Security
im Zeitalter von Industrie 4.0 und Digitalisierung

CONNECT INFORMUNITY

Mittwoch, 20. November 2019
9.00–13.30 Uhr

Alcatel-Lucent Enterprise
1220 Wien, Leonard-Bernstein-Str. 10

- **Security-Risiken steigen durch die zunehmende Vernetzung – Digitalisierung und Industrie 4.0**
- **Quo vadis? – Was wir aus Angriffen auf Industrieanlagen lernen können**
- **IoT, BYOD und DSGVO: Warum der Schutz von Netzwerken Priorität #1 sein sollte**
- **Ausnahmeregelungen zerschmettern Ihre Firewall und die Nerven Ihres Admins**
- **Cyber-Security-Modellierung: der sichere Standpfeiler für IoT**
- **Datenschutzverordnung – Lessons learned bis 3/2019**

ReferentInnen:
Florian Brunner (PwC), **Markus Frank** (FrankLaw), **Ing. Kurt Glatz** (ALE Austria GmbH), **Orsolya Nemeth** (Sparx Services CE), **Philipp Preisinger** (SBA), **Benedikt Stürmer-Weinberger** (Cordaware), **Salomé Wagner** (Sparx Services CE)

Moderation:
Christoph Schmittner (AIT)

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

Mit freundlicher Unterstützung von:

Alcatel·Lucent Enterprise · AIT Austrian Institute of Technology · CORDAWARE Informationslogistik · LieberLieber · pwc · SBA Research · SPARX Systems · ZTP IT-Ziviltechnikergesellschaft · Future Network

AGENDA

9.00 **Eröffnung**

9.15 **Security-Risiken steigen durch die zunehmende Vernetzung – Digitalisierung und Industrie 4.0**
Philipp Reisinger (SBA Research)

9.50 **Quo vadis? – Was wir aus Angriffen auf Industrieanlagen lernen können**
Florian Brunner (PwC)

10.30 **IoT, BYOD und DSGVO: Warum der Schutz von Netzwerken Priorität #1 sein sollte**
Ing. Kurt Glatz (ALE Austria GmbH)

11.00 **Pause**

11.30 **Ausnahmeregelungen zerschmettern Ihre Firewall und die Nerven Ihres Admins**
Benedikt Stürmer-Weinberger (Cordaware)

12.00 **Cyber-Security-Modellierung: der sichere Standpfeiler für IoT**
Orsolya Nemeth, Salomé Wagner (Sparx Services CE)

12.30 **Mittagspause**

13.00 **Datenschutzverordnung – Lessons learned bis 3/2019**
Markus Frank (FrankLaw)

13.30 **Ende der Veranstaltung**

Security-Risiken steigen durch die zunehmende Vernetzung – Digitalisierung und Industrie 4.0

Philipp Reisinger (SBA Research)

Es ist allgemein bekannt, dass durch die fortschreitende Digitalisierung und die zunehmende Vernetzung, die mit Entwicklungen wie Industrie 4.0 einhergeht, die Risiken und Verwundbarkeit einzelner Unternehmen sowie der gesamten Gesellschaft kontinuierlich steigen. Aus diesem Grund gewinnt das Thema der OT-Security immer weiter an Bedeutung.

In dem Vortrag wird ein Überblick zu essentiellen in der IT-Security etablierten technischen und organisatorischen Sicherheitsmaßnahmen gegeben und deren Anwendbarkeit in OT-Umgebungen diskutiert. Als Einstieg werden zuerst Unterschiede und Herausforderungen im IT- vs. OT-Bereich aufgezeigt, um eine einheitliche Diskussionsgrundlage zur Bewertung der Sicherheitsmaßnahmen zu schaffen. Abschließend werden verschiedenste Literaturempfehlungen und Quellen rund um das Thema OT-Security vorgestellt, die Interessierten eine tiefere Auseinandersetzung mit dem Thema ermöglichen.

Quo vadis? – Was wir aus Angriffen auf Industrieanlagen lernen können

Florian Brunner (PwC)

Im Zeitalter der steigenden Digitalisierung und der zunehmenden Komplexität wird es immer schwieriger, auf die gesteigerte Bedrohungslage reagieren zu können. Erfolgreiche Angriffe auf Industrieunternehmen in der Vergangenheit haben gezeigt, dass es für Produktionsleiter, Sicherheitsverantwortliche und IT-Leiter immer wichtiger wird, gemeinsam an diesen Herausforderungen zu arbeiten. Anhand von realen Angriffen und fiktiven Szenarien wird anschaulich erklärt, warum es wichtig ist, geeignete Schutzmaßnahmen zu treffen. Eine große Gefahr dabei stellt nicht etwa ein Hacker-Angriff dar, sondern etwa menschliches Versagen, technisches Gebrechen oder auch die hohe Laufzeit von Anlagen. Der Vortrag gibt auch Ausblick auf mögliche Lösungsansätze für einen sicheren Betrieb von Steuerungs- und Kontrollsystemen in der Industrie und anderen Sparten.

IoT, BYOD und DSGVO: Warum der Schutz von Netzwerken Priorität #1 sein sollte

Ing. Kurt Glatz (ALE Austria)

Im Fokus bei der Digitalisierung steht seit Jahren die Informations- und Datensicherheit. Die neuesten IT-Reports vermelden bei cyberkriminellen Aktivitäten einen deutlichen Aufwärtstrend. Das Bildungswesen zählt dabei zu den Top 3 der gefährdetsten Branchen. Im Rahmen der Digitalisierung von Schulen und Universitäten gehört demnach die Netzwerkzugriffssicherheit zu den wichtigsten Investitionen, auf dem Weg modernes Lernen zu ermöglichen. Warum es jetzt höchste Zeit ist, über eine Network Security Strategie nachzudenken?

- Das IoT (Internet of Things), das Systeme, Prozesse, Apps, Daten und Geräte permanent vernetzt, kommt!
- Modernes E-Learning inklusive dem BYOD (Bring-Your-Own-Device) für Schüler, Studenten und Lehrkräfte kommt!
- Und die DSGVO ist schon da!

Sichere Netzwerktechnologien und insbesondere Strategien, die vor Cyberkriminalität schützen und gleichzeitig bei High-Speed Performance das Risiko von Ausfallszeiten minimieren können, sollten also ab sofort ganz oben auf der Agenda der digitalen Transformation von Hochschulen stehen.

Ausnahmeregelungen zerschmettern Ihre Firewall und die Nerven Ihres Admins

1. Generelles Problem: Das klassische CIA-Dreieck
2. Strafen im Rahmen der EU-DSGVO
3. Gängige Methoden – deren Aufwände und Risiken
4. Der Zero-Konfigurations-Firewall-Ansatz

Benedikt Stürmer-Weinberger
(Cordaware)

Cyber-Security-Modellierung: der sichere Standpfeiler für IoT

Orsolya Nemeth
(Sparx Services CE)

Als wichtigen Meilenstein im Rahmen des Europäischen Förderprojekts »ITEA3 COMPACT« haben wir eine Methode entwickelt, welche Software und Systemmodellierung mit dem Cyber Security Threat Modeling zusammenführt. Zusätzlich zu der Identifikation bekannter Gefahren arbeiten wir aktuell auch an der automatisierten Erfüllung von ISO27000-Anforderungen für sichere IoT-Systeme. Zeit und Aufwand für die Entwicklung lassen sich damit signifikant reduzieren.

Salomé Wagner
(Sparx Services CE)

Datenschutzverordnung – Lessons learned bis 2019

Markus Frank
(FrankLaw)

1. Was der Europäische Datenschutzausschuss 9 Monate nach Wirksamwerden der DSGVO am 25. Mai 2018 über deren Umsetzung in der EU berichtet.
2. Was in Österreich seit 25. Mai 2018 im Datenschutz (nicht) geschehen ist.
3. Beispiel-Thema: Löschen von Daten – Entscheidungen der Datenschutzbehörden seit 25. Mai 2018 – siehe https://www.frank-law.at/news/
4. Bisherige Bußgeldbescheide der Datenschutzbehörden und die Rolle der Kartellbehörden im Datenschutzrecht – siehe https://www.frank-law.at/news/
5. DatDOK – Wirtschaftlich vertretbare Umsetzung der DSGVO – ist das für KMUs und EPUs überhaupt möglich – auch unter Berücksichtigung der umfangreichen Dokumentationspflichten gemäß der DSGVO?

ReferentInnen

Ing. Florian Brunner, MSc *ist im Bereich Cybersecurity und Privacy bei PwC Österreich tätig und verantwortet national die Themen OT-Security sowie Identity und Access Management. Er verfügt über langjährige Beratungserfahrung im internationalen Umfeld, unter anderem bei Banken, Versicherungen sowie Industrie- und Technologieunternehmen. Neben der Durchführung von technischen Audits oder der Umsetzung von Sicherheitsprogrammen, unterstützt Herr Brunner seine Mandanten auch bei der Umsetzung sicherheitskritischer Projekte.*

Dr. Markus Frank, LLM, *ist als Rechtsanwalt spezialisiert auf interdisziplinäre Untersuchungen von Schadenursachen bei Wirtschaftsdelikten und Vertragsverletzungen. Vor diesem Hintergrund ist er als Rechtsexperte im Beirat der Zertifizierungsorganisation CIS vertreten und fungiert im Rahmen der CIS-Zertifikatslehrgänge als Trainer.*

Kurt Glatz *hatte bei Alcatel-Lucent Enterprise und deren Vorgesellschaften über die letzten Jahre verschiedene Leadership Aufgaben inne. Seit 1. 1. 2017 leitet er den Bereich Carriers und Service Provider für Europe and North (DACH, BENELUX, Central and Eastern Europe). Er beschäftigt sich seit längerer Zeit mit Marktanalysen im Bereich Telekommunikation.*

Orsolya Nemeth. *Seit 15 Jahren agiert Fr. Orsolya Nemeth als professionelle Trainerin, davon 7 Jahre als Senior Trainerin im Bereich Business-Softwarelösungen. Seit 2017 ergänzt Fr. Nemeth das Team*

von Sparx Systems sowie Sparx Services Central Europe als Beraterin und Trainerin in Schlüsseldomänen wie Versicherung, IT-Security und Retail, in dem Sie die Unternehmensarchitektur von anspruchsvollen Kunden anhand von Modellierungssprachen wie BPMN (Business Process Modeling & Notation), UML oder Archimate, sowie das TOGAF-Framework, Software-gestützt modelliert.

Benedikt Stürmer-Weinberger *ist seit 2010 bei der Firma Cordaware und aktuell als Key Account Manager tätig. Zu seinen Aufgaben gehören Vertrieb, Marketing und die Organisation, Planung, Beratung und Durchführung von externen Projekten. Diese beziehen sich zum einen auf die Informationslogistik, wo es darum geht, im Unternehmen die Anwender mit der richtigen Nachricht zur richtigen Zeit über das entsprechend relevante Thema proaktiv zu informieren. Zum anderen beziehen sich seine Projekte auf den Bereich der IT Sicherheit, wo durch optimierte Sicherheitskonzepte z. B. die Netzwerkstrukturen stark vereinfacht und die Bereitstellungsprozesse für Services deutlich verkürzt werden können.*

Salomé Wagner *(MAS Services Marketing & Management) ist seit über 15 Jahren an der Schnittstelle von Kommunikation und Informationstechnologie tätig. Ihre berufliche Erfahrung umfasst Expertenrollen in internationalen Konzernen (Oracle, Verizon) in den Bereichen strategische Partnerschaften, Serviceportfolio und Marktkommunikation sowie die Entwicklung von technologischen Start-ups.*

CONNECT BUSINESS ACADEMY

CISSP® (Certified Information Systems Security Professional Training)

Referent: Philipp Reisinger
(SBA Research)

Termin: 4.–8. November 2019, Wien

- Tiefgehende Kenntnisse in Sicherheitskonzepten, Umsetzung und Methodologie
- ISC²
- Entwicklung von Sicherheitsrichtlinien
- Sicherheit in der Softwareentwicklung
- Angriffsarten und die korrespondierenden Gegenmaßnahmen
- Kryptographische Konzepte und deren Anwendung
- Notfallplanung und -management
- Risikoanalyse
- Forensische Grundlagen

Teilnahmegebühr: € 3.000,– (Alle Preise + 20 % MwSt.)

CONNECT BUSINESS ACADEMY

Windows Hacking – Wie Hacker und Betriebsspione arbeiten

Referent: Ing. Reinhard Kugler, MSc
(SBA Research)

Termin: 15.–17. April 2020, Wien

Der Kurs behandelt die typischen Sicherheitslücken und Angriffspunkte sowie geeignete Schutzmaßnahmen in Windows-Netzwerken.

- Sicherheitslücken und deren Absicherung bei Windows Clients
- Hacking-Angriffe und deren Bekämpfung
- Verschlüsselung und Passwort Cracking
- DMA und Coldboot-Attacken
- Ganzheitliches Patchmanagement
- Client Hardening
- Smart Card Security
- Privilege Escalation
- Aufspüren von Schwachstellen
- Memory Forensic
- DLL Hijacking
- Umgehen von Gruppenrichtlinien
- Windows Security Insights (UAC, Integrity Levels, …)
- Malware-Analyse und Malware-Bekämpfung
- Mobile Device Security

Teilnahmegebühr: € 1.960,–(Alle Preise + 20 % MwSt.)

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, Projektleiter, Security- und Risk-Experten, Security Manager, Sicherheitsverantwortliche, IT-Vorstand, IT-EntscheiderInnen, IT-Verantwortliche sowie VertreterInnen 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 im Zeitalter von Industrie 4.0 und Digitalisierung« am 20. 11. 2019 an:
  - ☐ Als IT-Anwender aus Wirtschaft und öffentlicher Verwaltung kostenfrei
  - ☐ Als IT-Anbieter/-Berater zu € 390,– (+ 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.

19084 Layout: Gerhard Krill