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

Am 6. Mai 2021 fand wieder das Event Security Trends: Cybersecurity, Pentesting, Schutz von Software und DSGVO 2021 statt. Dabei waren die Schwerpunktthemen: die uns weiter begleitende Herausforderung die DSGVO, Security mit Homeoffice und Security Management. Das Event wurde gemeinsam von Future Network und CON•ECT Eventmanagement (www.conect.at) in Kooperation mit dem AIT – Austrian Institute of Technology, SCCH – Software Competence Center Hagenberg und dem Joanneum Research veranstaltet. Das Event wurde virtuell veranstaltet.

Autor: Christoph Schmittner (AIT – Austrian Institut of Technology)

Dr. Markus Frank von Frank Law präsentierte einen Überblick über die DSGVO in 2021. Besonders beleuchtet wurden dabei aktuellen Entwicklungen in der internationalen Rechtslage im Datenaustausch mit der USA und, unter Berücksichtigung des Brexits, auch mit der UK. Die Herausforderung DSGVO kann nicht ausgelagert werden, auch bei kleineren Unternehmen die Daten erheben müssen wird sich diese Herausforderung stellen.

Markus Frank (Frank Law)

Benedikt Stürmer-Weinberger (Cordaware)

Im letzten Jahr wurde das Thema Homeoffice zur neuen Herausforderung. **Benedikt Stürmer-Weinberger** von Cordaware präsentierte Sicherheitsrisiken beim Einsatz von VPN und RDP und einen innovativen neuen Zero-Trust-Ansatz.

Peter Lieber (Lieber-Lieber)

Das Thema Security Management wurde über den kompletten System-Lebenszyklus betrachtet. Herr **Peter Lieber** von LieberLieber Software GmbH stellte das gemeinsam mit dem AIT entwickelte Tool ThreatGet vor. ThreatGet wird zur frühzeitigen und modelbasierten Erkennung von Sicherheitslücken eingesetzt. Auch wenn ThreatGet derzeit primär im Automotivebereich angewandt wird, so kann es dennoch auch in anderen Bereichen zum Einsatz kommen.

Katharina Hofer-Schmitz (Joanneum Research)

Frau Dipl-Ing. Dr. Katharina Hofer-Schmitz vom Joanneum Research demonstrierte die formale Verifikation von Sicherheitseigenschaften im IoT. Hier ist wichtig, dass solche Ansätze gezielt für kritische Elemente eingesetzt werden.

Frau Katharina Hofer-Schmitz aus der Forschungsgruppe Cyber Security and Defence von JOANNEUM RESEARCH – DIGITAL präsentierte in ihrem Vortrag die Anwendung von formalen Verifikationsmethoden zur frühzeitigen Erkennung von Cyberrisiken. Am Beispiel eines smarten Wasserversorgungssystems wurde eine Cyberrisikoabschätzung mit formalen Methoden demonstriert. Am IoT-Protokoll EnOcean wurde die Verifikation und Falsifikation von Sicherheitseigenschaften mit einem Model Checker für Sicherheitsprotokolle gezeigt.

Dr. Thomas Ziebermayr vom SCCH – Software Competence Center Hagenberg berichtete von einem neuen Ansatz, der derzeit in einem europäischen Pilotprojekt entwickelt wird. Eine Software-Komponente kann unter Nutzung von individuellen und einzigarten Merkmalen in der Hardware gegen Angreifer und Reverse Engineering geschützt werden.

Thomas Ziebermayr (SCCH)

Christoph Ritter (SySS GmbH)

Zwei Perspektiven auf das Thema Red-Teaming / Penetration-Testing gab es von **Christoph Ritter** (SySS), **Dr. Wolfgang Prentner** (ZTP.digital) und **Dominik Rieder** (ZTP.digital). Christoph Ritter von SySS zeigte die Unterschiede zwischen Red-Teaming und Penetration-Testing und mögliche Vorgehensweisen beim Red-Teaming für Security. Interessant ist hierbei, dass Red-Teaming nicht nur durchgeführt wird um Sicherheitslücken zu identifizieren, sondern die Ergebnisse auch benutzt werden können, um bessere Akzeptanz für Investition in Sicherheit zu erreichen. Dr. Wolfgang Prentner (ZTP.digital) & Dominik Rieder (ZTP. digital) gaben einen Überblick wie Red-Teaming und Penetration-Testing nachvollziehbar und gerichtsfest durchgeführt und dokumentiert werden können um die Vorgaben für ein IT-Ziviltechnikergutachten zu erreichen. Der Nachweis von Cybersicherheit wird für das EUCC (Common Criteria based European cybersecurity certification scheme) wichtig, zu dem die ENISA (Agentur der Europäischen Union für Cybersicherheit) eine öffentliche Konsultation gestartet hat. Die neue Zertifizierung soll die bestehenden Regelungen im Rahmen des SOG-IS MRA für IKT-Produkte ersetzen, neue Elemente hinzufügen, den Anwendungsbereich auf alle EU-Mitgliedstaaten ausdehnen sowie die bestehenden Normen (ISO/IEC 15408 und ISO/IEC 18045) berücksichtigen.

Wolfgang Prentner (ZTP.digital)

Normen waren das Thema des Abschlussvortrags von Herrn **Erwin Schoitsch** vom AIT der einen Überblick über Standards und Cybersecurity Herausforderungen in Smart Manufacturing gab und die Notwendigkeit der Koordination dieser Entwicklungen betonte.

Erwin Schoitsch (AIT)

CON•ECT .VIDEO

Die Aufzeichnungen der Vorträge des Events finden Sie auf unserem YouTube-Kanal

- https://youtu.be/fE1StjfwQcc – **Peter Lieber** (Lieber-Lieber)
- https://youtu.be/WxMVVQtmgEg – **Christoph Ritter** (SySS GmbH)
- https://youtu.be/Xa-wpdoL5xk – **Benedikt Stürmer-Weinberger** (Cordaware)
- https://youtu.be/sZZoAb4SKgU – **Thomas Ziebermayr** (SCCH)
- https://youtu.be/OljZhhrE_8Q – **Wolfgang Prentner** / **Dominik Rieder** (ZTP.digital)

Kommende Veranstaltungen

- **3. IT-Enterprise Architecture Management (EAM) Hybrid-Konferenz 2021** – am 14. Juni 2021
- **Hybrid Event: 18. Swiss Business & IT-Servicemanagement Forum 2021 (Zürich)** – am 17. September 2021

Kontakt

CON•ECT Eventmanagement | Kaiserstraße 14/2, 1070 Wien | Tel. +43–1-522 36 36 36 | E-Mail: hainschink@conect.at | Website: www.conect.at | Youtube

AGENDA DER VERANSTALTUNG

DSVGO – Lessons learned 2021
Markus Frank (Frank Law)

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

Gerichtstaugliches Pentesting nach ASVS
Wolfgang Prentner (ZTP.digital)

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

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

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

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

Cybersecurity-Herausforderungen in Smart Manufacturing
Erwin Schoitsch (AIT)

Folgende Firmen waren präsent:

DEPS
Innovation für den Schutz von Software

scch { }

- DEPS
  - Kombination von Sicherheitsmechanismen
  - Neu: Verknüpfung von Diversity und PUFs
- Neuigkeiten sowohl in den Teilfeldern, als auch deren Kombination
  - ***Diversity***: Exogene vs. Endogene Eigenschaften
  - ***PUFs***: Periodische Abfrage, größerer Zufallsraum
  - ***Synergie***: Kombination mehr als Summe der Teile
- Hohes Potential
  - Sicherheit
  - Anwendbarkeit

Co-funded by the European Union

What is Smart Manufacturing?

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY TOMORROW TODAY

Acknowledgement:

Most of this work on SM was done in IEC TC65 WG23 in developing SM standards IEC TR 63283-x, in IEC SC65A MT 61508 (Functional safety) and ISO/IEC JTC1 SC42 WG03 (AI Trustworthiness). Figures and tables are taken from working documents to show the directions in which concepts and ideas are developing. Beware that these are intermediate results of work still ongoing, not final standards and recommendations.

AIT contributions were co-funded by the European Commission mainly in ECSEL-projects.

"Smart manufacturing" is defined by ISO/TR 22100-4:2018 as follows:

- manufacturing that improves its performance aspects with integrated and intelligent use of processes and resources in cyber, physical and human spheres to create and deliver products and services, which also collaborates with other domains within enterprises' value chains.
  - Note 1 to entry: Performance aspects include agility, efficiency, safety, security, sustainability or any other performance indicators identified by the enterprise.
  - Note 2 to entry: In addition to manufacturing, other enterprise domains can include engineering, logistics, marketing, procurement, sales or any other domains identified by the enterprise.

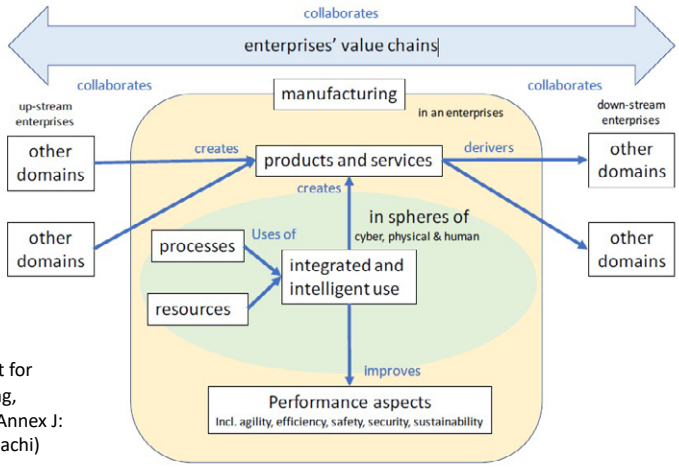
Smartness means Digitalization and Intelligence

- **Note:** ISO/TR 22199-4:2018 - **Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects**
- **Note:** IEC TR 63283-1 ED1; Smart Manufacturing – Part 1: Terms and definitions

What is Smart Manufacturing?
Value Stream between Enterprises

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY TOMORROW TODAY

Graphical representation of the definition of Smart Manufacturing



Source: IEC TC65 WG23, Working draft for IEC TR 63283-1, Smart Manufacturing, Part 1: Terms and definitions, former Annex J: Background and motivation (Koji Demachi)