ISSS NewsFlash Januar 2012



Editorial

Das Thema **Cloud Computing Security** stiess an der Berner Tagung im November auf sehr grosses Interesse. Grund genug, einen Aufruf zur **Gründung einer SIG** zu diesem Thema zu machen. Interessierte melden sich bitte baldmöglichst bei Umberto Annino umberto.annino@isss.ch. Die SIG wird voraussichtlich als erstes eine Stellungnahme zur Cloud Strategie der Schweizer Behörden verfassen.

Mitglieder der Task Force **„Elektronisches Patientendossier“** lieferten kurz vor Weihnachten ihre ausführlich Stellungnahme ab. Einen Kurzbericht lesen Sie in dieser Ausgabe.

Die SIG „Cyber Defense Strategie“ verfasste trotz Vernehmlassung über die Feiertage eine Stellungnahme zum Entwurf der **„Nationalen Cyber Defense Strategie“**. ISSS-Vorstandsmitglied Ivan Bütler gibt zu diesem Thema in der vorliegenden Ausgabe ein Interview.

Im März würden wir Sie gerne an unserer dritten St. Galler Tagung zum Thema **„iPhone im Unternehmen“** begrüssen. Die Tagung war in den letzten zwei Jahren jeweils schnell ausgebucht. Zudem führen wir im März einen Security Lunch in Zürich durch.

Dr. Thomas Dübendorfer
Präsident, ISSS
president@isss.ch

Highlights in dieser Ausgabe

ISSS:

- Revisor gesucht
- Delegationsreise für ICT-KMUs zur CeBIT 2012
- SuisseID kommt auf die Identitätskarte
- Neues Kurzvideo stellt die ISSS vor

SIGs:

- Gründung der SIG „Cloud Computing Security“
- ISSS-Stellungnahme zum ePatientendossier

Focus:

- „Nationale Cyber Defense Strategie“ - Interview mit Ivan Bütler

Agenda:

- Nächste ISSS Events
  - ISSS Security Lunch am 15.3.2012 in Zürich: „Die Verbindlichkeit von Information im Internet“
  - ISSS St. Galler Tagung 2012 am 28.3.2012: “iPhone im Unternehmen“
- Partnerevent: Meet the Wireshark Geek

ISSS: Kurznews

Revisor für ISSS gesucht!

An der nächsten ISSS Generalversammlung im April 2012 müssen neue Revisoren gewählt werden. Diese Aufgabe ist dank unserem Sekretariat, welches die Buchhaltung tadellos führt, mit geringem Aufwand verbunden. Als Entschädigung für das Prüfen der Buchhaltung (findet jeweils im Januar statt) und Schreiben des kurzen Revisionsberichtes (in der Regel eine Seite lang), erhalten die Revisoren am Ende ihrer Amtsdauer an der GV ein Geschenk.
Interessierte (auch Nichtmitglieder) melden sich bitte umgehend bei umberto.annino@isss.ch.

Delegationsreise für ICT-KMUs zur CeBIT 2012

Gemeinsam mit der **Osec** arbeiten einige Mitgliedorganisationen von **ICTswitzerland** (asut, epower, simsa, SWICO, SwissICT, TCBE.ch) seit April 2011 in einer Arbeitsgruppe am **Ziel, den Export von Schweizer ICT Dienstleistungen und Produkten langfristig und nachhaltig zu erhöhen.** Im Rahmen dieser Zielsetzung will die Gruppe die Wahrnehmung von ICT-Produkten im Ausland verbessern. Da ISSS auch bei ICTswitzerland Mitglied ist, können sich auch Mitglieder von ISSS einbringen.

In Zusammenarbeit mit ICTswitzerland organisiert die Osec am **Freitag, 9. März 2012** eine kompakte Eintagesreise an die CeBIT Hannover. Die Delegation ist angeführt von Ruedi Noser, Nationalrat und Präsident von ICTswitzerland, sowie Tim Guldimann Schweizer Botschafter in Deutschland.

Das Programm umfasst neben Besuchen ausgewählter Stände auch einen gemeinsamen Steh-Lunch der Delegation mit geladenen Gästen. Kontakte zu Brasilien, dem Gastland der CeBIT 2012, können als Abschluss am gemeinsamen Apéro geknüpft werden.

Nutzen Sie die Gelegenheit und treffen Sie an nur einem Tag potenzielle Kunden, Geschäftspartner und wichtige Entscheidungsträger an einem Ort.

Der Preis von nur 500 CHF für Sie als ISSS-Mitglied (1‘000 CHF für Nicht-Mitglieder) beinhaltet den Flug, alle Transporte sowie die Verpflegung während des Tages. Als Option kann die Delegationsteilnahme ohne Flug gebucht werden.

Melden Sie sich direkt online an via Webseite Osec. Bei Fragen steht Ihnen Alberto Silini <asilini@osec.ch>, Telefon +41 44 365 53 15 gerne zur Verfügung.

Da ISSS auch eine direkte Partnerschaft mit der CeBIT hat, können ISSS-Mitglieder ein Gratisticket zur CeBIT 2012 beziehen unter diesem Link:
http://www.cebit.de/de/aktion?ek8ed

SuisseID kommt auf die Identitätskarte

Die heutige bereits 16 Jahre alte Identitätskarte soll es danach in vier verschiedenen Versionen geben, wie das EJPD heute mitteilt. Neben einem Modell ohne Chip sollen Bürger und Bürgerinnen dann auch zwischen einem Modell mit elektronisch gespeicherten Daten (Foto sowie zwei Fingerabdrücke), einem mit integrierter "elektronischer Identität" für E-Government und E-Business-Anwendungen, sowie einer Karte, die beides enthält, wählen können. Für die "elektronische Identität" ist die SuisseID bereits gesetzt, wie Markus Waldner vom Bundesamt für Polizei gegenüber inside-it.ch sagte.
Quelle:
http://m.inside-it.ch/articles/27347, 16.12.2011

Neues Kurzvideo stellt die ISSS vor

Wir haben den grossen Erfolg der 14. Berner Tagung 2011 mit ca. 330 Teilnehmenden zum Anlass genommen, einen Kurzvideo zu erstellen, welcher die Information Security Society Switzerland (ISSS) anhand der Tagung kurz vorstellt.

http://youtu.be/zuoe6wBvqc4

SIGs: Neue Special Interest Group “Cloud Computing Security“

Interessenten für die aktive Mitarbeit in dieser SIG melden sich bitte vor Ende Januar 2012 beim SIG-Lead Umberto Annino umberto.annino@isss.ch.

Motivation

Cloud Computing ist als Trend der Informatik etabliert und auch unter ICT-Laien kein Fremdwort mehr - u.a. aufgrund der sog. “consumerisation” von Informatikprodukten (Durchdringung des Endkonsumenten-Marktes mit ICT-Systemen verschiedenster Funktionalität und Grösse sowie entsprechender Services).
Auf behördlicher Seite haben einige Länder begonnen, Cloud Computing Strategien zu entwickeln. Unter anderem wurde bereits ein Entwurf für eine Cloud-Strategie der Schweizer Behörden unter Federführung des ISB (Informatiksteuerungsorgan Bund) erstellt.
Cloud Computing stellt zwar im Kern keine grundlegend neuen Technologien oder Arten der Dienstleistungserbringung dar - aufgrund der hohen angestrebten Marktdurchdringung und “ubiquity” (Allgegenwart) von Cloud-Services ist dem Aspekt der Sicherheit allerdings eine höhere Beachtung zu schenken. Sicherheit als wesentliche Anforderung ist auch im Cloud Computing nicht “integrated-by-design”. Nebst den technischen Herausforderungen gibt es auch offene Fragen rechtlicher Art sowie betreffend Definition der Cloud-Services.

Ziele

Eines der Ziele der SIG ist es, ein Security-Whitepaper für Cloud Computing zu erstellen, das die wesentlichen Themen für Anbieter und Abnehmer von Cloud-Services abdeckt. In diesem Zusammenhang sollen unter anderem folgende drei Punkte bearbeitet werden.

1) Definitionen und Dimensionen

Welche (aus sicherheitstechnischer Sicht) relevanten Definitionen für Cloud Computing gibt es und inwieweit sind diese Begriffe bereits etabliert, bekannt und verstanden? Welche Aspekte des Cloud Computings sind noch unklar oder nicht definiert?

2) Sicherheit in den drei Dimensionen: Verfügbarkeit, Vertraulichkeit und Integrität.

Welches sind die zentralen Anforderungen an die Sicherheit, wie sind diese zu spezifizieren? Wie kann sich der Kunde von Cloud-Services Transparenz über die sicherheitsrelevanten Aspekte von solchen Service-Angeboten verschaffen?

3) Stellungnahme zum Entwurf zur Cloud-Strategie der Schweizer Behörden

Am 14. Dezember 2011 hat das ISB den Entwurf für die Cloud-Strategie des Bundes online verfügbar gemacht. Die hier vorgestellte SIG kann per Freitag, 10. Februar 2012 (Eingabefrist) eine entsprechende ISSS-Stellungnahme eingeben - vorausgesetzt, es finden sich bis dahin genügend Interessenten für die Mitarbeit an einer solchen Stellungnahme.

Erwartete Ergebnisse

Die SIG erstellt eine Stellungnahme zum Entwurf der Cloud-Strategie für Schweizer Behörden des ISB per Freitag, 10. Februar 2012.

Die SIG erstellt ein Whitepaper zu CloudComputing Security, worin die Sicherheitsaspekte des Cloud Computings, spezifische Herausforderungen und Problemstellungen und mögliche Lösungen dokumentiert und wo sinnvoll und anwendbar, auch definiert werden.

Die SIG verfolgt das Thema Cloud Computing aus dem Blickwinkel der Informationssicherheit - auf nationaler und internationaler Ebene in Bezug auf Service-Entwicklung, Standardisierung und Normierung.

Die SIG beobachtet die Abdeckung des Themas Cloud Computing Security durch andere interessierte Organisationen (Verbände, Vereine, Behör-

SIGs: Neue Special Interest Group "Cloud Computing Security" (Forts.)

den, Privatwirtschaft etc.).

Die SIG informiert die ISSS Mitglieder regelmässig via NewsFlash, Referate oder Publikationen über sicherheitsrelevante Aspekte des Cloud Computings.

Teilnehmende

Als Idealgrösse werden 8 – 12 Teilnehmende betrachtet. Wichtig ist die aktive Mitarbeit aller Personen (keine „Zaungäste"), damit die spezifischen Erfahrungen mit verschiedenen Cloud-Services auch wirklich eingebracht werden können. Die Teilnehmenden sollten selbst aktiv Cloud-Services nutzen oder anbieten, im privaten oder geschäftlichen Kontext. Ideal ist eine ausgewogene Durchmischung von Anbietern und Abnehmern von Cloud-Services im Schweizer ICT Umfeld von behördlicher und privatwirtschaftlicher Seite.

Termine

Bis Ende Januar 2012: Konstitution der SIG und Festlegung, ob eine Stellungnahme für den Entwurf der Cloud-Strategie der Schweizer Behörden per 10. Februar 2012 erstellt werden kann.

Die Konstitution der SIG ist unabhängig von einer allfälligen Stellungnahme zum Entwurf der Cloud-Strategie der Schweizer Behörden.

1. Juni 2012: Fertigstellung der Kernthemen der SIG Cloud Computing Security

31. Dezember 2012: Vorliegen eines ersten Entwurfes ("request for comment") des Whitepapers zu Cloud Computing Security zur Publikation und Möglichkeit zur Stellungnahme durch ISSS Mitglieder

30. März 2013: Publikation des fertiggestellten Whitepapers "Cloud Computing Security" durch die SIG.

Weitere Themen und Termine können durch die SIG festgelegt werden

Interessenten für diese SIG melden sich bitte beim SIG-Leiter und ISSS-Vorstandsmitglied Umberto Annino <umberto.annino@isss.ch>.

Die ISSS lebt dankt aktiven Mitgliedern

Der Verein ISSS ist das, was aktive Mitglieder daraus machen:

- Haben Sie Ideen für Projekte, neue Dienstleistungen oder Partnerschaften für ISSS?
- Wollen Sie die Zukunft der ISSS im Vorstand selbst mitbestimmen?
- Wollen Sie das Netzwerk von Security Professionals der ISSS aktiv nutzen?
- Ist Ihre Firma an Sponsoringgelegenheiten bei ISSS-Anlässen interessiert?
- Kennen Sie einen Referenten, der ein spannendes Security Thema verständlich präsentieren kann im Rahmen eines ISSS Security Lunches oder einer Tagung?

Dann kontaktieren Sie bitte den ISSS-Präsidenten unter president@isss.ch und Sponsoringanfragen richten Sie bitte an sponsoring@isss.ch.

Die ISSS lebt von den Ideen und der Mitarbeit seiner Mitglieder. Gemeinsam erreichen wir mehr.

Information Security Society Switzerland

SIGs: ISSS-Stellungnahme zum elektronischen Patientendossier

Die Information Security Society Switzerland (ISSS) hat im Dezember 2011 in der Vernehmlassung zum Entwurf des Bundesgesetzes über das elektronische Patientendossier eine ausführliche Stellungnahme verfasst und publiziert. Diese wurde durch eine ISSS Task Force mit eHealth und Security Spezialisten erarbeitet.

Die ISSS befürwortet darin grundsätzlich die Schaffung der gesetzlichen Grundlagen für ein gesamtschweizerisches ePatientendossier. Patientendaten sind besonders sensible Daten und das ePatientendossier muss daher hohen Anforderungen bezüglich Datenschutz und Datensicherheit genügen. In ihrer Stellungnahme weist die ISSS auf Punkte hin, in denen der Gesetzesentwurf diesen Anforderungen noch nicht genügt.

So sind die Verantwortlichkeiten im Zusammenhang mit dem Betrieb des ePatientendossiers und der Verwaltung der darin enthaltenen Daten klarer zu formulieren, insbesondere betreffend die so genannte Stammgemeinschaft, die das Dossier für den Patienten eröffnet. Die Rechte der Patienten sind zu präzisieren und zu ergänzen, z.B. im Zusammenhang mit der Einwilligung und deren allfälligem Widerruf betreffend die Eröffnung des ePatientendossiers und die Aufnahme von Dokumenten in dieses. Die Patienten sollten auch berechtigt sein, die Entfernung von Daten aus dem Dossier zu verlangen (und nicht nur die Sperrung des Zugriffs auf die Daten) und sie sollten die Möglichkeit haben, die Protokollierung über die erfolgten Zugriffe auf ihre Daten einzusehen.

Weitere Punkte betreffen Vereinfachungen bei der Zertifizierung der am ePatientendossier teilnehmenden medizinischen Leistungserbringer (Arztpraxen, Spitäler etc.), die Verankerung der Mitwirkung der interessierten Kreise bei der Ausarbeitung aller Ausführungsvorschriften (insbesondere betreffend Normen, Standards und Mindestanforderungen) sowie die Förderung der Schulung von Patienten im Umgang mit dem Dossier.

Es ist geplant, dass der Bundesrat im Frühjahr 2012 basierend auf den Ergebnissen der Vernehmlassung über das weitere Vorgehen entscheidet. Bis Herbst 2012 soll dann eine Botschaft für das Parlament ausgearbeitet werden, so dass dieses ab Frühjahr 2013 mit der Beratung des Gesetzes beginnen kann.

Autor: Konrad Bähler, Lead ISSS Task Force „Vernehmlassung Bundesgesetz elektronisches Patientendossier“

Focus: "Nationale Cyber Defense Strategie" – Interview mit Ivan Bütler

Der Bund arbeitet momentan mit Hochdruck an einer "Nationalen Cyber Defense Strategie". Die ISSS hat tiefe Einblicke erhalten und sich mit einer Special Interest Group unter der Leitung von Mark Saxer dem Thema angenommen und mehrfach in Workshops fachlichen Input geliefert. Am 20.1.2012 hat sich die ISSS in Absprache mit SwissICT, deren Security Fachpartner sie ist, im Rahmen einer Stellungnahme zur Version 6 des Strategiedokumentes öffentlich geäussert. Die ISSS-Stellungnahme zur Nationalen Cyber Defense Strategie finden Sie online zum Download.

ISSS-Vorstandsmitglied Ivan Bütler, welcher das Thema auch in der SIG intensiv bearbeitet hat, steht in unserem Interview Red und Antwort zur Nationalen Cyber Defense Strategie.

Wie hat sich die Bedrohungslage im Bereich Cyber Attacken in den letzten Jahren verändert?

Durch den Erfolg des Internets werden zunehmend wichtige Geschäftsprozesse, Automationen und Daten auf Computern und in Netzwerken verarbeitet. Aus IT-Insellösungen sind in den letzten Jahren grossartige, vernetzte und komplexe Systeme entstanden, welche alle Arten von Informationen verarbeiten. Die Industrie, Staaten und Leistungserbringer hängen zunehmend von der Verfügbarkeit von diesen Systemen ab und so muss man heute einen Ausfall derselben in die eigene Krisenüberlegung einbeziehen. Die Anreicherung von immer neuen Funktionen wirkt sich in der Kombination von immer wechselnden Technologien negativ auf die Sicherheit aus. Unsere Gesellschaft hat sich eine eigene Achillesferse geschaffen, ein stark verwundbar- und angreifbares System höchster Komplexität. Die Schwachstellen werden längst nicht mehr nur von Hobby Hackern und Script Kiddies ausgenützt, ein Underground Business ist gewachsen, das die Wirtschaft und auch Staaten bedroht. Eine höchst unangenehme Situation für technologisch führende Länder, zu denen auch die Schweiz gehört.

Könnte ein grosser Cyber Angriff auf die Schweiz heute kritische Infrastrukturen lahmlegen? Was wären mögliche Folgen für die Bevölkerung?

Ein solches Ereignis ist möglich, müsste jedoch von langer Hand geplant und mit mehrstufigen Massnahmen durchgeführt werden. Insbesondere müsste der Ausfall auch eine gewisse Zeit andauern, eingeleitete Notfallkonzepte fehlschlagen, um die Schweizer Nation in eine tiefe Krise zu stürzen. Aber wie unangenehm schon kurze Systemausfälle für die Bevölkerung sein können, weiss jeder, der schon einmal wegen einer technischen Panne am Flughafen nicht einchecken konnte.

Was sind die Kernpunkte der Cyber Defense Strategie des Bundes?

Diese Frage kann abschliessend nur der Bund beantworten. Ich verrate aber sicher kein Geheimnis, wenn ich so viel sage: Die Strategie baut auf den Kernkompetenzen der Antizipation, Prävention und Reaktion auf.

Was erwartet die ISSS von der Strategie des Bundes?

Wichtig ist, dass klar festgesetzt wird, wer verantwortlich ist: Für die technische Umsetzung und für die zentrale Koordination im Ereignisfall. Das klingt zwar banal, ist aber angesichts der Vielzahl beteiligter Akteure (Bund, Kantone, Städte, kritische Infrastrukturen, Firmen, …) sicher eine Herausforderung der Umsetzungsplanung. Dennoch: Jemand muss dafür verantwortlich sein, im Ereignisfall die richtigen Entscheide zu fällen, um die Sicherheit der Schweiz zu gewährleisten. Dazu sollen meines Erachtens zunächst vorhandene Instrumente gestärkt und gegebenenfalls besser vernetzt werden.
Weiter ist es unserer Ansicht nach ein Muss, dass in der Antizipation nicht nur aktuelle Bedrohungen analysiert werden, sondern dass mittels Forschung und Lehre auch nach neuen Angriffsmethoden und Abwehrmassnahmen gesucht wird.

Können Sie "Cyber War" definieren? Fällt "Cyber War" auch unter diese Strategie?

Ich nehme an, die Strategie heisst „Cyber Defense“, weil es keine „war“-Strategie werden soll. Die reine Kriegsführung im Cyberspace wird unter Experten aber ohnehin als unrealistisch bezeichnet. Die Streitkräfte der USA bezeichnen Cyber als eine "New Domain of Operations" und haben neben Space, Air, Land und Sea ein fünftes Kompetenzzentrum ins Leben gerufen. Ich gehe davon aus, dass Cyber dabei ein unterstützendes Element bei der Durchsetzung von Interessen in Krisenzeiten darstellt. Grundsätzlich gewinnen durch die zunehmende Vernetzung sowohl das Abwehr- als auch das Angriffsdispositiv stark an Bedeutung. Denn eine Bedrohung im Cyberspace ist im Gegensatz zur realen Bedrohung durch militärische Angriffe permanent latent vorhanden. Darum ist die Entwicklung entsprechender Kompetenzen für die Schweiz zentral und un-

Focus: "Nationale Cyber Defense Strategie" – Interview mit Ivan Bütler (Forts.)

erlässlich.

Der Anhörungsentwurf der Strategie sieht auch Cyber Gegenangriffe vor. Was ist ihre Haltung dazu?

Er sieht die Abwehr von Cyber-Angriffen vor – wie es von einer Cyber Defense Strategie zu erwarten ist. Dazu gehören meines Erachtens gewisse Gegenangriffs-Kompetenzen. Sie müssen aber klar zugeordnet sein, und ihr Einsatz muss klar definiert werden. Eine leichtsinnige und unkoordinierte Reaktion auf Einzelangriffe muss verunmöglicht werden. Ein zentrales – und oft unterschätztes – Problem des Gegenangriffes ist auch die Problematik des Urhebers. Denn es ist oft nicht einfach, den echten Urheber eines Angriffs im Cyber Space zu identifizieren – das ist im richtigen Leben einfacher.

Was nützt der Schweiz diese Cyber Defense Strategie?

Das wird in 10 Jahren zu beurteilen sein. Ich hoffe aber, dass die Strategie die Resistenz gegenüber Cyber Bedrohungen erhöht und die Schweiz auf ein solches Notfallszenario vorbereitet. Durch die konstruktive Zusammenarbeit der Verantwortlichen von wichtigen Infrastrukturen sollen Kompetenzen und Abläufe geregelt werden, die im Ernstfall zum Tragen kommen. Ohne eine solche Vorbereitung herrscht Chaos und der Weg zum Normalbetrieb wird unnötigerweise verlängert. Jedoch nicht nur die aktive Reaktion soll verbessert werden, sondern auch die Antizipation von zukünftigen Bedrohungen, sodass die Schweiz sich auch präventiv und nicht nur reaktiv schützen kann.

Welchen Beitrag leistet die ISSS bei der Erstellung und Umsetzung dieser Cyber Defense Strategie?

Die ISSS ist ein Fachverein mit kompetenten IT Security Spezialisten aus Schweizer Unternehmen. Daraus ergibt sich ein Netz aus Vertrauen und Know-How, welche Werte der Schweiz vertreten. Wir sehen uns als idealen Review- und Koordinationspartner bei der Erstellung der Strategie und namentlich bei der konkreten Umsetzungsplanung.

Ivan Bütler ist im Vorstand von ISSS und CEO von Compass Security AG. Er hat in verschiedenen Workshops des Cyber Defense Projektteams in Vertretung von ISSS und SwissICT mitgearbeitet und engagiert sich in der Special Interest Group zum Thema in der ISSS.

Event: ISSS Security Lunch “Verbindlichkeit von Information im Internet”

Am **15. März 2012, 12:00 – 14:00** findet der nächste ISSS Security Lunch mit Vortrag und Mittagessen in **Zürich** statt. Anmeldeschluss ist der 12. März 2012.

Kurzbeschreibung

Das Gleichgewicht zwischen Erinnerung und Vergessen im Internet ist nachhaltig gestört. Die Auswirkungen dieses Ungleichgewichtes sind aus gesellschaftlicher, geschäftlicher und gerade auch rechtlicher Sicht brisant und diskussionswürdig. Denn die bestehenden Regeln im Umgang mit verbindlichen Informationen für Papier und E-Dokumente gelten auch im Web. ISSS widmet sich diesem aktuellen Thema mit diesem Lunch und betrachtet das Thema aus verschiedenen Blickwinkeln.

- Regulatorische Rahmenbedingungen
  Bruno Spicher, Leiter Kanalentwicklung E-Business der SBB
  Der renommierte Records Management Experte Dr. iur. Bruno Wildhaber informiert in einem Kurzreferat „Die Archivierung von Webseiten – zwingende Notwendigkeit oder „Nice-to-have“? über die regulatorischen Rahmenbedingungen im Kontext des Online-Kanals.

- Umsetzung
  Dr. iur. Bruno Wildhaber, Wildhaber Consulting
  Bruno Spicher, Leiter Kanalentwicklung E-Business, stellt im Anschluss vor, wie die SBB auf einfache Art und Weise Ihre Webinhalte mit der Lösung der Schweizer Firma qumram AG (www.qumram.ch) archiviert und wie sie damit einerseits den Historisierungs-Vorgaben gerecht werden und andererseits die Migrationsrisiken des kürzlich abgeschlossenen Website-Relaunches senken konnten.

Referenten

Bruno Spicher bringt mehrere Jahre Erfahrung als IT Projektleiter und Account Manager im Bereich der Telekommunikation mit. Seit 2003 arbeitet er bei den Schweizerischen Bundesbahnen SBB (Division Personenverkehr) als IT Projektleiter und Produktmanager in den Fachbereichen Intranet, Internet und Mobile. Zuletzt war er als Senior Produktmanager der SBB online Fahrpläne tätig und bringt langjähriges Fachwissen im Internet-, Mobile- und Fahrplanbereich mit. Seit dem April 2011 leitet er die E-Business Kanalentwicklung.

Bruno Wildhaber ist Unternehmer und IT Experte seit 1979. Nach einer praktischen IT Ausbildung und anschliessender Vertiefung in IT Sicherheit bei Banken sowie Studium der Rechte wird er Partner von r3 security engineering ag (Zürich); später Verkauf des Unternehmens und Gründung einer eigenen Beratungsgesellschaft (Wildhaber Consulting) im Jahr 1999. Erfahrung mit internationalen Projekten und Beteiligung an mehreren Gesellschaften mit Schwerpunkt Information Governance & Compliance, u.a. dem Kompetenzzentrum Records Management. Dr. Wildhaber ist AIIM Professional Member sowie ISO27001 Auditor und anerkannter Datenschutz Sachverständiger beim ULD Schleswig-Holstein sowie Dozent an der Hochschule für Wirtschaft (Zürich).

Anmeldung

https://www.isss.ch/veranstaltungen/2012/security-lunch-2012-03-15/

Event: ISSS St. Galler Tagung 2012 „iPhone im Unternehmen“

Besuchen Sie am Mittwoch **28. März 2012** die 3. Durchführung der ISSS St.Galler Tagung, diesmal zum Thema **„iPhone im Unternehmen“**. Stehen Sie in der Evaluation einer Mobile Device Management Lösung? Kennen Sie die Gefahren bei der Nutzung von Mobilen Geräten im Unternehmen? Im ersten Talk erfahren Sie mehr über die Bedrohungen anhand von Theorie und einer Live Hacking Demonstration. Im Anschluss nehmen Vertreter von MobileIron und Good Technologies Stellung und erklären die entsprechenden Lösungsansätze. In der Podiumsdiskussion können Sie direkt Vor- bzw. Nachteile der Lösungen ansprechen und Ihre Fragen an die Experten stellen.

Ort und Zeit

Die Tagung findet in der Migros Klubschule im Bahnhofsgebäude St.Gallen ab 16:30 Uhr im Raum 122 im 1. Stock statt.

Teilnehmende

IT Security Interessierte und Security Professionals sowie Verantwortliche für Informatik aus Wirtschaft, Politik, Verwaltung sowie Wissenschaft und Forschung.

Programm

16:00 – 16:30	**Ankunft und Registrierung**
16:30 - 16:45	**Begrüssung / Einleitung** Referent: Ivan Bütler
16:45 - 17:30	**iPhone (In)Security im Unternehmen** Referent: Riccardo Trombini Abstract und Short Bio
17:30 - 18:15	**Good for Enterprise - Secure Device Management** Referent: Martin Ottiger Abstract und Short Bio
18:15 - 18:30	Kurze Pause
18:30 - 19:15	**MobileIron - Secure Device Management** Referent: Philipp Klomp Abstract und Short BioDetails
19:15 - 19:45	**Podiumsdiskussion**
ab 19:45	**Apéro**

Anmeldung

Eine online Anmeldung ist erforderlich.

Regulärer Preis: CHF 80.00, Partnerpreis: CHF 60.00, ISSS bzw. SwissICT-Mitglieder: CHF 50.00, Studierende CHF 20.00.

Riccardo Trombini, Compass Security AG

Riccardo Trombini arbeitet seit 2009 als Security Analyst bei der Compass Security AG. Als Apple Crack und iPhone Entwickler hat er in diversen Kundenprojekten die Sicherheit bei der Integration von iPhones in das Unternehmen analysiert und Lösungen von Goods als auch MobileIron beurteilt. Riccardo Trombini zeigt in seinem Eröffnungstalk die Gefahren und Bedrohungen auf.

Martin Ottiger, Comdirect AG

Martin Ottiger ist der CEO von Comdirect AG, welche Lösungen und professionelle Beratung in allen Fragen des mobilen Computings anbietet. Martin Ottiger wird den Lösungsansatz von Good Technologies erläutern und von seinen Erfahrungen bei der Integration von iPhones in das Unternehmen berichten.

Philipp Klomp, Nomasis AG

Philipp Klomp ist Gründer und Geschäftsführer der Nomasis AG und befasst sich seit über 10 Jahren mit Mobile Security. Er hat mit der Nomasis AG wegweisende Projekte zum Thema iPhone und iPad konzeptioniert und umgesetzt. Philipp Klomp wird den Lösungsansatz des IOS Device Management mit dem Produkt MobileIron präsentieren und demonstrieren.

Agenda: Security Events

Nächste ISSS Fachtagungen

Do, 15.03.2012	12:00 14:00	–	**ISSS Security Lunch: "Die Verbindlichkeit von Informationen im Internet"** Details, Anmeldung	Zürich
Mi, 28.03.2012	16:30 19:45	–	**ISSS St. Galler Tagung 2012 "iPhone im Unternehmen"** Details	St. Gallen
Di, 12.06.2012	13:30 18:00	–	**ISSS Zürcher Tagung 2012 - Wie sicher sind "sichere" IT-Systeme?** Sicherheitsprüfung von IT-Systemen - Lästige Pflicht oder zwingende Notwendigkeit? Details	Zürich
Di, 27.11.2012	13:00 17:30	-	**15. Berner Tagung für Informationssicherheit "Bring your own device: Chancen und Risiken"** Details	Bern

Nächste Events unserer Partner

Mo, 06.02.2012	13:30 18:00	–	**Meet the Wireshark Geek** Erleben Sie Gerald Combs, den Gründer des Open Source Netzwerkanalyse Tools Wireshark (vormals Ethereal) in Zürich. Die Teilnahme ist kostenlos. Details, Anmeldung	Zürich Airport

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

Impressum
Information Security Society Switzerland
Wasserwerkgasse 37
3000 Bern 13
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 http://www.isss.ch/