5. SECURITY & RISK-MANAGEMENT KONGRESS

NACHBERICHT

14.–15. MAI 2013

Das Schloss an der Eisenstraße
Waidhofen a. d. Ybbs

* Aktuelle Bedrohungsszenarien
* Cyber-Security
* Umgang mit Daten
* Infrastruktur & Network Security
* Governance, Risk, Compliance & Legal Topics

VORWORT

Sehr geehrte Damen und Herren,
liebe Teilnehmer/-innen am Security-Kongress,

Der 5. Security & Risk-Management Kongress in Waidhofen a. d. Ybbs ist erfolgreich über die Bühne gegangen und hat sich wie schon die Jahre zuvor mit einem reichen Teilnehmerfeld und angeregten Diskussionen als „runde" Veranstaltung und Plattform zum Erfahrungsaustausch der österreichischen IT-Security-Verantwortlichen bewährt.

Wir freuen uns über das durchgehend sehr positive Feedback, und dass wir eine große Zahl von CISOs & Risk-Managern nun schon zum wiederholten Mal bei uns begrüßen durften. Allseits beliebt ist hier die Mischung aus Vorträgen, Diskussionsrunden und Zeit zum Gespräche führen und Networken in gelockerter Atmosphäre, bei dem der Spaß auch nicht zu kurz kommt.

Bei – nicht nur von extern - ständig wachsenden Anforderungen an das Security & Risk-Management hoffen wir so, Ihnen Anregungen, Ideen und Best Practices liefern zu können, um Sie im Tagesgeschäft zu unterstützen.

Mit dem Kongress ist es uns ein Anliegen, eine jährliche Plattform und ein „get-together" zu schaffen, bei dem Sie sich ungezwungen mit Kollegen und Experten der Anbieter-Seite austauschen können. Im Sinne des persönlichen Netzwerkens hilft Ihnen der eine oder andere geknüpfte Kontakt sicher auch um neue Herangehensweisen kennenzulernen bzw. zu wissen, wo man anklopften kann wenn wirklich einmal „der Hut brennt".

Ein wesentlicher Bestandteil des Konzepts ist darum auch, dass Sie sich vorab schon mit Themen-Vorschlägen einbringen & in weiterer Folge die Themen wählen, die für Sie unmittelbar interessant sind. Für die inhaltliche Unterstützung, die zahlreichen Beiträge & kreativen Ideen-Poolings in den Themen-Workshops dürfen wir uns recht herzlich bei allen Teilnehmenden bedanken!

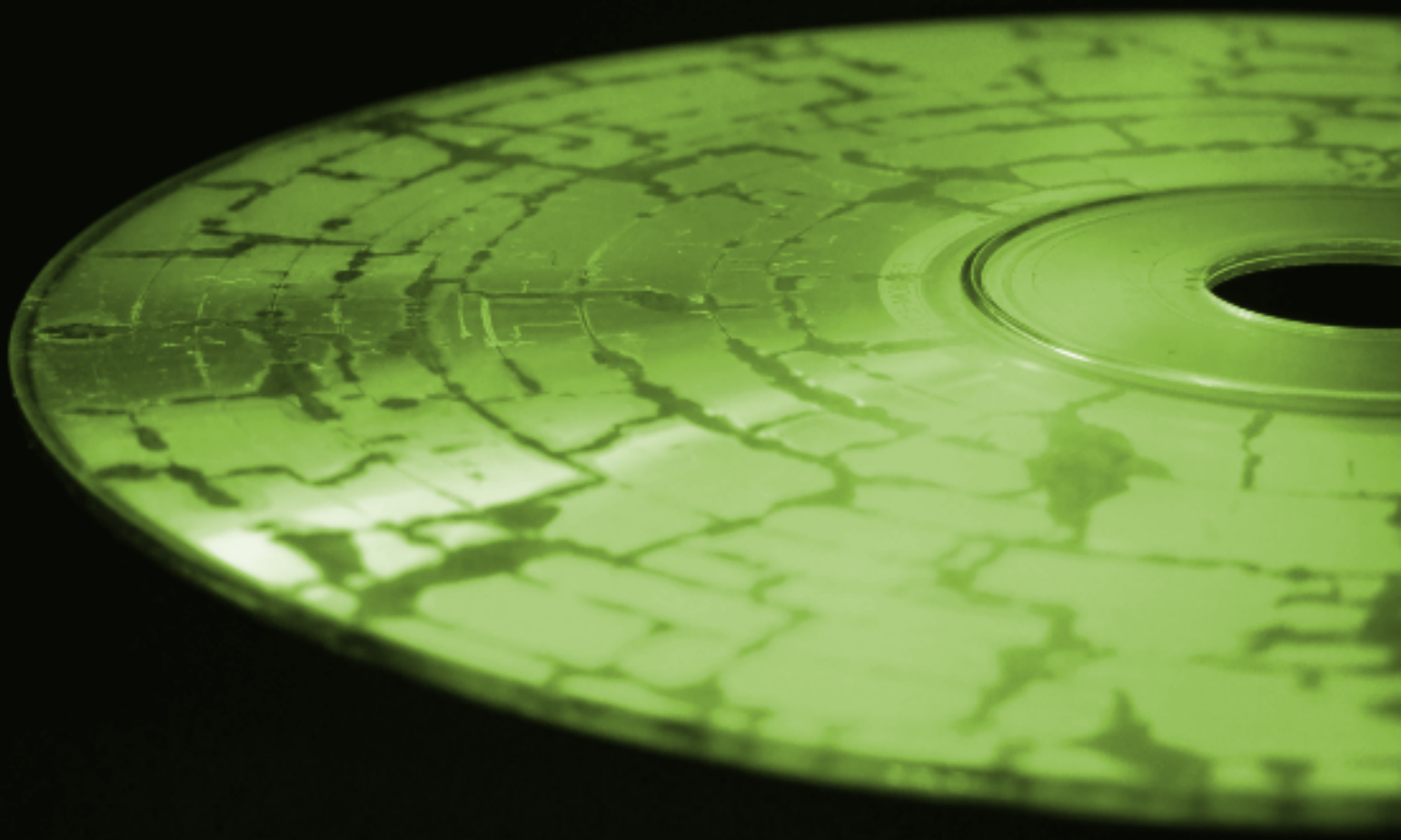
In Vorfreude befinden wir uns damit bereits in den Vorbereitungen für den LSZ Security & Risk-Management Kongress 2014 und hoffen natürlich darauf Sie wieder begrüßen zu dürfen!

Herzliche Grüße schickt stellvertretend für das gesamte LSZ Team,

Stefan Reischl
Projektleitung

INHALTSVERZEICHNIS

DER SECURITY & RISK-MANAGEMENT KONGRESS 2013



IMPRESSIONEN








SafeNet





LSZ
Consulting
THE WAY
TO NETWORK
since 1988

PARTNER DER VERANSTALTUNG

Die **Antares-NetlogiX Netzwerkberatung GmbH** unterstützt Sie in Sachen Sicherheit und Zuverlässigkeit Ihrer IT Infrastruktur und hat sich seit der Gründung 2000 als kompetenter IT Dienstleister bewährt. Vom Schwerpunkt Netzwerk- und System Management kommend, wurde der Fokus zunehmend um Hoch-Sicherheitslösungen erweitert. Tech Support mit 6 Mitarbeitern und die hohe Kompetenz der Consultants mit minimaler Fluktuation sorgen für technische Leistungen auf höchstem Niveau und eine unaufdringliche vertriebliche Beratung. Die technischen Organisationseinheiten umfassen jeweils Experten für Netzwerk & Security, System Management, Software-Entwicklung sowie ein mehrköpfiges Auditorenteam. Viele der größten IT Infrastrukturen in Österreich vertrauen bereits seit vielen Jahren auf die Betreuung von Antares.

›› www.netlogix.at/antares_netlogix

Bacher Systems EDV GmbH unterstützt seine Kunden beim Aufbau und der Optimierung eines zukunftssicheren Rechenzentrums – ein Next Generation Data Center. Dabei steht die umfassende IT-Security für Bacher Systems im Mittelpunkt, um das moderne Rechenzentrum effektiv vor den Bedrohungen von heute und morgen zu schützen und eingehende Sicherheit zu gewährleisten. Bacher Systems bietet umfassenden Service aus einer Hand - von der Beratung und Konzepterstellung, über die Implementierung von IT-Projekten, bis hin zum Betrieb der IT-Systeme. Damit ermöglicht Bacher Systems seinen Kunden die Vorteile eines Next Generation Data Center voll und sicher auszuschöpfen.

›› www.bacher.at/it-security

Ca Technologies bietet im Bereich Informationssystemsicherheit agile und flexible Sicherheitslösungen, mit der Benutzer problemlos, schnell und sicher auf Anwendungen und Informationen zugreifen können. In Österreich hilft CA Technologies Unternehmen wie der Ersten Bank, der OMV AG, der Raiffeisen Gruppe, Telekom Austria, der Universität Wien oder der Technischen Universität Graz dabei, ihre komplexen und heterogenen IT-Umgebungen zu verwalten und die Migration von Anwendungen und Daten in die Cloud und/oder Virtualisierungssysteme abzusichern.

›› www.ca.com/at/identity-and-access-management-solutions.aspx

Die **Certex Information Technology GmbH** hat sich auf Beratungsdienstleistungen und Anwendungsentwicklung für rollenbasierte Zugriffskontrolle in Unternehmen spezialisiert. Zu den Kunden zählen sowohl namhafte, internationale Konzerne als auch hochspezialisierte Unternehmen aus dem Mittelstand in den Regionen DACH, Benelux und Skandinavien. ISM – die integrierte Lösung für Identity & Accessmanagement - ermöglicht die unternehmensweite Verwaltung von Benutzerkonten und Berechtigungen von einem zentralen Punkt aus.

›› www.certex.at

CSC zählt zu den weltweit führenden Dienstleistungsunternehmen im Bereich der Informationstechnologie (IT). In Österreich ist CSC seit über 30 Jahren vertreten und beschäftigt 340 Mitarbeiter an den Standorten Wien, Linz, Graz und Klagenfurt. Der Fokus liegt dabei auf den Top 200 Unternehmen. Bei der Integration in die Geschäfts- und IT-Prozesse unserer Kunden berücksichtigen wir die anerkannten Standards sowie die wirtschaftliche Aspekte. Dabei basieren unsere IT-Lösungen auf einem ganzheitlichen risikobasierten Ansatz. Mit unserem umfassenden Dienstleistungportfolio beraten und schützen unsere Cybersecurity-Spezialisten Unternehmen aller Wirtschaftszweige auf der ganzen Welt und machen diese ein Stück sicherer.

›› www.csc.com/at

Das 1999 gegründete Unternehmen **Cyber-Ark** ist ein global agierender Anbieter von Informationssicherheits-Software. Das Unternehmen hat sich auf die Verwaltung und den Schutz von privilegierten Nutzerkennungen und sensiblen Daten spezialisiert. Die Lösungen von Cyber-Ark helfen Unternehmen, gesetzliche Richtlinien einzuhalten sowie Insider-Bedrohungen und externen Angriffen vorzubeugen. Der Hauptsitz des Unternehmens befindet sich in Newton (Massachusetts, USA). In Deutschland ist Cyber-Ark seit 2008 mit einer eigenen Niederlassung in Heilbronn vertreten.
Die Cyber-Ark PIM Suite sorgt für die regelmäßige, automatische Änderung von Administratoren-Kennwörtern und ermöglicht damit eine Lückenlose Nachvollziehbarkeit aller Superuser-Zugriffe auf Desktops, Server, Datenbanken, Netzwerkgeräte und Applikationen.

›› www.cyber-ark.com/de

Palo Alto Networks (NYSE: PANW) entwickelt, produziert und vermarktet leistungsstarke Next Generation Firewalls, die Unternehmen und Organisationen jeder Größe zuverlässig vor Angriffen auf allen Netzwerkebenen schützen. Anders als klassische Stateful Inspection Firewalls, die lediglich Ports und IP-Adressen überwachen, sind die Plattformen von Palo Alto Networks in der Lage, sowohl Applikationen als auch Anwender zu kontrollieren. Auf diese Weise können Unternehmen auch Attacken auf Anwendungsebene zuverlässig stoppen. Palo Alto Networks wurde 2005 von Nir Zuk im kalifornischen Sunnyvale gegründet und gehört heute zu den am schnellsten wachsenden Anbietern im Firewall-Markt. Die Lösungen von Palo Alto Networks sind in mehr als 10.000 Unternehmen im Einsatz, in über 100 Ländern weltweit.

>> www.paloaltonetworks.com

RSA arbeitet eng mit Kunden zusammen, um Herausforderungen in den Bereichen Management von Advanced Threats, Management von Cybercrime und Fraud, IT-Risiko Management sowie dem Nachweis von Compliance erfolgreich zu lösen.

>> www.austria.emc.com/emc-plus/rsa-thought-leadership/index.htm

SafeNet, einer der größten Anbieter für Informationssicherheit, sorgt weltweit für den Schutz sensibler Daten führender Unternehmen. Durch einen datenorientierten Ansatz schützt SafeNet Informationen über den gesamten Lebenszyklus hinweg - vom Datencenter bis zur Cloud. Über 25.000 Unternehmen vertrauen auf SafeNet beim Schutz und der Kontrolle des Zugangs zu sensiblen Daten, beim Risikomanagement, bei der Einhaltung gesetzlicher Vorschriften und der Sicherung von virtuellen und Cloud-Umgebungen.

>> www.safenet-inc.de

Security Research ist als forschungsnaher Technologieführer in Österreich Ihr Partner in den Bereichen IT-Sicherheitsberatung, Schulung und Umsetzung, Prozessberatung und kontrollorientiertem Prozessdesign mit dem Ziel, die Anforderungen aus Sicht einer Revision zu erfüllen. Dabei werden wissenschaftliche Erkenntnisse aus der IT-Sicherheitsforschung mit Prozessmanagemen-Methodologien und Wissen um regulative Anforderungen kombiniert, um unter Berücksichtigung sowohl technischer als auch organisatorischer Sicherheitsaspekte Geschäftsprozesse zu optimieren.
Zu diesem Zweck beschäftigen wir in unserem Team Experten, die ihr fundiertes theoretisches Wissen im Bereich von IT-Prüfungs-, IT-Sicherheit- und IT-Managementstandards mit langjähriger praktischer IT-Erfahrung kombinieren.

>> www.securityresearch.at

Symantec schützt Informationen in der digitalen Welt und ist ein führender Anbieter von IT-Lösungen für Sicherheit, Backup und Hochverfügbarkeit. Unsere innovativen Produkte und Dienstleistungen schützen Personen und Informationen in jeder Umgebung – angefangen bei Mobilgeräten über Rechenzentren bis hin zu Cloud-basierten Systemen. Unsere langjährige Expertise beim Schutz von Informationen und Personendaten gibt unseren Kunden das Vertrauen, in der vernetzten Welt miteinander zu interagieren.

>> www.symantec.de

Websense, Inc. (NASDAQ: WBSN), einer der weltweit führenden Anbieter integrierter Web-, Daten und E-Mail-Content-Sicherheitslösungen, bietet Zehntausenden von Unternehmen jeder Größenordnung den bestmöglichen Schutz vor modernen Bedrohungen – und dies zu den geringsten Gesamtbetriebskosten (Total Cost of Ownership).
Die integrierten Content-Sicherheitslösungen von Websense, die über ein globales Netz von Vertriebspartnern angeboten werden und als Software, Appliances und Security-as-a-Service (SaaS) erhältlich sind, helfen Organisationen, neue Kommunikations-, Kollaborations- und Web 2.0-Business Tools effektiv zu nutzen. Gleichzeitig bieten sie Schutz vor erweiterten persistenten Bedrohungen, verhindern den Verlust vertraulicher Daten und erzwingen die Einhaltung von Richtlinien für Internet-Nutzung und Sicherheit. Websense hat seinen Hauptsitz in San Diego (Kalifornien) und betreibt Niederlassungen weltweit.

>> www.websense.com

1. TAG OPEN SPACE ARBEITSKREISE

1 AKTUELLE BEDROHUNGEN

LEITUNG:
MAG. (FH) MARKUS RIPKA, CISSP
DenizBank AG

SECURITY ANFORDERUNGEN DER NÄCHSTEN JAHRE: WO GEHT DIE REISE HIN?

THEMENMODERATION:
DI Dr. Thomas C. Stubbings, CISA |
Raiffeisen Bank International AG

ZWISCHEN CYBERWAR UND HACKTIVISM - FÜR WELCHE BEDROHUNGEN MÜSSEN WIR GERÜSTET SEIN?

THEMENMODERATION:
Dipl. Inf. Ing. Candid Wüest |
Symantec Austria GmbH

APTs: WIE SCHÜTZEN WIR UNS GEGEN GEZIELTE & NACHHALTIGE ANGRIFFE?

THEMENMODERATION:
Mario Fritzer |
Palo Alto Networks

PHISHING, SOCIAL ENGINEERING & THREATS VIA SOCIAL NETWORKS

THEMENMODERATION:
Harald Haselbauer |
Amt der Burgenländischen Landesregierung

2 UMGANG MIT DATEN

LEITUNG:
DI MAG. ANDREAS TOMEK, CISA, CISSP
Security Research Sicherheitsforschung GmbH

WER HAT SEINE FINGER AUF DEN UNERNEHMENSDATEN? WO LIEGEN IM WEB + BEI MOBILE DEVICES DIE HERAUSFORDERUNGEN?

THEMENMODERATION:
Michael Rudrich |
Websense Deutschland GmbH

APTs & DIE AUSWIRKUNGEN AUF DIE DATENSICHERHEIT

THEMENMODERATION:
DI Mag. Andreas Tomek, CISA, CISSP |
Security Research Sicherheitsforschung GmbH

IT-BERECHTIGUNGEN: LEIDEN WIR NOCH ODER MANAGEN WIR SCHON?

THEMENMODERATION:
Helmut Semmelmayer, BSc, MSc |
certex Information Technology GmbH

KLASSIFIZIERUNG VON DATEN & WER KÜMMERT SICH DARUM?

THEMENMODERATION:
Clemens Peyerl, MSc, MBA |
Stryker GmbH

3 INFRASTRUKTUR & NETWORK SECURTIY

LEITUNG:
ING. DI HERBERT DIRNBERGER, MA, CISM
Cyber Security Austria

VULNERABILITY MANAGEMENT - PROAKTIVE AKTIVITÄTEN & ÜBERPRÜFUNG DER SYSTEM-/ NETZWERKSICHERHEIT

THEMENMODERATION:
Dipl-HTL-Ing Andreas Schaupp, MSC, MAS |
CSC Computer Sciences Consulting Austria GmbH

KRITISCHE INFRASTRUKTUREN: OFFENHEIT DER SYSTEME & MÖGLICHE FOLGEN

THEMENMODERATION:
Ing. DI Herbert Dirnberger, MA, CISM |
Cyber Security Austria

CLOUD-NUTZUNG OHNE SCHLAFLOSE NÄCHTE? IT-SECURITY & CLOUD-SERVICES

THEMENMODERATION:
Christian Linhart |
SafeNet Germany GmbH

SICHERHEIT VON INDUSTRIE-KONTROLL / SCADA-SYSTEMEN SIND WIR GERÜSTET?

THEMENMODERATION:
Dipl-HTL-Ing Andreas Schaupp, MSC, MAS |
CSC Computer Sciences Consulting Austria GmbH

4 GOVERNANCE, RISK, COMPLIANCE & LEGAL

LEITUNG:
GEORG BEHAM, MSC
KPMG Advirsory AG

100%IGE SICHERHEITSERFÜLLUNG: WAS IST REALISTISCH UND WIEVIEL INFORMATION SECURITY IST GENUG?

THEMENMODERATION:
Wolfgang Ertl, MAS | Verbund AG

ISO 27001 VS. IT-GRUNDSCHUTZ VS. RISK-IT

THEMENMODERATION:
DI Stefan Leitner |
s IT Solutions AT Spardat GmbH

RISK-MANAGEMENT: SCHNITTSTELLEN, REPORTING & MESSBARKEIT VON MASSNAHMEN

THEMENMODERATION:
Jürgen Englert, MSc |
A1 Telekom Austria AG

BCM & TOTALAUSFÄLLE DER IT: WAS UND WIE WIRD GETESTET?

THEMENMODERATION:
Reinhold Wochner, MSc |
Raiffeisen Bank International AG

2. TAG OPEN SPACE ARBEITSKREISE

1 AKTUELLE BEDROHUNGEN

LEITUNG:
MAG. (FH) MARKUS RIPKA, CISSP
DenizBank AG

DER SCHLÜSSEL ZUM KÖNIGREICH: WIE UNGESCHÜTZTE ADMIN-ZUGÄNGE HACKERN DIE ARBEIT ERLEICHTERN

THEMENMODERATION:
Tilman Epha |
Cyber-Ark Software Inc.

FÜR DEN ERNSTFALL: VORBEREITUNG, NOTFALLKOMMUNIKATION & ZUSAMMENARBEIT VON KRISENSTÄBEN

THEMENMODERATION:
Ing. Johannes Mariel |
Bundesrechenzentrum GmbH

2 UMGANG MIT DATEN

LEITUNG:
DI MAG. ANDREAS TOMEK, CISA, CISSP
Security Research Sicherheitsforschung GmbH

DATENDIEBSTAHL: PRÄVENTION & KONTROLLMÖGLICHKEITEN?

THEMENMODERATION:
Ing. Leopold Rehberger |
A1 Telekom Austria AG

MOBILITÄT VON DATEN: ZUGRIFF VON ÜBERALL - WIE SICHERE ICH DAS AB?

THEMENMODERATION:
DI Herbert Schindelka |
Wiener Stadtwerke Holding AG

3 INFRASTRUKTUR & NETWORK SECURTIY

LEITUNG:
ING. DI HERBERT DIRNBERGER, MA, CISM
Cyber Security Austria

BYOD 2.0 - WO STEHEN WIR IM ADAPTIONS-PROZESS? BEWÄHRTE MANAGEMENT-SYSTEME

THEMENMODERATION:
MR Dipl. Ing. Dr. Robert Kristöfl |
BM für Unterricht, Kunst und Kultur

INTRUSION PREVENTION & DETECTION

THEMENMODERATION:
Christian Proschinger, BSc |
CERT.at

4 GOVERNANCE, RISK, COMPLIANCE & LEGAL

RISIKEN KOMPLEXER IT-UMGEBUNGEN: COMPLEXITY CRISIS

THEMENMODERATION:
Ing. Mag. Markus Ripka |
DenizBank AG

DATA BREACH: VERHALTEN BEIM BREACH & ERWARTETE ÄNDERUNGEN IM LICHT DER EU-DATENSCHUTZ-VERORDNUNG

THEMENMODERATION:
Dr. Günther Leissler |
Schönherr Rechtsanwälte GmbH

AK1 AKTUELLE BEDROHUNGEN

Leitung: Mag. (FH) Markus Ripka, CISSP | DenizBank AG

WORKSHOP 1:
„SECURITY ANFORDERUNGEN DER NÄCHSTEN JAHRE: WO GEHT DIE REISE HIN?"

DI Dr. Thomas C. Stubbings, CISA | Raiffeisen Bank International AG

Ergebnisse / behandelte Themen

Mandian APT1 Report (Muster bei Angriffen, ca. 1000 Hacker mit möglichem chinesischem Militärhintergrund)

Cloud services: Stellen neue Anforderungen an die Sicherheit. Dropbox blockieren als erster Schritt, aber dann den Bedarf erkennen und sicher erfüllen. Kunden verwenden Dropbox und USB zur Datenübertragung. Cloud services in die Awareness Maßnahmen einbinden, aber Awareness alleine reicht nicht aus. Welche Cloud Services nutzen die User ohne Wissen der IT (Dropbox, VOIP, Google Talks,...) Enterprise Storage Lösungen in der Cloud (rechtlich Fragen, SLA, patriot Act). Unkontrollierte Anschaffung von Cloud Services durch Fachabteilungen.

Advanced persistent threats werden Standard. Gegenstrategien: Sicherheitsprüfung oder Vulnerability scan neuer Software. Maßnahmen gegen den Abfluss von Unternehmensdaten: Strategien zur Entdeckung von Datenlecks z.B. Honeypot Systeme, IDS, DLP. Datenverschlüsselung, secure Datarooms, sandboxing, getrennte Netzwerke als alternative Sicherheitsmaßnahmen. Probleme mit USB Datenträgern nach wie vor aktuell. Anomalie-erkennung ist schwierig zu realisieren, die Angreifer verbessern die Datenexfiltrations-kommunikation.

Sicherheit bei BYOD: Mentalität bestimmt ob BYOD oder nicht, Asien kein BYOD, Amerika stark BYOD Qualitativ bessere Hardware (Notebooks, Pads, Smartphones) von Unternehmensseite gegen BYOD oder als Hürde mit Vorstandsunterschrift.

Schwerpunkte:
- Sicherheit bei BYOD
- Maßnahmen gegen den Abfluss von Unternehmensdaten
- Advanced persistent threats
- Cloud services

WORKSHOP 2:
„ZWISCHEN CYBERWAR UND HACKTIVISM – FÜR WELCHE BEDROHUNGEN MÜSSEN WIR GERÜSTET SEIN"

Dipl. Inf. Ing. Candid Wüest | Symantec Austria GmbH

Ergebnisse / behandelte Themen

Cyberwar: Momentan hauptsächlich Spionage von Unternehmensdaten. Vorfälle in derselben Branche helfen bei der Durchsetzung von Maßnahmen wenn die Awareness zeitnah genutzt wird. Penetrationtests zeigen Schwachstellen auf, können aber aufgrund beschränkter Ressourcen nie vollständig sein.

Angriffe über Subunternehmer. Zuerst wird der kleine, schlecht abgesicherte Subunternehmer angegriffen und über diese das eigentlich Zielunternehmen.

EU formuliert derzeit europäische Cybersecurity Strategie. Entwurf Feb. 2013. Inhalte: ein CERT pro Land, Cyberdefense. EU wird Cybersecurity-Projekte fördern. ENISA erstellt Whitepapers und Policies. Operative Absicherung eigener Netze und Systeme bleibt bei den Betreibern.

Hacktivism: Shitstorm: soziale Netzwerke werden als Auslöser für Hackangriffe genutzt. Selber Google Alerts oder Facebook, Twitter „follow" nutzen um Nachrichten zum eigenen Unternehmen zu verfolgen. Pastebin als Webservice verfolgt online Nachrichten zum Unternehmen. Nicht nur Firmennamen sonder auch Namen hochrangiger Manager überwachen. Passwort reuse der User. Möglichkeiten von Schäden und Absicherung der sozialen Netzwerkzugänge des Unternehmens prüfen. Meldungen von Sicherheitsschwachstellen über soziale Netzwerke ernst nehmen.

Meldepflicht von Datenverlusten oder Informationssicherheitsvorfällen wenig zielführen. Der Imageschaden wird sofort voll schlagend (diginotar ging pleite). Verwertbarer Nutzen der Meldepflicht fraglich. Kommunikation der Vorfälle wahrheitsgetreu, herunterspielen stachelt Angreifer weiter an. Einen Pressesprecher für den Vorfall definieren und strikt einhalten. Richtiges Mediengefühl für Twitter, Facebook und co. erforderlich.

Schwerpunkte:

- Kommunikation von Vorfällen
- Hacktivism
- Angriffe über Subunternehmen
- EU Cybersecurity Strategie
- Behandlung von Vorfällen

WORKSHOP 3:
„APTS: WIE SCHÜTZEN WIR UNS GEGEN GEZIELTE & NACHHALTIGE ANGRIFFE"

Mario Fritzer | Palo Alto Networks

Ergebnisse / behandelte Themen

Attacke auf RSA war APT Attacke (social engineering mit water holing)

Angriffe laufen heute auch über water holing. Dabei werden normale Webseiten mit Download Trojanern gespickt, die teilweise nur bei bestimmten IP Bereichen aktiv werden. Es wurden auch schon Web ADs (Werbeeinschaltungen) Netzwerke gehackt und neben der Werbebotschaft ein Trojanerdownload geschalten.
Woran kann man erkennen, dass man möglicherweise Opfer einer ATP Attacke wurde: Server verhalten sich komisch, Information von Externen, DNS Logs enthalten, sonderbare Abfragen, Firewall Logs enthalten gehäuften Netzwerkverkehr, gehäufter SSL Datenverkehr

http://www.infoworld.com/d/security/5-signs-youve-been-hit-advanced-persistent-threat-204941

- APT sign No. 1: Increase in elevated log-ons late at night
- APT sign No. 2: Finding widespread backdoor Trojans
- APT sign No. 3: Unexpected information flows
- APT sign No. 4: Discovering unexpected data bundles
- APT sign No. 5: Detecting pass-the-hash hacking tools

Was hilft nicht gegen ATP: Virenscanner , Perimeterdefense (Firewall)

Was kann gegen ATP helfen:
- Sandboxing von Browser, PFD, Java
- Baselining im Unternehmen von: DNS, Netzwerk Verkehr, Firewall, SSL traffic
- Verwendung mobiler Geräte (Ipad, Android) beim Surfen und Kombination Citrix zum Zugriff auf Unternehmensdaten
- Netwerksegmentierung
- Host based IDS
- Appblocker oder ähnliche Anwendung mit Whitelist über checksum

WORKSHOP 4:
„PHISHING, SOCIAL ENGINEERING & THREATS VIA SOCIAL NETWORKS"

Harald Haselbauer | Amt der Burgenländischen Landesregierung

Ergebnisse / behandelte Themen

Im Gegensatz zu 2009 sind in den meisten Unternehmen die sozialen Netzwerke wie Facebook und twitter für die Mitarbeiter offen zugänglich.

Social Engineering läßt sich nicht allein mit technischen Mitteln in den Griff bekommen.

Awareness schaffen als Kernmaßnahme:
- Social media guideline wie mit sozialen Netzwerken umzugehen ist
- Anpassen der Awarnessschulungen für verschiedene Zielgruppe
- Meldestelle für Mißbrauch oder Fragen einrichten. Benutzer brauchen die Möglichkeit dubiose Anfragen überprüfen zu lassen

Phishing und social Engineering nutzen alle Kommunikationswege und Applikationen: Email, Facebook, Twitter, Foren, ebay, ebanking

Einzelne Phishingfälle sind so gefinkelt, dass der Benutzer selbst alle Sicherheitsmaßnahmen umgeht. Beispiel: Angebot besonderer Verzinsung über eingeschleuste Werbung in ebanking webseite.

Für den Fall eines Schadens sollte zudem Möglichkeiten der Schadenseindämmung und der Krisenkommunikation überlegt werden.

WORKSHOP 5:
„DER SCHLÜSSEL ZUM KÖNIGREICH: WIE UNGESCHÜTZTE ADMIN-ZUGÄNGE HACKERN DIE ARBEIT ERLEICHTERN“

Tilman Epha | Cyber-Ark Software Inc.

Ergebnisse / behandelte Themen

Policy ist wichtig, sie muss aber auch umgesetzt werden.
Meist wird die Policy so gestaltet, dass jeder nur die Rechte erhält, die er auch wirklich für seinen Tätigkeitsbereich benötigt. Die Schwierigkeit liegt aber darin, zu bestimmen, wer welche Rechte benötigt.
Wie identifiziert sich der User?
Viele Angriffe zielen auf Admin-PW ab. Damit kann auch der meiste Schaden angerichtet werden.
Wie „verwahre“ ich Passwörter?
Viele Unternehmen haben sich individuelle Lösungen geschaffen.
Warum fühlt sich ein UN genötigt etwas in diesem Bereich zu tun? gesetzliche Vorschriften, Anregungen durch Prüfer,...
Externer Dienstleister: zuerst muss ich ihn prüfen; wie kann er mir reporten?; lückenlose Transparenz einfordern!;
Thema wird immer wichtiger; Nachfrage nach Lösungen steigt; nach wie vor viele offene Fragen bei UN.

Schwerpunkte:

- Risiko
- Angriffe
- rechtl. Fragen
- Berechtigungen
- Audit
- Passwort Policy/Vergabe
- I & AM

WORKSHOP 6:
„FÜR DEN ERNSTFALL: VORBEREITUNG, NOTFALLKOMMUNIKATION & ZUSAMMENARBEIT IN KRISENSTÄBEN"

Ing. Johannes Mariel | Bundesrechenzentrum GmbH

Ergebnisse / behandelte Themen

Umgang mit Krisen und Notfällen erfordert spezielles Management (BCM) und Kommunikation. Sicherstellen der Entscheidungswege, Stellvertreterregelung bzw. Befugnisregeln für Notfälle.

Einteilen von Funktionen in der Krisenorganisation auch nach persönlichen Skills. (z.B. Feuerwehr, Miliz, Vereinsobmann, rotes Kreuz)

Kommunikationsliste mit wichtigen Personen und Partnern erstellen und periodisch aktualisieren. Kommunikation ist im Krisenfall existentiell. Periodisch üben mit den Kommunikationspartnern und der Kommunikationswege.
Alternative Kommunikationsmittel auswählen und vorbereiten (Internet offline, kein Email, kein Mobilfunknetz & SMS , Festnetz) z.B. Funk, Melder, Festnetz, Fahrrad.

Kommunikation nach außen mit Partnern, Management, Politik und Kunden berücksichtigen. Pressesprecher bzw Medienbetreuung. Sprachen/Know beachten

Kommunikation zwischen Krisenstäben und mit den Einsatzorganisationen. Verbindung zu anderen Krisenstäben mit „Verbindungsoffizieren" und Kommunikationsmitteln.

Checklisten erleichtern die strukturierte Kommunikation.

Unangekündigte Übungen steigern die Aufmerksamkeit und die Improvisationsgabe. Schwierigkeitsgrad der Übungen anpassen an die Fähigkeit der Organisation. Überfordern schadet, unterfordern bringt keinen Fortschritt.

Nationale Cybersecurity Strategie für Österreich. Erst gemeinsame Notfallübungen zwischen staatlichen und privaten Stellen. Noch wenig Organisation vorhanden, aber Improvisationsgabe der Beteiligten.

Szenarien entwickeln und im Plan durchspielen für verschiedene Krisen. Lösungen für „Münchhausen" Szenarien bedenken.

AK2 UMGANG MIT DATEN

Leitung: DI Mag. Andreas Tomek, CISA, CISSP | Security Research Sicherheitsforschung GmbH

WORKSHOP 1:
„WER HAT DIE FINGER AUF DEN DATEN - WEB & MOBILE DEVICES"

Michael Rudrich | Websense Deutschland GmbH

Ergebnisse / behandelte Themen

- Proaktive/Reaktive Kommunikation bei Datenverlust, als Kunde proaktives Vorgehen gewünscht. Im Unternehmenskontext schwierig.
- Datendiebstahl, wer weiß davon? Langanhaltende Attacken -> APTs.
- Soziale Medien, sowie im privaten Bereich als auch bei professionellen Netzwerken als Leak Quelle.
- BYOD und Cloud nehmen zu. Wenig bzw. keine Kontrolle über Firmendaten. Firmendaten gehören der Firma -> Bewusstseinsbildung
- Missbräuchliche Verwendung oft seitens Entwicklern und Senior Management (Statussymbole)
- Komplexität der IT-Umgebungen und Nicht-IT Medien wie Flipcharts sind Herausforderungen in Organisationen
- Scheinsicherheit oft ein Problem. Wer ist dafür verantwortlich, darf sich das Management blind auf die Sicherheit von der IT zur Verfügung gestellten Lösungen verlassen.
- Externe Kommunikation mit Behörden und Beratern/Lieferanten oft als Ursache. Sicherheit am Zielort.
- Man muss wissen wir Daten verwendet werden (Unterschied Managementsicht und realer Datenfluss)

Schwerpunkte:

- Wie sicher sind die Daten, Aussage: 95% der Unternehmen hatten bereits einen Datenverlust
- Mobile Datenmedien und Devices
- Social Media
- Compliance und Vorfälle als Treiber für Maßnahmen
- Sensibilisierung und Awareness als wichtigste Maßnahme



WORKSHOP 2:
„APTS & DIE AUSWIRKUNGEN AUF DIE DATENSICHERHEIT“

DI Mag. Andreas Tomek, CISA, CISSP | Security Research Sicherheitsforschung GmbH

Ergebnisse / behandelte Themen

Ponemon 58% APTs als Bedrohung
2013 Infosec Study: 93% large 87% small, 63-78% from outside attackers
APT anbieter Fireye: 95% of customers compromised
Advanced Persistent Thread: Virus/Bot/APT Erklärung
Hardening, Zusätzliche Maßnahmen, Extrusion Prevention,
Social Engineering Angriffe auf Basis von Spam ist eine wesentliche Bedrohung. Bei der Awareness der Mitarbeiter muss nachjustiert werden.
Der Aufwand für Protection und Analyse ist gewaltig. Vor allem um die letzten paar Prozent Risiko auszuschließen/ minimieren. Frage der Wirtschaftlichkeit!
Großteil der User hat nur noch eingeschränkte Berechtigungen – Ausnahme vllt. Entwickler.
APTs in Zusammenhang mit Social Media (SM) Policy bzgl. SM ist nahezu in allen UN vorhanden. IT MUSS Traffic einschränken.
Einschränken der Nutzung von SM auf Firmen-PC hilft nur tlw., da MA SM auch auf Smartphone usw. nutzen können.
Technische Möglichkeiten stoßen an Grenzen, darum ist es wesentlich die Awareness der Mitarbeiter zu stärken.
Monitoring allein ist natürlich nicht genug, man muss sich die Protokolle anschauen. Das ist sehr aufwendig, man braucht Manpower und dann wird’s auch wieder eine Frage der Wirtschaftlichkeit.

WORKSHOP 3:
„IT-BERECHTIGUNGEN: LEIDEN WIR NOCH ODER MANAGEN WIR SCHON?“

Helmut Semmelmayer, BSc, MSc | certex Information Technology GmbH

Ergebnisse / behandelte Themen

- Wege um Berechtigungen zu managen: Vom User aus und vom System aus.
- Bilden von Rollen über defacto Berechtigungen
- Wichtig Einbindung aller Systeme auch Eigenentwicklungen und Proprietäre
- Welche Mitarbeiter haben auf welche Daten zum Zeitpunkt X Zugriff
- Reporting ist bei heterogenen Systemen sehr schwierig.
- Meldung und Review von benötigten Berechtigungen inkl. Dokumentation und Einstellungen durch wen?
- Automatisierung wünschenswert
- Unstrukturierte Daten sind sehr schwierig
- Was ist wenn jemand die Berechtigungen braucht und dann Daten leaked?
- Need ist da, Budget für Lösungen oft nur schleppend oder nach Vorfällen und wg. Compliance Richtlinien.
- Berechtigungen bei Cloud Lösungen

Schwerpunkte:

- Identifikation von Berechtigungen
- Management von Berechtigungen
- Berechtigungen bei unstrukturierten Daten
- Auswertbarkeit und Reporting von Berechtigungen

WORKSHOP 4:
„KLASSIFIZIERUNG VON DATEN“

Clemens Peyerl, MSc, MBA | Stryker GmbH

Ergebnisse / behandelte Themen

- Klassifizierung aus Folge globaler Compliance-Anforderungen
- Owner der Datenklassifikation
- Klassifikation von Neudaten vs. Altdatenbestände
- Zwei Zugänge entweder über technische Mittel oder Awareness
- User/Owner bezogen oder Systembezogen
- Legal vs. IT vs. Business Owner
- Problem wer klassifiziert
- Technische Lösung durch DLP und Datenklassifizierungstools mit Optionen Protokollierung, Begründung und Blockieren.

Schwerpunkte:
- Wer klassifiziert, wer ist zuständig
- Wo wird klassifiziert
- Strukturierte Daten vs. Unstrukturierte Daten

WORKSHOP 5:
„DATENDIEBSTAHL: PRÄVENTION & KONTROLLMÖGLICHKEITEN“

Ing. Leopold Rehberger | A1 Telekom Austria AG

Ergebnisse / behandelte Themen

- Was ist eigentlich schützenswert? Es kommt drauf an mit wem man spricht
- Problem der Klassifizierung und Durchdringung bis zum Mitarbeiter
- Awareness als zentrales Thema
- Policies die beschreiben sind meistens vorhanden
- Austauschlaufwerke/Shares bergen ein hohes Risiko und werden zweckentfremded
- Welche Awareness kommt wirklich an?
- Mischung Awareness und technisches Enforcement, es muss Betroffenheit bei der Zielgruppe (Top-Mmgt) erzeugt werden
- Fremder Blick auf die Klassifizierung ist sehr wichtig um alle wichtigen Daten zu identifizieren.

Schwerpunkte:
- Klasssifizierung
- Sicherheit mobiler Endgeräte
- Awareness und Verhaltensänderung
- Technische Maßnahmen flankierend oder als Baseline bei Themen wie Verschlüsselung

WORKSHOP 6:
„MOBILITÄT VON DATEN: ZUGRIFF VON ÜBERALL - WIE SICHERE ICH DAS AB?“

DI Herbert Schindelka | Wiener Stadtwerke Holding AG

Ergebnisse / behandelte Themen

- Mehrwert von Mobilität stark abhängig vom Anwendungsfall (zB notwendig für Außendienst vs. Plattformdiskussion)
- Image vs. Mehrwert
- Die Mehrheit sieht Mehrwert in Mobilität
- Die Mehrheit sieht Mobilität als Security Herausforderung
- Die Anforderungen des Fachbereichs in Bezug auf Mobility werden nicht klar an die IT kommuniziert -> keine 100% Lösung ohne klare Anforderung möglich.
- Tendenziell ist die gelebte Awareness mittel-niedrig aber tendenziell setzt sich die Security bei Entscheidungen durch.

AK3 INFRASTRUKTUR & NETWORK SECURITY

Leitung: Georg Beham, MSC | KPMG Advisory AG

WORKSHOP 1:
„VULNERABILITY MANAGEMENT - PROAKTIVE AKTIVITÄTEN & ÜBERPRÜFUNG DER SYSTEM-/NETZWERKSICHERHEIT“

Dipl-HTL-Ing. Andreas Schaupp, MSc, MAS | CSC Computer Sciences Consulting Austria GmbH

Ergebnisse / behandelte Themen

- Proaktives Vuln Management mit der Nutzung von Informationen und Services von z.B. Secunia, Cert.at, ICS Cert, CVE ist sinnvoll um das Patchmanagement und Schwachstellenscans zu unterstützen bzw. auch geeignete Workarounds zu entwickeln.
- Schwachstellen-Scans werden von vielen Unternehmen zur Erkennung von aktuell vorhandenen Schwachstellen periodisch eingesetzt. Die Periodizität reicht hier bei Scans von exponierten Systemen von 1 Woche bis hin zu 1 Jahr für Systeme im ICS Bereich.
- Es empfiehlt sich Vuln Scans nur nach entsprechender Ankündigung bei den betroffenen Systemadministratoren durchzuführen.
- Nicht nur unsichere Applikationen sondern auch unsichere Konfigurationen werden mit Schwachstellenscans, Pentests usw. entdeckt.
- Alternativen zu Vulnerability Management bzw. in Kombination können eingesetzt werden: Applikation Whitelistening, Hardening und Segmentierung.
- Wichtig ist das die erkannten Schwachstellen zusammen mit den Bedrohungen im Risikomanagement richtig betrachtet, werden und die richtigen Maßnahmen zur Risikominimierung gesetzt werden.

Schwerpunkte:

- Vulnerability Management, Patch Management, Schwachstellenscans.



WORKSHOP 2:
„KRITISCHE INFRASTRUKTUREN: OFFENHEIT DER SYSTEME & MÖGLICHE FOLGEN"

Ing. DI Herbert Dirnberger, MA, CISM | Cyber Security Austria

Ergebnisse / behandelte Themen

Für die Entwicklung unserer modernen Wohlstandsgesellschaft ist der Einsatz von Technologie aber auch eine weiterschreitende Vernetzung notwendig. IPv6, Internet of Things und konvergierende Netzwerke bringen neue Chancen, aber beinhalten auch enorme Risiken, die mit Segmentierung und Zellenschutz beherrschbar bemacht werden sollten. Probleme gehen speziell von Legacy Systemen und Alt Protokollen aus, die heute nicht mehr den aktuellen Sicherheitsstandards entsprechen.
Allgemein ist die Vernetzung nicht mehr aufzuhalten. Früher geschützte Bereiche aus kritischer Infrastruktur und Industrieanlagen werden mit dem allgemeinen Cyberraum verbunden. Anhand der Suchmaschine shodanhq.com kann aufgezeigt werden, dass sehr sehr viele unsichere System im Netz sind, die ohne Password konfiguriert worden sind bzw. leicht zu finden sind. Die Offenheit der Systeme ist nicht nur der guten Seite bekannt.
Praktisch zeigt sich anhand der ***viewer und VPN Problematik im Unternehmen, dass die User sehr rasche und einfache Lösungen anstreben und die Sicherheit meist in den Hintergrund gestellt wird.
Um die neuen Chancen durch die Vernetzung nützen zu können, sollte aktiv folgende Punkte stark fokussiert werden.

- Awareness schaffen
- Sicherheitskultur aufbauen
- Kommunikation fördern
- Ausbildung zu Sicherheit stärken
- Staatliche Regulierungen und Gesetze schaffen

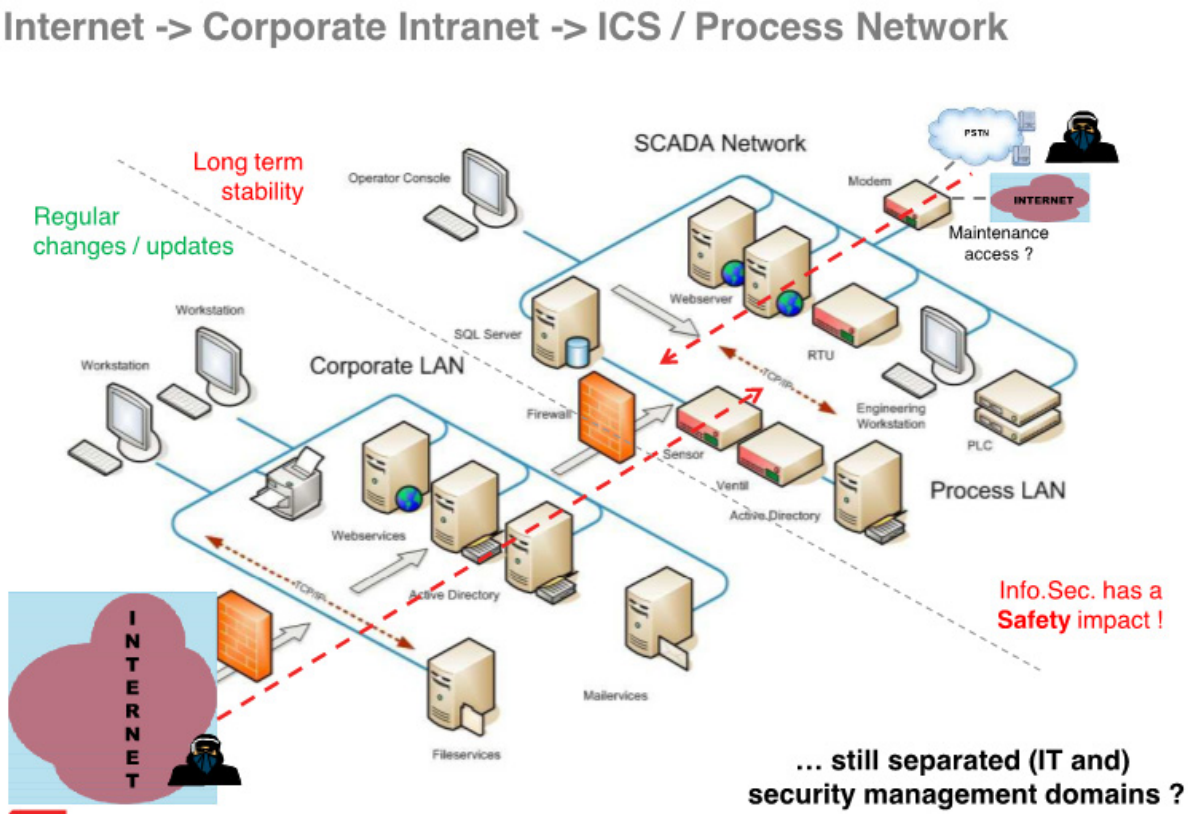
Allgemein darf die Abhängigkeit von Energie nicht unterschätzt werden und die Vernetzung geht laufend weiter: Smart Meter – Smart Grid – Smart Cities

- Schwerpunkte: Netzwerke, Konvergenz, Sicherheit, Awareness, kritische Infrastruktur, Industrie, ICS

WORKSHOP 4:
„SICHERHEIT VON INDUSTRIEKONTROLL- / SCADA-SYSTEMEN SIND WIR GERÜSTET?"

Dipl-HTL-Ing. Andreas Schaupp, MSc, MAS | CSC Computer Sciences Consulting Austria GmbH

Ergebnisse / behandelte Themen



Das Thema sichere industrielle IT kommt durch die laufende Vernetzung, Einsatz von COTS und Konvergenz der Systeme enorme Bedeutung zu. Einige Industrieunternehmen haben sich schon seit lange auf die Herausforderungen vorbereitet, andere sind erst am Beginn mit den Bemühungen die ICS Systeme sicherer zu machen.
Weiters löst dieses Thema starke Kontroversen zwischen IT und Automatisierung aus und es entwickelt sich auch neue Paradigma wie zB die ICS Security.

Nichts destotrotz gibt es erfolgreiche Implementierung mit verschiedensten Werkzeugen.

- ISO 27001
- ISO 27001 + BDE Whitepaper

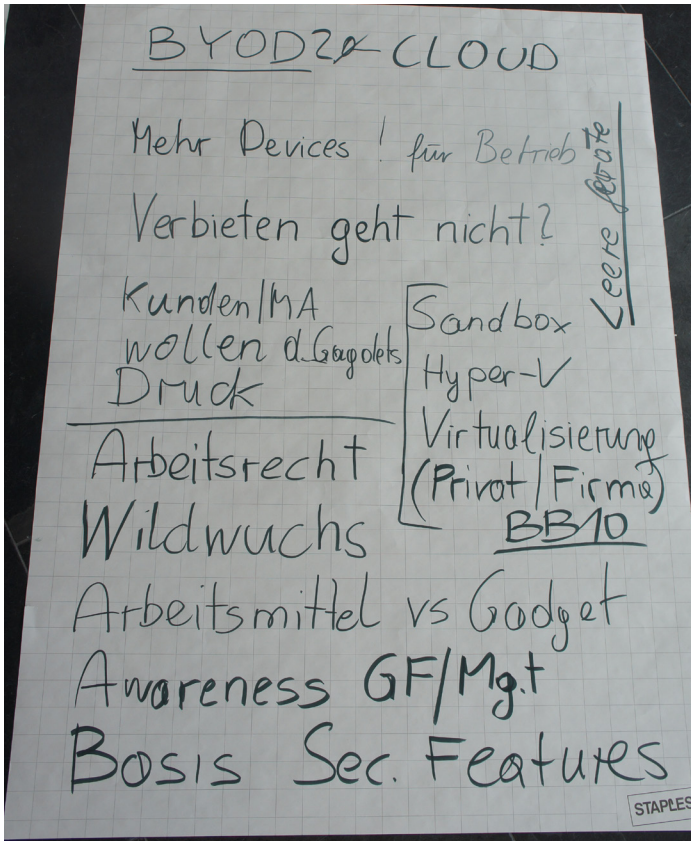
Aber es kommen auch noch neue Standards wie ISA S99, IEC 62443 und bzw. VDI 2182 zum Einsatz.

Ein wesentliches, zu lösendes Problem ist das Verständnis der jeweils an Terminologie (IT vs. ICS) durch beide involvierten Teams (IT und Automatisierungstechnik).

Im Großen und Ganzen wird es noch einige Zeit brauchen, dass sich ICS Security hat. Wichtig ist jedoch, dass das Thema richtig behandelt, egal ob von IT, Automatisierung und Produktionsabteilungen bzw. von externen Beratern.

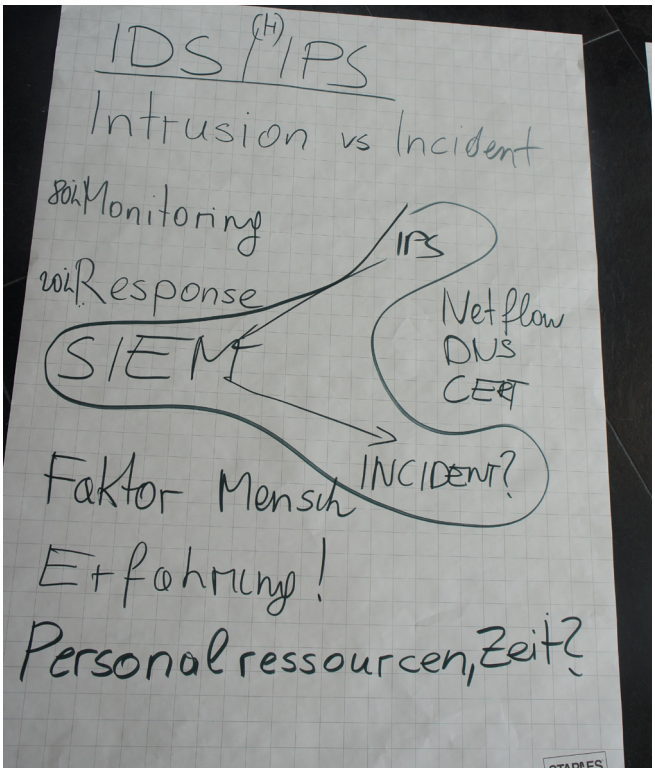
WORKSHOP 5:
„BYOD 2.0 - WO STEHEN WIR IM ADAPTIONS-PROZESS? BEWÄHRTE MANAGEMENT-SYSTEME"

MR Dipl. Ing. Dr. Robert Kristöfl |
BM für Unterricht, Kunst und Kultur



WORKSHOP 6:
„INTRUSION PREVENTION & DETECTION"

Christian Proschinger, BSc | CERT.at



AK4 GOVERNANCE, RISK, COMPLIANCE & LEGAL

Leitung: Georg Beham, MSc | KPMG Advirsory AG

Die Protokolle der folgenden Workshops finden Sie auf den nächsten Seiten als Mindmaps festgehalten:

WORKSHOP 1:
„100%IGE SICHERHEITSERFÜLLUNG: WAS IST REALISTISCH UND WIEVIEL INFORMATION SECURITY IST GENUG?"
Wolfgang Ertl, MAS | Verbund AG

WORKSHOP 2:
„ISO 27001 VS. IT-GRUNDSCHUTZ VS. RISK-IT"
DI Stefan Leitner | s IT Solutions AT Spardat GmbH

WORKSHOP 3:
„RISK-MANAGEMENT: SCHNITTSTELLEN, REPORTING & MESSBARKEIT VON MASSNAHMEN?"
Jürgen Englert, MSc | A1 Telekom Austria AG

WORKSHOP 4:
„BCM & TOTALAUSFÄLLE DER IT: WAS UND WIE WIRD GETESTET?"
Reinhold Wochner, MSc | Raiffeisen Bank International AG

WORKSHOP 5:
„RISIKEN KOMPLEXER IT-UMGEBUNGEN: COMPLEXITY CRISIS?"
Ing. Mag. Markus Ripka | DenizBank AG

WORKSHOP 6:
„DATA BREACH: VERHALTEN BEIM BREACH & ERWARTETE ÄNDERUNGEN IM LICHT DER EU-DATENSCHUTZVERORDNUNG"
Dr. Günther Leissler | Schönherr Rechtsanwälte GmbH

Arbeitskreis 4

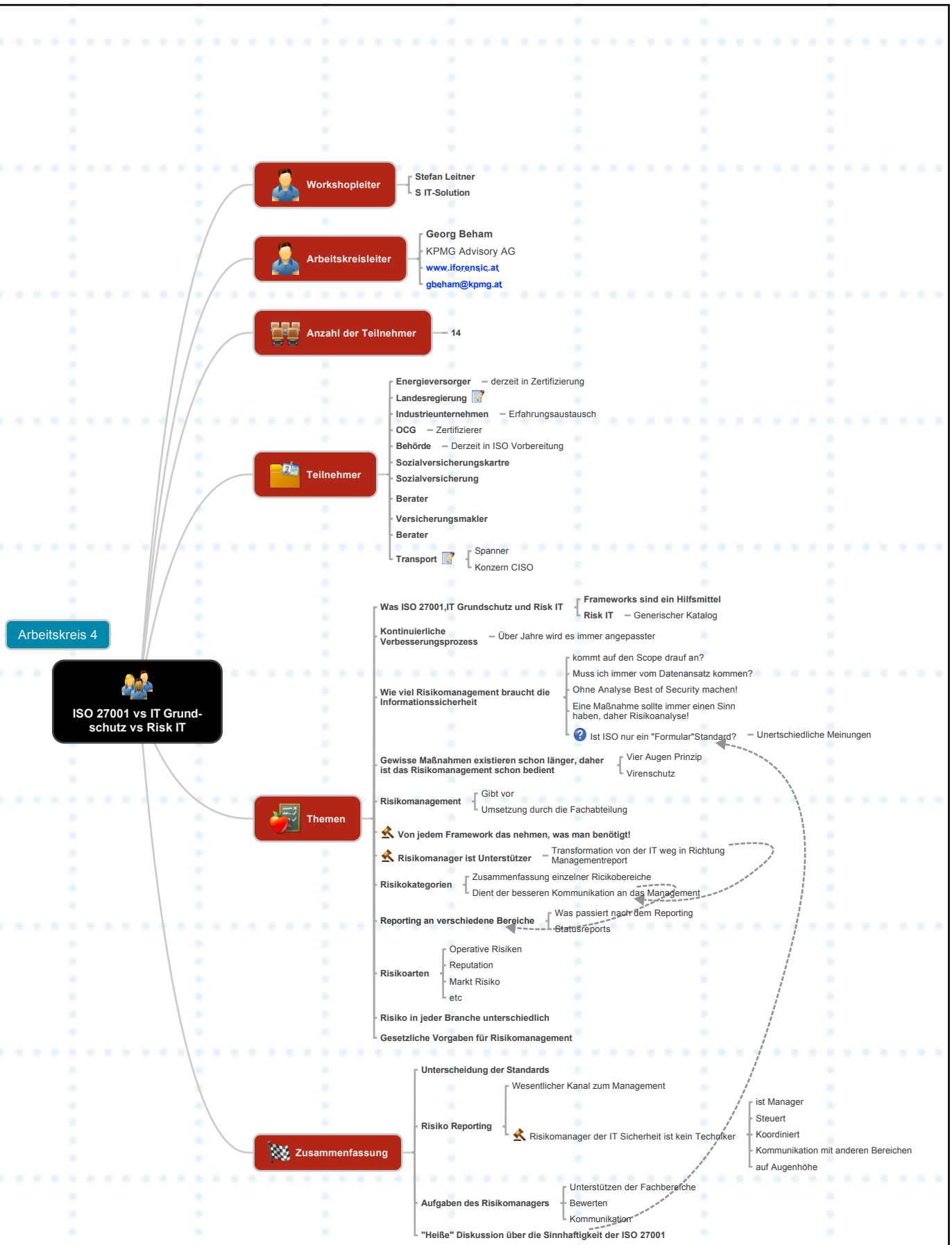
100 % Sicherheitserfüllung

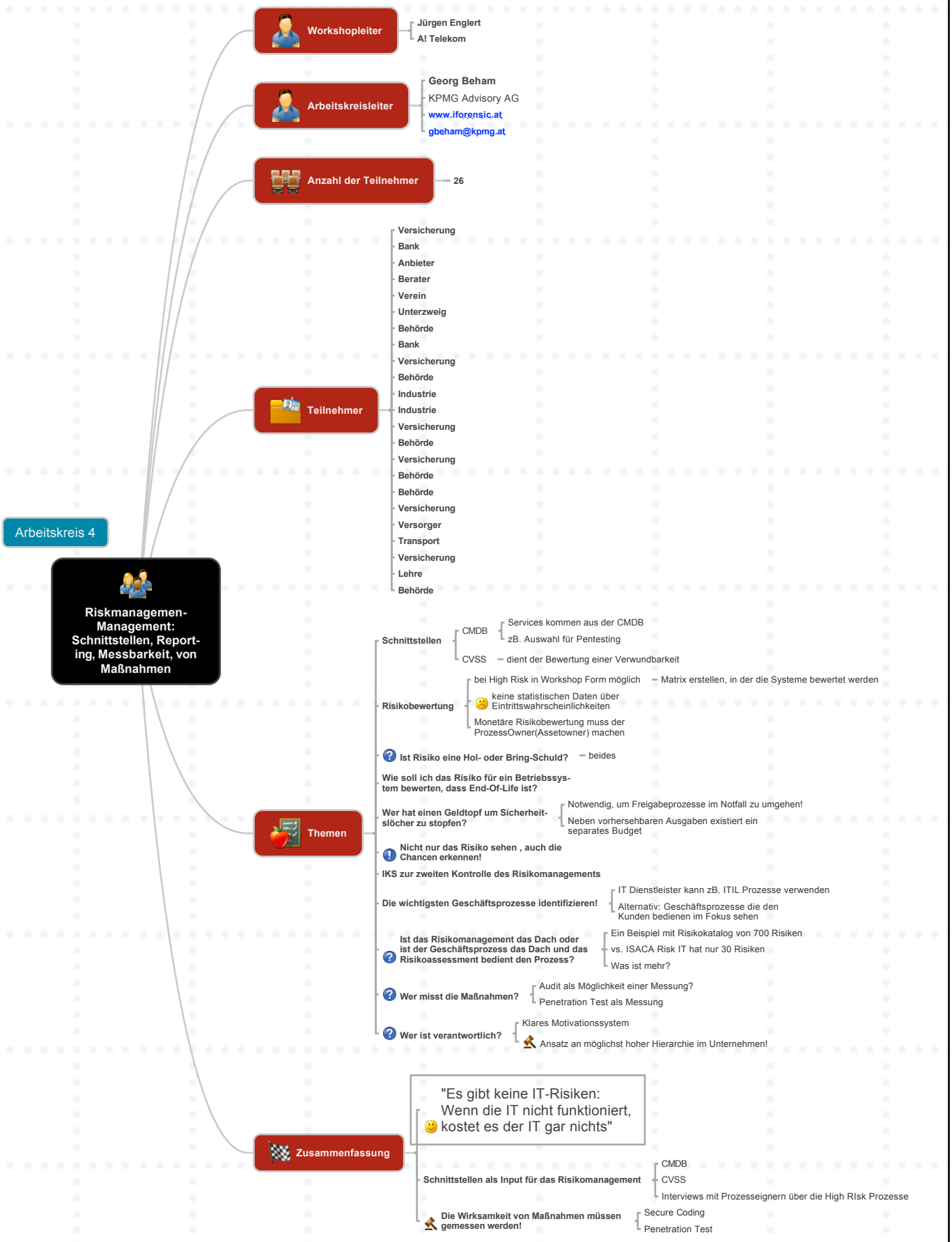
- **Workshopleiter**
  - **Wolfgang Ertl**
  - Verbund AG
  - CISO
- **Arbeitskreisleiter**
  - **Georg Beham**
  - KPMG Advisory AG
  - www.iforensic.at
  - gbeham@kpmg.at
- **Anzahl der Teilnehmer** — **14**
- **Teilnehmer**
  - **Energie Versorger** — Was sind die richtigen Maßnahmen?; Derzeit in Zertifizierung
  - **Banken IT Diensteister** — Awareness; Technologie; Abläufe
  - **Direktbank** — Aufbau eines ISMS derzeit
  - **Telekomikationsanbieter** — Was sind die High Risks!?
  - **Landesregierung** — Awareness
  - **Pharma Unternehmen** — Was ist der praktische Ansatz?
  - **Versicherung** — Derzeit in Zertifizierung
  - **Berater** — Drei Faktoren - in einem Framework: Infrastruktur; Awareness; Prozesse
  - **Versicherungsmakler** — Wo hört die Sicherheit praktisch auf?; Wo beginnt die Aufgabe der Versicherung?; Wo ist die Risikoakzeptanz der Unternehmen?
  - **Magistrat** — Finden des Mittelweges; Grundschtzansätze; Absicherung von Kernprozessprozessen
  - **Versicherung** — Wie weit möchte man Sicherheit betreiben?; Die Policy definiert wohin man gehen will!
  - **Berater**
  - **Betreiber Sicherer Infrastruktur** — Awareness; Was machen die anderen Teilnehmer im Bereich der Awareness?
- **Themen**
  - **Versicherung gegen CyberSchaden?**
  - **ISO Zertifizierung als Ziel um die Motivation zu bekommen** — Das System muss leben, um wirklich effektiv zu sein!
  - **Self-Assessments**
  - **Schwachstellen Management**
  - **Konsequenzen** — Meldungen werden positiv verwertet; Nachschulungen bei Verstoß!; Welche Konsequenzen gibt es wirklich für Verstöße? — Keiner der Teilnehme zeigt auf!; Mitarbeiter macht einen Fehler nur einmal!
  - **Ist am Markt ein zu hoher Kostendruck, der Sicherheit keinen Platz hat?** — Sicherheit muss nicht immer ein Kostentreiber sein; Weniger Schulung bewirkt weniger Sicherheit!; Der Fisch fängt am Kopf zum stinken an!
  - **Management Committment** — bei AG nicht sehr vorhanden; am Papier schon aber nicht im Alltag; bei Familienunternehmen höher, da ja dann auch die Erben und "Erbeserben" von einem Schaden betroffen sind!; C-Level Policies! — Standardisierung vorhanden, jedoch wird sich nicht daran gehalten (vom Management); iPads und Co als Standard eingeführt
  - **DLP als Lösung?** — Wenn wir fünf Jahre zurück könnten, dann würden wir DLP nicht mehr kaufen!; Kostet und bindet unheimlich viel Ressourcen?
  - **Priorisierung der Schäftsprozesse**
  - **Schadensstatistiken sind nicht vorhanden**
  - **Ist der Vorfall versicherbar?**
  - **Security as a Service** — Security schon in Projekte einfüehen
    - Vorprojektphase
    - In Projektrichtlinien einzubauen
    - Auch ins Leben zu rufen
    - Laufend AWARENESS — Tools wis Virtual Company ale Unterstützung
    - Kann auch als Damoklesschwert sein!
  - **Awareness**
    - Auch bei den IT "Hardcore" Technikern notwendig
    - Techniker muss sich als Teil eines übergeordneten Prozesses sehen
    - Im Leittechnikbereich ist die Awareness noch nicht verankert
    - "Das Nicht glauben können, wie Angreifer vorgehen würden"
    - Administratoren haben die meisten Ausnahmen! — es darf da keine Sonderstellung
    - **Schadensstatistiken sind nicht vorhanden**
- **Zusammenfassung**
  - **Management Committment existiert nur am Papier** — das führt zu Kostenkonflikten für die Sicherheit
  - **Awareness um die Mitarbeiter abzuholen als wesentliche Maßnahme!** — "Das Nicht glauben können, wie Angreifer vorgehen würden"
  - **Konsequenzen beim Verstoß tatsächlich nicht vorhanden!**
  - **IS als fixer Bestandteil im Projektmanagement?**

Schwierig Fachexperten zu überzeugen

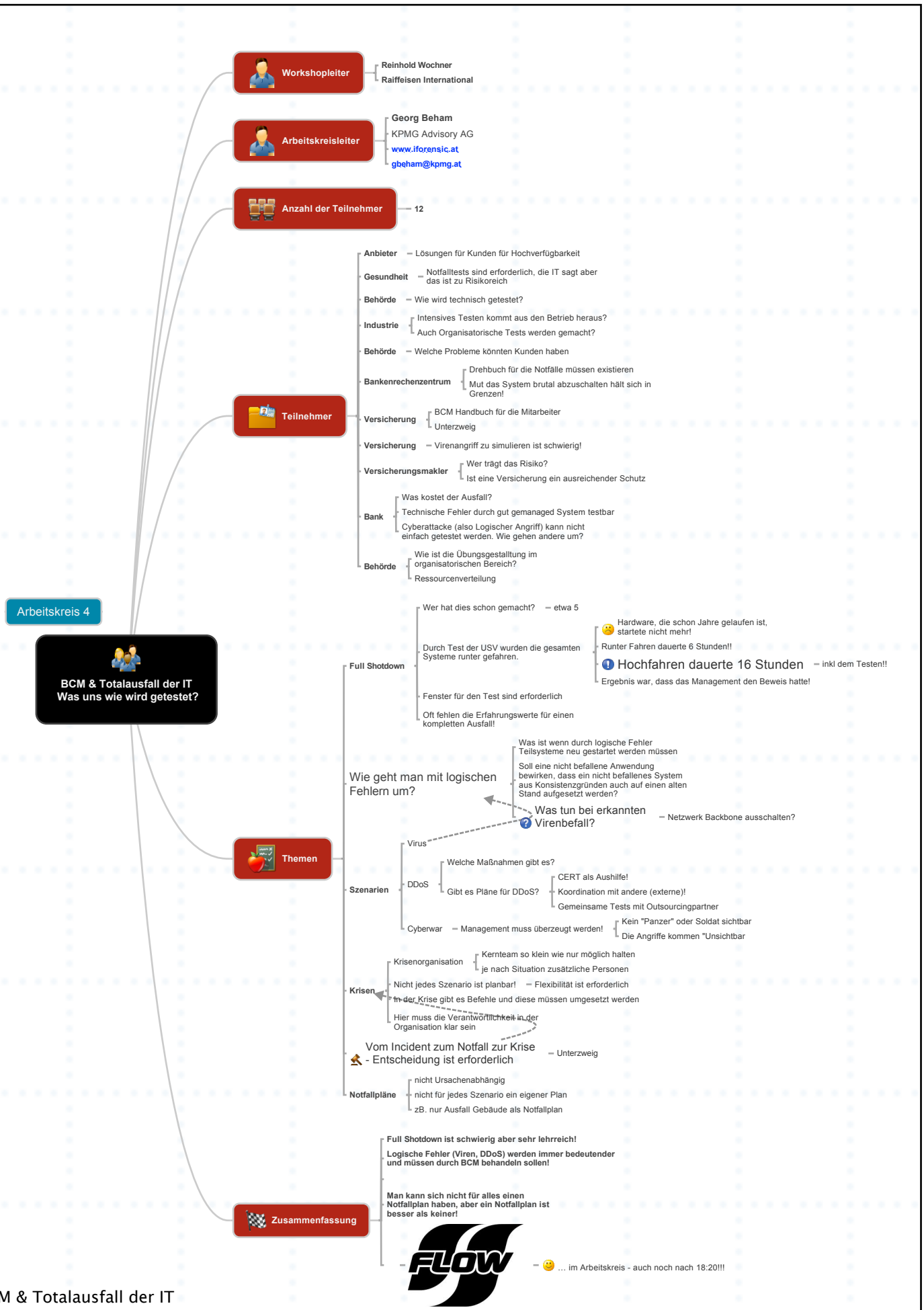
Versteht der Sicherheitsexperte die Technik immer im Detail?
Stichwort - KRITISCHE INFRASTRUKTUR

100 % Sicherheitserfüllung - 14.05.13 - Mindjet

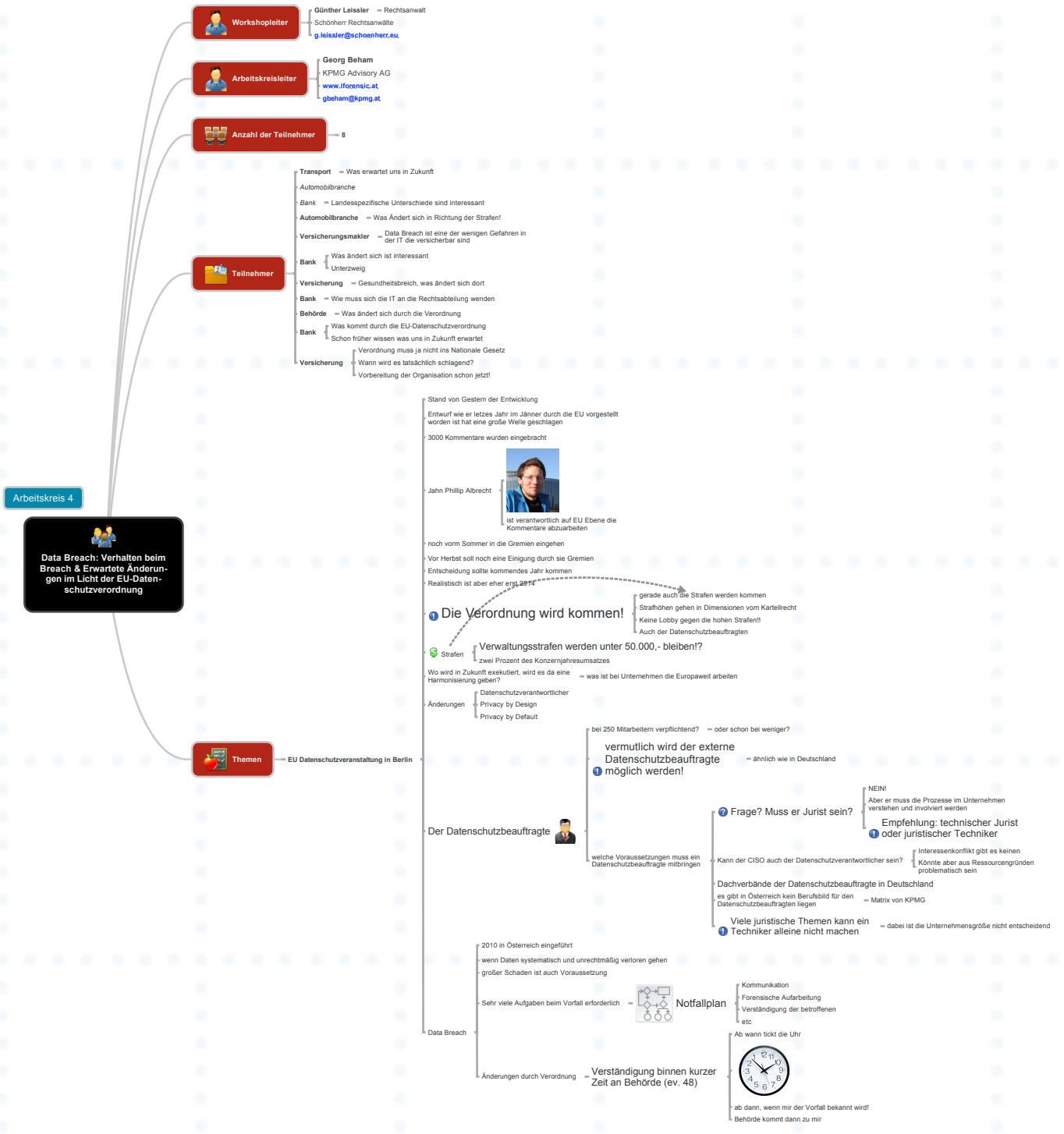

Arbeitskreis 4
ISO 27001 vs IT Grund-schutz vs Risk IT
Workshopleiter
Stefan Leitner
S IT-Solution
Arbeitskreisleiter
Georg Beham
KPMG Advisory AG
www.iforensic.at
gbeham@kpmg.at
Anzahl der Teilnehmer
14
Teilnehmer
Energieversorger – derzeit in Zertifizierung
Landesregierung
Industrieunternehmen – Erfahrungsaustausch
OCG – Zertifizierer
Behörde – Derzeit in ISO Vorbereitung
Sozialversicherungskartre
Sozialversicherung
Berater
Versicherungsmakler
Berater
Transport
Spanner
Konzern CISO
Themen
Was ISO 27001,IT Grundschutz und Risk IT
Frameworks sind ein Hilfsmittel
Risk IT – Generischer Katalog
Kontinuierliche Verbesserungsprozess – Über Jahre wird es immer angepasster
Wie viel Risikomanagement braucht die Informationssicherheit
kommt auf den Scope drauf an?
Muss ich immer vom Datenansatz kommen?
Ohne Analyse Best of Security machen!
Eine Maßnahme sollte immer einen Sinn haben, daher Risikoanalyse!
Ist ISO nur ein "Formular"Standard? – Unertschiedliche Meinungen
Gewisse Maßnahmen existieren schon länger, daher ist das Risikomanagement schon bedient
Vier Augen Prinzip
Virenschutz
Risikomanagement
Gibt vor
Umsetzung durch die Fachabteilung
Von jedem Framework das nehmen, was man benötigt!
Risikomanager ist Unterstützer – Transformation von der IT weg in Richtung Managementreport
Risikokategorien
Zusammenfassung einzelner Rickobereiche
Dient der besseren Kommunikation an das Management
Reporting an verschiedene Bereiche
Was passiert nach dem Reporting
Statusreports
Risikoarten
Operative Risiken
Reputation
Markt Risiko
etc
Risiko in jeder Branche unterschiedlich
Gesetzliche Vorgaben für Risikomanagement
Zusammenfassung
Unterscheidung der Standards
Risiko Reporting
Wesentlicher Kanal zum Management
Risikomanager der IT Sicherheit ist kein Techniker
ist Manager
Steuert
Koordiniert
Kommunikation mit anderen Bereichen
auf Augenhöhe
Aufgaben des Risikomanagers
Unterstützen der Fachbereiche
Bewerten
Kommunikation
"Heiße" Diskussion über die Sinnhaftigkeit der ISO 27001



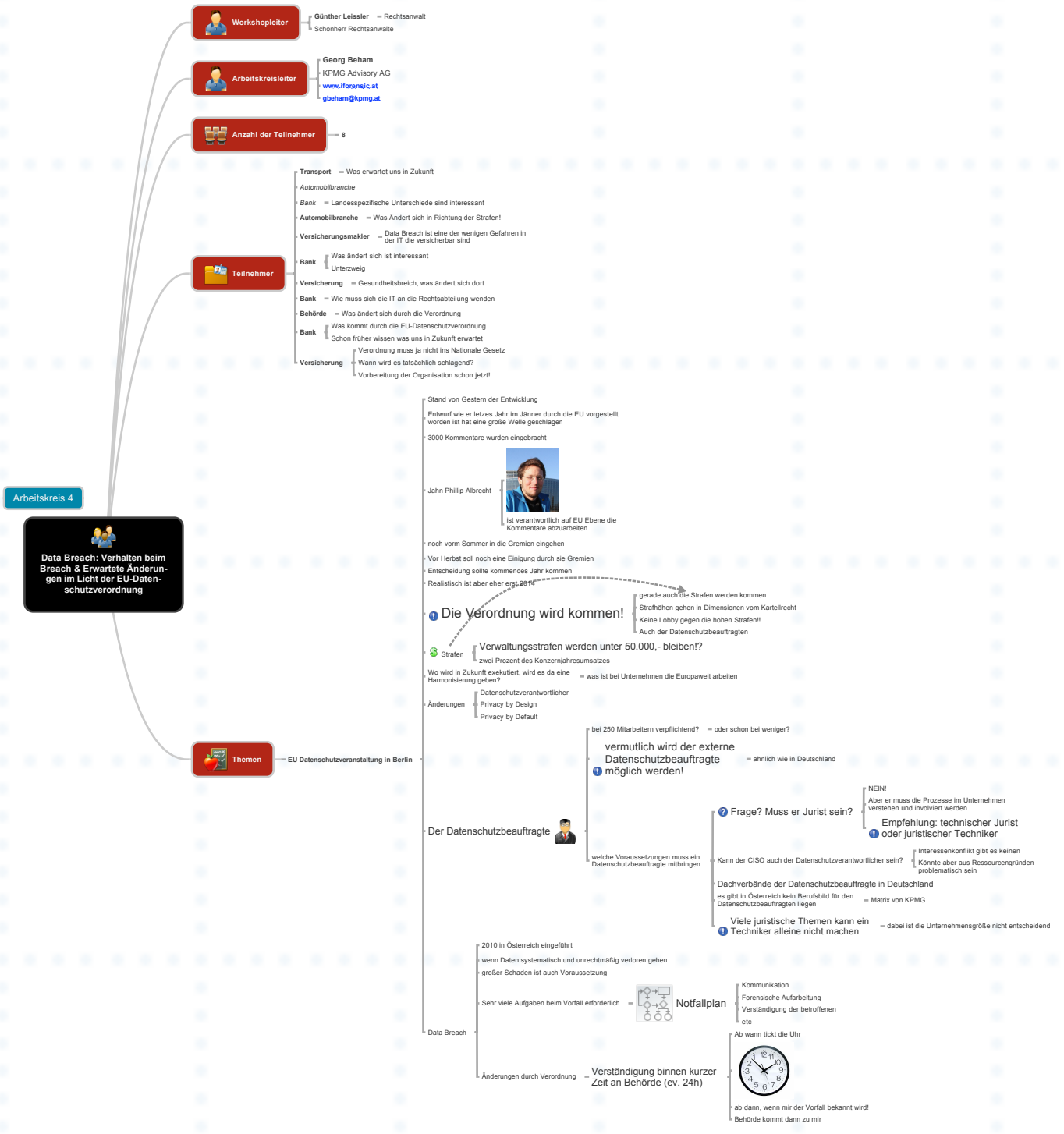
Riskmanagemen-Management:
Schnittstellen, Reporting, Messbarkeit, von Maßnahmen - 14.05.13 - Mindjet



BCM & Totalausfall der IT
Was uns wie wird getestet?
- 14.05.13 - Mindjet



Data Breach: Verhalten beim Breach & Erwartete Änderungen im Licht der EU-Datenschutzverordnung - 15.05.13 - Mindjet



Data Breach: Verhalten beim Breach & Erwartete Änderungen im Licht der EU-Datenschutzverordnung - 15.05.13 - Mindjet

AGENDA DIENSTAG, 14.5.

BIS 09:30
INDIVIDUELLE ANREISE

Registratur am LSZ Infodesk im Seminarbereich

09:30
Empfangserfrischung im Kongresszentrum

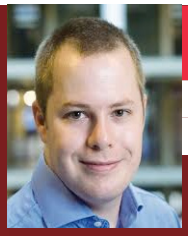
(Workshop Moderatoreneinschulung)

10:00
Begrüßung der Teilnehmer und Hinweis auf den organisatorischen Ablauf / Open Space
Mag. Stefan Reischl | Projektleitung LSZ Consulting

10:15
The DigiNotar Incident and Aftermath

AART JOCHEM, NSCS | GOVCERT.NL

The DigiNotar Case: So long and thanks for all the certificates. The report of a fraudulent certificate issued by DigiNotar came as a bombshell to GOVCERT.NL. The seriousness of the situation was clear immediately, though the real impact on Dutch society became apparant later that week. Aart will present the chain of events which led from the report from CERT Bund to the management takeover of DigiNotar by the government. He will provide a unique view behind the scenes.



10:35
Wie Angreifer wirklich an Ihre Firmendaten kommen

Dipl. Inf. Ing. CANDID WÜEST | Principal Security Engineer | Symantec Austria GmbH

In den Medien überschlagen sich die Berichte von erfolgreichen Cyber Attacken auf Firmen.
Viele dieser gezielten Angriffe sind gar nicht so ausgeklügelt wie man denkt, aber nichts desto trotz erfolgreich.
Lernen Sie, wie sich gezielte Spionage-Angriffe vom Malware Grundrauschen, wie z.B. den Erpressungstrojanern, abheben. Anhand von konkreten Beispielen zeigen wir, wie je nach Motivation sich auch die Methoden ändern.

10:55
ISMS in der Praxis eines Industriebetriebes - Lessons Learned

MAG. (FH) MICHAEL DANZL | IT Security Officer | Fritz Egger GmbH & Co. OG

Der Nutzen eines Information Security Management Systems ist in Fachkreisen unbestritten. Dem gegenüber steht die Frage nach der richtigen „Flughöhe" für ein ISMS: Welche Risiken sind relevant, welche Maßnahmen sind sinnvoll, wie wird die Umsetzung in Zusammenhang mit Best Practices und Zertifizierungen verfolgt. Im Vortrag werden pragmatische und erprobte Lösungen eines europaweit agierenden Industriebetriebs vorgestellt.

11:15
KAFFEEPAUSE

11:45
WORKSHOPS TEIL 1

Parallel für alle Arbeitskreise; Detailinformationen siehe Workshop-Übersicht

AGENDA DIENSTAG, 14.5.

12:45
WORKSHOPS TEIL 2

Parallel für alle Arbeitskreise; Detailinformationen siehe Workshop-Übersicht

13:45
MITTAGESSEN UND GET TOGETHER IM HOTELRESTAURANT

14:50
KEYNOTE:
Lug und Trug - was treibt die Menschen dazu?
Einsichten aus der Verhaltensökonomie

Univ.-Prof. Dr. MATTHIAS SUTTER | Professor of Experimental Economics and Head of Departement | Uni Innsbruck, Institut für Finanzwissenschaften

Warum verhalten sich Menschen nicht immer wahrheitsgemäß, warum umgehen sie Richtlinien, warum täuschen sie andere - und warum tun viele Menschen das nicht? Die moderne Verhaltensökonomie studiert menschliches Verhalten unter dem Mikroskop und untersucht, warum Lug und Trug von Informationsvorteilen einzelner und von den Kosten des Lügens abhängt und warum Fairnessnormen wichtig sind für das Verständnis von menschlichem Verhalten. Der Vortrag beleuchtet diese Aspekte unter dem Blickwinkel neuester Forschungsergebnisse.

15:20
Vertrauen ist gut - Verschlüsseln ist besser

CHRISTIAN LINHART | Regional Sales Manager - Austria | SafeNet Germany GmbH

Schutz und Kontrolle sensibler Daten vom Rechenzentrum bis in die Cloud. Wir zeigen Ihnen, wie Sie Herr über Ihre Daten bleien trotz Outsourcing oder Cloud Nutzung. Anwendungsszenarien in der Praxis.

15:40
Pause | Zeit für Networking

16:10
WORKSHOPS TEIL 3

Parallel für alle Arbeitskreise; Detailinformationen siehe Workshop-Übersicht

17:10
WORKSHOPS TEIL 4

Parallel für alle Arbeitskreise; Detailinformationen siehe Workshop-Übersicht

18:10
Pause - Erholung

18:40
Abendessen im Hotelrestaurant

Abendprogramm ab 19:30 Uhr:
Bocciaturnier und Slacklining bei der Tiki Beach Bar Waidhofen

Danach abschließendes Get-together an der Hotelbar

AGENDA MITTWOCH, 15.5.

08:50
kurze Zusammenfassung des 1. Tages

09:00
The Malware Problem – Managing the Foreseen & Unforeseen

ACHIM KRAUS | Senior Consultant Strategic Accounts | Palo Alto Networks

Der Modern Malware Review repräsentiert eine 3-monatige Analyse von 1000 realen Enterprise Endkunden Netzwerken, wo mit Hilfe von WildFire™ (Palo Alto Networks™ Feature zur Detektion & Abwehr von neuer & unbekannter Malware) das Verhalten von 26000 (!) Malware Samples nicht nur am "Infected Host", sondern auch eine vollständige Level-Analyse des infizierten Verkehrs, sowie den gesamten Verkehr, der von der Malware generiert wurde, detektiert und abgewehrt wird.

09:20
Privileged Identity Management

JOCHEN KÖHLER | Regional Director DACH & Middle East | Cyber-Ark Software

Nach wie vor unterschätzen viele Unternehmen die Gefahren eines unzureichenden oder überhaupt nicht vorhandenen Passwort-Managements.
Die Sicherheitsrisiken sind gravierend, denn privilegierte Benutzerkonten, wie sie Administratoren besitzen, ermöglichen einen Zugriff auf alle unternehmenskritischen Datenbestände. Abhilfe bietet hier u.a. die Cyber-Ark PIM Suite.

09:40
IT Security as a Service - Sicherheit aus der Cloud

ALFRED BACH | Solution Strategist | CA Technologies

Ausgehend von der prinzipiellen Frage, ob IT-Sicherheit ausgelagert werden sollte, befasst sich der Vortrag mit aktuellen Möglichkeiten das zu tun und stellt eine Success Story vor.

10:00
Pause | Zeit für Networking

10:30
WORKSHOPS TEIL 5

Parallel für alle Arbeitskreise; Detailinformationen siehe Workshop-Übersicht

11:30
WORKSHOPS TEIL 6

Parallel für alle Arbeitskreise; Detailinformationen siehe Workshop-Übersicht

12:30
Pause | Zeit für Networking

12:50
Zusammenarbeit von Krisenstäben & Notfallkommunikation im Ernstfall

ING. JOHANNES MARIEL | Leiter der Stabsabteilung | Bundesrechenzentrum GmbH u.a.

Wie kommunizieren wir, wenn wir über die herkömmlichen Infrastrukturen nicht mehr können? Welche Szenarien müssen erwogen werden? Und welche Überlegungen, Konzepte und Denkanstöße gibt es dazu bereits?
Im Sinne eines Gedankenanstoßes werden aus dem Ideen-Pooling im vorangegangenen Themenworkshop unter der Ägide von Herrn Mariel kurz Ideen & bereits erarbeitete Konzepte aus Unternehmen & Behörden vorgestellt

13:10
Zusammenfassung der Arbeitskreise und Schlussworte

13:30
Abschließendes Mittagessen und gemütlicher Ausklang der Veranstaltung

LISTE DER TEILNEHMENDEN UNTERNEHMEN

A1 Telekom Austria AG
Allgemeines Krankenhaus der Stadt Wien - Medizinischer Universitätscampus
Amt der Burgenländischen Landesregierung
Amt der Niederösterreichischen Landesregierung
Amt der Oberösterreichischen Landesregierung
Antares-NetlogiX Netzwerkberatung GmbH
Aon Jauch & Hübener Gesellschaft m.b.H.
AUSTRO CONTROL Österreichische Gesellschaft für Zivilluftfahrt mit beschränkter Haftung
AUVA Allgemeine Unfallversicherungsanstalt
AVL List GmbH
Bacher Systems EDV GmbH
BMW Motoren GmbH
Bundesministerium für Finanzen
Bundesministerium für Gesundheit
Bundesministerium für Landesverteidigung und Sport
Bundesministerium für Unterricht, Kunst und Kultur
Bundesrechenzentrum GmbH
CA Technologies
CERT.at
certex Information Technology GmbH
CSC Computer Sciences Consulting Austria GmbH
Cyber Security Austria
Cyber-Ark Software Inc.
Deloitte Österreich GmbH
DenizBank AG
EMC Computer Systems Austria GmbH / RSA The Security Division of EMC
Energie AG Oberösterreich Data GmbH
Erzdiözese Wien
Fachhochschule Technikum Wien
FRITZ EGGER GmbH & Co. OG
GOVCERT.NL
Grazer Wechselseitige Versicherung AG
Haas Food Equipment GmbH
Hagenberger Kreis
ING-DiBa Direktbank Austria
IT-Services der Sozialversicherung GmbH
KPMG Advisory AG
Land-, forst- und wasserwirtschaftliches Rechenzentrum GmbH
Magistrat der Stadt Wien - MA 14 IKT für die Stadt
Magistratsdirektion der Stadt Wien - Geschäftsbereich Organisation und Sicherheit
Magistratsdirektion der Stadt Wien - GB Personal & Revision, Gruppe Interne Revision
nic.at GmbH
NÖM AG
Novartis Pharma GmbH
ÖBB Holding AG
Oesterreichische Kontrollbank AG
OMV Aktiengesellschaft
OÖGKK - Oberösterreichische Gebietskrankenkasse
Österreichische Computer Gesellschaft OCG & ECDL

Österreichische Lotterien GmbH
Österreichische Post AG
Österreichische Staatsdruckerei GmbH
Palo Alto Networks
Porsche Informatik Gesellschaft m.b.H.
Raiffeisen Bank International AG
s IT Solutions AT Spardat GmbH
SafeNet Germany GmbH
SBA Research g GmbH
Schönherr Rechtsanwälte GmbH
SEC Consult Unternehmensberatungs GmbH
Security Research Sicherheitsforschung GmbH
Sozialversicherungs-Chipkarten Betriebs- und Errichtungsgesellschaft m.b.H. - SVC
Stryker GmbH
SVD Büromanagement GmbH
Symantec Austria GmbH
Team Cymru, Inc.
Treibacher Industrie AG
UBIS UniCredit Business Integrated Solutions Austria GmbH
Unicredit Bank Austria AG
UNIQA Versicherungen AG
Universität Innsbruck Institut für Finanzwissenschaft
Verbund AG
Verfassungsgerichtshof Österreich
voestalpine Edelstahl GmbH
voestalpine group-IT GmbH
Vorarlberger Illwerke AG
Websense Deutschland GmbH
WIENER STÄDTISCHE Versicherung AG Vienna Insurance Group
Wiener Stadtwerke Holding AG
XSEC infosec GmbH
8Man - protected-networks.com GmbH

Wir freuen uns
auf ein Wiedersehen am

SECURITY & RISK-MANAGEMENT KONGRESS 2014!

LSZ Consulting
Loisel.Spiel.Zach Ges.m.b.H
Gußhausstraße 14/9
1040 Wien
+43 1 5050 900

Mag. Stefan Reischl
Projektleitung

+43 1 50 50 900 - 76
stefan.reischl@lsz-consulting.at

LSZ Consulting
THE WAY TO NETWORK
since 1988