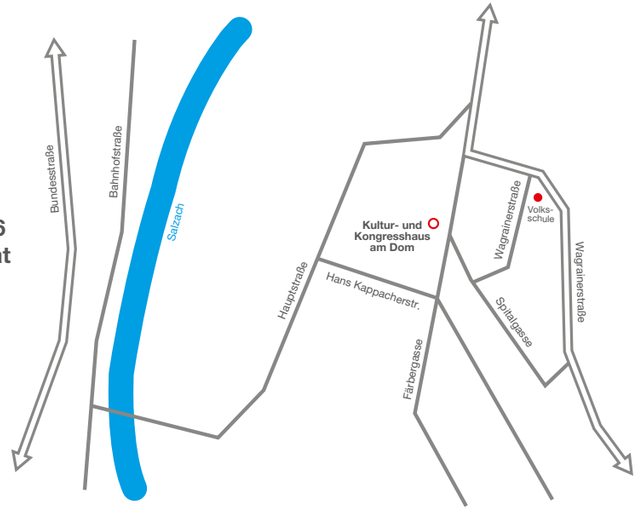
IKT-SICHERHEITS-KONFERENZ 2016

KULTUR- UND KONGRESSHAUS AM DOM

Um Anmeldung für die Veranstaltung bis **29.09.2016** wird gebeten unter **https://seminar.bundesheer.at**
Rückfragen: ikt.sih.info@bmlvs.gv.at

Anreise:
KULTUR- UND KONGRESSHAUS AM DOM
Leo-Neumayr-Platz 1, 5600 St. Johann im Pongau
Telefon: +43 (0)6412 8080-0

Anfahrtsplan über Google Maps!
Besucherparkplatz gemäß Anmeldeseite



upart

NCI AGENCY · Bundesministerium der Verteidigung · CODE Forschungszentrum Cyber Defence Universität der Bundeswehr München · Universität der Bundeswehr München · Ministerie van Defensie · INTERPOL

BM.I Republik Österreich Bundesministerium für Inneres · Bundeskanzleramt Österreich · FH Oberösterreich · sicsict · si Sichere Informationssysteme · T-Systems

PAN AMP · NSIDE Attack Logic · CYBER SECURITY AUSTRIA · AIT Austrian Institute of Technology Tomorrow Today · ZAMG

A1 · HISOLUTIONS · COMPASS SECURITY · innoSec · Barracuda · HACKNER Security Intelligence

Atos · austro CONTROL · itWatch GmbH · KORAMIS · kapsch challenging limits · UNINET It-consulting GmbH

www.bundesheer.at

IKT-SICHERHEITS-KONFERENZ 2016

ABWEHR AMT

IKT-SICHERHEITS-KONFERENZ

Sankt Johann Alpendorf · St. Johann Salzburg · LAND SALZBURG

SCHUTZ DURCH HILFE

PROGRAMM 11. UND 12.10.2016

08:00–09:30
Administration und Empfang

09:30–09:45
Agenda und Begrüßungen

09:45–10:05
11.10.2016:
Cyber threat and Defence

Brigadier General J.M. (Hans) FOLMER MSc MSS / Defence Cyber Command, NL

12.10.2016:
Next Generation of NATO's Cyber Defence: consolidation, modernization and collaboration

Ian J WEST / Cyber Security NATO Communications and Information Agency, BE

10:05–10:25
11.10.2016:
Digitale Transformation – die Chancen sind klar, die Gefahren auch?

Dr. Wieland ALGE / BARRACUDA Networks AG

12.10.2016
Innovation versatility at the borders of assured networks

Anders STRÖMBERG / Advenica, SE

10:30–11:10
Der russisch-ukrainische Cyberwar – eine Analyse der Aktionen im Cyberraum aus offenen Quellen

Volker KOZOK / BMVg Bundeswehr, DEU

11:15–11:55
A new concept of a self-learning intelligence platform

Frederic BOUY / Atos IT Solutions and Services GmbH

11:55–13:15
Mittagspause

13:15–13:55
Live-Hacking 4.0 – Internet of Things als neue Spielwiese für Cyberattacken

Marco DI FILIPPO / KORAMIS, DEU

14:00–14:40
Die Rolle von INTERPOL bei der Bekämpfung der Cyber-kriminalität

Dr. Thomas HERKO / INTERPOL Global Complex for Innovation, SINGAPUR

14:45–15:25
Social Engineering:
The devil is in the details

Ivano SOMAINI / Compass Security, CH

15:25–16:00
Pause

16:00–16:40
Ein Ex-Hacker redet wieder Tacheles

Gunnar PORADA / InnoSec GmbH, CH

16:45–17:25
11.10.2016:
Offline! Wie abhängig sind wir vom Internet?

Dr. Thomas GRÜTER, DEU

12.10.2016:
Cyberwar – Sorglosigkeit in Zeiten der vernetzten Kriegsführung

Bert WEINGARTEN / PAN AMP AG, DEU

17:30–18:00
Cyber Security Challenge-Präsentation der Challenges, Cyber Verteidigungszentrum – aktuelle Lage

AbwA

18:00–20:00
Networking Lounge
Music

IKT-Sicherheit stellt uns ständig vor neue Herausforderungen. Deshalb: Gemeinsam für Österreichs Sicherheit.

FACHVORTRÄGE 11.10.2016

CYBERSECURITY

10:30–11:10
Intelligent Network Reconnaissance – Tactial Network Mapping

DI Stefan MARKSTEINER / Joanneum Research

11:15–11:55
Digitale Ausweise für physische Identifikation?

Dr. Rene MAYRHOFER / JKU

13:15–13:55
Thunderstorm in the cloud – investigating security incidents in the cloud

Mathias FUCHS / Mandiant

14:00–14:40
Die Malwarelandschaft im Wandel der Zeit

Florian BOGNER / Kapsch BusinessCom AG

14:45–15:25
Neue Cybersecurity-Trends: Wie können Sie Ihre Netzwerke und Kommunikation vor Malware und Spionage schützen?

DI Volker MAX / Rohde&Schwarz

16:00–16:40
Angewandte Forschung für Law Enforcement

Dr. Edgar WEIPPL / SBA Research

16:45–17:25
Cyber-Cluster an der Universität der Bundeswehr München

Dr. Gabi DREO RODOSEK, Forschungszentrum Cyber Defence, Universität der Bundeswehr, DEU

KRITISCHE INFRA

10:30–11:10
DDOS Attacke gegen A1 Telekom Austria 2016

Dr. Wolfgang SCHWABL / A1 Telekom Austria AG

11:15–11:55
Krankenhäuser im Feuer der Ransomware – über die Angreifer, die Angriffe und Gegenmaßnahmen

Mag. Harald REISINGER / Radar Services Smart IT-Security GmbH

13:15–13:55
Dealing with state sponsored attacks

Diego SCHMIDLIN / Ruag Schweiz AG

14:00–14:40
Terrorabwehr in 4 Dimensionen

Bgdr Mag. Karl GRUBER / BMLVS Leiter Teilstab Luft

14:45–15:25
How to hack your critical infrastructure

DI Thomas BLEIER, MSc

FACHVORTRÄGE 11.10.2016

16:00–16:40
Schutz kritischer Infrastruktur in Österreich – eine wichtige Aufgabe des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung

Mag. Sylvia MAYER, DI Philipp BLAUENSTEINER / Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung

16:45–17:25
IKT Sicherheit in der Luftfahrt

Dr. Werner LANGHANS / Austro Control

INDUSTRIE 4.0

10:30–11:10
Cyber Security in industrial supply chains

DI Herbert DIRNBERGER, Florian BRUNNER / Cyber Security Austria

11:15–11:55
CEO Fraud – im Spannungsfeld zwischen Technik und dem Faktor Mensch

DI Robert LAMPRECHT / KPMG Austria GmbH

13:15–13:55
Erkennen von Anomalien in IKT Netzen mit AECID und reale Anwendungsbeispiele

Roman FIEDLER / AIT

14:00–14:40
Das Märchen vom Air-Gap – Angriffe auf Industrieanlagen

Rainer GIEDAT / NSIDE ATTACK LOGIC GmbH, DEU

14:45–15:25
Industrial Security Qualifizierung als Wegbereiter für die Industrie 4.0

DI Dr. Franz FIDLER, DI Dr. Paul TAVOLATO / FH St. Pölten

16:00–16:40
Industrie 4.0 – nicht ohne adäquate IT-Sicherheit

Ramon MÖRL / itWatch GmbH, DEU

16:45–17:25
Wenn das Werk nicht mehr an der Werksgrenze aufhört. Security in der total vernetzten Industrie

Dr. Wieland ALGE / BARRACUDA Networks AG

FACHVORTRÄGE 12.10.2016

INTERNET OF THINGS

10:30–11:10
Überblick über IT-Trust im Zeitalter des Kontrollverlustes

Dr. Alexander LÖW / Data-Warehouse GmbH, DEU

11:15–11:55
Gefahren und Risiken im Bereich der Medizintechnik

DI Alexander MENSE / Technikum Wien

13:15–13:55
SmartCity und SmartLiving – Anonymisierung und Pseudonymisierung

Philipp SCHAUMANN / Sicherheitskultur.at

14:00–14:40
Sicherheit und vernetzte Mobilität – ein Widerspruch?

DI Oliver SCHMEROLD / ÖAMTC

14:45–15:25
Datenrecovery von Mobilen Geräten

DI Robert KOLMHOFER / FH Hagenberg/Uninet

16:00–16:40
Strengthening cybersecurity at the Tour de France

Daniel MIEDLER / Dimension Data

16:45–17:25
Cyber-Risiken – Mittelstand in Gefahr!

Dipl.-Betriebswirt (Ba) Hendrik Florian LÖFFLER / Funk International Austria GmbH

KRITISCHE INFRA

10:30–11:10
Sonnig mit der Aussicht auf /if/dev=zero

DI Mag. TSCHABUSCHNIG / ZAMG

11:15–11:55
Houston – we have a problem! Cyber Crisis Communication done right

Martin KRUMBÖCK / Mandiant

13:15–13:55
Meta-Risk: Meta-Risiko-Modell für kritische Infrastrukturen

Di Johannes GÖLLNER, MSc / BMLVS, DI Christian Meurers, / BMLVS, Univ.prof. Ddr. Gerald Quirchmayr / Uni Wien

14:00–14:40
IT-Gefahren im Hinblick auf militärische Auslandseinsätze

Christoph Willer / Militärischer Abschirmdienst, DEU

14:45–15:25
Kritische Infrastrukturen – IT-Security am Beispiel Red Bull

Jimmy HESCHL / Red Bull

FACHVORTRÄGE 12.10.2016

16:00–16:40
Sind wir bereit? Katastrophenvorsorge im E-Government Bereich

ADir Florian BILEK / BKA

16:45–17:25
Netz- und Informationssicherheit in Europa/ Österreich – eine rechtliche Einführung

Dr. Peter BURGSTALLER / FH Hagenberg

INDUSTRIE 4.0

10:30–11:10
Security in der smart factory

Hans-Peter ZIEGLER / Copa-Data GmbH

11:15–11:55
Industrie 4.0 und die daraus resultierenden Sicherheitsanforderungen

Andreas SALM / HiSolutions AG, DEU

13:15–13:55
Industrial Security: Red Team Operations

Thomas HACKNER / Hackner Security Intelligence

14:00–14:40
IT-Sicherheit für den Einsatz von Smart Metering – besonders schützenswerte Datenströme und Daten, Risiko-Szenarien in Smart Metering Umgebungen und die Konzeption von IT-Sicherheitsmaßnahmen

Mag. Harald REISINGER / Radar Services Smart IT-Security GmbH

14:45–15:25
Das Märchen vom Air-Gap – Angriffe auf Industrieanlagen

Rainer GIEDAT / NSIDE ATTACK LOGIC GmbH, DEU

16:00–16:40
Detektive und reaktive Sicherheitsmaßnahmen in industriellen Umgebungen

Thomas MASICEK, MSc und Herwig KÖCK / T-Systems Austria GesmbH

16:45–17:25
Digitalization Requires Intelligent Information Security

Anders Strömberg / Advenica, SWE

KRITISCHE INFRASTRUKTUR – 11 10 2016

DDOS ATTACKE GEGEN A1 TELEKOM AUSTRIA 2016 – A1 TELEKOM AUSTRIA AG - DR. WOLFGANG SCHWABL

Erfahrungen aus der bisher größten DDoS Attacke in Österreich.
Wie lief die Attacke ab?
Was bewirkte die Attacke?
Warum waren Internetdienste für Kunden beeinträchtigt?
Welche Maßnahmen ergriff A1?
Welche Lehren können daraus gezogen werden?

KRANKENHÄUSER IM FEUER DER RANSOMWARE – ÜBER DIE ANGREIFER, DIE ANGRIFFE UND GEGENMAßNAHMEN – RADAR SERVICES – MAG. HARALD REISINGER

Dieser Vortrag analysiert die derzeitige Welle von Ransomware-Angriffen auf Krankenhäuser und öffentliche Einrichtungen in DEU, USA und Kanada. Hintergründe, Vorgehensweise und Motivation der Angreifer werden beleuchtet. Zudem werden konkrete Präventions- und Schutzmechanismen für solche Angriffe sowie Reaktionsmaßnahmen erläutert.

DEALING WITH STATE SPONSORED ATTACKS. - RUAG SCHWEIZ AG – DIEGO SCHMIDLIN

TERRORABWEHR IN 4 DIMENSIONEN – BMLVS/LEITER TEILSTAB LUFT - BGDR MAG. KARL GRUBER

Die Überwachung und Durchsetzung eines Flugbeschränkungsgebietes zum Schutz einer Großveranstaltung gegen terroristische Einwirkung aus der Luft stellt in Hinblick auf Raum und Zeit eine besondere Herausforderung an die eingesetzten Kräfte und Mittel dar. Die Produktion eines als Entscheidungsgrundlage für Warnungen oder einen Waffeneinsatz rechtlich und betrieblich geeigneten Luftlagebildes bedarf einer Verknüpfung von Daten innerhalb weniger Sekunden. Das eingesetzte Führungsinformationssystem muss kritische Abläufe innerhalb weniger Minuten gewährleisten. Entsprechend groß und Komplex ist die den Entwicklern des IKT-Systems gestellte Aufgabe.

HOW TO HACK YOUR CRITICAL INFRASTRUCTURE – DI THOMAS BLEIER MSC

In letzter Zeit hört man immer öfter erfolgreiche, gezielte Angriffe auf die Infrastruktur von Unternehmen oder Organisationen wie zuletzt beispielsweise auf das Stromnetz der Ukraine, der Cyber-Bankraub in 2015 oder der Angriff auf Sony Pictures. Daraus kann man inzwischen schon fast sowas wie ein „How to“ ableiten, wie man am besten die IT-Infrastruktur eines Unternehmens angreift oder aber sich ansehen, was man aus diesen Angriffen für den Schutz der eigenen Systeme lernen kann, und genau das ist das Ziel dieses Vortrags.

SCHUTZ KRITISCHER INFRASTRUKTUR IN ÖSTERREICH – EINE WICHTIGE AUFGABE DES BUNDESAMTES FÜR VERFASSUNGSSCHUTZ UND TERRORISMUSBEKÄMPFUNG –

BUNDESAMTES FÜR VERFASSUNGSSCHUTZ UND TERRORISMUSBEKÄMPFUNG - MAG. MAYER SYLVIA, DI BLAUENSTEINER PHILIPP

Der Schutz kritischer Infrastrukturen ist seit 2014 eine gesetzliche Aufgabe der Sicherheitsbehörden in Österreich. Seitdem wurden umfangreiche organisatorische Maßnahmen getroffen, um die durch Kriminalität, Terrorismus und vor allem Hackerangriffe gefährdeten strategisch wichtigsten Unternehmen Österreichs vor einem Ausfall oder einer Störung schützen zu können – Stichwort: Prävention.

Dieser Vortrag informiert über die staatlichen Strukturen in Österreich, deren Zielsetzungen, die Mittel und Maßnahmen sowie über aktuelle Entwicklungen im Zusammenhang mit dem Thema „Schutz kritischer Infrastrukturen" unter besonderer Berücksichtigung des Aspekts „Cyber-Sicherheit".

IKT SICHERHEIT IN DER LUFTFAHRT – AUSTRO CONTROL - DR. LANGHANS WERNER

INDUSTRIE 4.0 – 11 10 2016

CYBER SECURITY IN INDUSTRIAL SUPPLY CHAINS – CYBER SECURITY AUSTRIA - DI HERBERT DIRNBERGER, FLORIAN BRUNNER

Die technologischen Fortschritte verändern die Art der Zusammenarbeit in Organisationen und Lieferketten. Geschäftsprozesse werden digitalisiert, effektiver und disruptive Innovationen verändern das Zusammenspiel am Markt. Von diesen digitalen Transformationen sind nicht nur einzelne Unternehmen betroffen sondern auch gesamte Industrielle Wertschöpfungsketten. Grundlage für die Zusammenarbeit von Unternehmen in der Wertschöpfungskette sind Vertrauen, Transparenz und gemeinsames Verständnis für Risiken und Chancen.
Mit dem Tempo der technologischen Veränderungen steigen unter anderem auch die Bedrohungen durch Cyber Kriminalität, Wirtschaftsspionage und Datenmanipulation speziell entlang Lieferkette unternehmensübergreifend. Zudem ist vermehrt festzustellen dass die Systeme komplexer und Resilienzfähigkeit von beteiligten Organisationen und Mitarbeitern rapide abnimmt.
Industrielle Supply Chains sind meist global vorhanden und bieten eine immense Angriffsfläche für Cyberangriffe. Meist werden unsichere Zulieferer gewählt, um die gesamte Lieferkette zu gefährden. Die Bedrohungen von Supply Chains sind vielfältig: Diebstahl, Erpressung, Wirtschaftsspionage, Sabotage uvm.
In diesen Vortrag werden möglichen Bedrohungen, Schwachstellen und daraus resultierende Risiken in industriellen Lieferketten und Versorgungsnetzen kritischer Infrastruktur vorgestellt und konkrete Maßnahmen erläutert wie die Risiken gemindert werden können.

CEO FRAUD - IM SPANNUNGSFELD ZWISCHEN TECHNIK UND DEM FAKTOR MENSCH – KPMG AUSTRIA GMBH - DI ROBERT LAMPRECHT

Österreich erlebte vor knapp einem Jahr durch die Medien, dass der CEO Fraud auch hierzulande Einzug gehalten hat. Einige Fälle wurden medial bekannt jedoch beim Großteil der Vorfälle schweigen Unternehmen. Die kolportieren Schäden nehmen unglaubliche Ausmaße an und schädigen Unternehmen nachhaltig, ja können sogar existenzbedrohend sein. In der Wahrnehmung vieler Personen manifestiert sich der Eindruck, dass es mit technischen Mitteln zu lösen sein muss, andere wiederum meinen dass ausschließlich Awareness das probate Mittel ist. Im Rahmen des Vortrags sollen unterschiedliche Vorgehensweise der Angreifer aufgezeigt werden, Lösungsansätze vorgestellt werden und ein Lagebild zur Situation bei österreichischen Unternehmen vorgestellt werden

ERKENNEN VON ANOMALIEN IN IKT NETZEN MIT AECID UND REALE ANWENDUNGSBEISPIELE – AIT - ROMAN FIEDLER

Entwicklung von neuartigen Anomalieerkennungsalgorithmen für kritische Infrastrukturbetreiber um Abweichungen im Systemverhalten von IKT Netzen zu erkennen, die potentiell aus Angriffen und IKT-Sicherheitsproblemen resultieren. Mittlerweile ist dieses System bei Industriepartnern einige Zeit im Einsatz. Im Vortrag wird das neuartige Konzept, als auch Lessons learned vorgestellt.
Die Präsentation ist sehr stark technisch und v.a. für Personen im operativen IKT Umfeld relevant -- hat aber v.a. in Bezug auf Diskussionen rund um APTs und mehrstufiger Angriffe höchste Relevanz, welche mit den gängigen Signaturbasierten Ansätzen nicht mehr hinreichend bewältigt werden können.

DAS MÄRCHEN VOM AIR-GAP - ANGRIFFE AUF INDUSTRIEANLAGEN - NSIDE ATTACK LOGIC GMBH, DEU - RAINER GIEDAT

Die Vernetzung von Industrieanlagen wird durch Industrie 4.0 weiter zunehmen, war aber lange vorher schon an der Tagesordnung. Versucht ein Angreifer in Steuerungsnetzwerke einzudringen und dort entsprechenden Zugang auf die Fertigungsanlagen zu erlangen, kann er sich diese Vernetzung zu Nutze machen. Diesem Risiko wurde bisher häufig mit einer strikten Trennung der Netze (Air-Gap) begegnet, doch diese hat sich in all unseren bisherigen Tests als überwindbar herausgestellt. Der Vortrag zeigt mit Live-Demonstrationen, wie Angreifer vorgehen und berichtet von Erfahrungen aus zahlreichen Penetrationstests von Industrieanlagen.

INDUSTRIAL SECURITY QUALIFIZIERUNG ALS WEGBEREITER FÜR DIE INDUSTRIE 4.0 - FH ST. PÖLTEN - DI DR. FRANZ FIDLER/DI DR. PAUL TAVOLATO

Mit der zunehmenden Vernetzung von Fertigungsanlagen, von Maschinen und von Stakeholder - vom Lieferanten über den Produzenten bis zum Kunden - im Rahmen von Industrie 4.0, steigt auch das Angriffsrisiko. Wie gelingt aber die Absicherung von Stakeholder- und unternehmensübergreifenden Wertschöpfungsketten? Wie kann IT-Security in vernetzten Produktionsanlagen und in den sogenannten Cyber-physischen Systemen effizient gestaltet werden? Das sind neue Herausforderungen, die alle Produktionsstätten mit zunehmender Digitalisierung betreffen und mit denen sowohl Betreiber als auch Entwickler in Zukunft konfrontiert werden. Der Vortrag postuliert Industrial Security als einen der zwingend notwendigen Wegbereiter für die Produktion der Zukunft. Damit rücken auch neue Qualifizierungsanforderungen und -angebote in den

Vordergrund, die als eine notwendige Grundausbildung aktuellen Trends vermitteln, über Schwachstellen diskutieren, Risiken identifizieren und passende Methoden der Industrial Security vermitteln.

INDUSTRIE 4.0 - NICHT OHNE ADÄQUATE IT-SICHERHEIT – ITWATCH, DEU - RAMON MÖRL

Industrie 4.0 senkt die Kosten, steigert die Effizienz und ermöglicht gleichzeitig kleinere Produktionschargen. Industrie 4.0 ist nur durch eine verstärkte Vernetzung und intensivere Nutzung klassischer ITK möglich – dabei ersetzen kostensenkende Funktechnologien zunehmend die teuren Kabelbäume. Als Nebeneffekt sind klassische Angriffe auf ITK dadurch eine Bedrohung für Industrie 4.0 Systeme.
Im Vortrag werden die versteckten Angriffsvektoren aufgezeigt und geeignete Lösungsarchitekturen dargestellt, die für jeden Geldbeutel passen. Wesentliches Augenmerk liegt auf Skalierung in der Steigerung der IT-Sicherheit und der Skalierung der Menge / Größe, Durchsatzfaktoren, so dass jeder seine "adäquate" Lösung nach Leistung, Preis und Ergonomie definieren kann.

WENN DAS WERK NICHT MEHR AN DER WERKSGRENZE AUFHÖRT. SECURITY IN DER TOTAL VERNETZTEN INDUSTRIE – BARRACUDA – DR. WIELAND ALGE.

CYBERSECURITY – 11 10 2016

INTELLIGENT NETWORK RECONNAISSANCE – TACTIAL NETWORK MAPPING – JOANNEUM RESEARCH - DI STEFAN MARKSTEINER

Durch die stetige Entwicklung und zunehmende Komplexität moderner IKT-Netzwerke hat sich die Aufgabe, potentielle Sicherheitslücken zu finden und entsprechende Audits durchzuführen, zu einem wichtigen Element entwickelt, um diese Netzwerke abzusichern. Der erste Schritt hierzu ist es, einen möglichst detaillierten Überblick über deren Struktur zu erhalten, was auch als Network Reconnaissance oder Mapping bezeichnet wird. Gerade die Komplexitätszunahme macht diese Aufgabe jedoch zunehmend aufwändig, umso mehr, als Network Mapping - im Gegensatz zu simplen Host-Scanning - noch immer einen hohen Anteil an manueller Arbeit erfordert.

Hier wird daher ein Werkzeug vorgestellt, welches das Scanning und Mapping von unbekannten und nicht-kooperativen Netzwerken automatisiert und dadurch dazu beiträgt, die Cybersicherheit durch das Entdecken von potentiellen Schwachstellen zu erhöhen. Darüber hinaus erleichtert das Tool, Audits durchzuführen, indem es erlaubt, existierende Netzwerkdokumentationen mit der Realität zu vergleichen und unautorisierte Geräte zu entdecken.

Das Tool bietet einen neuartigen Ansatz, der effektiv State-of-the-Art Netzwerkscanner in einem iterativen Prozess mit proprietären Analysemodulen kombiniert, welche die gefundenen Daten mit Kontext bereichern. Das erlaubt die Topologie eines Netzwerks darzustellen anstatt nur eine Liste gescannter Geräte zu erzeugen. Das Ziel ist es dabei, mit einem Minimum an nötigem Vorwissen ein möglichst umfassendes Bild der Topologie zur Verfügung zu stellen. Ferner ist ein Visualisierungsmodell enthalten, welches einen klaren, verständlichen Überblick über das Netzwerk in Form einer interaktiven Topologiekarte bietet. Das Werkzeug verfügt über einen hochmodularen

Aufbau. Dadurch lässt sich das Tool einfach um weitere Funktionalitäten erweitern. Ein revisionsbasiertes Datenspeichersystem ermöglicht Vergleiche zwischen Scans zu verschiedenen Zeitpunkten und in verschiedenen Netzwerken.

DIGITALE AUSWEISE FÜR PHYSISCHE IDENTIFIKATION? – JKU – DR. RENE MAYRHOFER

Digitale Identitäten werden bereits vielfach für die Anmeldung bei digitalen Diensten verwendet. Österreich hat durch die Bürgerkarte bereits seit langer Zeit die Möglichkeit zur Identifikation bei e-Governent und anderen Web-Anwendungen auf hohem technischen Niveau geschaffen, und andere Länder haben zum Teil ähnliche Lösungen entwickelt und ausgerollt. Der nächste Schritte in der Digitalisierung von Identitäten ist die physische Personen-Identifikation, also alle Anwendungsfälle, in denen aktuelle, physische Lichtbildausweise verwendet werden. Von der Vertragserstellung über Verkehrskontrollen bis hin zu Grenzübertritten sind solche physischen Ausweise weiterhin notwendig. In diesem Vortrag werden die grundlegenden Herausforderungen diskutiert, welche beim Einsatz digitaler Identitäten für solche Anwendungsfälle zu lösen sind. Besonders das Zurückrufen von zuvor ausgestellten digitalen Ausweisen für Geräte, die nicht ständig online sein können, ist ein noch nicht vollständig gelöstes Problem. Dieser Vortrag skizziert zukünftige Möglichkeiten, Identitätsdokumente sicher am Mobiltelefon zu verwalten und gibt einen kleinen Einblick in aktuelle Forschungsarbeiten zu diesem Thema.

THUNDERSTORM IN THE CLOUD - INVESTIGATING SECURITY INCIDENTS IN THE CLOUD – MANDIANT - MATHIAS FUCHS

Currently more and more companies are outsourcing or cloud-sourcing parts of their IT-Services or even their full IT. This creates a great deal of complications when it comes to security incident. In this talk we will explain strategies on how to use Cloud services and still be able to react to a security breach. Furthermore, we will elaborate how investigations in the cloud differ based on a case study.

DIE MALWARELANDSCHAFT IM WANDEL DER ZEIT – KAPSCH BUSINESSCOM AG – FLORIAN BOGNER

Die IT im Allgemeinen und die IT Security im Speziellen sind extrem schnelllebige Themengebiete. Taktiken die von Angreifern bis vor wenigen Jahren sehr erfolgreich eingesetzt wurde, gehören heute zum alten Eisen. Dafür setzen die Betrüger heute auf andere Tools und Techniken, die vor allem auf den Faktor Mensch abzielen. Genau diese modernen Bedrohungen, wie Cryptolocker, Phishing Scams und DDOS möchten wir Ihnen in diesem Vortrag anhand von ausgewählten Beispielen näherbringen und Live demonstrieren. Natürlich lassen wir sie nicht mit den Problemen im Regen stehen, sondern stellen auch mögliche Techniken zum Schutz vor.

NEUE CYBERSECURITY-TRENDS: WIE KÖNNEN SIE IHRE NETZWERKE UND KOMMUNIKATION VOR MALWARE UND SPIONAGE SCHÜTZEN? – ROHDE&SCHWARZ –DI VOLKER MAX

Heutige Cyberangriffe benötigen intelligentere Abwehrmaßnahmen, um das eigene Netzwerk vor Malware zu schützen und die eigene Kommunikation abzusichern.
Es werden typische Angriffe und dazugehörige Schutzmechanismen vorgestellt. Dabei wird ein proaktiven Schutz auf verschiedenen Ebenen eingesetzt.
Neben der Absicherung von Standortnetzen und WAN, ist der Schutz der eigenen Rechnerinfrastruktur vor Malware essentiell wichtig. Darüber hinaus müssen die Übertragungen in Netzwerken verschlüsselt erfolgen.
Die zunehmende Verwendung von Smartphones für alle Sprach- und Datendienste werden dadurch zu einem präferierten Ziel für Angreifer. Es müssen berufliche von privaten Daten streng und sicher separiert werden, um keine Attacken auf die sensiblen Geschäftsdaten zuzulassen.

ANGEWANDTE FORSCHUNG FÜR LAW ENFORCEMENT – SBA RESEARCH – DR. EDGAR WEIPPL

Entscheidungen, die auf Fakten basieren, sind leichter zu kommunizieren und zu verstehen. Forscherinnen und Forscher können helfen, gesetzliche Regelungen und die Arbeit von Law Enforcement mit unabhängig gewonnenen und ausgewerteten Daten zu unterstützen und zu optimieren. Wofür beispielsweise Tor Hidden Services verwendet werden, war lange Zeit nicht nachvollziehbar: Manche sahen darin ein Service, das beinahe ausschließlich dem Drogen-, Waffen- und Kinderpornohandel diente, andere glaubten, dass die Dienste unerlässlich für das Weiterbestehen unserer Freiheit und Demokratie sei. Wissenschaft hilft, dass diese Diskussion nicht länger eine Glaubensfrage ist, sondern auf nachvollziehbaren Daten basiert.

CYBER-CLUSTER AN DER UNIVERSITÄT DER BUNDESWEHR MÜNCHEN - FORSCHUNGSZENTRUM CYBER DEFENCE, UNIVERSITÄT DER BUNDESWEHR - DR. GABI DREO RODOSEK

KRITISCHE INFRASTRUKTUR – 12 10 2016

SONNIG MIT DER AUSSICHT AUF /IF/DEV=ZERO - ZAMG - DI MAG. TSCHABUSCHNIG

HOUSTON - WE HAVE A PROBLEM! CYBER CRISIS COMMUNICATION DONE RIGHT – MANDIANT - MARTIN KRUMBÖCK

Large scale security incidents are all over the news lately. Big breaches cover the headlines of even main stream media nowadays. Whereas this creates awareness about the importance of cyber security and incident response in particular, it is a very thin line to walk for the company in the news.

We have seen several companies fail to do proper communication which in general leads to mistrust of the competence of the victimized company. In return this can have a huge impact on the perception and reputation. But what factors are to consider when going public? . Mandiant will share it's expertise of clients who went through this situation and we will learn some best practices of what to do and what not to do.

META-RISK: META-RISIKO-MODELL FÜR KRITISCHE INFRASTRUKTUREN - DIPL.ING. JOHANNES GÖLLNER, MSC - BMLVS, DIPL.-ING. CHRISTIAN MEURERS - BMLVS UND UNIV.PROF. DDR. GERALD QUIRCHMAYR UNIVERSITÄT WIEN, FAKULTÄT INFORMATIK

Ein umfassendes Risikomanagement ist die Grundlage aller Führungs-, Kern- und Unterstützungsprozesse einer Organisation und bildet den Hintergrund aller Maßnahmen zur fähigkeitenbasierten Steuerung, Entwicklung und Führung auf Basis eines Wissensmanagement-Systems in einer Organisation. Gerade im sicherheitsrelevanten Umfeld kommt dem Risikomanagement auf strategischer und operativer Ebene aufgrund der sensiblen Aufgabenstellungen und Herausforderungen eine besondere Bedeutung zu.

Das vorliegende Projekt beschäftigt sich daher mit dem Aufbau eines sensorunterstützten Risiko-Analyse und Managementsystems, das nicht nur unter Anwendung eines generischen Ansatzes modelliert und konzipiert, sondern auch in einen Demonstrator umgesetzt wird. Dabei werden bereits vorliegende F&E Ergebnisse, Methoden, Verfahren und Technologien, aber auch vorhandene und erarbeitete Prozesse, Steuerungslogiken, Risikomodelle etc. in ein generischen Meta-Risiko-Modell integriert und im System abgebildet. Expertenwissen trägt dazu bei, die Zusammenhänge zwischen Erfolgsfaktoren (Key Performance Indicators) und Risikofaktoren (Key Risk Indicators) zu erkennen, zu formalisieren und zu strukturieren. Schnittstellen zu Basis-Sensoren und externen Analyseinstrumenten (z.B. Soziale Netzwerkanalyse SNA, KIRAS-MDL Demonstrator etc.) ergänzen und komplettieren das Gesamtsystem. Diese Faktoren können kennzahlenbasiert aus der Sicht „Risikobilanz versus Wissensbilanz“ bzw. in Relation zu Wissens- und Risiko-Mapping bzw. Wissens- und Risiko-Controlling formuliert werden.

Das zu entwickelnde Meta-Risiko-Modell ist daher generisch und unter Anwendung eines ganzheitlichen Ansatzes (comprehensive approach) und der Abstützung auf spezifische, ebenfalls zu erarbeitende Heuristiken, zu entwickeln. Der Fokus liegt dabei auf der Anwendbarkeit im strategischen und operativen Kontext zu IKT und Kritischen Infrastrukturen und der Integration der Personen und Einzeltätigkeiten in ein work-flow gestütztes operatives Lagebildsystem. Abgeleitet aus dem Meta-Risiko-Modell ergeben sich Risiko-Metriken, die in weiterer Folge als Basis für die Konzeption einer web-basierten Demonstrator-Plattform zur Modellierung und Visualisierung von Zusammenhängen und Kollaboration auf operativer Ebene für die Unterstützung von Decision Making Prozessen dienen.

IT-GEFAHREN IM HINBLICK AUF MILITÄRISCHE AUSLANDSEINSÄTZE – MILITÄRISCHER ABSCHIRMDIENST, DEU – CHRISTOPH WILLER

KRITISCHE INFRASTRUKTUREN – IT-SECURITY AM BEISPIEL RED BULL – RED BULL - JIMMY HESCHL

SIND WIR BEREIT? KATASTROPHENVORSORGE IM E-GOVERNMENT BEREICH – BUNDESKANZLERAMT – ADIR FLORIAN BILEK

Ohne IT Prozesse ist das E-Government der modernen Bundesverwaltung nicht umsetzbar. Katastrophen sind weder vorherseh- noch in irgendeiner Form planbar. Welche Maßnahmen werden daher seitens der Bundesregierung unternommen, die IT-Prozesse und deren Daten gegen Bedrohungen zu schützen? Können diese Maßnahmen den Daten-GAU verhindern? Ein Blick in die Aufgaben des "Zentrales Ausweichsystems ZAS", eine Dienststelle des Bundeskanzleramts.

NETZ- UND INFORMATIONSSICHERHEIT IN EUROPA/ÖSTERREICH - EINE RECHTLICHE EINFÜHRUNG – FH HAGENBERG – DR. PETER BURGSTALLER

Am 8. Dezember 2015 haben sich das Europäische Parlament, der Rat und die EU-Kommission im Wesentlichen auf den Kommissionsvorschlag der EU-Kommission aus 2013 zur Erreichung einer hohen gemeinsamen Netz- und Informationssicherheit geeinigt, mit folgenden Eckpunkten:

- Die EU-Mitgliedstaaten werden verpflichtet, ihre Abwehrbereitschaft und Zusammenarbeit im Bereich der Sicherheit des Internets bzw der privaten Netze und Informationssysteme untereinander zu verbessern und müssen eine „NIS-Behörde“ sowie ein CERT (Computer Emergency Response Team) etablieren.

- Betreiber kritischer Infrastrukturen insb im Bereich des Energie-, Verkehrs-, Banken- und Gesundheitssektor sowie Betreiber zentraler digitaler Schlüsseldienste wie Suchmaschinenbetreiber oder Cloud Diensteanbieter und die öffentlichen Verwaltungen werden angehalten, geeignete Sicherheitsmaßnahmen zu ergreifen und Schritte zur

Beherrschung von Sicherheitsrisiken zu unternehmen sowie der nationalen NIS-Behörde gravierende Sicherheitsvorfälle zu melden (Frühwarnsystem).

- Betreiber kritischer Infrastrukturen und Betreiber zentraler digitaler Schlüsseldienste müssen Informationssicherheitsaspekte „managen“, dh ein ISMS einführen – siehe dazu auch die EU Datenschutzgrundverordnung 2016.

INDUSTRIE 4.0 – 12 10 2016

SECURITY IN DER SMART FACTORY – COPA-DATA GMBH – HANS-PETER ZIEGLER

Wie "Industrie 4.0" und "Industrial IoT" die Welt der industriellen Automation beeinflusst. Vom gehärteten System über sichere Kommunikation bis hin zum authentifizierten und legitimierten Bediener im Spannungsfeld "Security vs. Safety".

INDUSTRIE 4.0 UND DIE DARAUS RESULTIERENDEN SICHERHEITSANFORDERUNGEN – HISOLUTIONS, DEU – ANDREAS SALM

Die fortschreitende horizontale und vertikale Integration industrieller Steuerungssysteme konfrontiert die Betreiber mit zunehmenden Sicherheitsrisiken. Neue, dynamische Kommunikationsbeziehungen teilweise über öffentliche Netze in Verbindung mit dem Einsatz von Standardkomponenten der klassischen IT (commercial of the shelf) exponieren Steuerungssysteme und erhöhen die Angriffsfläche. Klassische auf Isolation ausgerichtete Sicherheitskonzepte greifen nicht mehr; zugleich sind in der Büro-IT etablierte Sicherheitsstrategien nur bedingt übertragbar. Dieser Vortrag veranschaulicht dieses Spannungsfeld und zeigt Lösungsansätze auf.

INDUSTRIAL SECURITY: RED TEAM OPERATIONS – HACKNER SECURITY INTELLIGENCE – THOMAS HACKNER, MSC

IT-SICHERHEIT FÜR DEN EINSATZ VON SMART METERING – BESONDERS SCHÜTZENSWERTE DATENSTRÖME UND DATEN, RISIKO-SZENARIEN IN SMART METERING UMGEBUNGEN UND DIE KONZEPTION VON IT-SICHERHEITSMAßNAHMEN – RADAR-SERVICES – MAG. HARALD REISINGER

Das umfassende Konstrukt an Daten und Datenströmen beim Einsatz von Smart Metering wird analysiert und klassifiziert. Verschiedene Risikoszenarien werden dargestellt. Die Konzeption von IT-Sicherheitsmaßnahmen wird Schritt für Schritt verdeutlicht und die modernsten Werkzeuge und ihre Anwendungsbereiche dafür beschrieben.

DAS MÄRCHEN VOM AIR-GAP - ANGRIFFE AUF INDUSTRIEANLAGEN - NSIDE ATTACK LOGIC GMBH, DEU - RAINER GIEDAT

Die Vernetzung von Industrieanlagen wird durch Industrie 4.0 weiter zunehmen, war aber lange vorher schon an der Tagesordnung. Versucht ein Angreifer in Steuerungsnetzwerke einzudringen und dort entsprechenden Zugang auf die Fertigungsanlagen zu erlangen, kann er sich diese Vernetzung zu Nutze machen. Diesem Risiko wurde bisher häufig mit einer strikten Trennung der Netze (Air-Gap) begegnet, doch diese hat sich in all unseren bisherigen Tests als überwindbar herausgestellt. Der Vortrag zeigt mit Live-Demonstrationen, wie Angreifer vorgehen und berichtet von Erfahrungen aus zahlreichen Penetrationstests von Industrieanlagen.

DETEKTIVE UND REAKTIVE SICHERHEITSMAßNAHMEN IN INDUSTRIELLEN UMGEBUNGEN – T-SYSTEMS AUSTRIA GESMBH – THOMAS MASICEK, MSC UND HERWIG KÖCK

DIGITALIZATION REQUIRES INTELLIGENT INFORMATION SECURITY – ADVENICA, SWE – ANDERS STRÖMBERG

Customers expect information diligent, frequently and tailored for use in the digitized world. This is essential to generate new revenue streams and improve workflow to save cost. The information provided is a combination of traditional business information but also operations information. In the context of smart grids, Internet of Things and computerization of traditional production technology the need to create information exchange might be slowed down due to the risk of cyberattacks. It is time to re-think how this challenge is managed. It is time for Digital accountability.

INTERNET OF THINGS – 12 10 2016

ÜBERBLICK ÜBER IT-TRUST IM ZEITALTER DES KONTROLLVERLUSTES – DATA-WAREHOUSE, DEU – DR. ALEXANDER LÖW

IOT als vollvernetzte Umgebungen sind in aller Munde. Jedoch beinhaltet IOT auch Kontrollverlust auf vielen Ebenen, da man nicht mehr alle Prozesse in der eigenen Hoheit hat. Dieser Vortrag beschäftigt sich mit den Hintergründen und Vor- und Nachteilen von Lösungsszenarien um technische Vertrauensstellungen als Ersatz für Kontrollmöglichkeiten zu implementieren und den Auswirkungen für Verantwortliche und Entscheider.

GEFAHREN UND RISIKEN IM BEREICH DER MEDIZINTECHNIK – TECHNIKUM WIEN – DI MENSE ALEXANDER

Dass unsere medizinischen Versorgungseinrichtungen Sicherheitsrisiken unterliegen ist nicht unbedingt neu. Allerdings bekommt das Problem nun mit dem schnell steigenden Vernetzungsgrad von Systemen und Medizingeräten und der zunehmenden Verlagerung von Diensten in unser Heimumfeld eine neue Dimension und schnell werden neue erschreckende Begriffe wie „Medical Ransomware“ geboren. Bestehende Sicherheitskonzepte scheinen nicht genug und Konzepte wie Security und Privacy by Design scheinen hoffnungsvoll, aber zu spät – müssen wir also zurück in Vergangenheit um die Katastrophe zu abzuwehren? Und hindert uns das daran die Fehler, die wir gerade wieder im

Bereich der mobilen Vernetzung von Medizintechnik im IoT machen zu verhindern? Der Vortrag zeigt anhand praktischer Beispiele die Risiken bestehender und neuer Services im Bereich der Medizintechnologie auf und diskutiert notwendige Lösungsansätze.

SMARTCITY UND SMARTLIVING - ANONYMISIERUNG UND PSEUDONYMISIERUNG – SICHERHEITSKULTUR.AT – PHILIPP SCHAUMANN

Big Data in Form von SmartCity und SmartLiving funktioniert nur, wenn die Algorithmen die Daten von uns allen kennen.
Fast alle Firmen versuchen derzeit auf den Big Data-Zug aufzuspringen und sammeln immer größere und sensiblere Datenmengen.
Datenschutzgesetz und Bankgeheimnis stellen diese Daten aber unter ihren Schutz und fordern strenge Rechtsgrundlagen für die Nutzung, auch im eigenen Unternehmen.
Das erfordert angemessene Anonymisierung und Pseudonymisierung.
Je mehr über Datenanalyse und Big Data gesprochen wird, desto mehr bekommt Anonymisierung und Pseudonymisierung an Bedeutung.
Moderne IT sammelt Berge von persönlichen und sensiblen Daten, die aber nur dann für andere Zwecke als den Ursprungszweck verwendet werden können, wenn sie anonymisiert oder zu mindestens pseudonymisiert sind.
Der Vortrag zeigt die grundlegenden Konzepte dieser beiden Techniken auf, demonstriert aber auch an Hand von vielen Beispielen, welche Fallstricke dort zu erwarten sind und welche Fehler dabei oft gemacht werden.
Dabei wird die Frage untersucht, ob SmartCity und SmartLiving möglich ist, ohne in Überwachung der Bürger auszuarten.

SICHERHEIT UND VERNETZTE MOBILITÄT – EIN WIDERSPRUCH? ÖAMTC - VERBANDSDIREKTOR DI OLIVER SCHMEROLD

Sicherheit und Mobilität stehen seit jeher in einem engen Zusammenhang. Ging es über Jahrzehnte um Leib und Leben so müssen wir uns in der Zukunft verstärkt der Datensicherheit widmen. Die Vernetzung der Fahrzeuge dient nicht mehr nur unkritischen Infotainments Services sondern steuerte mehr und mehr unsere Mobilität. Zur aktiven und passiven Sicherheit kommt somit die virtuelle Sicherheit hinzu. Jüngste Untersuchungen der europäischen Mobilitätsclubs haben dabei signifikante Lücken und Manipulationspotenzial offengelegt. Strengere Sicherheitsstandards sind die konsequente Forderung daraus. Diese dürfen aber nicht zu einer Einschränkung des Wettbewerbs beim Angebot von Diensten führen. Ein Spannungsfeld in dem der ÖAMTC eine klare Position hat.

DATENRECOVERY VON MOBILEN GERÄTEN – FH HAGENBERG/UNINET – DI ROBERT KOLMHOFER

STRENGTHENING CYBERSECURITY AT THE TOUR DE FRANCE – DIMENSION DATA – DANIEL MIEDLER

Dimension Data unterstützt seit 2015 die Durchführung der Tour de France mit der Erfassung von Positions- und Geschwindigkeitsdaten jedes einzelnen Fahrers. Dadurch war

es 2015 zum ersten Mal möglich, für über 3,5 Millionen Zuseher pro Rennen jederzeit die Position und Geschwindigkeit von 198 Fahrern in Echtzeit zu verfolgen. Diese Daten werden sowohl den Fernseh- und Radiostationen für Ihre Übertragungen als auch den Teams und Zusehern online im Internet zur Verfügung gestellt. Dimension Data betreibt aus diesem Grund eine umfassende Infrastruktur mit GPS-Sensoren auf jedem Fahrrad, Daten-Uplinks zu einem mobilen Rechenzentrum entlang der Rennstrecke und Online-Plattformen zur Darstellung der Daten im Internet. Durch die mediale Präsenz und die zur Verfügung gestellten Services hat sich die Angriffsfläche für Dimension Data massiv erhöht. Dieser Tatsache wurde im Vorfeld durch umfangreiche Härtungsmaßnahmen, durch eine ISO27001:2013 Zertifizierung und durch umfangreiche PEN-Tests Rechnung getragen. Während des Rennens wurde die Infrastruktur 24x7 durch ein SOC überwacht und auf Angriffe aktiv reagiert. Durch diese Aufwände konnte die Systemverfügbarkeit während des Rennens auf 100% gehalten werden. 1.716 gezielte Angriffe auf die Infrastruktur konnten abgewehrt werden. Es ist den Angreifern nicht gelungen, die zur Verfügung gestellten Services zu beeinträchtigen bzw. Zugriff auf Systeme bzw. Daten zu erlangen.

CYBER-RISIKEN – MITTELSTAND IN GEFAHR! – FUNK INTERNATIONAL AUSTRIA GMBH – DIPL. BETRIEBSWIRT (BA) HENDRIK FLORIAN LÖFFLER

Die Gefahren durch Hackerangriffe, Missbrauch von Kundendaten, Fehlbedienung oder andere IT-bezogene Risiken werden gerade von mittelständischen Unternehmen, aber auch öffentlichen Institutionen häufig unterschätzt.

Große Schadenfälle infolge Cyber-Kriminalität haben zunächst in den USA, aber nun auch zunehmend in Europa für Aufmerksamkeit gesorgt und regen Entscheidungsträger zunehmend zum Nachdenken an.

Dies zeigen die Studienergebnisse von Funk. Basis der Studie ist eine onlinegestützte Befragung von 400 mittelständischen Unternehmen und deren Entscheidungsträger. Die wesentlichen Schadenpotenziale werden laut der Studie im Missbrauch von Kundendaten sowie in der Verletzung von Betriebsgeheimnissen Dritter, aber auch in einer Betriebsunterbrechung aufgrund eines Ausfalls wesentlicher Elemente der Unternehmens-IT gesehen. Um mehr Transparenz in Unternehmen zu erzeugen und das Risikoverständnis für die Cyber-Risiken in Unternehmen zu verbessern, hat Funk einen speziellen Analyseansatz in Form eines interdisziplinären Workshops entwickelt. Im von einem Projektberater moderierten Workshop werden die Risikoszenarien entlang der Wertschöpfungskette diskutiert. Im Anschluss an den Workshop wird ein Risikobericht erstellt. Wenn Unternehmen die relevanten Cyber-Risiken an eine Versicherungsgesellschaft übertragen möchten, sollten einige Dinge beachtet werden. Häufig nehmen Unternehmen/Organisationen an, dass Cyber-Risiken grundsätzlich über die klassischen Versicherungsprodukte, z. B. die Betriebs-, Vermögensschadenhaftpflicht- oder Vertrauensschaden- Versicherung, abgedeckt sind. Dies ist aber häufig ein gefährlicher

Irrglaube. Zur Absicherung der Risiken sind besondere Deckungskonzepte erforderlich, die vielfach ganz individuell an den Risikobedarf der betroffenen Unternehmen/Organisationen erst angepasst werden müssen.