T.I.S.P. Community Meeting 2016

Kurzbeschreibungen der Vorträge und Workshops

Donnerstag 10.11.2016

Keynote: "10 Fakten über IT Security" Detlef Hauke, Footfalls Mit Aussagen wie "Die Cloud nutzen wir nicht", "BYOD gibt es bei uns nicht", "IoT ist für uns kein Thema", "Sicherheit kostet doch nur Geld" sind wir alle immer wieder konfrontiert und allzu oft nehmen wir diese aus falsch verstandener Rücksicht hin. Dabei sind es solche oder ähnliche Aussagen, die oft Wegbereiter für eine grundsätzliche Haltung sind, welche einem ganzheitlichen Sicherheitsansatz entgegenwirkt. Im Rahmen dieses Vortrags wird an zehn exemplarischen Aussagen (mit Beispielen aus dem Alltag) dargestellt, das auch evtl. kleine Fehleinschätzungen bzw. kleines Fehlverhalten mittel- und langfristig negative Folgen für das Sicherheitsniveau eines Unternehmens haben können. Die Teilnehmer sollen dafür sensibilisiert werden, auf Aussagen wie die o.a. angemessen zu reagieren und Kollegen/Kunden auf offensichtliche Fehler hinzuweisen.	
"Aussagekraft von Penetration Tests" Patrick Sauer, binsec "Sind Ihre IT-Systeme sicher?" ist eine typische Werbefloskel, um Penetrationstests zu vermarkten. Aber erhält man durch einen Penetrationstest wirklich eine Antwort auf diese Frage? Welche Aussagekraft haben Penetrationstests überhaupt? Dieser Vortrag soll darüber aufklären, welche Aussagekraft und Grenzen Penetrationstests besitzen und unter welchen Gesichtspunkten sie dennoch ein wichtiger Bestandteil einer Sicherheitsstrategie sein können.	
"Sicherer Zugang zu Intranet-Applikationen für Geschäftspartner" Reinhold Leitner, Primetals Technologies Austria Das Ziel ist, sichere Zugänge aus dem Internet zu schaffen und Hackern keine Chance zu geben. Bei diesem Vortrag werden folgende Punkte beleuchtet: - Netzinfrastruktur (Firewalls, DMZ) - Two-Factor Authentifizierung (PKI, One-Time Passwort etc.) - Proxies, Application Gateways - Beispiel für eine Remote Service Platform	

Donnerstag 10.11.2016

Einstieg ins T.I.S.P.-Café

Die Teilnehmer

a) Sie als Themengeber liefern den Anlass für ein Gespräch. Sie kennen sich im Thema gut aus.
   Sie stellen ein Thema aus Ihrer Praxis kurz vor (max 3 min).
   Ihre Fragestellung ist: Wer möchte mit mir über das Thema diskutieren oder sich austauschen?

b) Nach der Themenvorstellung ist Raum und Zeit, so dass sich die Gesprächsgruppen austauschen können.
   Sie achten darauf, dass Ihre Gruppe auch von Interessenten gefunden werden kann.
   Sie liefern notwendigen inhaltlichen Input.

c) Ein Feedback im Plenum schließt das T.I.S.P. -Café ab.
   Die Teilnehmer berichten kurz über das Diskussionsergebnis.

Freitag 11.11.2016

"State-of-the-Art-Sicherheitsmaßnahmen bei Verschlüsselung und Authentifizierung zur Risikobewertung"

Dennis Scherrer, BLUESITE

Geheimdienste, die bei Herstellern Unterstützung bei der Entschlüsselung von Smartphones anfordern, immer mehr Online-Dienste die Telefonnummern für 2-Faktor-Anmeldungen einsammeln und Gesichtserkennung für die Anmeldung am Arbeitsgerät sind aktuelle Trends. In diesem Vortrag wird eine Zusammenstellung der Verschlüsselungsverfahren, Schlüssellängen und Software-Implementierungen nach Stand der Technik mit Quellnachweisen und Informationen zu Verbreitung und zuverlässigerer Authentifizierungsverfahren (als Eingabe für die Aktualisierung der Risikobetrachtung im Konzern) gegeben.

"Die DIN 66398 – ein Löschkonzept auch für die Informationssicherheit"

Dr. Volker Hammer, Secorvo Security Consulting

Löschen und Vernichten sensibler Daten ist eine Aufgabe im Bereich Informationssicherheit. Das Löschen personenbezogener Daten wird auch vom BDSG gefordert. In der Praxis gibt es allerdings große Umsetzungsdefizite. Das hat zwei Ursachen: Die Löschregeln sind nicht definiert und es fehlen Löschmechanismen in Anwendungen. Mit der neuen DIN 66398 liegt eine "Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten" vor. Sie bietet umfangreiche Hilfestellungen, um ein Löschkonzept zu erstellen und im Unternehmen zu etablieren. Der Beitrag motiviert, Löschen als eine übliche Anforderung zu verstehen, die in Regelprozessen berücksichtigt werden muss. Er gibt einen Überblick über die Inhalte der Norm und zeigt die Bezüge zur Informationssicherheit auf. Kern der Norm ist eine Vorgehensweise, um **Löschregeln** zu definieren. Mit Hilfe von Standardfristen und Typen von Startzeitpunkten werden Löschklassen gebildet. Abgegrenzte Arten (personenbezogener) Daten können dann leicht

in die Löschklassen eingeordnet werden. Daraus ergeben sich Löschregeln mit je einem Startzeitpunkt und einer Regellöschfrist.

Bezüge zur Informationssicherheit:

- Die Vorgehensweise kann auch für nicht-personenbezogene Daten angewandt werden. Damit hat sie viel Potential für Löschregeln weiterer sensitiver Bestände, die in ein gemeinsames Löschkonzept eingebettet werden können.
- Durch ein gelebtes Löschkonzept werden zu schützende Datenbestände der Organisation transparenter.
- Überflüssige Angriffsziele können reduziert werden.
- Die Norm trifft keine direkten Vorgaben zur Sicherheit von Löschmechanismen. Eine Informationsklassifikation in einer Organisation könnte diese Vorgaben besteuern.
- Datenschutz und Informationssicherheit überprüfen Vorgaben durch Audits. Durch die Vorschläge der Norm für die Dokumentation des Löschkonzepts und der konkreten Löschprozesse werden dafür gute Voraussetzungen geschaffen.

Nutzen ergibt sich aus Löschkonzepten auch neben den Gewinnen für Datenschutz und Informationssicherheit, weil

- Geschäftsprozesse präzisiert werden,
- Systeme und IT-Prozesse entkoppelt werden,
- Vorgaben für die Datenhaltung getroffen werden,
- überflüssige Daten aufgeräumt und Redundanzen abgebaut werden. Dadurch sinken Kosten für den IT-Betrieb und für Migrationen.

Dieser erweiterte Nutzen kann Organisationen zusätzlich motivieren, ein Löschkonzept zu erstellen und umzusetzen.

"Knapp vorbei ist auch daneben – wo wir bei Risiken und Incidents seit Jahren unbemerkt am Ziel vorbeischießen"

Sebastian Klipper, CycleSEC

Das Management von Risiken und Incidents soll uns einerseits vor unerwarteten Überraschungen bewahren und andererseits unsere geregelten Abläufe sicherstellen, wenn es doch zum äußersten kommt. Seit Jahren beschleicht den Referenten das unschöne Gefühl, dass dabei nicht alles mit richtigen Dingen zugeht und in gängigen Implementierungen unbemerkte Fehlerquellen schlummern. Mit der Risiko-Isoquanten-Analyse (RIA) wird ein Weg vorgestellt, um einer dieser Fehlerquellen bei der Risikopriorisierung auf die Schliche zu kommen. Der Vortrag stellt insgesamt fünf gängige Fehler im Risikomanagement vor. Anhand von konkreten Beispielen wird darüber hinaus gezeigt, welche Incidents in den letzten Jahren zwar für mediales Aufsehen gesorgt haben, jedoch in kaum einem Unternehmen als Incident behandelt wurden.

"VdS 3473 – Informationssicherheit für KMU"

Michael Wiesner, Michael Wiesner GmbH

Seit Juli 2015 mischt ein neuer Standard den Markt für Informationssicherheit in kleinen und mittleren Unternehmen auf. Wo die Umsetzung von ISO 27001 und BSI IT-Grundschutz viel zu aufwändig ist und gleichsam der größte Nachholbedarf besteht, möchten die VdS-Richtlinien 3473 – Cyber-Security für KMU – eine umsetzbare Alternative sein. Dieser Vortrag gibt eine Einführung in die Richtlinien, zeigt Unterschiede zu den etablierten Standards und gibt einen Einblick in die Erfahrungen aus über einem Jahr VdS 3473.

"Praxisleitfaden für die Implementierung eines ISMS nach ISO/IEC 27001:2013"

Nico Müller, BridgingIT

Im Rahmen der ISACA-Fachgruppe Informationssicherheit wurde von den dort vertretenen Experten ein circa neunzig Seiten starker "Praxisleitfaden für die Implementierung eines ISMS nach ISO/IEC 27001:2013" erarbeitet mit vielen Praxistipps und Erklärungen zu oft diskutierten "Normauslegungen". Der Leitfaden bietet allen, die mit dem Aufbau und/oder Betrieb eines ISMS betraut sind, pragmatische Hilfestellungen und Herangehensweisen. Die Vorteile eines individuell angepassten und, sofern notwendig, gleichzeitig normkonformen ISMS werden klar herausgestellt. Insbesondere werden Praxisempfehlungen zur Etablierung bzw. Erhöhung des Reifegrads bestehender ISMS-Prozesse und typische Umsetzungsbeispiele verschiedener Anforderungen aufgezeigt.
Der Implementierungsleitfaden ist auf den Internetseiten der ISACA verfügbar:
https://isaca.de/sites/pf7360fd2c1.dev.team-wd.de/files/attachements/isaca_leitfaden_i_gesamt_web.pdf

"Humboldt vs. Franklin: Können wir uns Datenschutz noch leisten?"

Christoph Schäfer, Secorvo Security Consulting

Geht es um den Vorrang von Sicherheit vor Datenschutz wird gern der preußische Staatsmann Wilhelm von Humboldt zitiert: "Ohne Sicherheit ist keine Freiheit." Datenschützer kontern mit Benjamin Franklins Aussage: "Wer Freiheit für Sicherheit aufgibt, wird beides verlieren." Wer hat Recht? Wie passen über 200 Jahre alte Aussagen in die heutige Zeit? Wie viel Datenschutz können (und wollen) wir uns vor dem Hintergrund der Terrorbedrohung vor unserer Haustür noch leisten? Im Tagesschau-Interview vom 22.03.2016 wurde Bundesinnenminister Thomas de Maizière bezüglich der Brüsseler Anschläge deutlich: "Datenschutz ist schön, aber in Krisenzeiten (…) hat Sicherheit Vorrang". Doch was bedeuten solche Aussagen für unsere freiheitlich-demokratische Grundordnung? Der Vortrag springt von den historischen Aussagen Humboldts und Franklins in die Gegenwart und stellt das Spannungsverhältnis zwischen dem Grundrecht auf Datenschutz und den Forderungen von Sicherheitsbehörden, dieses Grundrecht den von ihnen definierten Sicherheitsanforderungen unterzuordnen, dar. Als Ergebnis soll die titelgebende Frage beantwortet werden: Können wir uns Datenschutz noch leisten?