Online-Event

Security Trends

Cybersecurity – Threat Get – AI-Recht

CONNECT INFORMUNITY

Mittwoch, 15. März 2023
14.00–16.30 Uhr

Online

- **Aktuelle Security-Studie (angefragt)**
- **Security und Artificial Intelligence**
- **Security Testing in complex AI systems – a new challenge**
- **Cyber Security by Design: wie Sie mit Threat Modeling+ Standards, Richtlinien und Normen erfüllen**
- **AI all-überall – Übersicht über Standardisierungsaktivitäten für vertrauenswürdige, sichere KI-Systeme**
- **Industrial Security Standard (IEC 62443) und ISO/SAE 214343 Road vehicles – Cybersecurity engineering**
- **IT-Recht: Hinweisgeberschutzgesetz und NIS-2**
- **Best Practices**

Referenten: **FH Prof. Dipl.-Ing. Peter Kieseberg, MSc.** (FH St. Pölten), **Christoph Schmittner** (AIT), **Dipl.-Ing. Erwin Schoitsch** (AIT), **Michael Krausz** (i.s.c.) und andere
Moderation: **Christoph Schmittner, MSc.** (AIT – Austrian Institut of Technology)

Bei freiem Eintritt!
IT-Anwender werden vorgereiht!

Mit freundlicher Unterstützung von:

AIT Austrian Institute of Technology · fh st.pölten · THREATGET

CONNECT BUSINESS ACADEMY · FUTURE NETWORK

AGENDA

13.30 **Registration und Break zum Networking**

14.00 **Begrüßung durch CON•ECT und Future Network**

14.10 **Security Testing in complex AI systems – a new challenge**
Peter Kieseberg (FH St. Pölten)

14.40 **Cyber Security by Design: Wie Sie mit Threat Modeling+ Standards, Richtlinien und Normen erfüllen**
Christoph Schmittner (AIT)

15.15 **AI all-überall – Übersicht über Standardisierungsaktivitäten für vertrauenswürdige sichere KI-Systeme**
Erwin Schoitsch

16.00 **IT und Recht: NIS-2-Richtlinie**
Michael Krausz (i.s.c.)

16.15 **IT und Recht: Hinweisgebergesetz**
Michael Krausz (i.s.c.)

16.30 **Schlussworte und Ende der Veranstaltung**

Moderation: Christoph Schmittner (AIT)

Security Testing in complex AI systems – a new challenge


Peter Kieseberg (FH St. Pölten)

Durch die stetige Durchdringung vieler Lebensbereiche mit AI, aber auch aufgrund neuer Regularien wie dem AI Act, rückt das Thema der »Vertrauenswürdigen AI« immer weiter in den Vordergrund. Sicherheit ist dabei ein wesentlicher Aspekt, der bisher allerdings etwas in den Hintergrund gerückt war. In diesem Vortrag beschäftigen wir uns damit, warum AI-basierte Systeme nicht einfach neue Programme sind, sondern neue, teils sehr komplizierte Anforderungen an das Thema IT-Sicherheit stellen.

Cyber Security by Design: Wie Sie mit Threat Modeling+ Standards, Richtlinien und Normen erfüllen


Christoph Schmittner (AIT)

Cyber Threats gehen auf 4 Problemfelder zurück. Die Komplexität von Systemen, wie sie die heutige Welt von IoT uns darstellt, sind offene, interagierende Systeme, die manuell nicht beherrschbar sind. Jede Software hat Fehler, was in der Folge alle Systeme eines Unternehmens vulnerabel macht. Bis diese Fehler erkannt werden, vergehen Tage, bis diese Lücken dann geschlossen sind, oft Wochen. Diese Schwachstellen im System erkennen Angreifer leider früher wie das Unternehmen, das Know-how von Angreifern und die Werkzeuge dazu sind heute frei verfügbar. Der Knackpunkt zeigt sich im Entwicklungsprozess von Systemen. Doch hier folgen Security-Überlegungen erst am Schluss, was zu einer unzureichenden Dokumentation führt.

Neue Spielregeln erfüllen mit Threat Modeling+
Diese unzureichende Dokumentation widerspricht branchenspezifischen Standards und Normen, die Unternehmen zu erfüllen haben. So ist zum Beispiel der Industrial Security Standard (IEC62443) zu erwähnen oder auch die ISO/SAE-214343, die Risikoanalyse und Systemdesign gleichermaßen verpflichtend vorsieht. Zukünftig wird durch den Cyber Resilience Act ein solcher Ansatz für alle digitalen Systeme vorgeschrieben.

Threat Modeling+: Digitalisierung der Lösungsfelder mit »Cyber Security by Design«
Mit welchen Lösungen lassen sich diese vier skizzierten Problemfelder gezielt lösen? Der Ansatz von »Cyber Security by Design« mit seiner Umsetzung in Threat Modelling existiert schon länger. Hier geht es darum, potenzielle Gefahren im Systemmodell auf Basis eines Gefahrenmodells zu erkennen. Das AIT Austrian Institute of Technology hat dieses Modellierungs-Verfahren mit Künstlicher Intelligenz und branchenspezifischen Gefahrenkatalogen unter den Namen »ThreatGet« weiterentwickelt. Diese neu entwickelte »Threat Modeling+«-Methodik berücksichtigt zusätzlich das potenzielle Angreifer-Modell und zeigt in der Risikoanalyse auch den Angriffsweg auf einzelne Systemelemente auf. Gefahren werden also über das gesamte System evaluiert, das Entwickeln ganzheitlicher Abwehrmechanismen wird möglich.

Für die Erfüllung von Standards, Normen und Richtlinien ist das Verfolgen dieses Prozesses und die damit verbundene Dokumentation verpflichtend. ThreatGet, wie es vom AIT entwickelt wurde, entdeckt nicht nur automatisiert diese Gefahren, sondern ermöglicht die Rückverfolgbarkeit und dokumentiert sie richtlinienkonform.

AI all-überall – Übersicht über Standardisierungsaktivitäten für vertrauenswürdige sichere KI-Systeme


Erwin Schoitsch (AIT)

- AI ist ein »Hype« – in fast allen Domänen wird KI eingesetzt und bilden sich Standardisierungsgruppen
- Das Ende klassischer Safety- und Security-Betrachtungen – verallgemeinerter Vertrauenswürdigkeitsbegriff (»Trustworthiness«)
- Allgemeine AI-Standardisierung in ISO/IEC JTC1 SC42, besonders in WG 03 »Trustworthiness«: Behandelte Aspekte im Überblick
- Funktionale Sicherheit und AI – Ergebnis der Zusammenarbeit der IEC 61508-3 (Funktionale Sicherheit, Software) und ISO/IEC JTC1 SC42 (Artificial Intelligence)
- Cybersecurity und AI: ETSI SAI Group (Secure AI) – Schutz von AI Systemen/Schutz durch AI
- Domänen-spezifische Anwendungen:
  - Sicherheit von AI in Straßenfahrzeugen (WG14, PAS 8800) und Automated Driving Systems (WG13, E06 AI/ML),
  - Smart Manufacturing und Cybersecurity

NIS-2


Michael Krausz (i.s.c.)

Die mit Ende 2024 gültig werdende NIS-2-Richtlinie erweitert den Kreis betroffener Unternehmen massiv. Umfasst sind künftig auch medizinische Labore, Hersteller von Medizinprodukten, Produktions- und Handelsbetriebe von chemischen Stoffen, Maschinenbauer, Automobilzulieferer, Forschungseinrichtungen, MSSP-Anbieter, Cloud-Anbieter, Rechenzentrumsdienstleister, sowie weitere. Da auch NIS-2 strafbewehrt ist, mit Strafen mit einem Höchstrahmen von mindestens 10 Millionen Euro oder 2 % des weltweiten Umsatzes, ist es notwendig, sich jetzt bereits entsprechend vorzubereiten. Der Vortrag umfasst die Kernelemente von NIS-2 und deren Zusammenspiel mit einem bestehenden ISMS mit oder ohne ISO 27001.

Hinweisgeberschutzgesetz

Michael Krausz (i.s.c.)

Mit Ende dieses Jahres wird das Hinweisgeberschutzgesetz wirksam. Betrieb über 50 Mitarbeitern müssen zwingend ein Meldesystem einrichten. Im Vortrag erfahren Sie, wie Sie dieses kostenoptimiert implementieren können.

Referenten

Peter Kieseberg *erhielt seinen Abschuss in »Technische Mathematik in den Computerwissenschaften« an der Technischen Universität Wien. Im Anschluss arbeitete er als Associate Consultant bei Benmark, sowie als Consultant bei NEWCON im Bereich Telekommunikation, speziell in den Bereich Interconnection Billing und DWH/BI. Set Mai 2010 ist er Research Manager und Forscher bei SBA Research, seine Spezialisierungen liegen dabei in den Bereich der digitalen Forensik, sowie des Fingerprintings strukturierter Daten, speziell auch im medizinischen Bereich. Zudem ist er Mitglied bei IEEE SMC und ACM. Seit November 2017 ist er Institutsleiter am Institut für Sicherheitsforschung an der FH St. Pölten.*

Michael Krausz *studierte Physik, Informatik und Rechtswissenschaften in Österreich und den USA. Er ist einer der Pioniere der Informationssicherheit im DACH-Raum, ISMS-Auditor seit 2002 und hat seit 1998 in 32 Ländern auf 4 Kontinenten ISMS-Projekte als Berater oder Auditor durchgeführt. Herr Krausz ist Autor von sechs einschlägigen Fachbüchern, darunter dem Bestseller Managing Information Security Breaches – Real Life Stories, der gerade in seine dritte Auflage geht. Seine Expertise ist weltweit gefragt, zu seinen Kunden gehören nationale und internationale Unternehmen von einem Mitarbeiter bis zu 500.000.*

Christoph Schmittner, MSc, *Center Digital Safety & Security, AIT Austrian Institute of Technology. Christoph Schmittner leitet ein Team für Safety und Security Engineering mit Fokus auf den Automobil- und*

Industriebereich. Er beschäftigt sich mit der Methode und Analyse von sicherheitskritischen / fehlertoleranten Systemarchitekturen, ist Experte in internationalen Normungsgruppen wie zum Beispiel TC65/AHG2 »Reliability of Automation Devices and Systems« sowie Projektleiter für die Entwicklung von ISO PAS 5112 »Road vehicles – Guidelines for auditing cybersecurity engineering«.

Dipl.-Ing. Erwin Schoitsch *arbeitet seit mehr als 50 Jahren in verschiedenen Positionen für das AIT Austrian Institute of Technology bzw. deren Vorgängerinstitutionen. Er war jahrzehntelang mit der Entwicklung sicherheitsrelevanter Systeme im industriellen und Forschungsbereich betraut. Seit seinem Pensionsantritt 2010 arbeitet er unter anderem auch für das AIT als »Freier Dienstnehmer« in verschiedenen großen, industrienahen EU Forschungsprojekten, z. B. AI4CSM (Automotive Intelligence for Connected, Shared Mobility), AIMS5.0 (Artificial Intelligence in Manufacturing leading to Sustainability and Industry5.0), oder dem nationalen FFG Projekt ADEX (AutonomousDriving Examiner). Schwerpunkt seiner Beiträge sind jeweils die Standardisierungsthemen (Transfer in beide Richtungen zwischen Projekt und Standards), betreffend die Sicherheit (Trustworthiness) von hochautomatisierten, kritischen und komplexen Systemen, aber auch der Nachhaltigkeits- und ethischen Aspekte. Von besonderer Bedeutung ist dabei die jahrelange Erfahrung und der umfassende Überblick über die relevanten Standardisierungs-Landschaften und Eco-Systeme. Er war von Beginn an (80-er Jahre) aktiv an der Entwicklung des grundlegenden Funktionalen Sicherheitsstandards IEC 61508 beteiligt, und ist es bis heute in der Erarbeitung der Ed. 3. Gegenwärtig kommen noch die industriellen Cybersecurity Standards (IEC 62443 Gruppe), Automotiven Standards (ISO TC 22 SC32 Safety, Cybersecurity, AI, Autonomes Fahren) und Smart Manufacturing Standards (Safety, Security, Digital Twin) in IEC, ISO und ISO7IEC JTC1 hinzu. Artificial Intelligence wird domänen-unabhängig in ISO/IEC JTC1 SC42 (AI) behandelt, wo er Mitglied in WG03 (Trustworthiness) und WG05 (Computational approaches and computational characteristics of AI) ist. Selbstverständlich ist er auch in den nationalen Spiegelkomitees ÖVE (für IEC, CENELEC, ETSI und Teile von ISO/IEC JTC1) und ASI (Austrian Standards International, für ISO, CEN und Teile von ISO/IEC JTC1), die ja die von Österreich zu entsendenden Experten benennen.*

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)

Termine auf Anfrage

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

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: IT Entscheidungsträger, CISOS, Security-Verantwortliche, Governance, Compliance, Softwareentwicklung und Verantwortliche für Security by Design, Digitalisierungsverantwortliche aller Branchen, Verantwortliche in der Produktion

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 15. März 2023 kostenfrei an (IT-Anwender werden vorgereiht:

Ich bin ☐ IT-Anwender, ☐ IT-Anbieter

☐ 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:

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.

23020 Layout: Gerhard Krill