Security Trends
Cybersecurity – Artificial Intelligence – Sichere Architekturen

CONNECT INFORMUNITY

Dienstag, 15. November 2022
11.45–14.30 Uhr

Palais Eschenbach, Exnersaal
1010 Wien, Eschenbachgasse 11

Vor Ort und über Stream

- **Präsentation der aktuellen PwC-Studie zum Thema Cybersecurity**
- **Sichere Architekturen**
- **Governance, Risk & Compliance (GRC)**
- **Digitale Security, IoT Security**
- **Cybercrime, Ransomware**
- **End to End Security**
- **Artificial Intelligence und Security**
- **Standards wie ISO 27001 / ISO 22301 / EN 50600**
- **IT und Recht**
- **Sichere Softwareentwicklung**
- **EU-Datenschutzgrundverordnung – Lessons learned**
- **IT-Architekten**
- **CIS**

Referenten:
Markus Hefler (Raiffeisen Rechenzentrum Süd), **Peter Kieseberg** (SBA Research), **Paul Mader** (Verbund), **Florian Prack** (Verbund), **Christoph Schmittner** (AIT), **Michael Strametz** (SySS)

Bei freiem Eintritt.
Anmeldung erforderlich!

AGENDA

11.30 **Registration**

11.45 **Cyber Security by Design: Angriffspfade in der Systemarchitektur erkennen, bevor es zu spät ist**
Christoph Schmittner (AIT – Austrian Institute of Technology)

12.15 **Pause**

12.30 **Ransomware: sicher verschlüsselt! – Festplatte: verschlüsselt sicher?**
Michael Strametz (SySS Cyber Security GmbH)

12.55 **Cyber Defense in einem Unternehmen der kritischen Infrastruktur**
Paul Mader, Florian Prack (Verbund)

13.25 **Best Practice**

13.50 **Networking**

14.30 **Ende der Veranstaltung**

In einer zunehmend vernetzten und technologiegetriebenen Geschäftswelt ist das Thema Vertrauen wichtiger denn je. Fast jedem zweiten Unternehmen weltweit gelingt es jedoch nicht, sich adäquat gegen digitale Bedrohungen zu wappnen und sie riskieren dadurch den Verlust des Vertrauens ihrer Kunden und der Gesellschaft: Nur gut die Hälfte der Unternehmen (53 Prozent) integriert Maßnahmen zum Management von Cyber und Datenschutzrisiken vollständig von Beginn an in ihre digitalen Transformationsprojekte. Zu diesem Ergebnis kommen die Digital Trust Insights, eine internationale Befragung von 3000 Führungskräften in 81 Ländern im Auftrag von PwC.

So zeigte die Studie etwa, dass Sicherheitsvorkehrungen vielfach nicht mit den Geschäftszielen in Einklang gebracht werden, Sicherheitsmaßnahmen aufgrund fehlender Hintergrundinformationen zu potenziellen Angreifern kaum risikoorientiert eingesetzt werden oder Security- und Privacy- Experten oftmals viel zu wenig in Digitalisierungsprojekten eingebunden werden.

(Quelle: Digital Trust Insights 2019 von Price Waterhouse)

Cyber Security by Design: Angriffspfade in der Systemarchitektur erkennen, bevor es zu spät ist

Christoph Schmittner (AIT)

»Cyber Security by Design« ist ein Gamechanger und reflektiert System-Anforderungen, wie wir sie heute im sicherheitskritischen IoT Umfeld antreffen. Als Grundlage dafür wird »Threat Modelling« als Methodik verwendet. Sie erkennt und analysiert potenzielle Gefahren bei der Entwicklung von komplexen Systemen durch Modellierung. In der Praxis ist diese Analyse oft umfangreich: Es stellt sich die schwierige Frage der Relevanz und Priorisierung der erkannten Schwachstellen. Ebenso sind branchenspezifische Regulatorien und Normen zu erfüllen.

Damit Security im vernetzten IoT Umfeld umsetzbar und in der Folge wirksam wird, muss sie Teil der gesamten Funktionalität werden. Es geht nicht nur um die Analyse potenzieller Schwachstellen einzelner Elemente im Systemmodell, sondern auch um das Erkennen möglicher Angriffspunkte und -pfade. Die Frage ist: Welche Ziele verfolgen Angreifer im System und welche Schritte auf welchem Pfad führen sie dorthin? Letztlich sind diese Pfade der Nerv jedes Systemmodells!

Das AIT Austrian Institute of Technology hat mit »ThreatGet« eine einzigartige Methodik für »Cyber Security by Design« entwickelt. Einerseits überprüft sie Systemmodelle und deren Elemente bei der Entwicklung und erspart damit teure Anpassungen zu einem späteren Zeitpunkt. Die wesentliche Grundlage dafür sind die von der AIT entwickelten Wissensdatenbanken und Gefahrenkataloge. Sie stehen aktuell für die Bereiche Automotive und Industrie zur Verfügung und berücksichtigen auch regulatorische Anforderungen. Andererseits erkennt ThreatGet auch potenzielle Angriffspunkte und -pfade. Jetzt ist es durch die Verbindung und gleichzeitige Visualisierung von Schwachstelle und Angriffspfad in der Systemarchitektur möglich, die Komplexität von Cyber Security zu reduzieren. Davon profitiert das gesamte Ökosystems des Unternehmens, weil Systeme über Organisationsgrenzen hinweg vor Angriff und Angreifer geschützt sind.

Ransomware: sicher verschlüsselt! – Festplatte: verschlüsselt sicher?

Michael Strametz
(SySS)

Die Daten wurden »sicher« verschlüsselt durch Ransomware! Warum funktioniert das »Geschäftsmodell« Ransomware so gut? Warum Lösegeld auch schon »gewinnbringend« veranlagt wurde und warum Kapital trotzdem besser nicht in Form von Lösegeldzahlungen veranlangt werden sollte.

Im Gegensatz dazu stehen externe Speichermedien wie Festplatten oder USB-Sticks, die extra damit werben sicher zu sein, weil eine AES-Hardwareverschlüsselung implementiert ist. Bei diesen Geräten ist es oftmals möglich die gespeicherten Daten zu entschlüsseln. SySS zeigt die aktuellen Ergebnisse einer Forschungsarbeit anhand eines praktischen Beispieles.

Cyber Defense in einem Unternehmen der kritischen Infrastruktur

Paul Mader, Florian Prack (Verbund)

Es wird gezeigt, wie das Security Operation Center, das SOC, als »Blue Team« durch ein internes »Red Team« gleichsam mit einem Katz- und Maus-Spiel immer wieder herausgefordert und getestet wird. Diese Vorgehensweise hilft dabei, existierende Schwachstellen und Lücken zu identifizieren und zu bearbeiten. Dargestellt wird das anhand eines Beispiels einer Zero-Day Schwachstelle. Über den internen Zuwachs von Wissen und Erfahrungen ist auch die Kommunikation in »Trusted Communities«, wie dem Austrian Energy CERT ein wichtiger Faktor in der Bewältigung der aktuellen Herausforderungen, sowie die Einbindung von internationalen Threat Feeds um immer auf dem neuesten Stand zu sein. In den vergangenen drei Jahren haben wir eine umfangreiche Systemlandschaft aufgebaut, welche wir gerne vorstellen und auch unseren Ansatz eines effizienten und effektiven Security Teams.

Referenten

Markus Hefler *(Raiffeisen Rechenzentrum Süd GmbH) wurde 1978 in Graz geboren. Während des Masterstudiums erfolgte der Wechsel zum Raiffeisen Informatik Center Steiermark – einer 100%-Tochter der Raiffeisen Landesbank – Steiermark AG in der Funktion als Chief Information Security Officer. Als Verantwortlicher für die Sicherheit der IT-Komponenten der steirischen Raiffeisenbanken wurde auch das Masterstudium erfolgreich abgeschlossen. Die aktuellen Tätigkeiten umfassen im Speziellen die Bereiche Information Security, Business Continuity und IT-Risiko-Management. Zusätzlich gehören die Planung und Begleitung externer ISO/IEC 20000, ISO/IEC 27001 und ANSI TIA-942 Audits als auch die Planung und Durchführung interner Audits im Zusammenhang mit den genannten Normen zu seinem Verantwortungsbereich. Die erlangten Zertifizierungen umfassen die eines CISA und eines CISM, sowie wurde kürzlich die Prüfung zum CISSP erfolgreich abgeschlossen.*

DI. Peter Kieseberg *erhielt seinen Abschluss in ›Technische Mathematik in den Computerwissenschaften‹ an der Technischen Universität Wien. Im Anschluss arbeitete er als Associate Consultant und Projektmanager bei Benmark sowie als Consultant bei NEWCON im Bereich Telekommunikation, speziell in den Bereich Interconnection Billing und DWH/BI. Im Mai 2010 war er Research Manager und Forscher bei SBA Research, seine Spezialisierungen lagen dabei im Bereich der digitalen Forensik sowie des Fingerprintings strukturierter Daten, speziell auch im medizinischen Bereich. Zudem ist er Mitglied bei IEEE SMC und ACM. Seit November 2017 ist er Dozent an der FH St. Pölten, seit August 2018 leitet er hier gemeinsam mit Sebastian Schrittwieser das Institut für IT Sicherheitsforschung.*

Christoph Schmittner, *MSc. ist wissenschaftlicher Mitarbeiter beim Austrian Institute of Technology im Bereich Safety and Security. Seine Schwerpunkte sind Safety Engineering, Road Safety, Embedded Systems, Autonomous Robotics, Automotive Systems Engineering, Computer Security and Reliability etc.*

Michael Strametz *hat Wirtschaftsinformatik sowie IT-Security studiert. Nach langjähriger Tätigkeit im IT-Sicherheitsumfeld eines Automobilzulieferers*

stieg Strametz 2016 als Penetrationstester und IT-Sicherheitsberater bei der SySS GmbH ein, 2017 wechselte er zur SySS Cyber Security GmbH. Strametz ist seit 2020 Standortleiter für Österreich. Der IT-Sicherheitsexperte tritt regelmäßig als Live-Hacker auf zeigt anschaulich, wie IT-Netze übernommen, Passwörter geknackt und Daten abgezogen werden können. Als Live-Hacker präsentiert Strametz u. a. Angriffe gegen Webshops, Google-Hacking, USB-Angriffe oder Angriffe in öffentlichen WLAN-Netzen.

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.

CON•ECT EVENTMANAGEMENT

Anmeldung

☐ Ich melde mich zu »Security Trends« am 15. 11. 2022 kostenfrei an:
☐ Vor Ort; ☐ Online per Livestream

☐ 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.

22069 Layout: Gerhard Krill