ISSS NewsFlash

Dezember 2012

Editorial

Liebe ISSS-Mitglieder

Das Jahr neigt sich dem Ende zu: Zeit, kurz inne zu halten und aufs aktuelle Jahr zurückzuschauen.
Die Information Security Society Switzerland (ISSS) ist innert drei Jahren von 575 (November 2009) auf 1064 (November 2012) Mitglieder um 85% gewachsen.

Die Vernetzung von Security Professionals und Security Interessierten wird immer wichtiger, da aufgrund der vielfältigen Sicherheitsanforderungen bei den je länger je stärker vernetzten und auch mobil verfügbaren unternehmenskritischen Informationen eine Einzelperson oder eine einzelne Firma kaum mehr alleine in allen relevanten Bereichen der Informationssicherheit über das notwendige Wissen verfügen kann. Deshalb werden wir Ihnen auch im neuen Jahr viele und interessante Möglichkeiten zur Vernetzung und zum Wissenstransfer bieten.

Ich wünsche Ihnen frohe Weihnachten, erholsame Festtage und ein in allen Belangen erfolgreiches und sicheres 2013.

Dr. Ursula Widmer
Präsidentin ISSS
president@isss.ch

Highlights in dieser Ausgabe

ISSS: News

Ausbilck auf die ISSS Security Talks im 2013

Auch im 2013 plant die ISSS die Durchführung von 10-12 Security Talks. Die meisten davon werden wir weiterhin in der Form von Security Lunches anbieten, weil sich das Format, bestehend aus einer Kombination von Mittagessen, spannendem Fachreferat zu einem aktuellen Thema der Informationssicherheit und anschliessender Diskussion, gemäss unseren Mitgliedern und Teilnehmern bestens bewährt hat. Die Anlässe finden grundsätzlich von 12 - 14 Uhr an zentralen Orten in Zürich oder Bern statt.

Der erste Security Lunch ist bereits definitiv und findet als Doppelanlass am 23. Januar in Bern und am Folgetag in Zürich statt. Thematisch wird es um die sichere Unternehmenskommunikation gehen und in diesem Zusammenhang insbesondere um die Fragestellung, wie die Nutzung privater Geräte (Stichwort BYOD) damit in Einklang gebracht werden kann - wobei sowohl die technischen als auch die rechtlichen Fragestellungen diskutiert werden. Weitere Details finden Sie gleich nachfolgend in diesem Newsflash und auf der ISSS Website, wo Sie sich für diese beiden Anlässe anmelden können.

Weitere Security Talks befinden sich in der Planungsphase. Themen, die wir 2013 gerne abdecken möchten, beinhalten u.A. die Sicherheit industrieller Leitsysteme, Aspekte der Cloud Security (auch unter Berücksichtigung des sich in Gründung befindlichen Chapter Switzerland der Cloud Security Alliance) oder auch Fragen rund um E-Health Security, wo sich durch das elektronische Patientendossier als Teil der eHealth Strategie Schweiz im 2013 sicher auch einiges bewegen wird. Neu planen wir auch einen Anlass, der sich speziell an Studierende richtet, da wir es als wichtig betrachten, dass der Kontakt von zukünftigen Security-Professionals mit der ISSS bereits während des Studiums stattfindet. Da die Studierenden tagsüber durch den Unterrichtsbetrieb meist stark ausgelastet sind, werden wir diesen Anlass am Abend, voraussichtlich von 18 - 20 Uhr durchführen, voraussichtlich im April.

Wir sind immer auch an konkreten Vorschlägen zu Security Talks interessiert. Wenn Sie also einen Vorschlag für ein Thema haben, das aus Ihrer Sicht im Rahmen eines Security Talks behandelt werden sollte oder wenn Sie sogar selbst Interesse haben, ein spannendes Referat im Rahmen eines Security Talks zu halten, dann zögern Sie nicht, mich per E-Mail zu kontaktieren.

Neue Security Talks werden laufend auf unserer Website www.isss.ch aufgeschaltet - es lohnt sich also bestimmt, wenn Sie regelmässig reinschauen. Wir würden uns freuen, Sie am einen oder anderen Security Talk im Jahr 2013 begrüssen zu dürfen.

Prof. Dr. Marc Rennhard, Vorstand ISSS
marc.rennhard@isss.ch

Elektronische Signatur: Stand Revision ZertES zur Förderung des elektronischen Geschäftsverkehrs

Die ISSS hat sich am Vernehmlassungsverfahren zur Revision des Bundesgesetzes über die elektronische Signatur (ZertES) beteiligt und hierzu eine SIG zur Erarbeitung einer Stellungnahme gebildet, welche im Juli 2012 eingereicht wurde. Gestützt auf die positiven Reaktionen, auf welche die geplante Gesetzesrevision im Rahmen der Vernehmlassung gestossen ist, hat der Bundesrat nun dem Eidgenössischen Justiz- und Polizeidepartement (EJPD) den Auftrag erteilt, bis Ende 2013 die Botschaft für eine entsprechende Änderung des ZertES auszuarbeiten. Ziel der Revision ist es, den elektronischen Geschäftsverkehr zu fördern, indem die Anwendung der elektronischen Signatur für juristische Personen und Behörden vereinfacht wird.

Vorschau: ISSS Security Lunches vom Januar 2013

Sichere Unternehmensmobilität – technische Machbarkeit und rechtliche Absicherung

23. Januar 2013, 12.00-14.00, Restaurant Schmiedstube, Bern
24. Januar 2013, 12.00-14.00, Zunfthaus zur Meisen, Zürich

Zielpublikum
Sichere Unternehmensmobilität im Hinblick auf den massiv zunehmenden Einsatz privater Geräte wie Smartphones, Tablets und Laptops und der Nutzung von Cloud Diensten für geschäftliche Zwecke steht heute ganz oben auf der Traktandenliste der Verantwortlichen in Unternehmen und Verwaltungen. Angesprochen sind hier die Entscheidträger für die sichere und rechtskonforme Nutzung solcher Geräte (CEOs, CIOs, CSOs, COOs, Personalverantwortliche, Rechtsabteilungen), aber auch die Anbieter entsprechender Lösungen.

Frau Dr. Ursula Widmer spricht zum Thema:
BYOD – Unternehmensmobilität rechtlich erfolgreich abgesichert?

Beim Einsatz von privaten Geräten (Smartphones, Tablets, Laptops) durch Mitarbeitende von unterwegs oder von zuhause aus, z.B. für den Remote-Zugriff auf Applikationen und Daten (E-Mails, Dokumente, Bilder) des Unternehmens oder für die Nutzung von Cloud Services für geschäftliche Zwecke, sind Massnahmen zum Schutz sowohl der Interessen der Mitarbeitenden wie derjenigen des Unternehmens rechtlich zwingend. Private und geschäftliche Daten und Anwendungen sollten getrennt werden können, als Voraussetzung für die notwendigen Schutzmechanismen und Kontrollen, zu denen der Arbeitgeber aufgrund rechtlicher Vorgaben (Daten- und Informationsschutz sowie sektorspezifische Compliance) verpflichtet ist, und zwar ohne dass dabei in die Privatsphäre der Mitarbeitenden eingegriffen und dadurch deren Persönlichkeit verletzt wird. Sie erfahren, welche klaren Regeln für die Nutzung privater Geräte und Applikationen Dritter (Cloud Services) zu beruflichen Zwecken in Policies festzulegen sind, etwa betreffend Speicherung und Löschung geschäftlicher Daten, der Nutzung und dem Download von Apps sowie dem Verhalten bei Verlust eines privaten Gerätes.

Herr Oliver Rükgauer spricht zum Thema**:**
Sichere Unternehmensmobilität mit Mobile Application Management

Die Nutzung privater Smartphones und Tablets in Unternehmen ist unaufhaltsam auf dem Vormarsch und stellt die IT-Abteilungen vor neue Herausforderungen beim standort- und geräteunabhängigen Zugriff auf Unternehmensdaten. Voraussetzung für eine sichere und rechtskonforme Umsetzung von Bring Your Own Device (BYOD) Programmen ist die vollständige Trennung von geschäftlichen und privaten Daten und Applikationen auf den Mobilgeräten. Die Unternehmen können sich dabei auf den Schutz ihrer Daten und Applikationen beschränken, wobei die Privatsphäre der Mitarbeitenden gewahrt, gleichzeitig das Haftungsrisiko verringert und der Verwaltungsaufwand minimiert wird.
Für die Mitarbeitenden bietet der Ansatz des Mobile Application Management den Vorteil, dass die Benutzbarkeit und Funktionalität der privaten Mobilgeräte nicht eingeschränkt wird, wie dies beim herkömmlichen Mobile Device Management heute häufig der Fall ist.
Es wird anhand eines Praxisbeispiels aufzeigt, wie BYOD-Nutzungsrichtlinien über ein App Center (als Cloud Service) zur Sicherung von iOS und Android Apps und zum Schutz von Unternehmensdaten aktiv durchgesetzt werden können.

Anmeldung für Bern: www.isss.ch/veranstaltungen/2013/security-lunch-2013-01-23/
Anmeldung für Zürich: www.isss.ch/veranstaltungen/2013/security-lunch-2013-01-24/

Rückblick: 15. Berner Tagung für Informationssicherheit

Die **15. Berner Tagung für Informationssicherheit** mit dem Thema **„Bring your own device“** ist bereits Geschichte. Die ISSS und das ISB durften auch dieses Jahr wieder über 300 Personen im Kursaal zur Tagung willkommen heissen. An dieser Stelle möchte ich als OK-Lead allen Teilnehmenden ganz herzlich für ihren Besuch und ihre Unterstützung danken.

Die guten Referate und der eloquente Moderator Kurt Aeschbacher trugen das ihre zu einer erfolgreichen Veranstaltung bei. Der Fokus der diesjährigen Referate konnte sehr gut aufzeigen, wo die grossen Herausforderungen liegen. Einerseits bei der vielfältigen Zahl von Arbeitsgeräten für den Zugriff auf interne Ressourcen. Andererseits ist der Trend, jederzeit und überall Unternehmensdaten verfügbar zu haben, nicht mehr aufzuhalten. Es braucht aber in jedem Fall klare verbindliche Regelungen für den Einsatz der Arbeitsmittel, ob es sich nun um ein von der Firma zur Verfügung gestelltes Gerät handelt oder ein selber gekauftes.

Aus den Referaten ging auch hervor, dass die strategischen Überlegungen für vorgenannten Einsatz ein sehr zentrales Element sein müssen. Sowohl die Anforderungen der Benutzer wie auch die Möglichkeiten des Betriebes müssen genau abgeklärt sein, bevor der Entscheid zur Zulassung privat beschaffter Hardware getroffen werden kann. In diesem Zusammenhang liessen insbesondere die rechtlichen Frage- und Feststellungen von Frau Beranek Zanon bei einigen Teilnehmenden nachdenkliche Gesichter zurück.

Dass es ein Gewinn sein kann, sich mit den neuen Einsatzmöglichkeiten verschiedenster Geräte zu befassen (und sie einzusetzen) und dabei gleichzeitig auch noch die Motivation der Mitarbeitenden zu fördern, zeigen die Beispiele von SBB und Emmi.

Das zur Tradition gewordene Abschlussreferat der etwas anderen Art, Einblicke in die Arbeiten und Informationssicherheitsvorkehrungen beim CERN in Genf, konnte die Besucher der Tagung trotz der fortgeschrittenen Stunde wiederum begeistern.

Wir dürfen auf eine gelungene Tagung zurückblicken und freuen uns mit neuen Devices :-) in Zukunft arbeiten zu können.

In diesem Sinne wünsche ich allen frohe Festtage (das eine oder andere Geschenk unter dem Tannenbaum) und einen guten Start im neuen Jahr. Ich freue mich, Sie an der 16. Berner Tagung für Informationssicherheit im 2013 wieder begrüssen zu dürfen. Details dazu entnehmen Sie bitte laufend unserer Webseite www.isss.ch.

Daniel Graf, Vorstand ISSS
daniel.graf@ISB.admin.ch

Rückblick: ISSS Security Lunch vom 6.11.2012

ISSS Security Lunch vom 6.11.2012 zum Thema „Internetplatz Schweiz − wie sicher sind wir?“

Viele interessierte Zuhörer fanden sich zum gemeinsamen Mittagessen in Zürich und zum Vortrag von **Dr. Serge Droz** zum Thema „Internetplatz Schweiz − wie sicher sind wir?“ ein. Nach einer kurzen Begrüssung und Vorstellung des Referenten durch Herrn Bernhard Tellenbach, Vorstandsmitglied der ISSS, eröffnete Herr Serge Droz, Leiter der Sicherheitsabteilung bei SWITCH, sein Referat.

SWITCH ist eine Förderstiftung mit dem Zweck, die nötigen Grundlagen für den effektiven Gebrauch moderner Methoden der Informations- und Kommunikationstechnologien im Dienste der Lehre und Forschung in der Schweiz zu schaffen, zu fördern, anzubieten, sich an solchen zu beteiligen und sie zu erhalten. Die Stiftung verfolgt weder kommerzielle Zwecke noch ist sie auf die Realisierung eines Gewinnes ausgerichtet.

Herr Droz erläuterte, wieso ihm seine Arbeit bei SWITCH ermögliche, eine gute Übersicht über den Internetplatz Schweiz und dessen Sicherheit zu haben. Als Betreiber des nationalen Hochschulnetzes sowie kritischer IKT-Infrastrukturen, wie z.B. des Domain-Name Systems (DNS) für die .ch Domain, habe SWITCH bereits eine gute Grundlage für tiefe Einblicke in die Sicherheit des Internetplatzes Schweiz. Dies alleine würde aber nicht reichen, um einen umfassenden Blick auf den Internetplatz Schweiz werfen zu können. Hierfür sei zentral, dass SWITCH auch Kunden aus dem Bankensektor habe sowie enge Kooperationen (primär auf informeller Ebene) mit nationalen und vor allem internationalen Partnern pflege. Weiter betonte Herr Droz, dass insbesondere der grosse Anteil an Forschung und Entwicklung von ca. 30% zentral sei, um im Sicherheitsbereich über das jeweils notwendige Wissen und die Technik zu verfügen, um an vorderster Front mitmachen zu können.

Mit einem im September vom Magazin „Beobachter“ gemeldeten neuen Virus, der in mit fehlerhaftem Deutsch verfassten und scheinbar von der Deutschen Post stammenden E-Mails verschickt wurde, leitete Herr Droz in die Diskussion der heutigen Bedrohungslage über. Er identifizierte finanziell motivierte, gut organisierte kriminelle Organisationen als Hauptbedrohung. Während die einen die notwendigen Tools entwickeln, bieten andere auf diesen Tools basierend diverse Dienstleistungen an. Vom Datendiebstahl über Spionage bis zum klassischen Denial-of-Service (DoS) Angriff ist alles möglich. DoS-Angriffe beobachtet man heute insbesondere im Zusammenhang mit Portalen, deren Geschäftstätigkeit stark terminabhängig ist. So z.B. Portale für Sportwetten, deren kurzzeitige Nichtverfügbarkeit bei wichtigen Ereignissen, wie z.B. den Spielen der Champions League, enorme finanzielle Einbussen zur Folge haben können. Herr Droz erklärte zudem, dass das schlechte Deutsch im erwähnten Beispiel vom gefälschten E-Mail der Deutschen Post oft gezielt schlecht sei. Dadurch würden nämlich Personen, die einen Angriff oder Betrugsversuch zu einem späteren Zeitpunkt wahrscheinlich erkennen würden, bereits rausgefiltert. Vor allem unaufmerksame respektive gutgläubige Personen würden mit dieser Methode leichte Opfer der E-Mail-Betrüger.

Als nächstes diskutierte er kurz die internationale Lage in Bezug auf den Beitrag einzelner Länder an die Anzahl Command and Control (C&C) Server, die der Kontrolle von Botnetzen dienen, als auch den weltweiten SPAM. Es zeigt sich, dass bei der C&C Problematik nicht nur China und Russland eine zentrale Rolle einnehmen, sondern genauso auch westliche Staaten wie die USA oder aufstrebende Länder, wie z.B. Brasilien Hort von C&C Servern sind. Die Schweiz, erklärte Herr Droz, stehe diesbezüglich gut da − und zwar nicht nur bei SPAM und Botnetzen, wie die Ländervergleiche verschiedener Sicherheitsreports diverser Hersteller von Antivirus-Produkten aufzeigen. Herr Droz gab zwar zu bedenken, dass die absoluten Zahlen dieser einzelnen Reports aufgrund der z.T. sehr unterschiedlichen Messmethoden mit Vorsicht zu geniessen seien, der Trend spreche aber klar für eine relativ gute Platzierung der Schweiz im globalen Sicherheitsökosystem. Diese Aussage stützte Herr Droz sogleich auch durch interessante Einsichten aus eigenen Beobachtungen im Falle der Torpig-Malware, für die das SWITCH-CERT entsprechende Erkennungsstrategien entwickelt hat. Infizierte Maschinen können so schnell gefunden und umgehend an die betreffende Institution gemeldet werden. Im Zeitraum von Januar bis September 2012 bewegte sich die Anzahl der Meldungen im Bereich von 50 Meldungen pro Woche. Spitzen konnten jeweils in kurzer Zeit abgebaut werden, was primär auf die schnelle Reaktion der betreffenden Institutionen zurückzuführen sei.

Rückblick: ISSS Security Lunch vom 6.11.2012 (Fortsetzung)

ISSS Security Lunch vom 6.11.2012 zum Thema „Internetplatz Schweiz − wie sicher sind wir?“

Zum Schluss präsentierte Herr Droz ein weiteres Beispiel, das eindrücklich aufzeigte, wieso es um den Internetplatz Schweiz eigentlich ganz gut steht. Durch die Verordnung über die Adressierungselemente im Fernmeldebereich ist die Registerbetreiberin für die .ch (und .li) Domäne ermächtigt und verpflichtet, bei begründetem Missbrauchsverdacht den betreffenden Domainnamen für maximal 5 Tage zu sperren. Ein Missbrauch im Sinne der Verordnung besteht, wenn ein Domain-Name benutzt wird, um mit unrechtmässigen Methoden an schützenswerte Daten zu gelangen oder um schädliche Software zu verbreiten.

Diese Verordnung gebe der Registerbetreiberin ein wirksames Mittel in die Hand, die Betreiber von Webseiten auf entsprechende Probleme nicht nur hinzuweisen, sondern nötigenfalls auch mit einer Sperrung Nachdruck zu verleihen. Herr Droz betonte allerdings, dass obwohl die Verordnung eine Sperrung und gleichzeitige Benachrichtigung vorsehe, dies in der Praxis nicht so gehandhabt werde. Der betreffende Betreiber werde jeweils vorgängig angeschrieben und über das entdeckte Problem informiert. Erst wenn er das Problem nicht innerhalb einer Frist von 24 Stunden ab Kontakt anerkenne resp. behebe würde eine Sperrung vorgenommen. Herr Droz betonte, dass dies selten notwendig sei. Die meisten der betroffenen Webseitenbetreiber wüssten nicht, dass ihre Webseite kompromittiert wurde und seien über die Benachrichtigung sehr dankbar.

Das gute Funktionieren dieses neuen Werkzeugs bestätigten auch die Zahlen, die Herr Droz für das Jahr 2012 präsentierte. So konnte z.B. im August, als aufgrund des Bekanntwerdens einer Schwachstelle in einem weitverbreiteten Tool zur Verwaltung von Webseiten plötzlich ein starker Anstieg verseuchter Webseiten zu beobachten war, deren Zahl innerhalb kürzester Zeit wieder auf ein normales Niveau reduziert werden.

Der Referent endete mit dem Fazit, dass der Internetplatz Schweiz bezüglich Sicherheit besser dastehe als meist angenommen. Dazu trügen nicht nur wirksame (nationale) regulatorische Werkzeuge, sondern auch die guten internationalen Kontakte der Schweizer Internetanbieter entscheidend bei. Nur dank diesen guten Kontakten sei auch ein effizientes Agieren über nationale Grenzen hinweg möglich.

Bernhard Tellenbach, Vorstand ISSS
betellen@tik.ee.ethz.ch

Rückblick: 10. Businessday vom 25.10.2012

10. Businessday des Verbandes Wirtschaftsfrauen Schweiz vom 25.10.2012 in Basel in Partnerschaft mit ISSS

Am 10. Businessday der Wirtschaftsfrauen standen Internetsicherheit für Privatpersonen und KMUs im Fokus. Neben Vorträgen zu aktuellen Themen wie „Cloud Computing“ und „Bring Your Own Device“ (BYOD) sowie Cyber Crime in Unternehmen und öffentlichen Verwaltungen wurde mittels eines durch Profis inszenierten Life Hackings auf Smartphones den Anwesenden auf eindrückliche Weise die Verwundbarkeit der modernen Kommunikationsmittel vor Augen geführt.

Das Thema Informatikkriminalität wird deshalb auch in KMUs immer aktueller und durch stets neue in den Medien publik werdende Fälle grossflächigen Datendiebstahls zusätzlich getrieben. Wie können Unternehmerinnen und Kaderfrauen dafür sensibilisiert werden und wie können sie sich schützen? Unternehmerinnen werden ausserdem immer öfter von Firmen angeschrieben, die sogenannte Cloud-Services anbieten. Was heisst genau „Cloud“ und welche Daten dürfen darin gespeichert werden?

Cloud Computing: was ist das und wem dient es?
Das ISSS Mitglied Cyrill Osterwalder, bei Google Schweiz verantwortlich für Sicherheits- und Datenschutzmechanismen, erklärte den Teilnehmerinnen, was Cloud Computing ist und wie es in Unternehmen nutzbringend eingesetzt werden kann. Dabei ging er vor allem darauf ein, was ein Unternehmen beachten muss, wenn es seine Daten in die Cloud zu verschieben gedenkt. Besonders hervorzuhaben ist sein Hinweis, dass Unternehmerinnen, die aufgrund ihrer Firmengrösse keine eigene IT-Abteilung haben, sich Hilfe von unabhängigen Fachleuten holen sollten. Zudem forderte Cyrill Osterwalder die Zuhörerinnen auf, auch die Ratschläge der eigenen IT-Abteilung zum Thema Cloud Computing kritisch zu hinterfragen, da diese Cloud Computing oft als Konkurrenz ihrer eigenen internen Dienstleistungen betrachteten.

Cloud Computing in der öffentlichen Hand
ISSS-Vorstandsmitglied Hanspeter Christ, IT-Projektleiter beim Bundesamt für Landestopografie swisstopo und verantwortlich für die Migration der gesamten Bundes Geodaten-Infrastruktur in die Amazon Public Cloud, knüpfte mit seinem Vortrag an denjenigen von Cyrill Osterwalder an.
Hanspeter Christ erklärte, dass bei der Planung eines Cloud Computing Projekts eine umfassende und mit gesundem Menschenverstand durchgeführte Chancen- und Risikobetrachtung aus der Businessperspektive unerlässlich sei. Im Fall von swisstopo musste dem Geoinformationsgesetz Art. 1 Folge geleistet werden, welches besagt, dass *„Geodaten über das Gebiet der Schweizerischen Eidgenossenschaft den Behörden von Bund, Kantonen und Gemeinden sowie der Wirtschaft, der Gesellschaft und der Wissenschaft für eine breite Nutzung, nachhaltig, aktuell, rasch, einfach, in der erforderlichen Qualität und zu angemessenen Kosten zur Verfügung stehen.“* – offensichtlich ein optimaler Use Case für ein Deployment in eine Public Cloud! Mit einem pragmatischen Vorgehen wurde Schritt für Schritt eine Geodatenablage in der Cloud aufgebaut, die auch bei Belastungsspitzen (z.B. infolge einer Medienmitteilung) einen unterbruchsfreien Betrieb ermöglicht. Ohne die enorme Skalierbarkeit der Cloud wäre es beim Go-Live des Geoportals Bund gemäss Hanspeter Christ mit grösster Wahrscheinlichkeit zum Crash gekommen.

Bring Your Own Device – Rechtliche Aspekte: Risiken und Lösungen
Bring Your Own Device ist unbestritten ein aktueller Trend, auch wenn die Beweggründe für dessen Einführung in den Unternehmen sehr unterschiedlich ausfallen. Während die einen primär eine Verringerung der Ausgaben für ihre interne Kommunikationsinfrastruktur anstreben erachten andere Unternehmen Punkte wie bessere Erreichbarkeit und höhere Produktivität der Mitarbeitenden als wesentlichen Treiber des BYOD. Aber was ist rechtlich zu beachten, wenn Unternehmensdaten auf privaten Smartphones und Tablets gespeichert werden? Zu dieser Frage nahm Ursula Widmer, Präsidentin der ISSS, in ihrem Vortrag kompetent Stellung und beleuchtete das Thema aus den verschiedensten rechtlichen Blickwinkeln. So seien bei BYOD nicht nur die Unternehmensdaten gebührend vor Zugriff durch unbefugte

Rückblick: 10. Businessday vom 25.10.2012 (Fortsetzung)

10. Businessday des Verbandes Wirtschaftsfrauen Schweiz vom 25.10.2012 in Basel in Partnerschaft mit ISSS

Dritte zu sichern, sondern aus Sicht der Datenschutzgesetzgebung und des Arbeitsrechts auch die Persönlichkeitsrechte des Arbeitnehmers entsprechend zu schützen. Daten über den Arbeitnehmer (z.B. Standortinformationen des Gerätes oder Nutzungsprofile) dürften nur erhoben und bearbeitet werden, soweit diese zur Durchführung des Arbeitsvertrags erforderlich seien. Zudem gebe es zu beachten, dass die private Gerätenutzung durch BYOD in keiner Weise beeinträchtigt werde und möglichst klar von der geschäftlichen Nutzung getrennt werde. Technisch kämen hierzu in der Regel sogenannte Device und Application Management Systeme zum Einsatz. Damit sei es aber nicht getan. Eine BYOD Policy sollte in jedem Fall die Spielregeln zwischen Arbeitgeber und Arbeitnehmer klären und im Arbeitsvertrag oder Personalreglement verankert werden.

Wie sicher sind Smartphones und Tablets?
Für die Bezahlung an Kassen können anstelle von etablierten Zahlungsmitteln wie Kreditkarte, Master- und Postcard oder Bargeld zunehmend auch Smartphones und Tablets eingesetzt werden, aber wie sicher ist das? Und ist es wirklich völlig unbedenklich, QR Codes mit dem Handy einzulesen?
Marco Di Filippo von der Compass Security AG, welche bei ISSS Mitglied ist, demonstrierte in einer Live Hacking Session eindrücklich, wie schnell und einfach handelsübliche Handys und Tablets gehackt werden können. Die Schäden, die Unternehmen und Privatpersonen dadurch entstehen können, sind immens. So passiere es häufig, dass erst in der Monatsrechnung des Telco-Providers ersichtlich werde, dass jemand illegal das persönliche Handy gehackt habe und z. B. bei einem Telefon-Voting 15‘000 Anrufe à 0.50 € getätigt habe – für den Handybesitzer eine böse Überraschung über 7‘500 € ! Jetzt müsse erst einmal bewiesen werden, dass nicht der Handyinhaber, sondern eine Person, die sich mittels Fremdzugriff die Telefonnummer des Besitzers ergattert habe, die Anrufe getätigt habe. QR Codes, z.B. auf öffentlichen Plakatwänden, könnten ausserdem ebenfalls sehr leicht mit gefälschte QR Codes, die auf Handy-Malware verweisen, überklebt werden. Sei die Malware einmal auf dem Handy installiert, werde diese dann wiederum zum Ausspionieren des Gerätes eingesetzt.
Michael Veit von SOPHOS zeigte in seinem Vortrag auf, dass die fehlende Trennung von geschäftlichen und privaten Daten auf Handys und Tablets eine grosse Gefahr darstelle. Angriffe seien mit der auf vielen Geräten installierten Software-Flut von Acrobat Reader, Flash Player, Java etc. von allen Seiten her möglich. Auch von modernen „Apps“ gehe ein oft unterschätztes Risiko aus und die möglichen Gefahren beim Verlust oder Diebstahl des Mobiltelefons oder Tablets seien nicht unerheblich. SOPHOS ist Anbieter einer Software, mit der diese Risiken minimiert bzw. weitestgehend eliminiert werden können.

Informatikkriminalität
- Gefahren für das Unternehmen
- Prävention
- Massnahmen bei Verdacht auf Informatikkriminalität im eigenen Unternehmen

Marc Henauer, Sektionschef MELANI, erklärte in seinem Vortrag, mit welch immenser krimineller Energie versucht wird, auf fremde Daten zuzugreifen. Das Netzwerk der Hacker ist gewaltig, hochgradig spezialisiert und äusserst dynamisch. Der Handel mit gestohlenen Daten, und hier ist nicht nur die Rede von Bankdaten, ist riesig. Bei Verdacht auf Informatikkriminalität sollte man sich unbedingt an die Polizei wenden, nur so könnten die Fälle in die Statistiken einfliessen sowie deren Art, Schweregrad und regionale Auffälligkeiten analysiert werden. Ohne eine Anzeige mit entsprechendem Niederschlag in den Kriminalstatistiken sei es schwierig, gezielt gegen Hacker vorzugehen (wo kein Kläger, da kein Richter).

Telebasel war vor Ort und berichtete in der Newssendung 7vor7 vom 10. Businessday. Unter folgendem Link finden Sie den Fernsehbeitrag (Beitrag beginnt bei 08:51):
http://www.telebasel.ch/de/tv-archiv/&id=366809036&search=25.10.2012&datefrom=&dateto=&group

Petra Breiting, Mitglied ISSS, Vorstand Verband Wirtschaftsfrauen Schweiz
pbreiting@gmx.net

Agenda: ISSS Events

Nächste ISSS Events

Programm und Anmeldung unter: http://www.isss.ch/veranstaltungen/veranstaltungen/

Datum	Zeit	Veranstalter	Titel und Details	Ort
Mi, 23.01.2013	12:00 - 14:00	ISSS	**ISSS Security Lunch: "Sichere Unternehmensmobilität - technische Machbarkeit und rechtliche Absicherung"** Details, Anmeldung	Bern
Do, 24.01.2013	12:00 - 14:00	ISSS	**ISSS Security Lunch: "Sichere Unternehmensmobilität - technische Machbarkeit und rechtliche Absicherung"** Details, Anmeldung	Zürich
Di, 12.03.2013	16:00 - 19:00	ISSS	**ISSS St. Galler Tagung: "Secure Unified Communication in der Praxis"**	St. Gallen
Mi, 05.06.2013	09:00 - 17:00	ISSS	**ISSS Zürcher Tagung: "IT-Sicherheit im Finanzbereich - Der Umgang mit operationellen Risiken"**	Zürich
Di, 01.10.2013	09:00 - 17:00	ISSS	**1. ISSS Information Security Switzerland Conference**	Lausanne
Do, 28.11.2013	13:00 - 18:00	ISSS	**16. Berner Tagung für Informationssicherheit**	Bern

Agenda: Partner Events

International Pavilion for IT Security an der CeBIT Hannover (5.-9. März 2013)

Der Ausstellungsbereich SECURITY WORLD an der CeBIT Hannover wächst. Das grosse Bedürfnis nach Sicherheit in der digitalen Welt beflügelt kreative Schweizer Unternehmen, Lösungen zu entwickeln, die es zu vermarkten gilt: SWISSNESS ist ein gefragtes Label. Mit dem „International Pavilion for IT Security“ wird eine Plattform geboten, welche eine ideale Grundlage für die erfolgreiche Vermarktung ihrer Produkte darstellt.

ISSS weist ihre Mitglieder auf die Möglichkeit hin, sich am International Pavilion for IT Security zu beteiligen. Gerne stellen wir den Kontakt zum Anbieter her.
Bei Interesse bitten wir die interessierten ISSS Mitglieder, sich via E-Mail bei unserem Sekretariat zu melden: sekretariat@isss.ch

TeleTrusT-Informationstag „IT-Sicherheit im Smart Grid“

Der nächste TeleTrusT-Informationstag „IT-Sicherheit im Smart Grid“ wird am 13.6.2013 in Berlin stattfinden. Bitte merken Sie sich schon jetzt dieses Datum vor, da ISSS-Mitglieder 20% Rabatt auf den Eintrittspreis erhalten werden.

Zum Thema „Smart Grid – Lagebild Schweiz“ wird ein Referent aus der Schweiz auftreten und für den Bereich IT-Sicherheit werden die Themen Netzanbindung/Vernetzung CH/EU, Back-up-Strukturen, Grid Codes und Verteilungssteuerung von grossem Interesse sein.

Weitere Hinweise dazu werden Sie zu gegebener Zeit unter www.teletrust.de/veranstaltungen finden.

Agenda: Security Events unserer Partner

Nächste Security Events unserer Partner

Programm und Anmeldung unter: http://www.isss.ch/veranstaltungen/veranstaltungen/

Datum	Zeit	Veranstalter	Titel und Details	Ort
Di, 08.01.2013	18:30 - 23:30	DEFCON Switzerland	**DEFCON Switzerland Beer on Tuesday** Ort: Blues Bar, Speichergasse 29, 3000 Bern Die Teilnahme ist kostenlos. Details	Bern
Di, 29.01.2013	13:00 - 17:00	Swiss Infosec AG	**MEET SWISS INFOSEC! Integrale Sicherheit: Kopf oder Zahl?** Event zu Informations- und IT-Sicherheit: Erleben Sie hochkarätige Referenten, lernen Sie uns und unser Partner kennen. kostenlos Details	Zürich-Flughafen
Di, 12.02.2013	18:30 - 23:30	DEFCON Switzerland	**DEFCON Switzerland Beer on Tuesday** Ort: Rheinfelder Bierhalle AG Niederdorfstrasse 76, 8001 Zürich Die Teilnahme ist kostenlos. Details	Zürich
Di, 12.02.2013	18:30 - 23:30	DEFCON Switzerland	**DEFCON Switzerland Beer on Tuesday** Ort: Rheinfelder Bierhalle AG Niederdorfstrasse 76, 8001 Zürich Die Teilnahme ist kostenlos. Details	Zürich

Agenda: Security Kurse unserer Partner

Nächste Security Kurse unserer Partner

Programm und Anmeldung unter: www.isss.ch/veranstaltungen/kurse

Datum	Zeit	Veranstalter	Titel und Details	Ort
Mo - Fr, 14.01.-18.01.2013	09:00 - 17:00	Swiss Infosec AG	**Informations- und IT-Sicherheitsbeauftragter (IT-SIBE)** Runden Sie Ihr Fachwissen ab! Wir führen Sie umfassend in die Grundlagen der Informations- und IT-Sicherheit ein. CHF 4200.- Details	Zürich
Mo - Mi, 14.01.-16.01.2013	13:30 - 16:30	iimt	**Strategy and Innovation Management - Module 1** Introduction to the concept of strategy / The tools of strategic analysis, market based / The nature of competitive advantages CHF 1900 Details, Anmeldung	Freiburg
Do - Sa, 17.01.-19.01.2013	08:30 - 12:00	iimt	**Marketing Management - Module 1** Introduction to Marketing & Markets / Marketing Research / Marketing Objectives / Marketing Strategies CHF 1900 Details, Anmeldung	Freiburg
Mo - Do, 21.01.-24.01.2013	09:00 - 17:00	Swiss Infosec AG	**Sicherheitsmanagement im IT-Umfeld** Mehr Sicherheit dank sicherer Technik! Der Lehrgang vermittelt Ihnen technisches Grundwissen im Bereich IT-Sicherheit. CHF 3500.- Details	Zürich

Vollständige Agenda mit Links zu Programm und Anmeldung unter: www.isss.ch

Information Security Society Switzerland
Monbijoustrasse 15
3011 Bern
newsflash@isss.ch
Tel. +41 31 311 5300
Auflage: Nur elektronische Auslieferung. Versand als PDF per E-Mail an alle ISSS-Mitglieder und Publikation auf www.isss.ch