Security-Trends, DSGVO und Riskmanagement

CONNECT INFORMUNITY

Dienstag, 9. April 2019
11.30–17.00 Uhr

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

- **Präsentation der aktuellen PwC-Studie zum Thema Cybersecurity & Cybercrime**
- **EU-Datenschutzgrundverordnung – Lessons Learned**
- **Secure Networks**
- **Security, Risk- und Compliance-Management in der Automotive-Domäne einbringen**
- **Management von digitalen Identitäten bzw. Multi-Faktor-Authentifizierung**
- **Governance, Risk & Compliance (GRC)**
- **Internet of Things (IoT)**
- **BYOx-Security**
- **Security-Automation**
- **Best Practices**
- **Podiumsdiskussion**
- **Standards wie ISO 27001 / ISO 22301**

Referenten:
Christian Angerer (ALE Austria GmbH), **Dr. Markus Frank** (FrankLaw), **Ing. Kurt Glatz** (ALE Austria GmbH), **Philipp Mattes-Draxler** (PwC), **Christoph Schmittner, MSc.** (AIT GmbH) und andere

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

Mit freundlicher Unterstützung von:

Alcatel·Lucent Enterprise

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

pwc

FUTURE NETWORK

AGENDA

11.30 **Registration**

12.00 **Begrüßung**

12.15 **Datenschutzverordnung – Lessons learned bis 3/2019**
Dr. Markus Frank (FrankLaw)

13.15 **Global State of Information Security Survey 2018: Digital Trust Insights 2019**
Philipp Mattes-Draxler (PwC)

14.45 **Best Practices**

15.15 **Pause**

15.45 **Secure Networks**
Ing. Kurt Glatz, **Christian Angerer** (ALE Austria GmbH)

16.25 **Security, Risk- und Compliance Management in der Automotive Domäne**
Christoph Schmittner, MSc. (AIT)

»Viele Organisationen müssen ihr digitales Risiko evaluieren und die Widerstandsfähigkeit im Hinblick auf das Unvermeidliche stärken.«
Dr. Christian Kurz, Leiter Forensic Technology Solutions und Cyberforensics, PwC Österreich

Datenschutzverordnung – Lessons Learned bis 3/2019

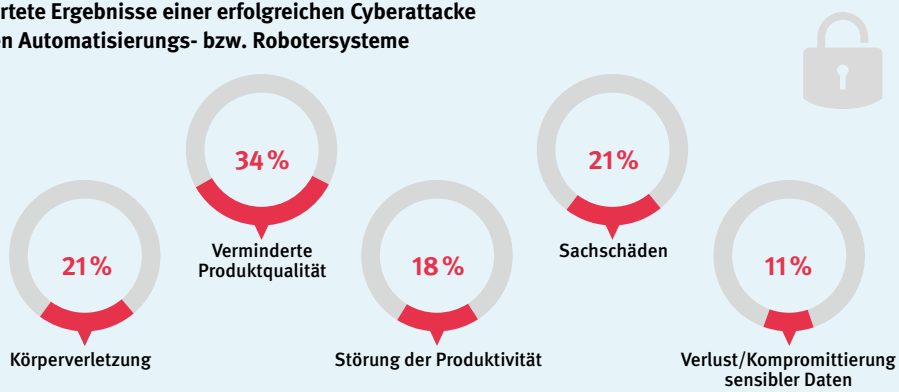
Markus Frank
(FrankLaw)

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?

Global State of Information Security Survey 2018: PwC Österreich

Massive Verstöße im Bereich der Cybersicherheit sind beinahe alltäglich geworden und sorgen regelmäßig für Schlagzeilen, die Konsumenten und

Erwartete Ergebnisse einer erfolgreichen Cyberattacke gegen Automatisierungs- bzw. Robotersysteme



Quelle: PWv, CIO und CSO. The Global State of Information Security® Survey 2018, 18. Oktober 2017; Basis 9500 Befragte

Führungskräfte in Unruhe versetzen. Trotz der Sensibilisierung für das Thema sind viele Organisationen auf der ganzen Welt nach wie vor unsicher, wie sie in einer zunehmend digitalen Gesellschaft mit Cyber-Risiken umzugehen haben. Das zeigt die aktuelle Studie von PwC »Global State of Information Security® Survey 2018« (GSISS).

Digital Trust Insights 2019

Philipp Mattes-Draxler (PwC)

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.

Der Vortrag wird auf die Studienergebnisse eingehen 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.

Die Studie wird von Dr. Christian Kurz (PwC) durchgeführt

Secure Networks

Kurt Glatz (ALE Austria GmbH)

Christian Angerer (ALE Austria GmbH)

Bei der Maslowschen Bedürfnispyramide steht Sicherheit nach den physiologischen Bedürfnissen bereits an zweiter Stelle und ist Teil unserer DNA. Dass wir IT-Infrastruktur schützen müssen, ist uns schon seit langem klar. Durch die Zunahme an Mobilität, Cloud-Diensten, BYOD und »Connected Things« ist die Herausforderung, Daten, Geräte und Firmenwerte zu schützen, größer denn je.

Es gibt unzählige weitere wichtige Faktoren – beispielsweise das Routing des IoT-Netzwerkverkehrs oder die Einrichtung von Geräteprofilen zur Authentifizierung. Daher müssen die Unternehmensnetze entsprechend angepasst werden. Durch das Definieren verschiedenster Parameter und Sicherheitsstufen können sich Organisationen bestmöglich auf das IoT vorbereiten.

Welche Netzwerktechnologien und Strategien können das Risiko von Ausfallszeiten minimieren und die Performance erhöhen?

5 Gründe, um über eine neue Netzwerk-Security-Strategie nachzudenken:

- Im Zeitalter des IoT hängt der Unternehmenserfolg immer stärker von einer sicheren und performanten Netzwerkinfrastruktur ab.
- Die Automatisierung von Geschäftsprozessen verspricht enorme Vorteile, solange Geräten, Anwendungen und Daten, sicher und zuverlässig untereinander ausgetauscht werden können.
- Der ungesicherte Umgang mit Mobilität, BYOD und Netzwerkzugriffen kann Ihre IT-Infrastruktur gefährden.
- IT/Netzwerk-Vereinfachung: Eine effektive Sicherheitsstrategie kann viele Komplexitätsebenen beseitigen.
- Die Kosten für die Cyber-Sicherheit von Unternehmen sind beträchtlich, daher müssen Multilayer EcoSysteme von Tools und Richtlinien, die über offene Standards und Schnittstellen interagieren, mit Bedacht gewählt werden.

Security, Risk- und Compliance-Management in der Automotive-Domäne

Christoph Schmittner (AIT)

Gezeigt wird ein neuer europäischer Ansatz für die Fahrzeugzulassung, der von den Herstellern und Zulieferern ein zertifiziertes Cybersecurity-Management-System fordert.

Referenten:

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.*

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.

Christoph Schmittner *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.*

CONECT BUSINESS ACADEMY

CISSP (Certified Information Systems Security Professional Training)

Referenten: Philipp Reisinger (SBA Research)

Termine: 8.–12. April, 4.–8. November 2019, alle 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,–, Prüfungsgebühr: € 520,– (Alle Preise +20 % MwSt.)

Information und Anmeldung: www.conect.at

CONECT BUSINESS ACADEMY

CSSLP (Certified Secure Software Lifecycle Professional)

Referent: Thomas Konrad (SBA Research)

Termine: 1.–5. April, 5.–9. November 2019 , alle Wien

Die TeilnehmerInnen dieses Kurses werden nach Abschluss gut für die CSSLP-Prüfung vorbereitet sein. Unabhängig davon, ob sie die Prüfung nun wirklich ablegen, werden gewonnene Erfahrung und das profunde Wissen für die Sicherheit Ihres gesamten Softwareentwicklungsprozesses von entscheidender Bedeutung sein.

- Secure Software Concepts
- Secure Software Requirements
- Secure Software Design
- Secure Software Implementation/Coding
- Secure Software Testing
- Software Acceptance
- Software Deployment, Operations, Maintenance and Disposal
- Supply Chain & Software Acquisition

Teilnahmegebühr: € 3.000,–; Prüfungsgebühr: € 480,– (Alle Preise + 20 % MwSt.)

Information und Anmeldung: www.conect.at

CONECT BUSINESS ACADEMY

Windows Hacking – Wie Hacker und Betriebsspione 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.

Der Kurs gliedert sich dabei in 3 Teile, in denen interaktiv bestehende Sicherheitslücken demonstriert und auch durch die TeilnehmerInnen selbst probiert werden können. So entsteht ein tiefes Verständnis für das damit verbundene Risiko. Des Weiteren werden den TeilnehmerInnen Schutzoptionen vermittelt, um die gezeigten Sicherheitslücken zu schließen:

- Sicherheitslücken und deren Absicherung bei Windows Clients
- Sicherheitslücken und deren Absicherung bei Windows Servern
- Sicherheitslücken und deren Absicherung im Netzwerk und auf mobilen Endgeräten

Teilnahmegebühr: € 1.290,– (Alle Preise + 20 % MwSt.)

Information und Anmeldung: www.conect.at

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-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-Trends und Riskmanagement« am 9. 4. 19 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.

19026 Layout: Gerhard Krill