ISSS NewsFlash

Februar 2013

Editorial

Liebe ISSS-Mitglieder

Dank grossem Interesse unserer Mitglieder an der Thematik Sicherheit und Smart Grid hat der ISSS Vorstand die Gründung einer **Special Interest Group zum Thema „Smart Grid Security“** beschlossen. Die SIG wird ihre Aktivitäten im März aufnehmen.

Weiter kommt es zu einem **Re-Launch** der **Special Interest Group „Cloud Computing Security“** unter der neuen Leitung von Bernhard Tellenbach.

Im **März** würden wir Sie gerne an unserer vierten St. Galler Tagung zum Thema **“Secure Unified Communication in der Praxis”** begrüssen. Die Tagung war in den letzten drei Jahren immer schnell ausgebucht.

Weiter führen wir **im April** zwei Security Lunches in Bern und Zürich zum Thema **„Verteidigung unter Angriff: Gemessene und getestete Limiten unserer Sicherheitstechnologien“ durch**.

Das Thema **Bring your own Device (BYOD)** stiess schon an der Berner Tagung 2012 auf sehr grosses Interesse. Grund genug, im Januar zu diesem Thema 2 Security Lunches in Bern und Zürich durchzuführen, welche das Thema von der rechtlichen und der praktischen Seite her vertieften. Wer den Lunch verpasst hat, kann dies im Rückblick nachlesen.

Dr. Ursula Widmer
Präsidentin ISSS
president@isss.ch

Highlights in dieser Ausgabe

ISSS: News aus den Special Interest Groups

Gründung der Special Interest Group (SIG) zum Thema „Smart Grid Security“ wurde beschlossen: Wollen auch Sie dabei sein?

Im Nachgang an den ISSS Security Talk vom Juni 2012 in Bern zum Thema „Smart Grid – Intelligente Stromnetze: Chancen und Risiken für die Sicherheit“, welcher auf eine sehr grosse Resonanz gestossen ist, mit zahlreichen Rückmeldungen und der Bitte an ISSS, das Thema zu vertiefen, erfolgte im 2012 eine Umfrage bei unseren Mitgliedern, wer sich an einer Special Interest Group (SIG) „Smart Grid Security“ beteiligen möchte. Dank des grossen Rücklaufs interessierter ISSS Mitglieder hat der Vorstand nun im Januar beschlossen, diese SIG zu gründen.

Auch in der Schweiz befassen sich die Elektrizitätsversorgungsunternehmen, der Regulator, Behörden und Private vermehrt mit Themen der Informationssicherheit und dem Datenschutz im Zusammenhang mit den zunehmend intelligenten Netzen (Smart Grid) und der Vermessung des Stromverbrauchs bis in die Haushalte (Smart Metering). Informationssicherheit wird Akteure und Stromkonsumenten gleichermassen in Zukunft beschäftigen.

Zu den im Einzelnen an der **Kick-Off Telefonkonferenz im März 2013** noch zu priorisierenden Aufgaben dieser neu gegründeten SIG könnten unter anderem folgende Themen gehören:

- Analyse der wesentlichen Sicherheitsrisiken im Bereich Smart Grid
- Priorisierung dieser Risiken pro Zielgruppe
- Vorschlag von Massnahmen zur Vermeidung eines Risikoeintritts
- Bestandsaufnahme der regulatorischen / gesetzlichen Rahmenbedingungen für die Informationssicherheit von Smart Grid in der Schweiz, unter Berücksichtigung der Situation im Ausland (Deutschland, EU, USA etc.)
- Erkennen eines allfälligen regulatorischen / gesetzlichen Handlungsbedarfs in der Schweiz, unter Kontaktaufnahme und Zusammenarbeit mit den zuständigen Ansprechpartnern bei Bund, Regulator und Datenschutzbehörden. Insbesondere auch Mitwirkung in der Arbeitsgruppe des BFE zur Erarbeitung einer Smart Grid Road Map, soweit Sicherheitsaspekte betroffen sind
- Betrachtung von technische Lösungen
- Kontakte etablieren zu in- und ausländischen Organisationen mit vergleichbaren Aufgaben
- Unterstützung zur Vernetzung der Sicherheitsspezialisten der verschiedenen Elektrizitätsversorgungsunternehmen auf Basis des ISSS Angebots (SIG, Security Talks oder andere Events)
- Weitere Themen können je nach aktuellen Vorkommnissen und Dringlichkeit ebenfalls integriert und prioritär behandelt werden.

An dieser Stelle kann darauf hingewiesen werden, dass unter der Federführung des Bundesamtes für Energie BFE im Rahmen der Strategie Stromnetze eine Arbeitsgruppe gegründet wurde, an welcher sich ISSS ebenfalls beteiligen darf. In dieser Arbeitsgruppe wird eine **Smart Grid Road Map für die Schweiz** erarbeitet werden. Es sollen die Entwicklung nötiger Schlüsseltechnologien, Richtlinien und Standards sowie politische Rahmenbedingungen antizipiert und ein Fahrplan dafür erarbeitet werden. Insbesondere sollen auch mögliche Mindestanforderungen an Smart Meter im Rahmen der Vernehmlassungsvorlage Energiegesetzes und seiner Konkretisierung herausgearbeitet werden

Bringen Sie Ihr Wissen und Ihre Expertise ein und werden auch Sie Teil dieser neuen Special Interest Group „Smart Grid Security“.

Sind Sie interessiert? Dann melden Sie sich bitte per E-Mail bis Ende Februar 2013 bei Dr. Ursula Widmer, Präsidentin ISSS, president@isss.ch, unter Angabe Ihres Interessengebietes und Ihrer Erfahrung und insbesondere auch, wie Sie sich selber in diese SIG einbringen wollen. **Die Kick-Off Telefonkonferenz wird Anfang März stattfinden.** Die genaue Uhrzeit und die Einwahldaten werden den Interessierten, welche sich bereits angemeldet haben, und den Neuinteressenten Ende Februar direkt bekanntgegeben werden.

Dr. Ursula Widmer, Präsidentin ISSS, president@isss.ch

ISSS: News aus den Special Interest Groups

Re-Launch der Special Interest Group "Cloud Computing Security"

Neue Leitung und Neuausrichtung der SIG CCS per März 2013:

- Ideen und Anregungen zu Themen sind sehr erwünscht.
  Bitte bis spätestens 25.02.2013 an bernhard.tellenbach@isss.ch senden.
- An einer Mitwirkung interessierte Personen mit Affinität zu CCS melden sich bitte bis spätestens 25.02.2013 per Email an bernhard.tellenbach@isss.ch

Aus Anlass des Rücktritts von Umberto Annino als Leiter der SIG Cloud Computing Security (CCS) erfolgt ein Re-Launch der SIG CCS per Anfang März 2013. Die ISSS dankt Umberto Annino für seine Leistungen und bedauert, dass er aus beruflichen Gründen von diesem Amt zurücktritt.
Per Ende Februar übernimmt Bernhard Tellenbach, seit 2008 Vorstandsmitglied der ISSS, die Leitung der SIG CCS.

Bernhard Tellenbach ist Dozent für Informationssicherheit an der School of Engineering der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW). Er arbeitet am Institut für angewandte Informationstechnologie (InIT), wo derzeit unter der Leitung von Thomas Bohnert, das InIT Cloud Comuting Lab (ICCLAB) aufgebaut wird. Bernhard Tellenbach führt im Rahmen der angewandten Forschung und Entwicklung Projekte im Bereich der Informationssicherheit durch. Seine Interessens- und Forschungsschwerpunkte sind die Sicherung und Überwachung von Kommunikationsnetzen sowie die Computer- und Netzwerksicherheit im Allgemeinen. Er interessiert sich insbesondere auch für die Herausforderungen, welche die Auslagerung (von Teilen) der IT Infrastruktur in die Cloud, resp. die Verlagerung von Diensten in die Cloud mit sich bringen.

Ziele
In seiner Position an der Schnittstelle zwischen Forschung und Praxis sieht es Bernhard Tellenbach als eine der möglichen zukünftigen Aufgaben der SIG an, in Form einer Übersicht aufzuzeigen, welche Probleme und Visionen im Bereich Cloud Computing Security vorhanden sind und wohin die Reise gehen könnte. Aber auch Hilfestellungen bei der Wahl eines Cloud Providers resp. beim Entscheid für oder gegen ein „in die Cloud gehen" sind denkbar. Hier wäre insbesondere eine Hilfestellung im Hinblick auf die Bedeutung und Relevanz der verschiedenen Zertifizierungen und ein Überblick über die bestehenden und geplanten CC Security Standards wünschenswert.
Welches **konkrete Ziel** die SIG ab März als erstes verfolgen wird, soll am Kick-Off Meeting Anfang März **von den SIG Mitgliedern gemeinsam festgelegt** werden. Ideen und Anregungen sind willkommen! Bitte schicken Sie diese bis spätestens den 25.02.2013 an bernhard.tellenbach@isss.ch

Teilnehmende
Als Idealgrösse werden 8 – 12 Teilnehmende (pro bearbeitetem Thema) betrachtet. Wichtig ist die aktive Mitarbeit aller Personen, damit die spezifischen Erfahrungen 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.

Kick-Off Meeting
Das Kick-Off Meeting wird Anfang März stattfinden. Zeit und Ort werden noch bekanntgegeben. Es wird ein Termin gesucht, an dem möglichst viele der interessierten Personen teilnehmen können.
Falls Sie Ihre Expertise in die SIG CCS einbringen und mitmachen möchten, schicken Sie bitte ein Email mit Betreff SIG CCS bis spätestens am 25.02.2013 an bernhard.tellenbach@isss.ch

ISSS: News generell

Neue technische Richtlinie „Ersetzendes Scannen“ des BSI:

Beweiswert von gescannten Dokumenten

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat eine neue technische Richtlinie „TR 03138 Ersetzendes Scannen“ geschaffen.

In vielen Unternehmen und Behörden werden Papierdokumente zur Archivierung durch Scannen digitalisiert, damit sie in elektronischer Form in entsprechenden Archivsystemen aufbewahrt werden können. Beispiele hierfür sind die Aufbewahrung von Dokumenten und Belegen im Zusammenhang mit der elektronischen Führung der Geschäftsbücher oder die Digitalisierung von Patientenakten in Spitälern zur Langzeitaufbewahrung.

Aus rechtlicher Sicht sind auch elektronische Dokumente als Beweismittel zugelassen. Sie sind jedoch nur dann beweisrechtlich den Original-Papierdokumenten gleichwertig, wenn durch entsprechende organisatorische und technische Massnahmen sichergestellt ist, dass bei der Vorbereitung und Durchführung des Scanning-Prozesses zur Digitalisierung und während der anschliessenden Speicherung keine Verfälschungen des Inhalts erfolgt sind.

Diesem Ziel der Sicherung des Beweiswerts von gescannten Dokumenten dient die neue BSI-Richtlinie, indem sie den Unternehmen und den von ihnen beauftragten Dienstleistern Anweisungen für das rechtssichere Scannen von Originaldokumenten gibt. Die Richtlinie ist auch für Schweizer Unternehmen und Behörden interessant, da hierzulande eine vergleichbare Regelung bisher fehlt.

Stärkung von Europol zur Bekämpfung der Cyber-Kriminalität

Das neue Europäische Zentrum zur Bekämpfung der Cyber-Kriminalität (EC3) wurde auf Initiative der EU eingerichtet, welche es auch finanziert. Das EC3 ist bei Europol in den Haag angesiedelt und hat per Anfang dieses Jahres seinen Betrieb aufgenommen. Das EC3 soll in seinem Vollausbau, der in etwa zwei Jahren erreicht sein wird, um die 50 Spezialisten beschäftigen.

Cyber-Kriminelle agieren grenzüberschreitend, die staatlichen Strafverfolgungsbehörden sind dagegen in ihren Aktivitäten an die nationalen Grenzen gebunden. Dem soll mit dem EC3 entgegengewirkt werden, indem dieses eine führende Rolle bei der Koordination und Ausbildung der nationalen Strafverfolgungsbehörden sowie bei der Auswertung von beschlagnahmten Daten spielen soll.

Zum Aufgabenbereich des EC3 gehört insbesondere auch der Schutz der Infrastruktur Europas gegen Cyber-Attacken.

Die ISSS Special Interest Group Cyber Defense wird mit Interesse die weiteren Aktivitäten von EC3 verfolgen.

Vorschau: ISSS St. Galler Tagung vom 12. März 2013

ISSS St. Galler Tagung "Secure Unified Communication in der Praxis"

12. März 2013, 16.00-20.40, Migros Klubschulgebäude, St. Gallen

Flexible Kommunikationsmöglichkeiten gewinnen an Bedeutung im privaten wie auch geschäftlichen Umfeld. Der Wunsch, ständig erreichbar zu sein, hat zu Implementierungen von bestehenden Kommunikationsformen wie Email oder Chat auf Smart- und Mobiltelephonen geführt. Eine Herausforderung bei der Verwendung von Chat und Voice (Telephonanruf) auf einem Mobiltelephon ist, dass üblicherweise unterschiedliche Identitäten zum Einsatz kommen. In anderen Worten: für den Telephonanruf wird die Telephonnummer verwendet, für einen Chat mit einer Freundin ein Pseudonym im jeweiligen Chat-Programm. Eine grosse Herausforderung bereitet diese Zuweisung der jeweiligen Identität sowie die Kombination mehrerer Identitäten, wenn es um eine Kommunikation mit mehreren Medien geht, z.B. Video und Audio kombiniert mit Chat.

Unified Communication (dt. *einheitliche Kommunikation*) schafft hierbei Abhilfe: Sie integriert verschiedene Kommunikationsformen unter einer einheitlichen Identität und stellt diese in einem "Wähl"-Verzeichnis dem Anwender bereit. Unified Communication ermöglicht so eine nie dagewesene Flexibilität in der Kommunikation durch die Integration unterschiedlicher – Multimedia (Audio, Video, Chat) – Datenformate in einen Kommunikationsvorgang. Kleinere, mittlere wie auch grosse und grösste Unternehmen profitieren von Unified Communication täglich von Eigenschaften wie der transparenten Arbeitsplatzflexibilisierung (Stichworte: *FollowMe*, *remote Collaboration, Offshoring*) oder der vereinfachten Realisierung von Automatisierungsvorgängen (Business Process Integration). Audio, Video, Messaging, Präsentationen wie aber auch die Ansicht entfernter Bildschirminhalte auf Tisch-Computern, Laptops oder Smartphones gehören zu den Medien, die bei Unified Communication nicht mehr wegzudenken sind. Die Einschränkungen einzelner Technologien – beispielsweise SMS mit nur 160 Zeichen – verschwinden indem verbesserte, gleichartige Funktionen bereitgestellt werden.

Grundsätzlich ist die Bereitstellung einer Unified Communication Plattform somit ein einfaches Unterfangen: Ein Verzeichnisdienst, ein entsprechendes Tool – et voilà. In der Praxis zeigen sich jedoch weitere Herausforderungen, die für eine sichere Unified Communication gelöst werden müssen. Chancen und Möglichkeiten, welche die Unified Communication bietet, bringen Risiken und Herausforderungen mit sich, die es in der Praxis zu reduzieren und abzusichern gilt, um eine sichere, einheitliche Kommunikationsplattform zu erhalten: Secure Unified Communication.

Die klassischen drei Sicherheitseigenschaften – Vertraulichkeit, Integrität, Verfügbarkeit – müssen den firmenspezifischen Anforderungen entsprechend definiert und in den Applikationen umgesetzt werden. Zusätzlich müssen rechtliche Vorgaben berücksichtigt werden, insbesondere wenn geschäftsrelevante Beschlüsse mittels Unified Communication Lösungen gefasst werden. Durch eine verstärkte Integration von öffentlich verfügbaren Kommunikationsanbietern (zum Beispiel Skype mit Lync von Microsoft oder die Dienste von Facebook, Viber oder WhatsApp) müssen Fragen zum Informationsschutz beantwortet ebenso wie Herausforderungen durch privat eingesetzte Geräte gelöst werden.

Die diesjährige ISSS St. Galler Tagung bietet mit einem interessanten Programm Einblick in Grundlagen und Technologie von Secure Unified Communication ebenso wie Erfahrungen aus Sicht eines Telekommunikationsanbieters und eines Anwenders bei deren Einführung und Betrieb.

Dr. Lukas Ruf, Vorstand ISSS

Weitere Informationen/Anmeldeformular:
https://www.isss.ch/veranstaltungen/2013/st-galler-tagung/

Vorschau: ISSS Security Lunches im April 2013

Verteidigung unter Angriff:
Gemessene und getestete Limiten unserer Sicherheitstechnologien

9. April 2013, 12.00-14.00, Hotel Kreuz, Bern
10. April 2013, 12.00-14.00, Zunfthaus zur Meisen, Zürich

Sicherheit im Cyberspace ist ein unerlässliches und unabdingbares Gut für das Funktionieren unserer Gesellschaft und Wirtschaft geworden. Cyberkriminelle hingegen fordern unsere Verteidigungsfähigkeit sowie die Effektivität der eingesetzten Sicherheitsprodukte unter Verwendung innovativster Angriffsmethoden, Verschleierungstechniken und hochspezialisierter Malware permanent heraus. Firmen schützen sich typischerweise durch mehrere Verteidigungsringe (Layered Security), ausgestattet mit unterschiedlichsten Sicherheitstechnologien.

In diesem Vortrag werden die Ergebnisse einer Untersuchung präsentiert, in welcher die Angriffskette und die gemessene Effektivität typischer Sicherheitstechnologien wie Firewalls, Intrusion Prevention Systems (IPS), Next Generation Firewalls (NGFW) und Desktop Antivirus/Malware Detektion analysiert wurde. Es werden empirische Resultate zur Effektivität dieser Schutztechnologien basierend auf harten und realitätsnahen Tests von NSS Labs präsentiert und in einer Demonstration wird gezeigt, wie Malware diverse Sicherheitsringe erfolgreich durchbricht.

Die Untersuchung hat aufgezeigt, dass heute eingesetzte Sicherheitsprodukte beträchtliche Detektionslücken, Stabilitätsprobleme sowie Leistungslimiten aufweisen. Dadurch wird es möglich, interaktiv Exploits zu modellieren und zu korrelieren, welche diverse Verteidigungsringe erfolgreich durchdringen. Ebenfalls werden die angegriffenen Produkte sowie Softwarehersteller identifiziert und die Exploits werden mit deren Verfügbarkeit in unterschiedlichen Crimeware- und Penetrationtesting Tools verknüpft.

Biographische Angaben zum Referenten:

Dr. Stefan Frei, Research Director, NSS Labs Inc. Als Research Director bei NSS Labs untersucht Dr. Stefan Frei Entwicklungen im Bereich Cybercrime aus der Sicht der Angreifer, um Trends und Bedrohungen frühzeitig zu erkennen und Geschäftsentscheide mit Daten und Fakten zu unterstützen. Dr. Frei verfügt über 15 Jahren Erfahrung im Bereich Internet Security und entwickelte Kernkompetenzen in den Bereichen Penetration Testing, Datamining und Security Consulting auf Stufe Technik und Management. Er ist angesehener Sicherheitsexperte und spricht regelmässig an führenden Konferenzen wie ISF, BlackHat, Defcon, FIRST und RSA. Dr. Frei ist Dozent für Netzwerksicherheit an der ETH Zürich und hat Abschlüsse in Elektrotechnik und Technologie & Businessmanagement; zudem er ist Autor mehrerer anerkannter Publikationen.

Weitere Informationen/Anmeldeformular:

Für Bern: www.isss.ch/veranstaltungen/2013/security-lunch-2013-04-09/
Für Zürich: www.isss.ch/veranstaltungen/2013/security-lunch-2013-04-10/

Rückblick: ISSS Security Lunches vom Januar 2013

Sichere Unternehmensmobilität – technische Machbarkeit und rechtliche Absicherung: ISSS Security Lunches vom 23./24.1.2013 in Bern und Zürich

Über 30 Personen fanden sich am 23. Januar in der Schmiedstube in Bern und am 24. Januar im Zunfthaus zur Meisen in Zürich ein, um sich beim gemeinsamen Mittagessen in ungezwungener Atmosphäre auszutauschen sowie den spannenden Fachreferaten von Frau Dr. Ursula Widmer zum Thema „BYOD – Unternehmensmobilität rechtlich erfolgreich abgesichert?“ und von Herrn Oliver Rükgauer zum Thema „Sichere Unternehmensmobilität mit Mobile Application Management“ beizuwohnen. Die den Fachreferaten anschliessende intensive Diskussionsrunde mit vielen Fragen und äusserst praxistauglichen und detaillierten Antworten, aber auch konkreten aktuellen Erfahrungsberichten aus dem Publikum zum Thema BYOD (Bring Your Own Device) und Unternehmensmobilität spiegelte den wertvollen und inspirierenden Praxisbezug der beiden Referate eindrücklich wider.

Frau Widmer, Präsidentin der ISSS, Inhaberin der auf Informatik-, Internet- und Telekommunikationsrecht spezialisierten Anwaltskanzlei Dr. Widmer & Partner, Bern, und Lehrbeauftragte an der Universität Bern und der ETHZ (Recht der Informationssicherheit) betonte in ihrem Referat bezüglich der rechtlichen Absicherung von BYOD insbesondere die Wichtigkeit der Festlegung verbindlicher und klarer Regeln zwischen Arbeitgeber und Arbeitnehmer, sogenannter BYOD-Policies, bei der geschäftlichen Nutzung privater Geräte. Eine im 2012 durch die National Cyber Security Alliance / McAffee international durchgeführte Studie hätte gezeigt, dass hier noch grosser Handlungsbedarf bestünde. So haben momentan noch über 50% der Firmen, die ihren Mitarbeitenden den Gebrauch persönlicher Geräte wie Smartphones, Tablets oder Laptops zu Geschäftszwecken erlauben, entweder gar keine BYOD-Nutzungsbestimmungen oder diese den Mitarbeitern nur ungenügend kommuniziert.

Durch diese Unterlassung setzen sich die besagten Unternehmen grossen Risiken aus, denn für vielerlei Schäden (wie z.B. aus der Verletzung von Geheimhaltungspflichten, des Datenschutzes oder von Compliance-Anforderungen) bleiben diese ohne verbindliche und im Arbeitsvertrag oder Mitarbeiterreglementen verankerte Regeln weiterhin haftbar. Darüber hinaus dürfe jedoch auch die mögliche Haftbarkeit des Unternehmens gegenüber den eigenen Mitarbeitenden nicht ausser Betracht gelassen werden. So könne es beispielsweise passieren, dass bei einer durch das Unternehmen auf einem persönlichen Gerät eines Mitarbeitenden durchgeführten Löschaktion fälschlicherweise auch private Daten gelöscht würden, wofür der Arbeitgeber in der Folge haftbar gemacht werden könnte. Auch zur Minderung dieser Risiken können klare BYOD-Policies entscheidend beitragen, z.B. indem der Mitarbeitende verpflichtet werde, von seinen privaten Daten regelmässig Sicherungskopien zu erstellen.

Wegen der mit BYOD verbundenen Vermischung von Arbeits- und Privatbereich müssen in den Policies sodann im Zusammenhang mit arbeitsrechtlichen Gesichtspunkten klare Regelungen getroffen werden, so bezüglich der geschäftlichen Nutzungszeiten, um unzulässige Ferien-, Nacht- und Sonntagsarbeit und die daraus resultierenden finanziellen Ansprüche zu verhindern, und bezüglich des Umfangs der Kostentragung durch den Arbeitgeber für Beschaffung, Betrieb, Reparatur und Ersatz der privaten Geräte. Zudem dürfe bei der Einführung einer BYOD-Policy auch nicht vergessen werden, bei Beendigung des Arbeitsverhältnisses die Übergabe bzw. Löschung aller geschäftsrelevanten Daten auf den privaten Geräten des Arbeitnehmers unmissverständlich zu regeln.

Rückblick: ISSS Security Lunches vom Januar 2013

Sichere Unternehmensmobilität – technische Machbarkeit und rechtliche Absicherung: ISSS Security Lunches vom 23./24.1.2013 in Bern und Zürich. (Forts.)

Im anschliessenden zweiten Fachreferat demonstrierte Herr Oliver Rükgauer, Mitbegründer und Marketingleiter der in Bern ansässigen und auf Mobile Enterprise Solutions spezialisierten Firma Jakoa Mobile, anhand eines eindrücklichen Praxisbeispiels, wie sich die im jeweiligen Unternehmen geltenden BYOD-Nutzungsrichtlinien über ein als Cloud-Service implementiertes App Center zur Sicherung von iOS und Android Apps und zum Schutz von Unternehmensdaten zuverlässig auf Einhaltung überwachen und wo nötig auch aktiv durchsetzen lassen.

Voraussetzung für eine sichere und rechtskonforme Umsetzung von BYOD-Policies, so Herr Rükgauer, sei die möglichst vollständige Trennung von geschäftlichen und privaten Daten und Applikationen auf den Mobilgeräten. Bei diesem Ansatz könnten sich die Unternehmen auf den Schutz ihrer eigenen Daten und Applikationen beschränken, wobei die Privatsphäre der Mitarbeitenden gewahrt, gleichzeitig das Haftungsrisiko verringert und der Verwaltungsaufwand minimiert werde.

Wichtig sei es auch, betonte Herr Rükgauer, dass man bei BYOD und Unternehmensmobilität vermehrt den Benutzer und nicht die diversen Endgeräte ins Zentrum rücke, denn schliesslich sei es ja der Benutzer, der situationsspezifisch mit verschiedensten Geräten, aber häufig denselben Anwendungen orts- und zeitunabhängig auf die Unternehmensdaten zugreife.

Der Ansatz, die Sicherheit primär auf Applikations- und Datenebene und nicht auf Geräteebene zu implementieren, sei deshalb nicht nur naheliegender, sondern bei der immer kürzeren Lebensdauer und stetig ansteigenden Zahl der im Markt verfügbaren Gerätetypen auch einfacher umsetzbar. Das Produkt von Jakoa Mobile setze deshalb konsequent auf das Konzept des sogenannten „App Wrapping“, das es ermögliche, bestehende Apps ohne Änderung des Quellcodes sozusagen in eine Sicherheitshülle zu packen, die dann ihrerseits die Einhaltung der im Unternehmen geltenden BYOD-Nutzungsrichtlinie sicherstelle.

Zum Schluss des Vortrags wurde den Anwesenden live demonstriert, wie beispielsweise einer handelsüblichen App mittels „App Wrapping“ mit wenigen Mausklicken gezielt die Fähigkeit, Text über Copy/Paste in eine andere Anwendung zu übertragen, entzogen werden oder die Fähigkeit, Daten verschlüsselt auf dem Gerät abzulegen, hinzugefügt werden konnte.

Hanspeter Christ und Marc Rennhard, beide Vorstand ISSS
Hanspeter.Christ@swisstopo.ch und rema@zhaw.ch

Agenda: ISSS Events

Nächste ISSS Events

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

Datum	Zeit	Veranstalter	Titel und Details	Ort
Di, 12.03.2013	16:00 - 19:00	ISSS	**ISSS St. Galler Tagung: "Secure Unified Communication in der Praxis"** Details, Anmeldung	St. Gallen
Di, 09.04.2013	12:00 - 14:00	ISSS	**ISSS Security Lunch: "Verteidigung unter Angriff : Gemessene und getestete Limiten unserer Sicherheitstechnologien"** Details, Anmeldung	Bern
Mi, 10.04.2013	12:00 - 14:00	ISSS	**ISSS Security Lunch: "Verteidigung unter Angriff : Gemessene und getestete Limiten unserer Sicherheitstechnologien"** Details, Anmeldung	Zürich
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

Vorschau: Events unserer Partner

CeBIT Hannover (5. - 9. März 2013): Gratiseintritte für ISSS Mitglieder

Die CeBIT Hannover ist die weltweit wichtigste Veranstaltung der digitalen Wirtschaft. Sie ist der Treffpunkt für Experten, Meinungsbildner und Topentscheider der IT-Welt. Die CeBIT Hannover 2013 präsentiert sich auf vier Plattformen:

- CeBITpro zeigt die komplette Bandbreite der ITK-Technologien für Unternehmen.
- CeBITgov bietet einen Überblick über die aktuellen Anwendungen für öffentliche Verwaltungen und das Gesundheitswesen.
- Auf der CeBITlab treffen sich Produkt- und Unternehmensentwickler aus allen Branchen, um ihre Innovationen zu präsentieren.
- Auf der CeBITlife werden ITK-Lösungen für professionelle Anwender und hightech-begeisterte Konsumenten vorgestellt.

Verschaffen Sie sich einen 360° Überblick über die aktuellen Produktneuheiten innerhalb der vier wichtigsten Kernmärkte der digitalen Welt und besuchen Sie die CeBIT Hannover 2013.

Gratiseintritte für ISSS Mitglieder:
Sichern Sie sich Ihren Gratiseintritt: Als ISSS-Mitglied erhalten Sie ein **gratis eTicket für alle Tage der CEBIT** unter folgendem Link: http://www.t-link.ch/index.php?article_id=109&clang=0

Weitere Informationen zur CeBit 2013
Details

15. Jahresfachkonferenz "DuD - Datenschutz und Datensicherheit" (17 .- 18. Juni 2013): Rabatt für ISSS Mitglieder

Am **17. und 18. Juni 2013** findet in Berlin die **15. Jahresfachkonferenz „DuD – Datenschutz und Datensicherheit“** vom Veranstalter COMPUTAS statt.

Rabatt für ISSS Mitglieder
ISSS-Mitglieder können zum Spezialpreis von EUR 600.- für beide Tage (statt EUR 1‘695.-) an der DuD teilnehmen. Bitte in der Anmeldung "ISSS-Mitglied" angegeben, damit Sie vom Rabatt profitieren können.

Weitere Informationen zur DuD:
Details

Vorschau: Events unserer Partner

InfoSocietyDays 2013 (4. - 8. März 2013): 15% Rabatt für ISSS Mitglieder

Vom 4.-8. März 2013 finden im Kongresszentrum der BERNEXPO die InfoSocietyDays 2013 statt, bei welchen auch die ISSS Partner ist.

Über 1‘000 Interessierte aus Wirtschaft, Verwaltung und Gesundheitswesen nehmen jedes Jahr an den InfoSocietyDays in Bern teil. Der Kongress für Anwendungen der Informations- und Kommunikationstechnologien (ICT) behandelt mit den drei Foren Swiss eEconomy Forum, Swiss eGovernment Forum und Swiss eHealth Forum drei wichtige Kernthemen der Informationsgesellschaft. Der Fokus liegt auf Einsatz und Nutzen der ICT für Wirtschaft, Verwaltung und Gesundheitswesen.

Swiss eEconomy Forum
4. März 2013 **Intelligent vernetzt – Lösungen für Unternehmen**

Die Digitalisierung und Vernetzung unserer Wirtschaft schreiten rasch voran. Cloud Computing und Social Media sind die meist diskutierten Themen der letzten Zeit. Im Swiss eEconomy Forum wird im Rahmen der 16. InfoSocietyDays in Bern aufgezeigt, was das digital vernetzte Unternehmen tun kann, um die Effizienz und Wettbewerbsfähigkeit zu steigern.

Die Plenumsreferate schaffen Überblick und zeigen Trends. Handlungsempfehlungen zu vier HotTopics helfen, Entscheide zur Optimierung von Geschäftsprozessen in die richtige Richtung zu lenken. Am Nachmittag geben interaktive Workshops Gelegenheit, die Thematik aus verschiedenen Blickwinkeln zu vertiefen. In Solution-Präsentationen werden wegweisende Projekte und innovative Konzepte vorgestellt.

Swiss eHealth Forum
Kongress für ICT-Anwendungen im Gesundheitswesen.

Wer im Gesundheitswesen auf der Suche nach Innovation und zukunftsweisenden Lösungen ist, findet diese am Swiss eHealth Forum 2013 in Bern. Die diesjährigen Leitthemen des Forums sind:
7. März 2013 **Elektronisches Patientendossier – Wege zur pragmatischen Umsetzung**
Mit speziellem Thementrack für Ärzte
8. März 2013 **Intelligent vernetzt – Lösungen für die integrierte Versorgung**
Mit speziellen Thementracks IHE und Gesundheitsinformatik

Swiss eGovernment Forum
Kongress für ICT- Anwendungen in der Verwaltung.

Wer in der Verwaltung auf der Suche nach Innovation und zukunftsweisenden Lösungen ist, findet diese am Swiss eGovernment Forum 2013 in Bern. Die diesjährigen Leitthemen des Forums sind:
5. März 2013 **Innovation in der Verwaltung – Besser. Schneller. Effizienter**
6. März 2013 **Elektronische Verwaltungsprozesse – Transparent. Nachvollziehbar. Rechtskonform**
Mit speziellem Thementrack für Städte und Gemeinden

Rabatt für ISSS Mitglieder
ISSS-Mitglieder erhalten 15% Rabatt auf 1-Tagesticket oder 2-Tagesticket an allen Foren. In der Anmeldung muss unter Coupon-Code "ISSS-B0X8FPL-15%" angegeben werden

Weitere Informationen / Anmeldung zu den InfoSocietyDays:
Details

Vorschau: Events unserer Partner

D·A·CH Security 2013 (17. - 18. September 2013) – Call For Papers

Nürnberg, 17. und 18. September 2013
Ziel der Veranstaltung ist es, eine interdisziplinäre Übersicht zum aktuellen Stand der IT-Sicherheit in Industrie, Dienstleistung, Verwaltung und Wissenschaft in Deutschland, Österreich und der Schweiz zu geben. Insbesondere sollen Aspekte aus den Bereichen Forschung und Entwicklung, Lehre, Aus- und Weiterbildung vorgestellt, relevante Anwendungen aufgezeigt sowie neue Technologien und daraus resultierende Produktentwicklungen konzeptionell dargestellt werden. Da IT-Sicherheit integrierter Bestandteil nahezu aller informationstechnischer Anwendungen und Prozesse ist, sind auch Beiträge zu rechtlichen Rahmenbedingungen und wirtschaftlichen Faktoren gewünscht.

Themen dieser Arbeitskonferenz

- Risiko- und Sicherheitsmanagement
- IT-Compliance
- Incident Handling und Business Continuity
- Sichere elektronische Geschäftsprozesse
- Multimedia und On-Demand-Dienste
- Identitäts- und Rechtemanagement
- Schutz kritischer Infrastrukturen
- Biometrische Verfahren und Anwendungen
- Computerkriminalität und Gegenmaßnahmen
- Botnetze, Spam und Phishing
- Trusted Computing und DRM
- Security Awareness
- Secure Embedded Systems
- WLAN, Mobilfunk und mobile Endgeräte
- Cloud- und Grid-Computing
- eGovernment, eHealth und eCommerce
- Sichere Webservices
- Sicherheit im automotiven Umfeld
- Aktuelle Angriffstechniken
- Industriespionage
- Sichere Steuerung von Industrieprozessen
- Verfügbarkeit und Notfallplanung
- Sicherheitsaspekte mobiler Betriebssysteme
- Intrusion Detection und Computer-Forensik
- Sicherheitsinfrastrukturen und PKI
- Authentifikation und Single-Sign-On
- Protokollierung und Überwachung
- Modellierung von Sicherheit
- Sicherheitstoken, Smartcards und RFID
- Pervasive und Ubiquitous Computing
- Netzwerklösungen, VPN und Remote Access
- Bürgerportal und neuer Personalausweis
- Jugendmedienschutz und Altersverifikation
- Netzzugang, Netzsperren
- Elektronische Signatur und Archivierung
- Netzneutralität
- Sichere Migration von Betriebssystemen
- Privacy, Datenschutz und Rechtsfragen
- Folgen, Akzeptanz, Trends und Perspektiven

Fachbeiträge und Überblicksarbeiten zu diesen und verwandten Themen sind als Extended Abstract (anonymisiertes PDF-Dokument in Deutsch, mindestens 4 DIN A4-Seiten), aus dem die Kernaussagen klar ersichtlich sind, unter https://syssec.at/conf einzureichen. Der Tagungsband wird zur Konferenz erscheinen.

Termine:

Einreichung des Extended Abstract:	**15. April 2013**
Benachrichtigung über die Annahme:	13. Mai 2013
Einreichung der Langfassung:	24. Juni 2013

Details zur Konferenz:
http://www.syssec.at/dachsecurity2013/

Agenda: Security Events unserer Partner

Nächste Security Events unserer Partner

Datum	Zeit	Veranstalter	Titel und Details	Ort
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 - Fr, 26.02.-01.03.2013	ganztags	RSA Conference	**RSA Conference 2013** TeleTrusT präsentiert an der RSA Conference 2013: IT Security made in Germany. Details, Anmeldung	San Francisco, USA
Mo - Fr, 04.03.-08.03.2013	ganztags	BERNEXPO	**InfoSocietyDays** ISSS Mitglieder erhalten 15% Rabatt. Rabatt Code: ISSS-B0X8FPL-15% Details, Anmeldung	Bern
Di - Sa, 05.03.-09.03.2013	ganztags	CeBIT	**CeBIT 2013** Freikarten zum Besuch der CeBIT 2013 für ISSS Mitglieder. Details, Anmeldung	Hannover, Deutschland
Di, 12.03.2013	18:30 - 23:30	DEFCON Switzerland	**DEFCON Switzerland Beer on Tuesday** Ort: Blues Bar, Speichergasse 29, 3000 Bern Die Teilnahme ist kostenlos. Details	Bern
Mo - Di, 17.06.-18.06.2013	ganztags	COMPUTAS	**DuD 2013 - Datenschutz und Datensicherheit** Spezialpreis (EUR 600.-) für ISSS-Mitglieder. Details, Anmeldung	Berlin
Di - Mi, 17.09.-18.09.2013	ganztags	GI, OCG, BIT-KOM, TeleTrusT	**D.A.CH Security 2013** Interdisziplinäre Übersicht zum aktuellen Stand der IT-Sicherheit in Industrie, Dienstleistung, Verwaltung und Wissenschaft. Details	Nürnberg, Deutschland

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

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, 11.02.-15.02.2013	08:30 - 17:00	Swiss Infosec AG	Vorbereitung CISSP Erfolgreiche CISSP-Zertifizierung dank seriöser Vorbereitung! Die Certified Information Systems Security Professional (CISS 4925.- Details	Zürich
Mo - Fr, 25.02.-01.03.2013	09:00 - 17:00	Swiss Infosec AG	Corporate Security Officer, Beauftragter Gesamtsicherheit Sicherheit ganzheitlich betrachtet! Wir vermitteln Ihnen eine umfassende 360°-Sicht zum Thema Integrale Sicherheit. 4200.- Details	Sursee
Mo - Do, 04.03.-07.03.2013	09:00 - 17:00	Swiss Infosec AG	Sicherheitsmanagement im IT-Umfeld Lehrgang Management und Grundlagen der IT-Sicherheit: Mehr Sicherheit dank sicherer Technik! 3500.- Details	Sargans
Mo - Fr, 04.03.-08.03.2013	10:00 - 16:00	Swiss Infosec AG	Betrieblicher Datenschutzverantwortlicher Wir führen Sie in die Aufgaben eines Datenschutzverantwortlichen ein und zeigen Problemstellungen aus der Praxis auf. 4200.- Details	Olten
Mo - Mi, 04.03.-06.03.2013	13:30 - 16:30	iimt	Organisational Behaviour & HR Management - Module 1 Personality / Teamwork / Motivation / Organisational Justice / Employee Engagement CHF 1900 Details, Anmeldung	Freiburg

Information Security Society Switzerland (ISSS)
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