

# Security im Zeitalter von Industrie 4.0 und Digitalisierung

CONNECT  
INFORMUNITY



Mittwoch, 20. November 2019  
9.00–17.00 Uhr

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

- Aktuelle PwC-Studie zum Thema Cybersecurity & Cybercrime
- Governance, Risk & Compliance (GRC)
- EU-Datenschutzgrundverordnung – Lessons Learned
- Digitale Security
- Cybercrime, Ransomware
- Industrie 4.0
- Internet of Things (IoT)
- SIEM – Security Incident Event Management
- Secure Opportunistic Networks
- Standards wie ISO 27001 / ISO 22301 / EN 50600
- Business Continuity Management
- Sichere Softwareentwicklung
- Best Practices
- Podiumsdiskussion

#### ReferentInnen:

**Florian Brunner** (PwC), **Markus Frank** (FrankLaw), **Ing. Kurt Glatz** (ALE Austria GmbH), **Philipp Mattes-Draxler** (PwC), **Orsolya Nemeth** (Spax Services CE), **Philipp Preisinger** (SBA), **Salomé Wagner** (Spax 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

LieberLieber

**pwc**

**SBA**  
Research

**SPARX**  
SYSTEMS

**FUTURE  
NETWORK**

## AGENDA

- 9.00 Eröffnung**
- 9.30 Security-Risiken steigen durch die zunehmende Vernetzung – Digitalisierung und Industrie 4.0**  
Philipp Reisinger (SBA Research)
- 10.00 Digital Trust Insights 2019**  
Philipp Mattes-Draxler (PwC)
- 10.30 Pause**
- 11.00 Quo vadis? – Was wir aus Angriffen auf Industrieanlagen lernen können**  
Florian Brunner (PwC)
- 11.30 Cyber-Security-Modellierung: der sichere Standpfeiler für IoT**  
Orsolya Nemeth, Salomé Wagner (Sparx Services CE)
- 12.00**
- 12.30 Datenschutzverordnung – Lessons learned bis 3/2019**  
Markus Frank (FrankLaw)
- 13.00**
- 13.30 Pause**
- 14.00 Best Practice**
- 14.30 Secure Networks**  
Ing. Kurt Glatz (ALE Austria GmbH)
- 15.00 Ende der Veranstaltung**

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

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.



Philipp Reisinger  
(SBA Research)

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.

## Digital Trust Insights 2019

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 3.000 Führungskräften in 81 Ländern im Auftrag von PwC.



Philipp Mattes-Draxler  
(PwC)

Der Vortrag wird auf die Studienergebnisse eingegangen und kommentieren.

So zeigt 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.

## Datenschutzverordnung – Lessons learned bis 2019

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.



Markus Frank  
(FrankLaw)

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 EPU's überhaupt möglich – auch unter Berücksichtigung der umfangreichen Dokumentationspflichten gemäß der DSGVO?

## 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.

## Cyber-Security-Modellierung: der sichere Standfeiler für IoT

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.



Orsolya Nemeth,  
Salomé Wagner  
(Sparx Services CE)

## 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.

**Philipp Mattes-Draxler** ist im Bereich *Cybersecurity und Privacy* bei PwC tätig. Zuvor war er unter anderem mehrere Jahre beim Österreichischen Bundesheer im Bereich der Informationssicherheit beschäftigt. Er ist auf die Beratung nationaler und multinationaler Unternehmen mit Schwerpunkt *Cybersecurity* spezialisiert.

Ein Schwerpunkt seiner Tätigkeit liegt im Bereich *IT-Sicherheitsvorfallmanagement* und *Incident Response* sowie *Threat Intelligence*.

Er ist ein Kenner von Querschnittmaterien und engagiert er sich für die Weiterentwicklung des Fachbereichs *IT Security Incident Management*, was sich auch in seiner Vortragstätigkeit an der FH Technikum Wien niederschlägt.

**Dr. Markus Frank, LL.M.**, 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-Software-*

lösungen. Seit 2017 ergänzt Fr. Nemeth das Team von Sparx Systems sowie Sparx Services Central Europe als Beraterin und Trainerin in Schlüssel-domänen 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.

**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.

## CISSP® (Certified Information Systems Security Professional Training)

**Referent: Christoph Falta**  
(SBA Research)



**Termin: 4.–8. November 2019,**  
**Wien**

- Tiefgehende Kenntnisse in Sicherheitskonzepten, Umsetzung und Methodologie
- ISC<sup>2</sup>
- Entwicklung von Sicherheitsrichtlinien
- Sicherheit in der Softwareentwicklung
- Angriffsarten und die korrespondierenden Gegenmaßnahmen
- Kryptographische Konzepte und deren Anwendung
- Notfallplanung und -management
- Risikoanalyse
- Forensische Grundlagen

**Teilnahmegebühr:** € 1.850,-; Frühbucher: € 1.750,-  
(Alle Preise + 20 % MwSt.)

## Windows Hacking – Wie Hacker und Betriebs-spione arbeiten

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



**Termin: 13.–15. November 2019,**  
**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-Attacks
- 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:** € 1.490,-; Frühbucher: € 1.390,-  
(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](mailto: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 Bearbeitungs-

gebühr 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

- 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.