Security Trends: Cybercrime & aktuelle Bedrohungen

CONNECT INFORMUNITY

Dienstag, 13. September 2016
9.00–14.00 Uhr

PwC Österreich
1030 Wien, Erdbergstraße 200

- **Präsentation der Studie »Global Economic Crime Survey 2016« von PwC**
- **EU-Datenschutz: die größten Fragezeichen vor der Umsetzung – von hohen Geldbußen bis zu unsicheren Pflichten**
- **Von Fahrerassistenz zu autonomen Fahrzeugen – Wird die automobile Zukunft zum Hackerparadies?**
- **Aktuelle Bedrohungsszenarien & Podiumsdiskussion zu Ransomware – Was tue ich als Betroffener? Wie wehre ich Targeted Attacks ab?**
- **Business Continuity Management**
- **SIEM – Security Incident Event Management**
- **Sicherheit von großen Datensätzen und mobilen Anwendungen gewährleisten**
- **Secure Opportunistic Networks**
- **Security Trends am Beispiel vom Internet of Things (IoT) oder Industrie 4.0**
- **Standards wie ISO27001/ISO22301/EN50600**

Referenten:
Dr. Ulrich Bayer (SBA Research), **Dr. Markus Frank** (LLM, Rechtsanwalt), **Christian Kurz** (PwC), **Mag. Krzysztof Müller** (A1 Telekom Austria), **Wolfgang Prentner** (ZT PRENTNER-IT), **Dipl.-Ing. Erwin Schoitsch** (AIT – Austrian Institute of Technology) u. a.
Moderation: Thomas Bleier (Future Network Beirat)

Beschränkte Teilnehmerzahl!
Anmeldung erforderlich!
Bei freiem Eintritt für IT-Anwender!

Mit freundlicher Unterstützung von:

AIT Austrian Institute of Technology · pwc · SBA Research · ZTP IT-Ziviltechnikergesellschaft · papers 4you · Future Network

AGENDA

Global Economic Crime Survey
Christian Kurz (PwC)

Kampf gegen Cyber Crime
Mag. Krzysztof Müller (A1 Telekom Austria)

Best Practice

Best Practice Ransomware
Dr. Ulrich Bayer (SBA Research gGmbH)

Pause

EU-Datenschutz: die größten Fragezeichen vor der Umsetzung – von hohen Geldbußen bis zu unsicheren Pflichten
Dr. Markus Frank (LLM, Rechtsanwalt)

Podiumsdiskussion zu Ransomeware und der neuen Datenschutz-Verordnung
Dr. Wolfgang Prentner (ZTP)

Best Practice

Von Fahrerassistenz zu autonomen Fahrzeugen – wird die automobile Zukunft zum Hackerparadies?
DI Erwin Schoitsch (AIT – Austrian Institute of Technology GmbH)

Security Bilanz Deutschland 2016: IT-Sicherheit in Mittelstand und öffentlichen Verwaltungen

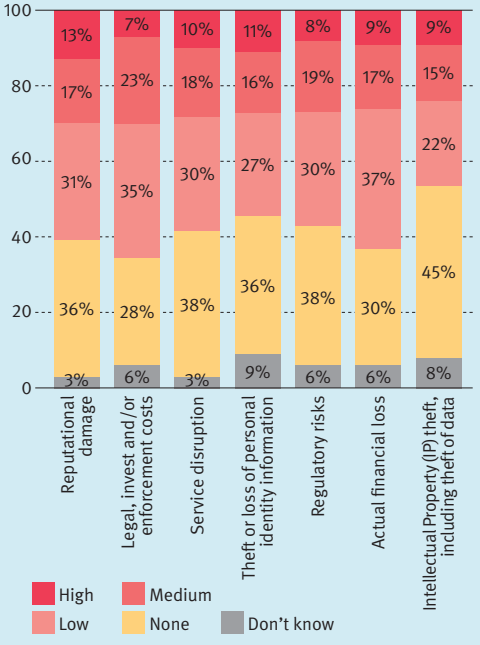
Die Studie »Security Bilanz Deutschland« ermittelt jährlich den Status quo der IT- und Informationssicherheit im Mittelstand und öffentlichen Verwaltungen.

»Durch eine intensivere Beschäftigung mit dem Thema wird auch häufiger festgestellt, dass es Probleme und Schwachpunkte gibt. Dass insbesondere die technische Dimension deutlich schlechter bewertet wird, könnte daran liegen, dass Unternehmen sich damit verstärkt befassen, weil es natürlich naheliegend ist, erst einmal die technischen Aspekte von IT-Sicherheit zu untersuchen. Das ergibt aber nur Sinn, wenn auch gleichzeitig auf organisatorischer, rechtlicher und strategischer Ebene nachgebessert wird. Um sich langfristig gegen Angriffe wie Ransomware zu wappnen, müssen neben technischer Absicherung auch organisatorische Maßnahmen wie beispielsweise Mitarbeitersensibilisierung in Form von Schulungen stattfinden, damit Mitarbeiter Angriffe besser erkennen können. Es müssen rechtliche Fragen geklärt sein, zum Beispiel welche Rechtsfolgen eine vernachlässigte IT-Sicherheit nach sich ziehen kann und ebenso muss IT-Sicherheit strategisch im Unternehmen verankert werden, indem beispielsweise eine eigene Position und ein Budget dafür definiert werden.« – Techconsult-Analyst Henrik Groß

Gegenüber 2015 lässt sich ein Anstieg von Problemen quer über alle Themenbereiche feststellen. Maßnahmen im Bereich Authentifizierung, Datenspeicherung und Datenübertragung sowie Netzwerksicherheit betrifft dies ebenso wie grundlegende Schutzmechanismen (z. B. Antiviren-Lösungen und Firewalls), anspruchsvollere Lösungen (z. B. zur Verschlüsselung von Daten und Kommunikation), komplexe integrierte Lösungen (z. B. zur Angriffsanalyse und -prävention) und Lösungen für mobile Endgeräte.

Der Anteil der Unternehmen, die die Umsetzung ihrer Maßnahmen oder Lösungen als nicht gut bewerten, liegt zwischen der Hälfte und drei Viertel der Befragten. Selbst bei einfachen Maßnahmen,

Level of Impact of Cybercrime



wie Passwortvorgaben, geben 57 Prozent der Unternehmen an, diese nicht gut umgesetzt zu haben (2015: 52 Prozent). Komplexere Maßnahmen und Lösungen, wie zum Beispiel biometrische Authentifizierung oder Security Information and Event Management (SIEM), werden von fast drei Viertel der Unternehmen nicht gut umgesetzt.

Quelle: Computerwelt 22. 4. 2016

Security Information and Event Management (SIEM)

Security information and event management (SIEM) technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources. It also supports compliance reporting and incident investigation through analysis of historical data from these sources. The core capabilities of SIEM technology are a broad scope of event collection and the ability to correlate and analyze events across disparate sources.

Global Economic Crime Survey

Christian Kurz (PwC)

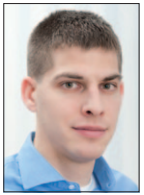
Mehr als ein Drittel der befragten Organistionen waren in den vergangenen 24 Monaten von Wirtschaftskriminialität betroffen. Digitale Technologie ermöglicht es Unternehmen neue Dienstleistungen anzubieten, erhöht allerdings auch das Risiko das Unternehmen Opfer von Cyberkriminalität werden. Daher überrascht es nicht, dass Cyberkriminalität stark zunimmt und dieses Jahr bereits Platz zwei der gemeldeten Vorfälle im Bereich der Wirtschaftskriminialität einnimmt.

Kampf gegen Cyber-Crime

Mag. Krzysztof Müller (A1 Telekom Austria)

Cyber-Crime und Cyber-Spionage sind leider ein Teil unserer digitalen Welt geworden. Berichte über Datenklau und DDOS sind in den Medien keine Seltenheit mehr. Kriminelle folgen den Firmen auf dem Weg in die Digitalisierung. Je mehr Geschäfte, Prozesse und Anwendungen digital abgewickelt werden, umso interessanter sind diese als Angriffsziel für Kriminelle. Es wundert also nicht, dass es inzwischen schon sehr viele Cyberattacken gibt, in denen die Angreifer versuchen, Geld von den Firmen zu erpressen. Cyberattacken kann man sehr bequem aus der Ferne und mit niedrigem Aufwand durchführen. Bitcoins als anonymes Zahlungsmittel eignet sich hervorragend für Abwicklung solcher Erpressungen. Das Risiko erwischt zu werden, ist für die Kriminellen sehr gering. Sind Unternehmen richtig auf diese neuen Gefahren vorbereitet? Sicherlich nicht alle. Wie Studien namhafter Beratungsunternehmen zeigen, wurden viele Unternehmen in der Vergangenheit attackiert. Die Mehrheit dieser Angriffe wurde zufällig entdeckt, nachdem der Angreifer die Firma oft monatelang penetriert hatte. Es ist also höchste Zeit, eine Cyber-Abwehr-Strategie zu entwickeln. Jedes Unternehmen muss sich heute regelmäßig über die aktuellen Bedrohungen informieren, einen geeigneten Schutz implementieren, eigene Prozesse und Infrastruktur auf Schwachstellen überprüfen und diese, falls gefunden, rasch fixen. Zunehmend wichtig ist die Fähigkeit, eine Attacke schnell zu entdecken und Gegenmaßnahmen einzuleiten, was üblicherweise mit Security Incident & Event Management (SIEM) und Security Operation Center (SOC) am besten zu bewerkstelligen ist.

Ransomware



Dr. Ulrich Bayer (SBA Research)

Ransomware stellt in den letzten Jahren eine wachsende Bedrohung dar. Alleine im Zeitraum von Oktober 2015 bis Februar 2016 wurde zehn Mal so viel Ransomware durch Virenscanner in Deutschland entdeckt. Egal, ob es sich um relativ harmlose ›Locker Ransomware‹ oder um die weitaus unangenehmere ›Crypto Ransomware‹ handelt, eine Infektion bedeutet Stillstand für mehrere Stunden und kann ohne Backups zu Datenverlust oder hohen Zahlungen führen. Ransomware kann durch einen falschen Mausklick ins Unternehmen gelangen, darum erfahren Sie in diesem Vortag, wie Sie sich bestmöglich vor Infektionen schützen können und wie Sie sich vorbereiten sollten, um im Fall einer Infektion minimalen Schaden zu erleiden.

EU-Datenschutz: die größten Fragezeichen vor der Umsetzung – von hohen Geldbußen bis zu unsicheren Pflichten

Dr. Markus Frank (LLM, Rechtsanwalt)

Die neue EU-Datenschutz-Grundverordnung wirft für die Unternehmen derzeit fast mehr Fragen auf, als sie Sicherheit gibt. Nationale Ausformungen und die Ausjudizierung bleiben abzuwarten. Jedenfalls werden anerkannte Datenschutz-Zertifizierungen – als ›Sicherheitsnetz‹ – zu einem zentralen Thema der kommenden Jahre. So lautet das Fazit von Wirtschaftsjurist und Rechtsanwalt Dr. Markus Frank, der in seinem Vortrag das jüngste EU-Regelwerk beleuchtet. Extrem hohe Bußgelder bis zu 20 Mio. Euro oder vier Prozent des weltweiten Konzernumsatzes sowie die Tatsache, dass der Schädiger bei Verstößen seine Nicht-Verantwortlichkeit im Sinne der Beweislastumkehr belegen muss, machen aus dem einst zahnlosen Papiertiger ein messerscharfes Datenschutz-Instrument. In seinem Vortrag geht Markus Frank auf wesentliche Neuerungen ein wie: Bestellung eines Datenschutzbeauftragten, Risikoabschätzung oder Datenschutz-Folgeabschätzung insbesondere im Zusammenhang mit sensiblen Mitarbeiterdaten oder Profiling, technische und organisatorische Schutzmaßnahmen wie Verschlüsselung und Pseudonymisierung, Haftungsminimierung und Nachweise durch anerkannte Zertifizierungen u. a.

Von Fahrerassistenz zu autonomen Fahrzeugen – wird die automobile Zukunft zum Hackerparadies?

Dipl.-Ing. Erwin Schoitsch (AIT)

Die Entwicklung der Straßenfahrzeuge war Jahrzehnte vom Sicherheitsdenken bestimmt: Wie mache ich diese so sicher wie möglich? Dass erhebliche Fortschritte erzielt wurden, steht außer Zweifel: Während es noch 1972 2948 Verkehrstote gab, waren es 2014 nur mehr 430. Diese Zahl wurde auf verschiedenste Art und Weise erreicht, doch der Mensch bleibt das Risiko Nummer 1: lt. EU-Roadmap werden 90 % der Unfälle durch den Menschen verursacht. Daher wird versucht, die Vision »Zero Accidents« besonders durch Automatisierung der Fahrzeuge bis hin zum vollautonomen Fahrzeug zu erreichen. Automatisierung bedeutet mehr Elektronik, Software, Sensorik, Aktorik und letztlich Vernetzung aller Systeme im Fahrzeug als auch der Fahrzeuge untereinander und mit der Infrastruktur. Damit wächst jedoch dramatisch eine neue Gefährdung heran, die bisher kaum in Sicherheitsbetrachtungen beachtet werden: Hackerangriffe – schon beim nichtvernetzten Fahrzeug sind etliche Fälle wie das berühmte Jeep-Cherokee-Beispiel bekannt geworden. Der Vortrag wird einige Beispiele erläutern sowie allgemein die Gefährdungspotentiale am hochautomatisierten Fahrzeug analysieren. Weiters werden entstehende Safety- und Cybersecurity-Standards im Automobilbereich behandelt, die für sichere Autos auch in der feindlichen Welt der Cyber-Security-Angriffe sorgen sollen. Ein Überblick wie verschiedene Roadmaps, die auch Grundlage aktueller Forschungsprogramme in Österreich (BMVIT) und der EU sind, die Entwicklung in Richtung vollautomatisierter Fahrzeuge sehen, wird ebenfalls kurz gegeben.

Referenten

Dr. Ulrich Bayer *(SBA Research) arbeitet als Senior Security Analyst bei Secure Business Austria und ist dort unter anderem für die Durchführung von Sicherheitsüberprüfungen sowie das Abhalten von Security-Schulungen verantwortlich. Davor arbeitete er als Projektassistent auf der TU Wien und forschte und programmierte auf dem Gebiet der Malware-Analyse.*

DI Thomas Bleier, *MSc. (AIT – Austrian Institute of Technology) leitet das ICT Security Forschungsprogramm am AIT – Austrian Institute of Technology GmbH. Das Forschungsprogramm beschäftigt sich mit anwendungsorientierter IKT-Sicherheitsforschung für den kompletten Lebenszyklus von IT-unterstützten Systemen zur Erhöhung der Sicherheit kritischer Infrastrukturen. Spezielle Forschungsschwerpunkte sind u. a. Secure System Design, National Cyber Defense, Secure Cloud Computing und Security-Aspekte von zukünftigen Energienetzen (Smart Grids).*

Vor der Tätigkeit am AIT war Thomas Bleier mehr als 10 Jahre in der Wirtschaft als Systemarchitekt, Projektmanager, Softwareentwickler und Consul-

tant tätig. Er hat ein Masterstudium in Informationssicherheitsmanagement und ein Diplomstudium in Technischer Informatik absolviert. Er ist ein »Certified Information Systems Security Professional« (CISSP), »Certified Information Security Manager« (CISM), »Certified Ethical Hacker« (CEH), zertifizierter Projektmanager (IPMA Level C), »Certified SCRUM Master« und besitzt weitere Zertifizierungen im technischen Bereich. Er war und ist am AIT als Arbeitspaketleiter, Projektleiter und Projektkoordinator in zahlreichen nationalen und internationalen Forschungsprojekten im Bereich kofinanzierter Forschung und Auftragsforschung tätig.

Christian Kurz *(PwC) arbeitet seit 2012 für PwC und war davor 7 Jahre in der IT-Beratung und 5 Jahre in der Forschung tätig. Parallel dazu unterrichtet er an der Fachhochschule St. Pölten im Masterstudiengang Information Security. Seine fachlichen Schwerpunkte liegen in den Bereichen Computer Forensik, Electronic Discovery und Untersuchungen im Bereich Cyberforensics. Er ist Certified Cyber Forensic Professional – European Union von (ISC)².*

Mag. Krzysztof Müller, *CISA, CISPP ist Leiter von Information & Data Security bei A1 Telekom Austria. In dieser Position ist Hr. Müller für die Sicherheitsstrategie, Risiko Management, Audits und Security Policies zuständig. Hr. Müller hat den Information Security Management Systems (ISMS) bei A1 aufgebaut und nach dem ISO 27001 Standard zertifiziert. Er war für die positive Umsetzung der SOX innerhalb der IT und die ISAE3402 Zertifizierung verantwortlich. Hr. Müller hat auch den A1 Cert aufgebaut, das Mitglied von österreichischen gov.Cert Verbund ist. Neben dem Job bei A1 unterrichtet Hr. Müller IT Compliance auf der FH St. Pölten und ist Vice-Chairman von ETIS Information Security Working Group.*

Dr. Wolfgang Prentner *(ZT PRENTNER-IT GmbH), seit 1998 IT-Ziviltechniker im Fachbereich Informationstechnologie. Geschäftsführer der ZT-PRENTNER-IT GmbH, Gerichtssachverständiger und promovierter Informatiker an der TU Wien. Als unabhängige Prüf- und Überwachungsstelle für Informatik, CyberSecurity, Datenschutz und dem INTERNET-SICHERHEITSGURT unterstützt er außerdem in ehrenamtlicher Funktion die Länderkammer, die Bundeskammer und das Bundeskomitee Die Freien Berufe Österreichs sowie das Bundeskanzleramt seit 2004.*

Dipl.-Ing. Erwin Schoitsch *Der Vortragende ist seit fast 50 Jahren auf dem Gebiet hochzuverlässiger und sicherer System im technisch-industriellen Bereich in der Forschung tätig. Dies umfasst auch intensive Beschäftigung mit Normen und Standards in den verschiedensten Domänen bezüglich Safety, Security und Dependability ganz allgemein, vor allem in den verschiedenen ISO- und IEC-Komitees und Ad-hoc-Arbeitsgruppen, in denen die Fragen auch in übergreifender, ganzheitlicher Sicht behandelt werden. Er war und ist in vielen Forschungs- und Industrieprojekten sowohl national als auch auf europäischer Ebene eingebunden (Rahmenprogramme, industriegetriebene ARTEMIS und ECSEL Projekte, Horizon 2020). Sein Schwerpunkt liegt heute auf dem Gebiet der Verlässlichkeit vernetzter Embedded Systems, Cyber-Physical Systems und Systems-of-Systems. Er war Mitautor bei der österreichischen Forschungsroadmap »Austrian Research, Development & Innovation Roadmap for Automated Vehicles« sowie der »ARTEMIS Strategic Research Agenda 2016« und ist auch jetzt laufend in Arbeitsgruppen zu diesen Themen aktiv (wobei es nicht nur um Straßenfahrzeuge, sondern auch um alle anderen Verkehrsmittel auf Schiene, Luftfahrt und Off-Road sowie um Robotik und industrielle Automatisierung, geht). Am FH Technikum hält er eine Vorlesung zu »Emerging and Converging Technologies«, in welcher auch diese Fragestellungen eine zentrale Rolle spielen.*

An
CON•ECT Eventmanagement
1070 Wien, Kaiserstraße 14/2

Tel.: +43 / 1 / 522 36 36-36
Fax: +43 / 1 / 522 36 36-10
E-Mail: registration@conect.at
http://www.conect.at

Zielgruppe: Unternehmensleitung, Sicherheitsverantwortliche, IT-Vorstand, IT-Entscheider, IT-Verantwortliche sowie Vertreter von Medien und Wissenschaft

ANMELDUNG: Nach Erhalt Ihrer Anmeldung senden wir Ihnen eine Anmeldebestätigung. Diese Anmeldebestätigung ist für eine Teilnahme am Event erforderlich.

STORNIERUNG: Sollten Sie sich für die Veranstaltung anmelden und nicht teilnehmen können, bitten wir um schriftliche Stornierung bis 2 Werktage vor Veranstaltungsbeginn. Danach bzw. bei Nichterscheinen stellen wir eine Bearbeitungsgebühr in Höhe von € 50,– in Rechnung. Selbstverständlich ist die Nennung eines Ersatzteilnehmers möglich.

ADRESSÄNDERUNGEN: Wenn Sie das Unternehmen wechseln oder wenn wir Personen anschreiben, die nicht mehr in Ihrem Unternehmen tätig sind, teilen Sie uns diese Änderungen bitte mit. Nur so können wir Sie gezielt über unser Veranstaltungsprogramm informieren.

Anmeldung

CON•ECT EVENTMANAGEMENT

- ☐ Ich melde mich zu »Security Trends: Cybercrime & aktuelle Bedrohungen« am 13. 9. 2016 an:
  - ☐ Als IT-Anwender aus Wirtschaft und öffentlicher Verwaltung kostenfrei
  - ☐ Als IT-Anbieter/-Berater zu € 700,– (+ 20 % MwSt.)
- ☐ Ich möchte Zugriff auf die Veranstaltungspapers zu € 99,– (+ 20 % MwSt.)
- ☐ Ich möchte in Zukunft weiter Veranstaltungsprogramme per E-Mail oder Post übermittelt bekommen.

Firma:

Titel: | Vorname:

Nachname:

Funktion:

Straße:

PLZ: | Ort:

Telefon: | Fax:

E-Mail:

Datum: | Unterschrift/Firmenstempel:

● Ich erkläre mich mit der elektronischen Verwaltung meiner ausgefüllten Daten und der Nennung meines Namens im Teilnehmerverzeichnis einverstanden.

● Ich bin mit der Zusendung von Veranstaltungsinformationen per E-Mail einverstanden.

(Nichtzutreffendes bitte streichen)

16069 Layout: Gerhard Krill