Security, Risk- und Compliance Management

CONNECT INFORMUNITY

Mittwoch, 7. Oktober 2020
9.00–13.30 Uhr

Wien

- **Studie zu Cybersecurity (angefragt)**
- **Welche Möglichkeiten in der digitalen Transformation für Sichere Kommunikation entstehen?**
- **DSGVO – Lessons learned 2020**
- **Aktuelle Studie zu Cybercrime und Cybersecurity und Digitaler Security**
- **Sichere Softwareentwicklung**
- **Security by Engineering: Zuverlässigkeit und Sicherheit als Qualitätsmerkmal**
- **Ausnahmeregelungen zerschmettern Ihre Firewall und die Nerven Ihres Admins**
- **Red Teaming: Der verdeckte Angreifer im internen Netzwerk**

Referenten:
Markus Frank (Frank Law), **Kurt Glatz** (Alcatel-Lucent Enterprise), **Christoph Ritter** (SySS), **Michael Strametz** (SySS), **Benedikt Stürmer-Weinberger** (Cordaware), **Thomas Ziebermayr** (SCCH) und andere

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

Mit freundlicher Unterstützung von:

Alcatel·Lucent Enterprise · CORDAWARE INFORMATIONSLOGISTIK · FRANKLAW OFFICE@FRANK-LAW.AT · scch software competence center hagenberg · SySS THE PENTEST EXPERTS. · FUTURE NETWORK

AGENDA

8.45 **Eröffnung**

9.00 **Studie**

9.40 **Security by Engineering: Zuverlässigkeit und Sicherheit als Qualitätsmerkmal**
Thomas Ziebermayr (SCCH)

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

11.00 **IoT, BYOD und DSGVO. Warum der Schutz von Netzwerken Priorität #1 sein sollte**
Kurt Glatz (Alcatel-Lucent Enterprise)

11.40 **Pause inkl. Networking**

12.15 **DSGVO – Lesson learned 2020**
Markus Frank (Frank Law)

12.55 **Red Teaming: Der verdeckte Angreifer im internen Netzwerk**
Christoph Ritter, Michael Strametz (SySS)

13.30 **Ende der Veranstaltung**

Security by Engineering: Zuverlässigkeit und Sicherheit als Qualitätsmerkmal

Thomas Ziebermayr (SCCH)

Die Anforderungen an Software steigen enorm, speziell an Security. Die zunehmende Vernetzung und immer zentralere Aufgaben der Software machen das Thema essentiell für Software Systeme. Security ist aber vielschichtig und muss sehr intensiv bei der Entwicklung von Software betrachtet werden. Nicht nur das Design der Software, sondern auch die Umsetzung der Algorithmen kann Software verletzlich machen. Neben Verschlüsselungs- und Authentifizierungsverfahren wurden daher Werkzeuge entwickelt, die Security Probleme erkennen können. Spezielle Analyseverfahren und Testmethoden helfen dabei, Security Probleme frühzeitig und bevor Auswirkungen befürchtet werden müssen, zu erkennen. Das SCCH forscht an der Weiterentwicklung dieser Methoden auf Basis der eigenen Analyse Expertise und hat Werkzeuge entwickelt, die speziell im Automatisierungsbereich und im IOT Umfeld einsetzbar sind. Im Vortrag wird, neben dem Überblick über diesem Bereich, ein Einblick in die aktuelle Forschung präsentiert.

Ausnahmeregelungen zerschmettern Ihre Firewall und die Nerven Ihres Admins

Benedikt Stürmer-Weinberger (Cordaware)

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

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

Kurt Glatz (Alcatel)

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?

DSGVO – Lessons learned 2020

Markus Frank (Frank Law)

Was Sie in meinem Kurz-Vortrag erwartet:

1. DS-Management-Systeme und Datenschutz-Audits gemäß DSGVO?
2. Dokumentations-Pflichten zur DSGVO-Compliance!
3. Entscheidungen und (Behörden-)Meinungen zu div. DSGVO-Pflichten und zu Schadenersatz- und Bußgeld-Risiken

Red Teaming: Der verdeckte Angreifer im internen Netzwerk

Christoph Ritter (SySS)

Michael Strametz (SySS)

Red Teaming ist eine Prüfmethode, welche immer verbreiteter wird, unter anderem auch auf Grund von gesetzlichen Vorgaben in bestimmten Branchen. Für viele Unternehmen ist diese Herangehensweise noch neu. Red Teaming ist eine Prüfmethode, bei welcher ein Dienstleister das Unternehmen über einen längeren Zeitraum angreift und auch Social Engineering-Techniken verwendet. Dabei werden Schwachstellen in den folgenden Bereichen erarbeitet:

- Systemsicherheit
- Unternehmensprozesse
- Mitarbeiter-Awareness

Ebenso kann diese Herangehensweise genutzt werden, um Notfallübungen im Bereich IT-Sicherheit durchzuführen oder die Fähigkeiten des internen IT-Security Teams zu testen.

Herr Ritter wird Red Teaming vorstellen und anhand von Beispielen aus vergangenen Projekten von den zu erwartenden Ergebnissen berichten.

Die 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 CISZertifikatslehrgänge als Trainer für ISO 27001.*

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.*

Christoph Ritter *hat eine duale Ausbildung zum Fachinformatiker für Systemintegration absolviert sowie Angewandte Informatik an der DHBW Mosbach studiert. Seit 2014 ist Ritter Penetrationstester und IT-Sicherheitsberater für die SySS GmbH. Zuvor war er als Serveradministrator, Netzwerkadministrator, Sicherheitsberater und Helpdesk-Mitarbeiter in einem Systemhaus für unterschiedliche mittelständische Unternehmen tätig. Seit 2016 bietet Ritter außerdem die Vorlesung »Penetration Testing und Computerforensik« an der Hochschule Aalen an. Red Teaming zählt neben der Analyse interner und externer IT-Infrastrukturen, Webanwendungen und Windows-basierter Verzeichnisdienste zu Ritters Arbeitsschwerpunkten bei der SySS. Neben Social Engineering liegen weitere Kompetenzen im Bereich Incident Response (v. a. Memory-Forensik). Seit Ende 2018 leitet Ritter die Red Teaming-Abteilung der SySS.*

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.*

Benedikt Stürmer-Weinberger *ist seit 2010 für die Firma Cordaware GmbH für Kommunikationsprojekte tätig und auf die Organisation, Planung, Beratung und Durchführung von internen und externen Projekten im Bereich der Informationslogistik und Kommunikation und Zusammenarbeit spezialisiert.*

Dr. Thomas Ziebermayr, *Area Manager Software Science leitet den Bereich Software Science. Die Forschungsschwerpunkte in diesem Schwerpunkt sind Software Qualität, Software Test, Code Analyse und Wissensextraktion aus Software, Software Architekturen, Redokumentation und Engineering von sicherer Software. Ein sehr wichtiges Thema ist auch das Engineering von KI-Systemen und die Integration von KI in kritische Software-Systeme sowie die Zukunft des Softwareengineerings auch mit KI. Das umfasst im Forschungsthema Human Centered Software Engineering auch das Thema Human Centered AI. Neben der Bereichsleitung leitet er das Projekt DEPS Pilot – hier geht es um die Erforschung von Methoden zur Absicherung von Software speziell im industriellen Umfeld.*

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:
Sicherheitsverantwortliche, CISOS, CISAS, Technologieverantwortliche für Security IT-Vorstand, IT-EntscheiderInnen, IT-Verantwortliche sowie Unternehmensleitung, 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, Risk- und Compliance Management« am 7. 10. 2020 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.

20075 Layout: Gerhard Krill