T.I.S.P. Community Meeting 2015

Kurzbeschreibungen der Vorträge und Workshops

Montag 02.11.2015

Ei des Kolumbus - oder Kuckucksei? Microsoft Office 365 und Datenschutz

Christoph Schäfer, Secorvo Security Consulting GmbH

IT-Outsourcing in "die Cloud" liegt im Trend. Die Anbieter locken mit skalierbaren und anpassungsfähigen Anwendungen und Infrastrukturen. Hard- und Software befinden sich ganz oder teilweise in den Rechenzentren des Anbieters. Auch kurzfristige Anpassungen an den tatsächlichen Bedarf sind oft viel schneller möglich als beim klassischen Outsourcing. Höhere Flexibilität bei geringeren Kosten ist die gewünschte Folge. Eine solche Lösung ist auch Microsoft Office 365, bei dem die Anwendung aus der Microsoft-Cloud bezogen und Dokumente und E-Mails in Microsoft-Rechenzentren gespeichert werden. Doch wie verträgt sich das mit dem Datenschutz? Bereits für die Auftragsdatenverarbeitung durch deutsche Dienstleister bestehen strenge gesetzliche Anforderungen. Microsoft hat den Datenschutz schon früh als Nadelöhr erkannt und den Austausch mit den europäischen Datenschutz-Aufsichtsbehörden gesucht. Der Vortrag "Ei des Kolumbus - oder Kuckucksei? Microsoft Office 365 und Datenschutz" gibt den aktuellen Stand der Diskussion und der Verhandlungen zwischen Microsoft, Datenschutzexperten und ausgewählten deutschen Unternehmen wieder, die zurzeit die Einführung von Office 365 erwägen.

Index der Gefährdungslage (Parallelvortrag)

Holger Himmel, Tengelmann Warenhandelsgesellschaft KG

Dashboards sind ein beliebtes Werkzeug, um mithilfe einer überschaubaren Anzahl von Key Performance Indicators (KPIs) und Indizes einen schnellen Überblick über die Lage des Unternehmens zu gewinnen. Wird der Verantwortliche für Informationssicherheit im Unternehmen nach seinem Beitrag für ein solches Dashboard gefragt, gilt es, das Geflecht der in der IT vorhandenen Metriken mit Bezug zur Informationssicherheit zu entwirren und eine Methode zu entwickeln, die diese Metriken zusammenführt. Der Vortrag beschreibt ein Modell zur Konsolidierung von Metriken der Verwundbarkeit und Bedrohungslage hin zu einem Index der Gefährdungslage.

Security @ Industry - Sicherheit in kritischen Infrastrukturen (Parallelvortrag)

inkl. Live Hacking

Thomas Haase, T-Sytems Multimedia Solutions GmbH

In kritischen Infrastrukturen (Energie, Wasser oder Verkehrsleitsysteme) werden durch die Industrie verschiedene Kontroll- und Steuerungssysteme eingesetzt (SCADA/ICS), um solche Szenarien zu verhindern. Die bisherige Absicherung solcher Systeme bestand hauptsächlich in der Abschottung und Trennung von anderen Netzwerken. Die aktuelle Entwicklung zeigt, dass diese Kontrollsysteme vermehrt in die Unternehmensnetzwerke integriert werden. Innerhalb des Vortrages wird verdeutlicht, warum dies aktuell keine gute Idee ist.

- Übersicht welche Security - Probleme entstehen durch die industrielle Automatisierung
- Demonstration aktueller Sicherheitsprobleme und Einschätzung der Bedrohungslage gesamt
- technische Möglichkeiten sich zu schützen

SAP Hacking

Christian Thiemann, Atos IT Solutions and Services GmbH

Anbei ein Fachartikel, der vor einiger Zeit im Magazin IT-Grundschutz erschienen ist. Ich werde das zweite Beispiel aus dem Artikel (Angriff auf eine SAP Instanz) erläutern und anhand einer virtuellen Maschine auf meinem Laptop auch live demonstrieren. Der Zuhörer soll mitnehmen, dass die abstrakten Gefahren aus den SAP-Empfehlungen ganz real existieren. Mit einem Stück C-Code aus der Präsentation wird der Zuhörer die Verwundbarkeit in der eigenen Firma testen (nicht ausnutzen!) können, d.h. dem fachkundigen Publikum werden technische Details gegeben.

Industrie 4.0 - Höchste Zeit für Risikomanagement? (Parallelvortrag)

Christian Dirnberger

Inhaltlich gehe ich zunächst kurz auf die Rahmenparameter und Spezifika von Industrie 4.0 ein. Im Anschluss wird folgende Fragen thematisiert: Kann man mit der zunehmenden Vernetzung unter dem Bussword Industrie 4.0 auf ein Risikomanagement verzichten? Welche Risiken bringt ein Verzicht mit sich? Zum Abschluss stelle ich ein einfaches und schnelles Verfahren zur Bewertung von Risiken vor.

Funktioniert "Secure Software Engineering"? (Parallelvortrag)

Andreas Poller, FhG-SIT

Der Vortrag soll einen Überblick über den Stand der Wissenschaft zur empirischen Forschung der Entwicklung sicherer Software geben. Anhand aktueller Beispiele aus der Forschung am Fraunhofer SIT wird erläutert, wie eine solche empirische Forschung ablaufen kann und welchen Mehrwert teilnehmende Entwicklungsteams daraus ziehen können. Gleichzeitig soll ein Bewusstsein dafür geschaffen werden, dass die IT-Sicherheitsforschung beim Transfer von der Theorie in die Praktiken von Softwareentwicklern viele tote Winkel hat, die wir als Forscher in der Zusammenarbeit mit Praktikern ausleuchten müssen.

Fragestellung/Aussagen: Der Vortrag möchte ein Bewusstsein bei den Zuhörern dafür zu schaffen, dass wir wenig über effektive Einbindung von Verfahren für die Entwicklung sicherer Software in Entwicklungspraktiken wissen. Aus den Ergebnissen der bisherigen Forschung am Fraunhofer SIT werden Hinweise zum praktischen Einsatz von Bedrohungsmodellierungsverfahren und Penetrationstests gegeben. Das Publikum soll angeregt werden, über die "blinden Flecken" aus der eigenen Entwicklungspraxis (Software, IT-Systeme, IT-Lösungen) zu diskutieren.

"(Un-) Sicherheit zum Anfassen - Wer sich vor Hackern schützen will, muss ihre Vorgehensweisen kennen." inkl. Live Hacking (Parallelvortrag)

Thomas Haase, T-Sytems Multimedia Solutions GmbH

Haben Sie das Buch "Blackout" oder die aktuellen Berichte über Angriffe auf kritische Infrastrukturen gelesen? Wollten Sie schon immer mal wissen, wie Hacker unsichere Webanwendungen ausnutzen um: Webseiten zu verunstalten, Kundendaten zu stehlen, Überweisungen im Onlinebanking zu manipulieren, Preise manipulieren und kostenlos einkaufen? Statt sich den x-ten Vortrag von sogenannten "Experten" über mögliche Angriffe und Bedrohungen anzuhören, können Sie sich anhand realer Szenarien, die Ihnen als Live-Hackings präsentiert werden, informieren. In diesem Vortrag lernen Sie aktuelle Angriffstechniken, Vorgehensweisen und die entsprechenden Schutzmaßnahmen kennen.

CERT-Management - ein kleines How-To (Parallelvortrag)

Detlef Hauke, Footfalls Ltd.

Keine Software ist fehlerlos und nicht jeder Fehler ist sofort kritisch. Aber kritische Sicherheitslücken müssen schnell und zielgerichtet behandelt werden. Der Vortrag behandelt die Informationsbeschaffung, den zielgerichteten Umgang mit Sicherheitsmeldungen und mögliche Quellen.

Ziel ist es, einen Einblick in den Umgang mit CERT-Meldungen zu geben. Es wird auf "Über-" bzw. "Unterversorgung" eingegangen und der Umgang mit CERT-Meldungen unter Grundschutzgesichtspunkten wird betrachtet. Außerdem wird ein zielgruppengerechter Umgang mit CERT-Meldungen thematisiert."

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.

Dienstag 03.11.2015

Workshop 1 Wie vermeide ich Stolpersteine bei Fremdvergabe von Produktentwicklung und Dienstleistungen

Dr. Irene Förster,

Zielsetzung: Reduktion von Projektverzögerungen und Mehrkosten bei der Fremdvergabe

IT-Sicherheitsanforderungen nicht erfüllt??? In unserer zunehmend vernetzten Weltsind die Informationswerte einer zunehmenden Zahl von Bedrohungen ausgesetzt. Die Integration von Schutzmaßnahmen in Produkte, Netze und Dienstleistungen gehört zu den strategischen Zielen in der Corporate Security. Bei Fremdvergabe von Produktentwicklung und Dienstleistung übernehmen der Einkauf und die Rechtsabteilung die Ausschreibungen und verhandeln die Verträge nach erprobten Spielregeln.

Es wird kurz gezeigt, welche Sicherheitsanforderungen ·bereits bei der Auswahl der Fremdfirmen/·bei Ausschreibungen abgefragt beziehungsweise berücksichtigt werden sollten/·und in den Verträgen zu verankern sind. Neben den eingespielten Teams aus Einkauf, Rechtsabteilung unter Einbezug der Technik und des Services tritt jetzt die Sicherheitsabteilung als weiteren Mitspieler bei Ausschreibungen und Verhandlungen auf. Die Sicherheitsanforderungen können zur Einschränkung des Bieterkreises führen. Es lassen sich nur dieAspekte der Informationssicherheit durchsetzen, deren Kosten/Nutzen ein ausgewogenes Verhältnis zu den Risiken der Geschäftsanforderungen haben.

Workshop 2 Informationssicherheit als Marke

Detlef Hauke, Footfalls Ltd.

Im Rahmen des TISP CM 2014 war das Thema "Was braucht es, damit wir gewinnend über Informationssicherheit sprechen können?" aufgeworfen worden, konnte aber leider nicht im Rahmen eines Workshops vertiefend bearbeitet werden. Aufgrund des großen Interesses will der Workshop "Informationssicherheit als Marke" an dieser Stelle ansetzen. Informationssicherheit als Marke (alias Produkt) zu platzieren ist ein möglicher Ansatz um das Thema Sicherheit positiv zu transportieren.

Zielsetzung: Den Workshop-Teilnehmern werden verschiedene Lösungsansätze aufgezeigt und anschließend diskutiert. Dabei ist es das Ziel, auf die unterschiedlichen Rahmenbedingungen und Persönlichkeiten einzugehen. Den Teilnehmern wird ein Lösungsangebot vorgestellt, aus dem sie den für sie passendsten Ansatz wählen können. Hierbei werden mögliche Parallel zum Marken (Produkt) Marketing aufgezeigt.

Workshop 3 Smartphone, Smartwatch und smarte Apps aus der Sicht des Risikomanagements

Sebastian Klipper, Ps(i)² - Sicherheit in Informationssystemen

Risikomanagement in kleinen wie großen Unternehmen ist kein Thema mit dem man viel Begeisterung auslösen kann. Während man als Security Professional das Thema Risikomanagement zu den Mitarbeitern tragen muss, tragen die Mitarbeiter Smartphone, Smartwatch und unzählige smarten Apps direkt ins Unternehmen. In diesem Workshop erarbeiten wir welche Risiken die Mitarbeiter mit dabei haben und welche Chancen in einem zu starren Risikomanagement untergehen könnten.

Workshop 4 Patchmanagement

Stephan Sachweh, Pallas GmbH

- Umgang mit Patchmanagement von Betriebssstem eigener Software und Third Party Software?
- Normale Patch Zyklen für - Deskops, - Server, - HA Server
- Umgang mit Patch Desastern wie - Heartbleed, - Shellshock

Abschlussvortrag

Einsparungen und Informationssicherheit - ein Widerspruch?

Axel Leitner, Aritron

Im Umfeld von IS-Management und IT Infrastruktur werden die teils divergierenden Interessen von Projekt und Betrieb im Spannungsfeld von Budget, Compliance, Bedrohungen, Herstellerinteressen und Betriebsrat betrachtet. Mit seiner unternehmerischen Sichtweise wird der Referent die Interessen und Spannungsfelder kurz skizzieren und thematisieren. Bezug genommen wird dabei unter anderem auf pragmatische Methoden ein IS Projekt zu gestalten, betriebliche Folgekosten zu vermeiden und einen effektiven Schutz vor aktuellen Gefährdungen zu erzielen. An Hand ausgewählter Beispiele gestützt durch Studienergebnissen wird aufgezeigt, wo gespart werden kann und wo man dies vermeiden sollte.