möglich.

Die Gefahren dieser Schnittstellen wurden durch die publizierten Dokumente von Edward Snowden im Jahre 2013 und die Abhöraffäre in Athen in den Jahren 2004 und 2005 illustriert. Bereits 2015 hielt James Bamford, US-amerikanischer Journalist und Nachrichtendienstexperte, den Eröffnungsvortrag zur DeepSec Konferenz und erläuterte darin wie die Mobiltelefone der griechische Regierung über rechtlich geforderte Hintertüren von Unbekannten

abgehört wurden. Kostas Tsalikidis, der zuständige Netzwerkverantwortliche, beging Tage nach Bekanntwerden der Abhörkonfigurationen Selbstmord. Die Täter der Abhöraktion wurden trotz größter langwieriger Ermittlungen nie ausfindig gemacht.

Mathematik ist in Australien nicht rechtskräftig

Sicherheitsforscher und Ingenieure sind sich der Gefahren schlecht implementierter und unsicherer Kommunikation sehr wohl bewusst. Aus diesem Grunde wird spätestens seit den Snowden Enthüllungen starke Kryptographie und sichere Kommunikation von Technologiefirmen und Entwicklerinnen forciert. Das Institute of Electrical and Electronics Engineers (IEEE) und die Internet Engineering Task Force (IETF) haben in allen Standards der letzten Jahre Protokolle standardisiert, die weder Hintertüren noch absichtlich geschwächte Algorithmen enthalten. Das moderne Internet, und damit unsere heutige Kommunikationsgesellschaft, basiert auf diesen Standards.

Die Techniker versuchen damit, das Pendant zu sicheren Brücken zu schaffen, die ja auch keine Sollbruchstelle haben dürfen. Infrastruktur muss verlässlich sein. Man darf dabei nicht vergessen, dass nicht nur Telefonate und Nachrichten von den gesetzlichen Schwachstellen betroffen sind. Forderungen nach Nachschlüsseln betreffen Finanztransaktionen, das komplette World Wide Web, sämtliche Anwendungen auf Smartphones, das Internet der Dinge, alle Smart Technologien, kurzum alle Unternehmen und Märkte weltweit.

Der ehemalige australische Premierminister Malcolm Turnbull hat den Forderungen, weltweit immer und überall sämtliche Kommunikation mitlesen zu können, höchste Priorität gegeben. Er sagt im Juli diesen Jahres, dass das Gesetzbuch Australiens über der Mathematik stehe. Damit bezog er sich auf die Kritik von Forschern der Kryptographie, die ein Teilgebiet der Mathematik ist. Diese Logik ist fragwürdig, denn niemand hat bisher die Gravitation für illegal erklärt, um Arbeitsunfälle zu verhindern oder leichter Berge besteigen zu können. Die Frage ist einzig und alleine, ob man echte Sicherheit haben möchte oder nicht. Der Brandschutz ist eine gute Analogie. Niemand möchte Schutzvorkehrungen gegen Brände, die nicht immer funktionieren. Genauso möchte auch niemand elektronische Zahlungsmittel nutzen, die bis auf Widerruf sicher sind.

Nationale Sicherheit schafft sich international ab

Die Forderung der Five Eyes lässt sich auch umformulieren. Da die Dienste ebenso die Mathematik zum Schutz ihrer Länder einsetzen, müssten sie sich selbst schwächen. Das betrifft dann insbesondere Wirtschaftsspionage, die sehr oft Ländergrenzen überquert. Eine komplette Zerstörung bzw. die Sabotage von wichtigen Komponenten der Informationssicherheit ist ein kurzsichtiger Reflex. Es geht nicht nur um die Vorzeigefirmen im Silicon Valley. Hintertüren und Nachschlüssel belasten jedwede Kommunikation über Geschäftsgeheimnisse bis hin zur sicheren

elektronische Kommunikation von Rechtsanwälten mit der Justiz und Behörden.

Man darf dabei nicht vergessen, dass diese Forderung nicht nur von den Five Eyes gestellt werden wird, sollte es zu einer Umsetzung durch Regierungen kommen. Die Vereinten Nationen führen momentan eine Liste von 206 Mitgliedsstaaten. Die Forderungen der Five Eyes werden dann von den "206 Eyes" auch gestellt werden. Politisch Verantwortliche sind sehr gut beraten, die Warnungen von Expertinnen nicht zu ignorieren. Stimmt man der Forderung nach Hintertüren zu, so müssen die Geheimdienste der Five Eyes dann auch den Diensten Europas, Russlands, Chinas und Nordkoreas jeweils ihre eigene nationale Kommunikation offenlegen, denn die Mathematik der Sicherheit oder Unsicherheit gilt für alle gleichermaßen. Die Forderung hat daher mit der Realität rein gar nichts zu tun, mit Informationssicherheit schon gar nicht.

Lösungen nicht im Monolog möglich

Sicherheitsforscher sitzen im selben Boot wie die Behörden. Auch sie müssen Angreifer finden und müssen mit oder gegen Schutzmaßnahmen arbeiten. Dennoch rücken IEEE, IETF und alle technischen Organisationen nicht von der Forderung nach starker Sicherheit ab. Da die Five Eyes Forderungen explizit legislative Maßnahmen ansprechen, ist das ein wertvolles Kompliment für die Techniker. Das bedeutet, dass die technische Umsetzung nur sehr schwer oder mit den derzeit verfügbaren Mitteln nicht angreifbar ist.

Die Implementation von Sicherheit ist immer ein Ergebnis interdisziplinärer Zusammenarbeit. Genau aus diesem Grund möchte die DeepSec Konferenz jährlich Vertreter aus Forschung, Behörden, Wirtschaft und der internationalen Hacker Community an einen Tisch bringen. Eine vernetzte Welt benötigt vernetztes Denken. Insellösungen oder kurzfristige Maßnahmen sind nicht zukunftsgerichtet. Daher hat die diesjährige DeepSec Konferenz ihren Schwerpunkt auf Infrastruktur, Internet der Dinge, Mobilität (sei es Funk, Gerät oder Transport) und auch Kryptographie gelegt. Spezialisten aus vier Kontinenten tauschen sich im November in Wien aus, um Bedrohungen der Zukunft zu begegnen. Wir freuen uns auf konstruktive Zusammenarbeit und Ihren Besuch.

Quellen, Programm und Buchung

Die DeepSec Konferenztage sind am 29. und 30. November. Die Trainings finden an den zwei vorangehenden Tagen, dem 27. und 28. November statt. Der Veranstaltungsort ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Sie finden das aktuelle Programm unter dem Link: https://deepsec.net/schedule.html

James Bamford hat in der Publikation "In-Depth Security - Proceedings of the DeepSec Conferences Volume 2" seinen Vortrag als Artikel mit dem Titel "A Death in Athens - The Inherent Vulnerability of "Lawful Intercept"" zusammengefasst. Das Buch ist im Handel und über die DeepSec Konferenz zu beziehen (es kann direkt bei der DeepSec GmbH bestellt werden). Sein Vortrag ist online unter https://vimeo.com/150691584 als Video einsehbar.

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

Aussender: DeepSec GmbH

Ansprechpartner: René Pfeiffer

Tel.: +43-676-5626390

E-Mail: deepsec@deepsec.net

Website: deepsec.net

pts20180911014 Computer/Telekommunikation, Medien/Kommunikation

Geheimdienste wollen Informationssicherheit abschaffen

DeepSec Konferenz kritisiert offenen Angriff auf sichere Ende-zu-Ende-Verschlüsselung

Wien (pts014/11.09.2018/09:25) - **Seit es Sicherheitsmaßnahmen gibt, existiert die Diskussionen um ihre Nutzen und um ihre Stärke. Bei digitaler Kommunikation kommt immer wieder das Thema der Hintertüren auf. Hochqualitative Schlösser sind in der analogen Welt erwünscht, um Werte vor Diebstahl zu schützen. In der digitalen Welt soll das nun anders werden. Die Five Eyes (sprich die Geheimdienste der Vereinigten Staaten, des Vereinigten Königreichs, Australiens, Neuseelands und Kanada) möchten nun alle Staaten der Welt bei verschlüsselter Kommunikation zum Einbau von Nachschlüsseln, also Hintertüren, zwingen. Dazu fand Ende August in Australien ein Treffen der Five Eyes Innenminister statt. Dieser Vorschlag birgt schwerwiegende Nachteile für die Wirtschaft und die nationale Sicherheit jedes Staates.**

Messenger statt Mobilfunk

Als die Mobiltelefone ihren Siegeszug antraten, gab es nur unverschlüsselte Kurznachrichten (auch bekannt als SMS, Short Message Service). Vor der Ära der Smartphones haben einige Hersteller eigene proprietäre Formate entwickelt, um den Inhalt der Nachrichten zu schützen. In den letzten Jahren gab es einen Schwenk in Richtung Messenger Apps, die das Internet für die Nachrichtenübertragung nutzen. Damit konnten und können Entwicklerinnen offene Standards mit starker Verschlüsselung einsetzen, die nicht den gesetzlich vorgeschriebenen Schnittstellen zur Telekommunikationsüberwachung in den Mobilfunknetzwerken unterliegen.

Diese Telekommunikationsüberwachung (international auch Lawful Interception genannt) ist fester Bestandteil der Netzwerkinfrastuktur und erfasst ständig Ortsdaten, Logins, Betriebszeiten, Adressen, Mobilfunkidentifikationen sowie weitere Daten. Moderne Messenger setzen daher meist das Prinzip der Ende-zu-Ende-Verschlüsselung ein, wo nur die kommunizierenden Endgeräte die Schlüssel zur Nachricht besitzen. Das Netzwerk kennt diese nicht und kann den Inhalt der Nachrichten nicht sehen. Dies ist nur über mobilen Datenzugang, sprich Internetzugriff, möglich.

Die Gefahren dieser Schnittstellen wurden durch die publizierten Dokumente von Edward Snowden im Jahre 2013 und die Abhöraffäre in Athen in den Jahren 2004 und 2005 illustriert. Bereits 2015 hielt James Bamford, US-amerikanischer Journalist und Nachrichtendienstexperte, den Eröffnungsvortrag zur DeepSec Konferenz und erläuterte darin wie die Mobiltelefone der griechische Regierung über rechtlich geforderte Hintertüren von Unbekannten abgehört wurden. Kostas Tsalikidis, der zuständige Netzwerkverantwortliche, beging Tage nach Bekanntwerden der Abhörkonfigurationen Selbstmord. Die Täter der Abhöraktion wurden trotz größter langwieriger Ermittlungen nie ausfindig gemacht.

Mathematik ist in Australien nicht rechtskräftig

Sicherheitsforscher und Ingenieure sind sich der Gefahren schlecht implementierter und unsicherer Kommunikation sehr wohl bewusst. Aus diesem Grunde wird spätestens seit den Snowden Enthüllungen

starke Kryptographie und sichere Kommunikation von Technologiefirmen und Entwicklerinnen forciert. Das Institute of Electrical and Electronics Engineers (IEEE) und die Internet Engineering Task Force (IETF) haben in allen Standards der letzten Jahre Protokolle standardisiert, die weder Hintertüren noch absichtlich geschwächte Algorithmen enthalten. Das moderne Internet, und damit unsere heutige Kommunikationsgesellschaft, basiert auf diesen Standards.

Die Techniker versuchen damit, das Pendant zu sicheren Brücken zu schaffen, die ja auch keine Sollbruchstelle haben dürfen. Infrastruktur muss verlässlich sein. Man darf dabei nicht vergessen, dass nicht nur Telefonate und Nachrichten von den gesetzlichen Schwachstellen betroffen sind. Forderungen nach Nachschlüsseln betreffen Finanztransaktionen, das komplette World Wide Web, sämtliche Anwendungen auf Smartphones, das Internet der Dinge, alle Smart Technologien, kurzum alle Unternehmen und Märkte weltweit.

Der ehemalige australische Premierminister Malcolm Turnbull hat den Forderungen, weltweit immer und überall sämtliche Kommunikation mitlesen zu können, höchste Priorität gegeben. Er sagt im Juli diesen Jahres, dass das Gesetzbuch Australiens über der Mathematik stehe. Damit bezog er sich auf die Kritik von Forschern der Kryptographie, die ein Teilgebiet der Mathematik ist. Diese Logik ist fragwürdig, denn niemand hat bisher die Gravitation für illegal erklärt, um Arbeitsunfälle zu verhindern oder leichter Berge besteigen zu können. Die Frage ist einzig und alleine, ob man echte Sicherheit haben möchte oder nicht. Der Brandschutz ist eine gute Analogie. Niemand möchte Schutzvorkehrungen gegen Brände, die nicht immer funktionieren. Genauso möchte auch niemand elektronische Zahlungsmittel nutzen, die bis auf Widerruf sicher sind.

Nationale Sicherheit schafft sich international ab

Die Forderung der Five Eyes lässt sich auch umformulieren. Da die Dienste ebenso die Mathematik zum Schutz ihrer Länder einsetzen, müssten sie sich selbst schwächen. Das betrifft dann insbesondere Wirtschaftsspionage, die sehr oft Ländergrenzen überquert. Eine komplette Zerstörung bzw. die Sabotage von wichtigen Komponenten der Informationssicherheit ist ein kurzsichtiger Reflex. Es geht nicht nur um die Vorzeigefirmen im Silicon Valley. Hintertüren und Nachschlüssel belasten jedwede Kommunikation über Geschäftsgeheimnisse bis hin zur sicheren elektronische Kommunikation von Rechtsanwälten mit der Justiz und Behörden.

Man darf dabei nicht vergessen, dass diese Forderung nicht nur von den Five Eyes gestellt werden wird, sollte es zu einer Umsetzung durch Regierungen kommen. Die Vereinten Nationen führen momentan eine Liste von 206 Mitgliedsstaaten. Die Forderungen der Five Eyes werden dann von den "206 Eyes" auch gestellt werden. Politisch Verantwortliche sind sehr gut beraten, die Warnungen von Expertinnen nicht zu ignorieren. Stimmt man der Forderung nach Hintertüren zu, so müssen die Geheimdienste der Five Eyes dann auch den Diensten Europas, Russlands, Chinas und Nordkoreas jeweils ihre eigene nationale Kommunikation offenlegen, denn die Mathematik der Sicherheit oder Unsicherheit gilt für alle gleichermaßen. Die Forderung hat daher mit der Realität rein gar nichts zu tun, mit Informationssicherheit schon gar nicht.

Lösungen nicht im Monolog möglich

Sicherheitsforscher sitzen im selben Boot wie die Behörden. Auch sie müssen Angreifer finden und müssen mit oder gegen Schutzmaßnahmen arbeiten. Dennoch rücken IEEE, IETF und alle technischen Organisationen nicht von der Forderung nach starker Sicherheit ab. Da die Five Eyes Forderungen explizit legislative Maßnahmen ansprechen, ist das ein wertvolles Kompliment für die Techniker. Das bedeutet, dass die technische Umsetzung nur sehr schwer oder mit den derzeit verfügbaren Mitteln nicht angreifbar ist.

Die Implementation von Sicherheit ist immer ein Ergebnis interdisziplinärer Zusammenarbeit. Genau aus diesem Grund möchte die DeepSec Konferenz jährlich Vertreter aus Forschung, Behörden, Wirtschaft und der internationalen Hacker Community an einen Tisch bringen. Eine vernetzte Welt benötigt vernetztes Denken. Insellösungen oder kurzfristige Maßnahmen sind nicht zukunftsgerichtet. Daher hat die diesjährige DeepSec Konferenz ihren Schwerpunkt auf Infrastruktur, Internet der Dinge, Mobilität (sei es Funk, Gerät oder Transport) und auch Kryptographie gelegt. Spezialisten aus vier Kontinenten tauschen sich im November in Wien aus, um Bedrohungen der Zukunft zu begegnen. Wir freuen uns auf konstruktive Zusammenarbeit und Ihren Besuch.

Quellen, Programm und Buchung

Die DeepSec Konferenztage sind am 29. und 30. November. Die Trainings finden an den zwei vorangehenden Tagen, dem 27. und 28. November statt. Der Veranstaltungsort ist das Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Sie finden das aktuelle Programm unter dem Link: https://deepsec.net/schedule.html

James Bamford hat in der Publikation "In-Depth Security - Proceedings of the DeepSec Conferences Volume 2" seinen Vortrag als Artikel mit dem Titel "A Death in Athens - The Inherent Vulnerability of "Lawful Intercept"" zusammengefasst. Das Buch ist im Handel und über die DeepSec Konferenz zu beziehen (es kann direkt bei der DeepSec GmbH bestellt werden). Sein Vortrag ist online unter https://vimeo.com/150691584 als Video einsehbar.

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

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

https://www.pressetext.com/news/20180904010

Bug Bounty Programme - Sicherheitslücken als lohnende Investition

DeepSec Konferenz bietet Weiterbildung für Sicherheitsforscher an

Wien (pts010/04.09.2018/08:30) - Die DeepSec In-Depth Security Konferenz bietet neben Vorträgen zum Versagen von Sicherheitsmaßnahmen dieses Jahr einen Workshop für das Finden von Schwachstellen an. Das Testen von Software im Rahmen der Qualitätssicherung reicht in der modernen, vernetzen Welt leider nicht mehr aus. Die Vorsilbe "Smart" ändert nichts an bestehenden Schwächen. Der Kurs richtet sich daher an Fachkräfte, die bereits in der Entwicklung arbeiten, und Sicherheitsexperten, um gezielt die Entwicklung sicherer Produkte in Industrie und Unternehmen zu stärken.

Komplexe Technologien und ihre Fehleranfälligkeit

Moderne Produkte kommen nicht erst seit der Geburt des Internet der Dinge nicht ohne Software aus. Fügt man Vernetzung und eine hohe Komplexität der Einzelteile hinzu, so ist dies ein Erfolgsrezept für Fehler. Natürlich gibt es oft eine Qualitätssicherung und Prüfungen auf die wichtigsten Funktionen, jedoch ist die Folge von schwerwiegenden Fehlfunktionen durch den Umfang der Codezeilen eine Frage der Statistik. Wie können sich Hersteller und Entwickler helfen? Zieht man die mathematische Spieltheorie zu Rate, so ist die Antwort: Kopfgeld für Fehler - Bug Bounties als Belohnung.

Organisierte Jagd nach Softwarefehlern

Die Bug Bounty Programme wurden vor einigen Jahren als feste Institution ins Leben gerufen, um einerseits Sicherheitsforscherinnen die Möglichkeit zu geben, ihre Arbeit beim Finden und Suchen von Fehlern zu würdigen. Auf der anderen Seite regelt ein solches Programm automatisch den Ablauf wie kritische Fehler gemeldet, dokumentiert, reproduziert und seitens der zuständigen Entwicklerinnen behoben werden. Es gibt leider immer noch sehr viele Hersteller, die nicht auf gemeldete Fehler reagieren und keine Updates zur Verfügung stellen. Das Anbieten von Bug Bounties spricht daher für das Engagement eines Unternehmens und sichert die Qualität der eigenen Produkte. Obendrein erfährt man dann vom Versagen des eigenen Produkts nicht aus der Presse oder aus dem Internet.

Der große Vorteil ist die gute Qualität der Fehlerberichte. Fehler in Software finden ist das tägliche Brot der Softwareentwicklung, aber kritische Schwachstellen, die ein Sicherheitsproblem darstellen, erkennt man oft nicht sofort. Die Informationssicherheit ist ein interdisziplinärer Bereich der Informatik, welche Fähigkeiten in Softwareentwick-

lung, Mathematik, Reverse Engineering (sprich die Nachkonstruktion einer Applikation oder eines Protokolls) und viel Geduld erfordert. Dazu ist fundiertes Wissen, ausreichend Erfahrung und eine gezielte Ausbildung erforderlich, die nicht alle im Entwicklungsteam besitzen.

Die Bug Bounty Programme werden sehr gut angenommen. HackerOne, eine Plattform zur koordinierten Publikation von Schwachstellen, führt Buch über die Ausschüttungen an Entdecker von Fehlern. Derzeit wurden in Summe über 20 Millionen US Dollar an Forscherinnen von verschiedenen Firmen ausgezahlt. Das erklärte Ziel ist das Erreichen von 100 Millionen US Dollar bis 2020.

Ausbildung zum Bug Bounty Hunter

Dies diesjährige DeepSec Sicherheitskonferenz hat einen zweitägigen Kurs zum Thema Bug Hunting. Der Trainer Dawid Czagan, selbst unter den Top 10 der Bug Hunter Liste von HackerOne, hat ein Curriculum ausgearbeitet, welches Fortgeschrittenen mit Kenntnissen von Praktiken der Softwareentwicklung die Ansätze und Denkweise von Sicherheitsexperten beibringt. Teilnehmerinnen lernen wie die vielen Teile von modernen Anwendungen wechselwirken, wo man in Protokolle zur Analyse einsteigt und worauf man achten muss. Da viele Arbeiten mittlerweile über Weboberflächen stattfinden, sei es sichtbar für den Benutzer oder unsichtbar hinter den Kulissen, wird die Webtechnologie der Fokus des Kurses sein. Dabei geht es nicht nur um die Kopfgeldjagd.

Der Workshop besteht nicht nur aus trockener Theorie. Dawid Czagan hat Fallbeispiele aus produktiven Umgebungen vorbereitet, um die verschiedenen Klassen von Fehler zu illustrieren. Der komplette Kurs ist eine Mischung aus kurzem Vortrag zur Erklärung gefolgt von praktischen Übungen, um das neu erworbene Wissen zu festigen. Die vermittelten Fähigkeiten sind eine wertvolle Ergänzung für jede Qualitätssicherung und eine gefragte Weiterbildung für Entwicklerinnen. Die Veranstaltung richtet sich gezielt an Sicherheitsforscherinnen, Penetration Tester, Consultants, Projektleiterinnen/Entwickler aus der Softwareentwicklung und IT-Architekten, die grundlegende Designs entwerfen, auf dem Anwendungen und Systeme aufbauen.

Die Angreifer haben diese Mittel schon. Es wird Zeit, dass Sie aufholen. Vernetzte Systeme schlafen nie.

Programm und Buchung

Die DeepSec Konferenztage sind am 29. und 30. November. Die Trainings finden an den zwei vorangehenden Tagen, dem 27. und 28. November, statt. Der Veranstaltungsort ist Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Sie finden das aktuelle Programm unter dem Link: https://deepsec.net/schedule.html

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

Das Blog der Konferenz mit neuen Informationen und Hintergründen zu den Vorträgen und Workshop finden Sie unter der Adresse: https://blog.deepsec.net

Aussender: DeepSec GmbH

Ansprechpartner: René Pfeiffer

Tel.: +43-676-5626390

E-Mail: deepsec@deepsec.net

Website: deepsec.net

pts20180904010 Computer/Telekommunikation, Produkte/Innovationen

Bug Bounty Programme - Sicherheitslücken als lohnende Investition

DeepSec Konferenz bietet Weiterbildung für Sicherheitsforscher an

Wien (pts010/04.09.2018/08:30) - **Die DeepSec In-Depth Security Konferenz bietet neben Vorträgen zum Versagen von Sicherheitsmaßnahmen dieses Jahr einen Workshop für das Finden von Schwachstellen an. Das Testen von Software im Rahmen der Qualitätssicherung reicht in der modernen, vernetzen Welt leider nicht mehr aus. Die Vorsilbe "Smart" ändert nichts an bestehenden Schwächen. Der Kurs richtet sich daher an Fachkräfte, die bereits in der Entwicklung arbeiten, und Sicherheitsexperten, um gezielt die Entwicklung sicherer Produkte in Industrie und Unternehmen zu stärken.**

Komplexe Technologien und ihre Fehleranfälligkeit

Moderne Produkte kommen nicht erst seit der Geburt des Internet der Dinge nicht ohne Software aus. Fügt man Vernetzung und eine hohe Komplexität der Einzelteile hinzu, so ist dies ein Erfolgsrezept für Fehler. Natürlich gibt es oft eine Qualitätssicherung und Prüfungen auf die wichtigsten Funktionen, jedoch ist die Folge von schwerwiegenden Fehlfunktionen durch den Umfang der Codezeilen eine Frage der Statistik. Wie können sich Hersteller und Entwickler helfen? Zieht man die mathematische Spieltheorie zu Rate, so ist die Antwort: Kopfgeld für Fehler - Bug Bounties als Belohnung.

Organisierte Jagd nach Softwarefehlern

Die Bug Bounty Programme wurden vor einigen Jahren als feste Institution ins Leben gerufen, um einerseits Sicherheitsforscherinnen die Möglichkeit zu geben, ihre Arbeit beim Finden und Suchen von Fehlern zu würdigen. Auf der anderen Seite regelt ein solches Programm automatisch den Ablauf wie kritische Fehler gemeldet, dokumentiert, reproduziert und seitens der zuständigen Entwicklerinnen behoben werden. Es gibt leider immer noch sehr viele Hersteller, die nicht auf gemeldete Fehler reagieren und keine Updates zur Verfügung stellen. Das Anbieten von Bug Bounties spricht daher für das Engagement eines Unternehmens und sichert die Qualität der eigenen Produkte. Obendrein erfährt man dann vom Versagen des eigenen Produkts nicht aus der Presse oder aus dem Internet.

Der große Vorteil ist die gute Qualität der Fehlerberichte. Fehler in Software finden ist das tägliche Brot der Softwareentwicklung, aber kritische Schwachstellen, die ein Sicherheitsproblem darstellen, erkennt man oft nicht sofort. Die Informationssicherheit ist ein interdisziplinärer Bereich der Informatik, welche Fähigkeiten in Softwareentwicklung, Mathematik, Reverse Engineering (sprich die Nachkonstruktion einer Applikation oder eines Protokolls) und viel Geduld erfordert. Dazu ist fundiertes Wissen, ausreichend Erfahrung und eine gezielte Ausbildung erforderlich, die nicht alle im Entwicklungsteam besitzen.

Die Bug Bounty Programme werden sehr gut angenommen. HackerOne, eine Plattform zur koordinierten Publikation von Schwachstellen, führt Buch über die Ausschüttungen an Entdecker von Fehlern. Derzeit wurden in Summe über 20 Millionen US Dollar an Forscherinnen von verschiedenen Firmen ausgezahlt. Das erklärte Ziel ist das Erreichen von 100 Millionen US Dollar bis 2020.

Ausbildung zum Bug Bounty Hunter

Dies diesjährige DeepSec Sicherheitskonferenz hat einen zweitägigen Kurs zum Thema Bug Hunting. Der Trainer Dawid Czagan, selbst unter den Top 10 der Bug Hunter Liste von HackerOne, hat ein Curriculum ausgearbeitet, welches Fortgeschrittenen mit Kenntnissen von Praktiken der Softwareentwicklung die Ansätze und Denkweise von Sicherheitsexperten beibringt. Teilnehmerinnen lernen wie die vielen Teile von modernen Anwendungen wechselwirken, wo man in Protokolle zur Analyse einsteigt und worauf man achten muss. Da viele Arbeiten mittlerweile über Weboberflächen stattfinden, sei es sichtbar für den Benutzer oder unsichtbar hinter den Kulissen, wird die Webtechnologie der Fokus des Kurses sein. Dabei geht es nicht nur um die Kopfgeldjagd.

Der Workshop besteht nicht nur aus trockener Theorie. Dawid Czagan hat Fallbeispiele aus produktiven Umgebungen vorbereitet, um die verschiedenen Klassen von Fehler zu illustrieren. Der komplette Kurs ist eine Mischung aus kurzem Vortrag zur Erklärung gefolgt von praktischen Übungen, um das neu erworbene Wissen zu festigen. Die vermittelten Fähigkeiten sind eine wertvolle Ergänzung für jede Qualitätssicherung und eine gefragte Weiterbildung für Entwicklerinnen. Die Veranstaltung richtet sich gezielt an Sicherheitsforscherinnen, Penetration Tester, Consultants, Projektleiterinnen/Entwickler aus der Softwareentwicklung und IT-Architekten, die grundlegende Designs entwerfen, auf dem Anwendungen und Systeme aufbauen.

Die Angreifer haben diese Mittel schon. Es wird Zeit, dass Sie aufholen. Vernetzte Systeme schlafen nie.

Programm und Buchung

Die DeepSec Konferenztage sind am 29. und 30. November. Die Trainings finden an den zwei vorangehenden Tagen, dem 27. und 28. November, statt. Der Veranstaltungsort ist Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Sie finden das aktuelle Programm unter dem Link: https://deepsec.net/schedule.html

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

Das Blog der Konferenz mit neuen Informationen und Hintergründen zu den Vorträgen und Workshop finden Sie unter der Adresse: https://blog.deepsec.net

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

https://www.pressetext.com/news/20180821014

DeepSec Konferenz veröffentlicht Programm für 2018

Unsicherheit der Dinge und Infrastruktur stehen im Fokus

Wien (pts014/21.08.2018/09:25) - Die DeepSec In-Depth Security Konferenz widmet sich in diesem Jahr dem Thema Insecurity of Things (IoT) und Komponenten alltäglicher Infrastruktur. Die stetig voranschreitende Vernetzung eröffnet Angreifern völlig neue Wege - schneller, als Entwickler und Hersteller Fehler beheben können. Statt Secure Design bei Produkten und Code einzusetzen, integriert man Machine Learning und Künstliche Intelligenz - leider implementiert durch passende Statistik und den Algorithmus der Woche aus dem Tagesmenü des Entwicklungsbaukastens. Die Vorträge auf der DeepSec Konferenz werden daher die vermeintlichen Techniken der Zukunft auf den Prüfstand stellen. Mobilfunknetzwerke, das Internet der Dinge, Kollaborationsplattformen in der Cloud, Customer Relationship Management Systeme und der Faktor Mensch stehen im Fadenkreuz.

Smart is the new Cyber

Die Informationstechnologie hat den berechtigten Ruf ständig neue Begriffe und Akronyme zu erfinden um Lösungen für technische Probleme vorzugaukeln. Meist handelt es sich um ein reines Versteckspiel, sehr gut illustriert durch die Schlagworte Cyber, Cloud und Virtual. Hinter den Kulissen sind einige Begriffe berechtigt, aber kaum jemand prüft was sich hinter einem Produkt wirklich versteckt. Bestes Beispiel ist der Trend nun alles Smart zu machen, ganz egal ob Sicherheit ein Designkriterium war oder nicht. Die Stromversorgung soll zum Smart Grid werden, Fragenkataloge werden zum Smart Assistant, etc.

Ein Blick ins Innere offenbart Komponenten, die oft ohne ein Konzept von Sicherheit irgendwie miteinander verbunden werden. Das beste Beispiel sind Smartphones, die zum Universalschlüssel mutiert sind. Auf einem einzigen Gerät befindet sich eine Vielzahl von Zugängen, die bestimmte Apps benötigen. Damit werden diese Gegenstände automatisch zu einem begehrten Angriffsziel. Im Workshop Mobile App Attacks 2.0 wird gezeigt, wie man Apps und die Smartphone Plattform als Basis für erfolgreiche Angriffe verwendet. Und auch ein Workshop zum Thema Mobilfunksicherheit ist Teil des Programms. Der Trainer David Burgess ist ein Veteran auf diesem Gebiet und hat schon 2009 auf der DeepSec schwere Sicherheitslücken in Mobilfunknetzen entdeckt und dokumentiert. Dieses Jahr ist er wieder auf der DeepSec und kann auch etwas zu den neuen Standards sagen.

Unsicherheit der Dinge überall

Sicherheitslücken von Gegenständen aus dem Internet of Things (IoT) werden in Vorträgen und Workshops ebenso

vorgestellt und analysiert. Johannes Pohl zeigt in seinem Training vor, wie man die Kommunikation von IoT Geräten analysiert. Diese Arbeit dient als Basis für daraus abgeleitete Angriffe. Wenige Hersteller sind wirklich in der Lage eine sichere Kommunikation als Protokoll zu entwerfen und zu implementieren, unabhängig ob das Protokoll neu erdacht ist oder auf etablierten Standards beruht.

Werner Schober, Sicherheitsforscher der Firma SEC Consult, stellt in seinem Vortrag Schwachstellen von "smartem" Sexspielzeug vor. Was wie ein schlechter Scherz klingt, ist leider keiner. Alle IoT-Geräte jeder Branche sind eine Gefahr. Da in Casinos schon über ein vernetztes Aquarium eingebrochen wurde, spielt der ursprüngliche Zweck des Gerät keine Rolle. Speziell bei Sexspielzeugen ist zusätzlich die Disziplin regelmäßiger Updates der Firmware betreffend sicher geringer als beim "smarten" Fernseher. Damit werden diese Gegenstände automatisch zu einem Risiko für Sicherheit und Privatsphäre zugleich. Im Alltag lassen sich mittlerweile zahllose weitere Dinge aufzählen, die für Angriffe auf Informationssysteme verwendet werden können.

Faktor Mensch

Egal welche Technologie man einsetzt, der Faktor Mensch bleibt wichtiger Teil der Informationssicherheit. Auch der menschliche Körper wird vernetzt. Ulrike Hugl von der Universität Innsbruck thematisiert implantierte RFID (radio-frequency identification) Chips. Mit solchen Fremdkörpern ist man dann selbst Teil von Fragen über Datensicherheit und Angriffen durch Dritte, denn RFID Komponenten tragen Daten und können ausgelesen werden. Behandelt werden Verbreitung, Nutzung und ethische Fragestellungen.

Darüber hinaus gibt es Vorträge zum Thema Bedrohungsanalyse, die ein wichtiger Teil der digitalen Verteidigung ist. Sie wird oft durch automatische Prozesse durchgeführt. Im Vortrag wird die Grenze zu den Fähigkeiten menschlicher Experten gezogen und wie man diese durch automatisierte Systeme unterstützen kann. Stefan Schumacher beleuchtet in seiner Präsentation wie sich das menschliche Gehirn manipulieren lässt und wie man mit Methoden die auf diesem Wissen basieren Social Engineering Angriffe umsetzen kann. Die meisten erfolgreichen Attacken verwenden immer eine Komponente, die den Faktor Mensch berührt.

Interdisziplinär und Verbindung zur Forschung

Die Informationssicherheit kommt aktuell nicht nur mit Technik alleine weiter. Sicherheitsprobleme müssen immer in einem interdisziplinären Team untersucht und gelöst werden. Das bedeutet, dass die DeepSec In-Depth Security Konferenz für ein Spektrum aus Forschung, Lehre, Industrie, Behörden und Unternehmen gedacht ist. Genau wie im letzten Jahr haben Besucherinnen und Besucher auch die Möglichkeit Vorträge des parallel stattfindenden Reversing and Offensive-oriented Trends Symposiums zu besuchen.

ROOTS ist ein akademischer Workshop, welcher parallel ort- und zeitgleich mit der DeepSec stattfindet. Der Anspruch ist es, zu zeigen, dass durch die Kombination von Wissenschaft und Informationstechnologie, und durch die Kombination von professionellem Insiderwissen, akademischer Forschung und praktischen Ansätzen, moderne digitale Infrastruktur besser als je zuvor verteidigt werden kann.
Nutzen Sie die Gelegenheit.

Programm und Buchung
Die DeepSec Konferenztage sind am 29. und 30. November. Die Trainings finden an den zwei vorangehenden Tagen, dem 27. und 28. November, statt. Der Veranstaltungsort ist Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Sie finden das aktuelle Programm unter dem Link: https://deepsec.net/schedule.html

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

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

pts20180821014 Computer/Telekommunikation, Unternehmen/Finanzen

DeepSec Konferenz veröffentlicht Programm für 2018

Unsicherheit der Dinge und Infrastruktur stehen im Fokus

Wien (pts014/21.08.2018/09:25) - **Die DeepSec In-Depth Security Konferenz widmet sich in diesem Jahr dem Thema Insecurity of Things (IoT) und Komponenten alltäglicher Infrastruktur. Die stetig voranschreitende Vernetzung eröffnet Angreifern völlig neue Wege - schneller, als Entwickler und Hersteller Fehler beheben können. Statt Secure Design bei Produkten und Code einzusetzen, integriert man Machine Learning und Künstliche Intelligenz - leider implementiert durch passende Statistik und den Algorithmus der Woche aus dem Tagesmenü des Entwicklungsbaukastens. Die Vorträge auf der DeepSec Konferenz werden daher die vermeintlichen Techniken der Zukunft auf den Prüfstand stellen. Mobilfunknetzwerke, das Internet der Dinge, Kollaborationsplattformen in der Cloud, Customer Relationship Management Systeme und der Faktor Mensch stehen im Fadenkreuz.**

Smart is the new Cyber

Die Informationstechnologie hat den berechtigten Ruf ständig neue Begriffe und Akronyme zu erfinden um Lösungen für technische Probleme vorzugaukeln. Meist handelt es sich um ein reines Versteckspiel, sehr gut illustriert durch die Schlagworte Cyber, Cloud und Virtual. Hinter den Kulissen sind einige Begriffe berechtigt, aber kaum jemand prüft was sich hinter einem Produkt wirklich versteckt. Bestes Beispiel ist der Trend nun alles Smart zu machen, ganz egal ob Sicherheit ein Designkriterium war oder nicht. Die Stromversorgung soll zum Smart Grid werden, Fragenkataloge werden zum Smart Assistant, etc.

Ein Blick ins Innere offenbart Komponenten, die oft ohne ein Konzept von Sicherheit irgendwie miteinander verbunden werden. Das beste Beispiel sind Smartphones, die zum Universalschlüssel mutiert sind. Auf einem einzigen Gerät befindet sich eine Vielzahl von Zugängen, die bestimmte Apps benötigen. Damit werden diese Gegenstände automatisch zu einem begehrten Angriffsziel. Im Workshop Mobile App Attacks 2.0 wird gezeigt, wie man Apps und die Smartphone Plattform als Basis für erfolgreiche Angriffe verwendet. Und auch ein Workshop zum Thema Mobilfunksicherheit ist Teil des Programms. Der Trainer David Burgess ist ein Veteran auf diesem Gebiet und hat schon 2009 auf der DeepSec schwere Sicherheitslücken in Mobilfunknetzen entdeckt und dokumentiert. Dieses Jahr ist er wieder auf der DeepSec und kann auch etwas zu den neuen Standards sagen.

Unsicherheit der Dinge überall

Sicherheitslücken von Gegenständen aus dem Internet of Things (IoT) werden in Vorträgen und Workshops ebenso vorgestellt und analysiert. Johannes Pohl zeigt in seinem Training vor, wie man die Kommunikation von IoT Geräten analysiert. Diese Arbeit dient als Basis für daraus abgeleitete Angriffe. Wenige Hersteller sind wirklich in der Lage eine sichere Kommunikation als Protokoll zu entwerfen und zu implementieren, unabhängig ob das Protokoll neu erdacht ist oder auf etablierten Standards beruht.

Werner Schober, Sicherheitsforscher der Firma SEC Consult, stellt in seinem Vortrag Schwachstellen von "smartem" Sexspielzeug vor. Was wie ein schlechter Scherz klingt, ist leider keiner. Alle IoT-Geräte jeder Branche sind eine Gefahr. Da in Casinos schon über ein vernetztes Aquarium eingebrochen wurde, spielt der

ursprüngliche Zweck des Gerät keine Rolle. Speziell bei Sexspielzeugen ist zusätzlich die Disziplin regelmäßiger Updates der Firmware betreffend sicher geringer als beim "smarten" Fernseher. Damit werden diese Gegenstände automatisch zu einem Risiko für Sicherheit und Privatsphäre zugleich. Im Alltag lassen sich mittlerweile zahllose weitere Dinge aufzählen, die für Angriffe auf Informationssysteme verwendet werden können.

Faktor Mensch

Egal welche Technologie man einsetzt, der Faktor Mensch bleibt wichtiger Teil der Informationssicherheit. Auch der menschliche Körper wird vernetzt. Ulrike Hugl von der Universität Innsbruck thematisiert implantierte RFID (radio-frequency identification) Chips. Mit solchen Fremdkörpern ist man dann selbst Teil von Fragen über Datensicherheit und Angriffen durch Dritte, denn RFID Komponenten tragen Daten und können ausgelesen werden. Behandelt werden Verbreitung, Nutzung und ethische Fragestellungen.

Darüber hinaus gibt es Vorträge zum Thema Bedrohungsanalyse, die ein wichtiger Teil der digitalen Verteidigung ist. Sie wird oft durch automatische Prozesse durchgeführt. Im Vortrag wird die Grenze zu den Fähigkeiten menschlicher Experten gezogen und wie man diese durch automatisierte Systeme unterstützen kann. Stefan Schumacher beleuchtet in seiner Präsentation wie sich das menschliche Gehirn manipulieren lässt und wie man mit Methoden die auf diesem Wissen basieren Social Engineering Angriffe umsetzen kann. Die meisten erfolgreichen Attacken verwenden immer eine Komponente, die den Faktor Mensch berührt.

Interdisziplinär und Verbindung zur Forschung

Die Informationssicherheit kommt aktuell nicht nur mit Technik alleine weiter. Sicherheitsprobleme müssen immer in einem interdisziplinären Team untersucht und gelöst werden. Das bedeutet, dass die DeepSec In-Depth Security Konferenz für ein Spektrum aus Forschung, Lehre, Industrie, Behörden und Unternehmen gedacht ist. Genau wie im letzten Jahr haben Besucherinnen und Besucher auch die Möglichkeit Vorträge des parallel stattfindenden Reversing and Offensive-oriented Trends Symposiums zu besuchen.

ROOTS ist ein akademischer Workshop, welcher parallel ort- und zeitgleich mit der DeepSec stattfindet. Der Anspruch ist es, zu zeigen, dass durch die Kombination von Wissenschaft und Informationstechnologie, und durch die Kombination von professionellem Insiderwissen, akademischer Forschung und praktischen Ansätzen, moderne digitale Infrastruktur besser als je zuvor verteidigt werden kann.
Nutzen Sie die Gelegenheit.

Programm und Buchung

Die DeepSec Konferenztage sind am 29. und 30. November. Die Trainings finden an den zwei vorangehenden Tagen, dem 27. und 28. November, statt. Der Veranstaltungsort ist Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

Sie finden das aktuelle Programm unter dem Link: https://deepsec.net/schedule.html

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

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

DeepSec Press Release 02/ 2018

23.03.2018

DeepSec In-Depth Security Conference Europe

27th to 30th November 2018

The Imperial Riding School Vienna, Austria

DEEPSEC MISSION STATEMENT

INTERNATIONAL, TRANS- & INTERDISCIPLINARY

We believe that security problems need to be addressed by a wide variety of experts with interdisciplinary skills. We want to encourage individuals, organizations and governments to meet and exchange, to improve the overall state of security and trust.

NEUTRAL GROUND

Our conference is an annual event where we can openly talk about ideas and points of view. It is the best place to get together informally, create new ideas, discuss a project, develop new contacts, get inspiration for your business and meet new friends.

USER FRIENDLY

The DeepSec In-Depth Security Conference is a non-product, non-vendor-biased conference. DeepSec is all about facts not ads. We are looking for serious talks about security:
If something breaks, tell us about it. If you can repair it, tell us about it. If you've discovered something, tell us about it. Be thorough, be honest. That's our goal.

FOCUSED ON NOVELTY, QUALITY & IMPACT

We focus only on novelty, quality and relevance when selecting talks & workshops for our conference.
We prefer to invite a newcomer to the stage if the content is more promising than the "safe choice" of well-known topics or standard presentations.

HERE TO SCOUT & SUPPORT

We actively scout and contact women who do research and projects in the field of information security. And we launched our special U21 initiative to support young researchers and

enable them to present their works and results in an appropriate manner.

… about René Pfeiffer

...is involved with cryptography and information security for over 20 years.

He is one of the organizers of DeepSec, Vienna's very own IT-Security Conference, known for bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community.

… a little Q+A

Mr. Pfeiffer please tell us about your conference.

The DeepSec In-Depth Security Conference is an annual European two-day in-depth conference on computer, network, and application security. Our goal is to bring together the leading security experts from all over the world.

How did it all start?

DeepSec was founded in 2007. The vision was to create an IT security conference right in the heart of Europe and use it as a neutral ground where professionals from academics, government, industry, and the underground hacking community can meet and exchange ideas.

What's special about DeepSec?

DeepSec is small compared to other events having thousands of participants. This is a dedicated advantage, because you can actually meet and talk to everyone. Furthermore we try to present a mix of talks connecting different aspects of information security. It's not always about technology. There's psychology, legal frameworks, human behaviour, and much more also at play.

Is there a matter particularly close to your heart?

We want to break down the barriers between technical and nontechnical experts. While information security will always have a strong technical component, it is paramount to foster collaboration.

Even decades ago network security wasn't implemented by one person alone. You need teams, you need to communicate, and you need creative ways of looking at your problems. If you want information security, you need to talk to others. No one is a cyber island.

IT-Security is a very delicate matter. Aren`t you afraid to offend someone?

DeepSec was the first conference to feature a talk about the broken GSM A5 encryption. When the talk went live we were certainly a bit nervous. The GSM A5 algorithm family is responsible for encryption of the voice calls between

mobile phones and the cells receiving their signals. GSM networks all over the world have billions of devices connected to it. Any vulnerability or design flaw affects a huge base of customers and companies, so having talks touching these big networks should not be taken lightly.However: We want to get the news out when it comes to vulnerabilities. Scientific research knows no controversy.

The next DeepSec is in November: What are you personally looking forward to the most?
Everything :) To meet our speakers, trainers and attendees and to discuss with them the state of affairs in information security. The world looks different after every DeepSec conference because of
the many new perspectives and insights one gets while talking to creative and brilliant minds.

What about the future?
Information security has grown: it touches all aspects of our lives. Once networks enter home, office and recreational environments, so does information security. The Internet of Things is becoming a reality - and a serious threat.We are confident that information security is here to stay.
The same is true for the DeepSec conference.

Year by year we adapt to the changes and include topics in the conference schedule. We have addressed mobile phone networks, Bluetooth connected devices, “cloud” technology, and many more issues in the past. In 2014 we selected smartphones, devious backdoors in hardware, wireless networks, the new IPv6 technology, and how to educate “new” hackers. DeepSec 2015 was all about the Internet, IT-Security, Digital Espionage and International Agreements; DeepSec 2016 about new challenges to information security, cryptography and infrastructure. DeepSec 2017 featured Science First! and DeepSec 2018 will deal with all aspects of mobility from electric cars to mobile data and the Internet of Data. We’ll keep you posted and are already looking forward to this years event :) Stay tuned!

Do you wanna know more?

DeepSec GmbH
eMail: deepsec@deepsec.net
Voice: +43 676 562 63 90
Web: https://deepsec.net
Blog: http://blog.deepsec.net

PRESS RELEASE 02

DEEPSEC 2018

DEEPSEC Mission Statement

INTERNATIONAL, TRANS- & INTERDISCIPLINARY

We believe that security problems need to be addressed by a wide variety of experts with interdisciplinary skills. We want to encourage individuals, organizations and governments to meet and exchange, to improve the overall state of security and trust.

NEUTRAL GROUND

Our conference is an annual event where we can openly talk about ideas and points of view. It is the best place to get together informally, create new ideas, discuss a project, develop new contacts, get inspiration for your business and meet new friends.

USER FRIENDLY

The DeepSec In-Depth Security Conference is a non-product, non-vendor-biased conference. DeepSec is all about facts not ads. We are looking for serious talks about security:

If something breaks, tell us about it. If you can repair it, tell us about it. If you've discovered something, tell us about it. Be thorough, be honest. That's our goal.

FOCUSED ON NOVELTY, QUALITY & IMPACT

We focus only on novelty, quality and relevance when selecting talks & workshops for our conference.
We prefer to invite a newcomer to the stage if the content is more promising than the "safe choice" of well-known topics or standard presentations.

HERE TO SCOUT & SUPPORT

We actively scout and contact women who do research and projects in the field of information security. And we launched our special U21 initiative to support young researchers and enable them to present their works and results in an appropriate manner.

DEEPSEC IN-DEPTH SECURITY CONFERENCE EUROPE
27TH TO 30TH NOVEMBER 2018
THE IMPERIAL RIDING SCHOOL VIENNA, AUSTRIA

...about

René Pfeiffer

...is involved with cryptography and information security for over 20 years.
He is one of the organizers of DeepSec, Vienna's very own IT-Security Conference, known for bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community.

...a little Q+A

Mr. Pfeiffer please tell us about your conference.

The DeepSec In-Depth Security Conference is an annual European two-day in-depth conference on computer, network, and application security. Our goal is to bring together the leading security experts from all over the world.

How did it all start?

DeepSec was founded in 2007. The vision was to create an IT security conference right in the heart of Europe and use it as a neutral ground where professionals from academics, government, industry, and the underground hacking community can meet and exchange ideas.

What's special about DeepSec?

DeepSec is small compared to other events having thousands of participants. This is a dedicated advantage, because you can actually meet and talk to everyone. Furthermore we try to present a mix of talks connecting different aspects of information security. It's not always about technology. There's psychology, legal frameworks, human behaviour, and much more also at play.

Is there a matter particularly close to your heart?

We want to break down the barriers between technical and non-technical experts. While information security will always have a strong technical component, it is paramount to foster collaboration. Even decades ago network security wasn't implemented by one person alone. You need teams, you need to communicate, and you need creative ways of looking at your problems. If you want information security, you need to talk to others. No one is a cyber island.

IT-Security is a very delicate matter. Aren't you afraid to offend someone?

DeepSec was the first conference to feature a talk about the broken GSM A5 encryption. When the talk went live we were certainly a bit nervous. The GSM A5 algorithm family is responsible for encryption of the voice calls between mobile phones and the cells receiving their signals. GSM networks all over the world have billions of devices connected to it. Any vulnerability or design flaw affects a huge base of customers and companies, so having talks touching these big networks should not be taken lightly.However: We want to get the news out when it comes to vulnerabilities. Scientific research knows no controversy.

The next DeepSec is in November: What are you personally looking forward to the most?

Everything :) To meet our speakers, trainers and attendees and to discuss with them the state of affairs in information security. The world looks different after every DeepSec conference because of the many new perspectives and insights one gets while talking to creative and brilliant minds.

What about the future?

Information security has grown: it touches all aspects of our lives. Once networks enter home, office and recreational environments, so does information security. The Internet of Things is becoming a reality - and a serious threat.We are confident that information security is here to stay.
The same is true for the DeepSec conference.

Year by year we adapt to the changes and include topics in the conference schedule. We have addressed mobile phone networks, Bluetooth connected devices, “cloud” technology, and many more issues in the past. In 2014 we selected smartphones, devious backdoors in hardware, wireless networks, the new IPv6 technology, and how to educate “new” hackers. DeepSec 2015 was all about the Internet, IT-Security, Digital Espionage and International Agreements; DeepSec 2016 about new challenges to information security, cryptography and infrastructure.
DeepSec 2017 featured Science First! and DeepSec 2018 will deal with all aspects of mobility from electric cars to mobile data and the Internet of Data. We’ll keep you posted and are already looking forward to this years event :) Stay tuned!

DeepSec GmbH
eMail: deepsec@deepsec.net
Voice: +43 676 562 63 90
Web: https://deepsec.net
Blog: http://blog.deepsec.net

...contact

DeepSec Press Release 01 / 2018

25.01.2018

…about

DEEPSEC

IN-DEPTH SECURITY CONFERENCE 2018 EUROPE

27th to 30th November 2018

The Imperial Riding School Hotel

Vienna, Austria

DEEPSEC TOP 5 FACTS:

INTERNATIONAL, TRANS- & INTERDISCIPLINARY

NEUTRAL GROUND

USER FRIENDLY

FOCUSED ON NOVELTY, QUALITY & IMPACT

HERE TO SCOUT & SUPPORT

INTERNATIONAL, TRANS- & INTERDISCIPLINARY

We believe that security problems need to be addressed by a wide variety of experts with interdisciplinary skills.

We want to encourage individuals, organizations and governments to meet and exchange, to improve the overall state of security and trust.

Diversity is a key aspect of information security.

A look through the tunnel of highly specialised expert knowledge always misses the details.

Security is interdisciplinary, and thus the body of wisdom needs to be diverse as well.

NEUTRAL GROUND

Our conference is an annual event where we can openly talk about ideas and points of view.

It is the best place to get together informally, create new ideas, discuss a project, develop new contacts, get inspiration for your business and meet new friends.

USER FRIENDLY

The DeepSec In-Depth Security Conference is a non-product, non-vendor-biased event.We are looking for serious talks about security: If something breaks, tell us about it. If you can repair it, tell us about it. If you've discovered something, tell us about it. Be thorough, be honest. That's our goal.

FOCUSED ON NOVELTY, QUALITY & IMPACT

We focus only on novelty, quality and relevance when selecting talks & workshops for our conference. We prefer to invite a newcomer to the stage if the content is more promising than the "safe choice" of well-known topics or standard presentations.

HERE TO SCOUT & SUPPORT

We actively scout and contact women who do research and work on projects in the field of information security.

And we launched our special U21 initiative to support young researchers and enable them to present their works and results in an appropriate manner.

DeepSec annually supports new talents who have never been on the stage of a security conference before.

Furthermore, we have a special academic discount programme for students and members of universities. If you want to help young talents by enabling them, please let us know and partner with us!

Do you wanna know more?

DeepSec GmbH

eMail: deepsec@deepsec.net

Voice: +43 676 562 63 90

Web: https://deepsec.net

Blog: http://blog.deepsec.net

PRESS RELEASE 01

DEEPSEC 2018

...about

DEEPSEC
IN-DEPTH SECURITY CONFERENCE 2018 EUROPE
27th to 30th November 2018
The Imperial Riding School Hotel
Vienna, Austria

DEEPSEC TOP 5 FACTS

INTERNATIONAL, TRANS- & INTERDISCIPLINARY

NEUTRAL GROUND

USER FRIENDLY

FOCUSED ON NOVELTY, QUALITY & IMPACT

HERE TO SCOUT & SUPPORT

INTERNATIONAL, TRANS & INTERDISCIPLINARY

We believe that security problems need to be addressed by a wide variety of experts with interdisciplinary skills.

We want to encourage individuals, organizations and governments to meet and exchange, to improve the overall state of security and trust.

Diversity is a key aspect of information security.
A look through the tunnel of highly specialised expert knowledge always misses the details.
Security is interdisciplinary, and thus the body of wisdom needs to be diverse as well.

NEUTRAL GROUND

Our conference is an annual event where we can openly talk about ideas and points of view. It is the best place to get together informally, create new ideas, discuss a project, develop new contacts, get inspiration for your business and meet new friends.

USER FRIENDLY

The DeepSec In-Depth Security Conference is a non-product, non-vendor-biased event.We are looking for serious talks about security: If something breaks, tell us about it. If you can repair it, tell us about it. If you've discovered something, tell us about it. Be thorough, be honest. That's our goal.

FOCUSED ON NOVELTY, QUALITY & IMPACT

We focus only on novelty, quality and relevance when selecting talks & workshops for our conference. We prefer to invite a newcomer to the stage if the content is more promising than the “safe choice” of well-known topics or standard presentations.

HERE TO SCOUT & SUPPORT

We actively scout and contact women who do research and work on projects in the field of information security.

And we launched our special U21 initiative to support young researchers and enable them to present their works and results in an appropriate manner.

DeepSec annually supports new talents who have never been on the stage of a security conference before.

Furthermore, we have a special academic discount programme for students and members of universities.

If you want to help young talents by enabling them, please let us know and partner with us!

DeepSec GmbH
eMail: deepsec@deepsec.net
Voice: +43 676 562 63 90
Web: https://deepsec.net
Blog: http://blog.deepsec.net

...contact

Contact

René Pfeiffer

rpfeiffer@deepsec.net

+43/676/5626390

DeepSec GmbH

c/o Mr. René Pfeiffer

Bräuhausgasse 32

1050 Vienna, Austria

VAT ID: ATU63522646

Business registration number: FN 294621 t

Customs EORI code: ATEOS1000025635