Security Trends:
Cybersecurity – Pentesting – Schutz von Software – DSGVO 2021

CONNECT INFORMUNITY

Donnerstag, 6. Mai 2021
8.45–14.00 Uhr

Online

- **DSGVO – Lessons learned 2021**
- **Red Teaming: Der verdeckte Angreifer im internen Netzwerk**
- **Gerichtstaugliches Pentesting nach ASVS**
- **Cyberrisiken frühzeitig erkennen – formale Verifikations-methoden für IoT**
- **VPN & RDP als Ressourcen-Killer mit Sicherheitslücken – Homeoffice umsetzen mit einem Zero-Trust-Ansatz?**
- **Sicherheit und Schutz von Software: Neue Methode gegen Raubkopien und Hackerangriffe**
- **Cybersecurity-Herausforderungen in Smart Manufacturing**

ReferentInnen:
Markus Frank (Frank Law), **Katharina Hofer-Schmitz** (Joanneum Research), **Peter Lieber** (LieberLieber), **Wolfgang Prentner** (ZTP.digital), **Christoph Ritter** (SySS GmbH), **Erwin Schoitsch** (AIT – Austrian Institute of Technology), **Benedikt Stürmer-Weinberger** (Cordaware), **Thomas Ziebermayr** (SCCH) und andere
Moderation: Christoph Schmittner (AIT)

Ehreneinladung bei freiem Eintritt.
Anmeldung erforderlich!

Mit freundlicher Unterstützung von:

CORDAWARE INFORMATIONSLOGISTIK · ifhIII st.pölten · JOANNEUM RESEARCH · LieberLieber · scch { } software competence center hagenberg · SySS THE PENTEST EXPERTS. · ZTP IT-PRÜFSTELLE · FUTURE NETWORK

8.45 **Einführung in die HOPIN-Plattform und Networking**

9.00 **Begrüßung**

9.05 **DSVGO – Lessons learned 2021**
Markus Frank (Frank Law)

9.50 **Red Teaming: Der verdeckte Angreifer im internen Netzwerk**
Christoph Ritter (SySS GmbH)

10.15 **Gerichtstaugliches Pentesting nach ASVS**
Wolfgang Prentner (ZTP.digital)

10.40 **Pause inkl. Networking und Ausstellungsrundgang**

10.55 **Cyberrisiken frühzeitig erkennen – formale Verifikationsmethoden für IoT**
Katharina Hofer-Schmitz (Joanneum Research)

11.25 **VPN & RDP als Ressourcen-Killer mit Sicherheitslücken – Homeoffice umsetzen mit einem Zero-Trust-Ansatz?**
Benedikt Stürmer-Weinberger (Cordaware)

11.50 **»Security by Design«: Mit Methode und Regelwerk Bedrohungen analysieren und Risiken bewerten**
Peter Lieber (LieberLieber)

12.15 **Pause inkl. Networking und Ausstellungsrundgang**

12.30 **Sicherheit und Schutz von Software: Neue Methode gegen Raubkopien und Hackerangriffe**
Thomas Ziebermayr (SCCH)

13.10 **Cybersecurity-Herausforderungen in Smart Manufacturing**
Erwin Schoitsch (AIT)

13.40 **Networking**

14.00 **Ende des Events**

Zum Thema

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)

Sicherheitstest für mobile Applikationen – Warum reines Vertrauen auf TLS/SSSL nicht genug ist
Sicherheitstests sind ein fundamentaler Aspekt in vielen weit verbreitete Methoden des Software-Testings. Allerdings ist es oftmals der Fall, dass die eingesetzten Security-Protokolle nicht hinterfragt oder getestet werden. In diesem Vortrag geben wir einen kurzen Überblick darüber, wie aufgrund dieser Praxis essentielle Sicherheitslücken im Rahmen von Sicherheitstests und der Qualitätskontrolle übersehen werden. Dabei konzentrieren wir uns auf zwei grundsätzliche Probleme:

External Megatrends Beyond Your Control

Quelle: Gartner Group

Die Definition eines korrekten und umfassenden Angreifermodells, sowie das Setzen von Vertrauen in den Client bei der Nutzung kryptographischer Algorithmen.

Peter Kieseberg, FH St.Pölten

DSGVO – Lessons learned 2021

Markus Frank (Frank Law)

Was Sie in meinem Kurz-Vortrag erwartet:

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

Red Teaming: Der verdeckte Angreifer im internen Netzwerk

Christoph Ritter (SySS GmbH)

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.

Gerichtstaugliches Pentesting nach ASVS

Wolfgang Prentner (ZTP.digital)

Pentesting und ganze Red Team Operations die wir durchführen, sind zumeist eine sehr individuelle und kreative Arbeit der einzelnen Pentester. Um das Pentesting in einen nachvollziehbaren und systematischen Rahmen zu pressen, bedienen wir uns von ZTP.digital dem OWASP Application Security Verification Standard (ASVS) um auch gerichtstaugliche Cyber-Security Prüfberichte in Form von IT-Ziviltechnikergutachten, staatlich befugt und beeidet, liefern zu können. Wir erklären dabei Vorgehensweise und Inhalt des ASVS-Standards und unserer Gutachten.

Cyberrisiken frühzeitig erkennen – formale Verifikationsmethoden für IoT

IoT-Geräte verfügen oftmals nur über geringe Rechen- und Speicher-Ressourcen. Dies erschwert die Erkennung von Cyberangriffen direkt am Gerät deutlich. Prävention durch eine frühzeitige Erkennung von potentiellen Schwachstellen ist daher essentiell. Eine rein funktionale Sicherheitsevaluierung ist dabei nicht ausreichend. Beispielsweise können Protokolle auch unter Verwendung von starken kryptographischen Primitiven durch die Art der Komposition der Kommunikation Sicherheitslücken aufweisen. Eine Methode, um strukturiert potentielle Sicherheitsprobleme aufzudecken, sind formale Verifikationsmethoden. Diese Technik beinhaltet logische und mathematische Methoden, mit der design-bedingte Schwachstellen frühzeitig erkannt werden können. Zwei Anwendungsfelder werden detaillierter betrachtet: Einerseits formale Verifikation von Sicherheitseigenschaften von IoT-Protokollen und anderseits formale Methoden für eine Risikoanalyse einer IoT-Architektur am Beispiel der smarten Steuerung einer Wasserversorgungsinfrastruktur.

Katharina Hofer-Schmitz (Joanneum Research)

VPN & RDP als Ressourcen-Killer mit Sicherheitslücken – Homeoffice umsetzen mit einem Zero-Trust-Ansatz?

Benedikt Stürmer-Weinberger (Cordaware)

Aufgrund der aktuelle Situation bleibt das Thema Homeoffice höchst aktuell. Viele Unternehmen entscheiden sich bei der Umsetzung, trotz großer Sicherheitslücken, hoher Investitionen in Hard- und Software und

kostspieligen IT-Know-how, für VPN- und RDP-Lösungen.

Hierbei stellt sich die Frage: Ist das überhaupt noch zeitgemäß und geht das nicht viel effizienter?

»Security by Design«: Mit Methode und Regelwerk Bedrohungen analysieren und Risiken bewerten

Peter Lieber (LieberLieber)

Sicherheitsanalysen etablieren sich nur langsam in den IT-Entwicklungsprozessen. Dabei sind jetzt Software intensive Branchen mit sicherheitskritischer Infrastruktur durch den Regulator dazu verpflichtet, wie zum Beispiel UNECE WP29 / ISO/SAE-21434. Cyber Security Modelling mit ThreatGet setzt »Security by Design« konsequent um. Damit werden mögliche Bedrohungspotenziale identifiziert, dokumentiert und sicherheitskritische Probleme mit Lösungsvorschlägen adressiert.

Als Grundlage dient ein einzigartiger Bedrohungskatalog, der vom Austrian Institut of Technology (»AIT«) entwickelt wurde und über 1'400 Bedrohungsparameter berücksichtigt. Mit ThreatGet steht auch unabhängigen Security-Experten ein neuartiges, methodisches Vorgehensmodell für ihre Kunden zur Verfügung.

ThreatGet wurde vom Report Magazin mit dem »eAward 2020« in der Kategorie »Industrie 4.0« als Kategoriesieger ausgezeichnet.

Sicherheit und Schutz von Software: Neue Methode gegen Raubkopien und Hackerangriffe

Thomas Ziebermayr (SCCH)

Produkte werden immer intelligenter. Angefangen von der smarten Zahnbürste hat mittlerweile beinahe jedes technische Produkt eine Software-Komponente. Insgesamt nimmt der Anteil der Software in Produkten zu. Das beeinflusst sowohl Kosten als auch Funktionalität. Auch die Intelligenz der Produktionsmaschinen wird zunehmend durch Software getrieben. Das bedeutet: immer mehr wertvolles Wissen steckt in der Software, die immer öfter zum Ziel für Hacker wird. Daher sind der Schutz der Software und der Urheberrechte essenziell. Es gibt bereits zahlreiche Lösungen, aber auch einigen Verbesserungsbedarf, sowohl was den praktischen Einsatz als auch die Sicherheit betrifft. Im Vortrag stellen wir einen neuen Ansatz vor an dem wir gerade forschen, um dieses komplexe Problem zu lösen. Das Ziel ist, die Software gegen Attacken von außen abzusichern, Raubkopien zu verhindern und somit das geistige Eigentum der Unternehmen zu schützen. Gemeinsam mit der Münchner Universität der Bundeswehr (Institut für Systemsicherheit), der École Polytechnique Fédérale de Lausanne, der belgischen KU Leuven (Institut für Informatik) und dem Embedded Systems Lab am FH Campus Hagenberg entwickeln die Hagenberger ForscherInnen gänzlich neue Methoden dafür.

Cybersecurity-Herausforderungen im Smart Manufacturing

Erwin Schoitsch (AIT)

Im Rahmen der CON•ECT Informunity wurden viele Themen und Anwendungsdomänen bezüglich (Cyber-)Security-Herausforderungen bereits behandelt, kaum aber das Gebiet der intelligenten industriellen Automation. Aber gerade im Umfeld von »Industrie 4.0« spielt die Vernetzung der (inhomogenen) Teilsysteme, untereinander im Produktionsprozess und mit Logistik- und Supply-Chain-Partnern in der Außenwelt, mit einer Vielzahl von betroffenen Stakeholdern, eine große Rolle, wodurch sie besonders angreifbar werden können für Bedrohungen im Sinne der IT-Sicherheit (Security). Völlig neue Maschinenkonzepte und autonome Entscheidungsprozesse in kritischen Abläufen bieten nicht nur ungeahntes Effizienzpotential in der selbstorganisierenden, flexiblen Produktion, aber im Bedrohungsfall können sowohl Personen als auch große Sachwerte gefährdet werden.

»Smart« kann am besten mit »intelligent« übersetzt werden, im Sinne der Definition durch das ISO Technical Management Board, Strategic Advisory Board bedeutet »smart« »capable of some independent action«, d. h. kann teilweise autonom unabhängige Entscheidungen treffen. Damit sind viele Angriffsflächen und deren Cybersecurity-Risiken offen – werden doch viele neue IT-Technologien miteinander verbunden, wie IIoT (Industrial Internet of Things), Künstliche Intelligenz und Machine Learning, Edge- und Cloud-Technologien, kollaborative und autonome Roboter, Fahrzeuge und

Maschinen, Digital Twin und vorausschauende und -planende Simulation und Wartung, drahtlose Kommunikation, neue Produktionstechnologien. Auch mögliche Industriespionage spielt eine Rolle.

Die Digitalisierung der industrielle Produktion und des gesamten wirtschaftlichen Umfeldes führte zu neuen Schwerpunkten in der Standardisierung: Industrie 4.0, Smart Manufacturing, die Zusammenführung verschiedenster »Assets« aus betroffenen technischen Bereichen, wobei sich in jedem Teilbereich eine Task Force/Task Group zur »Cybersecurity« gebildet hat. Der Vortrag wird einige Smart Manufacturing Use Cases herausgreifen und damit verbundene Cybersecurity-Herausforderungen diskutieren, vom Produktionssystem bis zur KI-Security.

ReferentInnen

Dr. Markus Frank *ist als Rechtsanwalt in Wien spezialisiert auf Datenschutz- und Wirtschaftsrecht. Er beschäftigt sich seit Jahren intensiv mit Datenschutz-Management-Systemen. Er ist als Rechtsexperte im Beirat der Zertifizierungsgesellschaft CIS vertreten und fungiert als Vortragender im Rahmen von Zertifizierungslehrgängen.*

Dipl.-Ing. Dr. Katharina Hofer-Schmitz *ist Senior Researcher in der Forschungsgruppe Cyber Security and Defence am Institut DIGITAL bei JOANNEUM RESEARCH. Sie beschäftigt sich mit ML/AI zur Erkennung von Cyberangriffen sowie formalen Methoden für Security by Design.*

Peter Lieber ist »Parallel Entrepreneur« in der Software Industrie. Seine aktuellen Unternehmen Sparx Systems CE, Sparx Services CE / Switzerland und LieberLieber Software bieten innovationsgetriebene Informationstechnologie: Modellbasierte Software, Consulting, Schulung und Training. Die strategische Ausrichtung dieser Unternehmen hat zum Ziel, Kunden einen substanziellen Beitrag an die digitale und soziale Wertschöpfungskette zu liefern. Mit seiner jüngsten Unternehmensinitiative »THREATGET« bietet er Partnern ein ganzheitliches Framework für das aktuell wichtigste Thema in der ICT: »Cyber Security by Design«.

Peter Lieber ist Präsident des Verbandes österreichischer Softwareindustrie und Präsident des österreichischen Gewerbevereins.

ZT Dr. Wolfgang Prentner, *seit 1998 IT-Ziviltechniker im Fachbereich Informationstechnologie. Geschäftsführer der ZT-PRENTNER-IT GmbH, Gerichtssachverständiger und promovierter Informatiker an der TU Wien. Als unabhängige Prüf- und Überwachungsstelle für Informatik, CyberSecurity, Datenschutz und dem INTERNET-SICHERHEITSGURT unterstützt er außerdem in ehrenamtlicher Funktion die Länderkammer, die Bundeskammer und das Bundeskomitee Die Freien Berufe Österreichs sowie das Bundeskanzleramt seit 2004.*

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.*

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.*

Dipl.-Ing. Erwin Schoitsch *studierte an der TU Wien Technische Physik und zusätzlich Rechentechnik. Er arbeitet seit über 40 Jahren im AIT Austrian Institute of Technology, Safety & Security Department, im Bereich der sicherheitsrelevanten und zuverlässigen Computersysteme, Prozesssteuerungen, Echtzeitsysteme und der kritischen eingebetteten Systeme. Er ist auch seit langem in der internationalen Standardisierung (IEC, ISO) der funktionalen Sicherheit als delegierter österreichischer Experte aktiv.*

Er war und ist in vielen nationalen und Europäischen Forschungsprojekten auf diesem Fachgebiet

tätig, derzeit vor allem in ARTEMIS Projekten (»Advanced Research and Technology for Embedded Intelligence and Systems«), einer spezielle industrienahe Förderschiene des Rahmenprogramms mit eher großen bis sehr großen Forschungsprojekten.

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.*

CONECT BUSINESS ACADEMY

Certified Information Systems Security Professional (CISSP)

In Zusammenarbeit mit SBA Research gGmbH

Referenten:
DI Philipp Reisinger, BSc,
Dr. Ulrich Bayer (SBA Research)

Termin: 13.–17. Sept. 2021, Wien

Inhalte des Seminars

Der Kurs vermittelt den TeilnehmerInnen alle Elemente und Bereiche des Common Body of Knowledge (CBK). Die TeilnehmerInnen lernen dabei die Entwicklung von Sicherheitsrichtlinien, Sicherheit in der Softwareentwicklung, Netzwerkbedrohungen, Angriffsarten und die korrespondierenden Gegenmaßnahmen, kryptographische Konzepte und deren Anwendung, Notfallplanung und -management, Risikoanalyse, wesentliche gesetzliche Rahmenbedingungen, forensische Grundlagen, Ermittlungsverfahren, physische Sicherheit und vieles mehr. Dies alles trägt zu einem stimmigen Sicherheitskonzept und -verständnis bei.

Teilnahmegebühr: € 3.000,–; Prüfung: € 650,–
(Alle Preise + 20 % MwSt.)

Information und Anmeldung: www.conect.at

CONECT BUSINESS ACADEMY

Certified Secure Software Lifecycle Professional (CSSLP)

In Zusammenarbeit mit SBA Research gGmbH

Referent:
Dr. Ulrich Bayer (SBA Research)

Termin: 26.–30. April 2021, Wien

Die Prüfung zum CSSLP umfasst 8 Bereiche, welche alle Bereiche der Softwareentwicklung abdecken. Die KandidatInnen bekommen durch diese Zertifizierung ein breites Verständnis für die technischen, organisatorischen und menschlichen Faktoren, welche für eine ganzheitliche Absicherung des Softwareentwicklungsprozesses zusammenspielen müssen.

1. Secure Software Concepts
2. Secure Software Requirements
3. Secure Software Design
4. Secure Software Implementation/Coding
5. Secure Software Testing
6. Software Acceptance
7. Software Deployment, Operations, Maintenance and Disposal
8. Supply Chain & Software Acquisition

Teilnahmegebühr: € 3.000,–; Prüfung: € 555,–
(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-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 6. 5. 21 kostenfrei an.
- ☐ 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.

2015 Layout: Gerhard Krill