ISSS NewsFlash

April 2013

Editorial

ISSS wird 20 Jahre alt: Feiern Sie mit uns dieses Jubiläum im Anschluss an unsere Generalversammlung am 24. April 2013.

Als eines unserer Jubiläumsgeschenke laden wir am 25. April Studierende zu einem kostenlosen ISSS Security Talk zum Thema "Hacking for Fun and Profit" ein. Lesen Sie mehr dazu in dieser Ausgabe.

Wer sich für operationelle Risiken im Finanzbereich interessiert findet an der ISSS Zürcher Tagung vom 5. Juni hochqualifizierte Referenten und interessante Teilnehmer zum Networken.

Und wer sich fachlich mit Gleichgesinnten zu den Themen Cloud Computing Security und Smart Grid Security austauschen möchte, laden wir herzlich ein, in diesen Special Interest Groups mitzuwirken.

Verpassen Sie auch nicht den TeleTrusT Informationstag "IT-Sicherheit im Smart Grid" und die Swiss Cyber Storm Konferenz 4, für welche ISSS-Mitglieder 20% respektive 15% Rabatt erhalten.

Alle weiteren Security Events finden Sie auch im Veranstaltungskalender auf unserer Website www.isss.ch, wo Sie sich auch gleich dazu anmelden können.

Dr. Ursula Widmer
Präsidentin ISSS
president@isss.ch

Highlights in dieser Ausgabe

Generalversammlung und Jubiläumsfeier 20 Jahre ISSS

Am 24. April 2013 sind wir mit unserer diesjährigen Generalversammlung zu Gast bei der Interxion (Schweiz) AG in Zürich Glattbrugg. Vorweg wird Peter Moebius, Managing Director von Interxion (Schweiz), aus seiner Optik die Vor- und Nachteile des Standortes Schweiz für ein Data Center darstellen. Im Anschluss an die Generalversammlung werden wir mit Ihnen das 20-jährige Jubiläum von ISSS feiern dürfen. Im Mittelpunkt steht das Referat von Herrn Prof. Dr. Ueli Maurer. Melden Sie sich rasch an.

Datum:	**Mittwoch, 24. April 2013**
Ort:	Interxion (Schweiz) AG, Sägereistrasse 35, 8152 Glattbrugg, Lageplan
	Die Teilnehmer benötigen für den Zutritt zur Gastgeberin einen gültigen Personalausweis (Pass, Identitätskarte oder Führerausweis)
Anmeldung:	Eine Anmeldung auf: https://www.isss.ch/veranstaltungen/2013/isss-generalversammlung-2013/ ist erforderlich. **Anmeldeschluss ist der 22.4.2013, 12:00 Uhr**
Teilnahme:	ISSS-Mitgliedschaft ist erforderlich. Eine Stimmvertretung für abwesende Mitglieder ist nicht möglich.
Kosten:	Gratis

Programm Generalversammlung

16:00	Begrüssung
16:10	**„Standort Schweiz: Attraktiv für Datacenter?“** Peter Moebius, Managing Director, Interxion (Schweiz) AG
16:30	**Generalversammlung** der Information Security Society Switzerland
17:30	Ende der Generalversammlung / Pause

Programm Jubiläumsfeier 20 Jahre ISSS

18:00	**Keynote: "Hat die Kryptografie in der heutigen Praxis versagt? Neue Ansätze in der Informationssicherheit"** Prof. Dr. Ueli Maurer, Professor für Informatik, ETH Zürich
19:00	**Apéro riche** mit Networking und **Betriebsbesichtigung der Interxion (Schweiz) AG** in kleinen Gruppen
21:00	Ende der Veranstaltung

Die Traktanden der Generalversammlung finden Sie auf der Webseite
https://www.isss.ch/veranstaltungen/2013/isss-generalversammlung-2013/
Die dazugehörigen Beilagen sind online in der ISSS Member Area verfügbar
https://www.isss.ch/mitgliederbereich/gv.php?page=gv.

Jubiläumsfeier 20 Jahre ISSS

Nehmen Sie an unserer Jubiläumsfeier teil, welche am 24. April 2013 um 18.00 Uhr mit dem Referat einer der „Gründungsväter“ von ISSS startet, mit Herrn Prof. Ueli Maurer zum Thema:

„Hat die Kryptografie in der heutigen Praxis versagt? Neue Ansätze in der Informationssicherheit“

Abstract des Referates:

Gegen kryptografische Protokolle (z.B. TLS) werden immer wieder zahlreiche Angriffe gefunden. Mit Hilfe von Patches werden die gefundenen Löcher jeweils wieder gestopft, bis neue Attacken entdeckt und Probleme gefunden werden. Angesichts dieser unbefriedigenden Situation stellt sich die grundsätzliche Frage, ob mit Hilfe der Kryptografie überhaupt sichere Systeme konstruiert werden können.

In seinem Vortrag zeigt Prof. Maurer die historische Entwicklung der Kryptografie auf, untersucht den Grund für die genannten Probleme und wirft einen Blick in die Zukunft der Kryptografie. Ein neues Paradigma, konstruktive Kryptografie genannt, wird vorgestellt. Sie erlaubt einen systematischen und beweisbaren Entwurf von Protokollen, was wesentlich zur künftigen Informationssicherheit beitragen wird."

Biographische Angaben zum Referenten:

Ueli Maurer ist ordentlicher Professor für Informatik an der ETH Zürich und Leiter der Forschungsgruppe für Informationssicherheit und Kryptografie. Seine Forschungsschwerpunkte sind Informationssicherheit, Theorie der Kryptografie, Anwendungen der Kryptografie (z.B. Hashfunktionen, symmetrische Verschlüsselung, digitale Signaturen, Public-Key Infrastrukturen, digitale Zahlungssysteme, E-Voting), theoretische Informatik, diskrete Mathematik und Informationstheorie. Er interessiert sich auch für die Auswirkungen der Informationstechnologie auf die Wirtschaft und die Gesellschaft.

Ueli Maurer diplomierte 1985 als Elektroingenieur an der ETH Zürich und promovierte 1990. Bis 1991 war er DIMACS Research Fellow an der Princeton University und kam 1992 an das Informatikdepartement der ETH. Er nimmt viele Aufgaben als Editor und Programmkomiteemitglied wahr. Maurer ist IEEE Fellow, IACR Fellow, Mitglied der Deutschen Akademie der Wissenschaften (Leopoldina), er war der 2000 Rademacher Lecturer am Department of Mathematics der University of Pennsylvania und ist häufiger Keynote Speaker an wissenschaftlichen Kongressen.

Ueli Maurer ist im Rahmen verschiedener Mandate in der Wirtschaft verankert. Unter anderem war er Verwaltungsrat der Tamedia AG, ist Mitglied des wissenschaftlichen Beirates von PricewaterhouseCoopers, sowie Mitgründer der Zürcher Sicherheitssoftwarefirma Seclutions AG, die mittlerweile an Phion verkauft wurde. Er patentierte mehrere kryptographische Verfahren und ist häufiger Interviewpartner der Medien.

Vorschau: ISSS Zürcher Tagung vom 5. Juni 2013

IT Sicherheit im Finanzbereich – Vom schwierigen Umgang mit operationellen Risiken

5. Juni 2013, 09.00 - 17.00 Uhr, Hotel Widder, Augustinergasse 24, 8001 Zürich

Ich lade Sie am 5. Juni 2013 ins Hotel Widder zur diesjährigen ISSS Zürcher Tagung ein. Operationelles Risikomanagement spielt nicht nur im Finanzsektor eine kritische und immer mehr an Bedeutung zunehmende Rolle. Dieses Thema wird ganzheitlich beleuchtet, beginnend mit den Anforderungen der Regulatoren und den juristischen Hintergründen des Rechnungslegungsrechts über zivil- und strafrechtliche Konsequenzen bei Verletzung dieser Anforderungen bis hin zu konkreten Implementierungsbeispielen von Rahmenwerken und Krisenmanagement-Prozessen für den Fall der Fälle. Es wird besonderer Wert darauf gelegt, dass nicht nur die Finanzdienstleister selbst, sondern auch deren Zulieferer und Leistungsempfänger von der Tagung profitieren werden. Hochkarätige Referenten und über 100 Fachexperten und Entscheidungsträger aus den Bereichen IT-Sicherheit und IT Risiko-Management werden an der Tagung zusammentreffen, um ihre Rollen im Kontext des Operationellen Risikomanagements zu diskutieren, zu verstehen und zu positionieren. Ich freue mich, Sie am 5. Juni begrüssen zu dürfen.

Frank Heinzmann, Head Operational Risk Management UBS Switzerland IT, UBS AG,
Vorstand ISSS und Tagungsmoderator, frank.heinzmann@isss.ch

Anmeldung: https://www.isss.ch/veranstaltungen/2013/zuercher-tagung/

Programm:

08.30	**Kaffee / Registrierung**
09.00	**Begrüssung** *Dr. Ursula Widmer, Rechtsanwältin, Dr. Widmer & Partner, Rechtsanwälte, Präsidentin ISSS*
09.15	**Keynote: "In The Eye Of The Storm: Risiken der Politik für den Finanzplatz Schweiz"** *Hans Kaufmann, Nationalrat (angefragt)*
10.00	**"Operationelle Risiken im Kapitalmarkt gestern, heute und morgen"** *Prof. Dr. Hannes P. Lubich, Dozent für ICT System & Service Management, FH Nordwestschweiz*
10.30	**"Einführung in die regulatorischen Anforderungen und deren Prüfung"** *Referent: Eidgenössische Finanzaufsicht FINMA (angefragt)*
11.00	**Kaffeepause**
11.30	**"Zivil- und strafrechtliche Konsequenzen bei Verletzung der regulatorischen Anforderungen"** *Prof. Dr. Rolf Sethe LL.M., Lehrstuhl für Privat-, Handels- und Wirtschaftsrecht, Universität Zürich (angefragt)*
12.00	**"Praktische Auswirkungen des Rechnungslegungsrecht auf das Risikomanagement von Finanz- und Industrieunternehmen sowie deren Kunden"** *Hans-Peter Wyss, Partner Audit & Advisory, Deloitte*
12.30	**Stehlunch**
14.00	**"Globales Operational Risk Management in der Praxis"** *Claus Norup, Managing Director, Head Operational Risk Management IT, UBS AG*
14.30	**"Operationelle Risiken reduzieren und sich zu Nutzen machen: Pragmatische Ansichten des Risikoverantwortlichen"** *Alfred Martin, Berater Operatives Bankgeschäft, Schweizerische Nationalbank*
15.00	**Kaffeepause**
15.30	**"IT Operation under fire - Umgang mit realen Bedrohungen in der Praxis"** *Dr. Olaf Ziegra, Regional Sales Manager Central Europe, Sourcefire Germany GmbH*
16.00	**"Krisenmanagement: Kommunikation von Vorfällen zu Kunden, Regulatoren und Mitarbeitern"** *Marco Marchesi, Chairman, ISPIN AG*
16.30	**Podiumsdiskussion** *Moderation: Dr. Lukas Ruf, Geschäftsführer, Consecom AG*
17.00	**Ende der Veranstaltung**

Vorschau: ISSS Security Lunch vom 28. Mai 2013

ISSS Security Lunch vom 28. Mai 2013:
„Sichere Verwendung von unsicherem Cloudspeicher mit SecureFolder Mobile"

12.00 -14.00 Uhr, Ristorante Certo, Zürich

In der heutigen Zeit werden die Speichermöglichkeiten im Internet immer extensiver genutzt, sowohl von privaten Nutzern als auch von Firmen. Angebote wie Dropbox bieten eine komfortable Art, auch grössere Dateien zu teilen und zu synchronisieren. Dabei wird die Sicherheit der Daten jedoch oft grob vernachlässigt. Für Firmenkunden ist in diesem Zusammenhang nicht nur die gesicherte Speicherung der Daten selbst essentiell, sondern auch die Möglichkeit, dass sich der Zugriff auf die Daten feingranular einschränken und damit kontrollieren lässt.

In diesem Referat stellen wir eine Lösung vor, welche die sichere Ablage von Daten auf unsicheren Cloudspeichern zulässt. Dabei wird der Komfort des einfachen Teilens von Daten beibehalten. Unsere Lösung bietet Unternehmen die Möglichkeit, den Mitarbeitern Speicherung in der Cloud zu ermöglichen, wobei die Datenhoheit aufrecht erhalten bleibt. Die erarbeitete Lösung funktioniert grundsätzlich unabhängig vom konkreten Speicheranbieter und dem verwendeten Client-Gerät (Mobile oder Desktop) und kann auch mit Netzwerkdateisystemen benutzt werden.

Im Referat wird der Schwerpunkt auf der Nutzung mit mobilen Geräten liegen. Dabei wird einerseits auf die technischen Aspekte eingegangen – insbesondere wie die Sicherheit und die Unabhängigkeit vom Speicheranbieter erreicht wird – und andererseits auf die Verwaltung und das Management der Applikation selbst, damit diese auch im Firmenumfeld effizient genutzt werden kann. Im Rahmen einer Demonstration werden Sie zudem einen konkreten Einblick in die praktische Anwendung der Lösung erhalten.

Biographische Angaben zu den Referenten:

Philipp Meier

David Reber

Philipp Meier und David Reber sind Software Engineers im R&D Team von Secude.
Beide erhielten 2012 den Bachelor of Science in Software Systems der Hochschule Luzern. Die Realisierbarkeitsstudie zu der im Referat vorgestellten Lösung haben die Referenten im Rahmen ihrer Bachelorarbeit an der Hochschule Luzern erstellt.
Nach dem Abschluss des Studiums sind sie bei der Firma Secude als Security Engineers eingestiegen und arbeiten nun daran, die Lösung zu einem professionellen Produkt weiterzuentwickeln.

Weitere Informationen und Anmeldung:

www.isss.ch/veranstaltungen/2013/security-lunch-2013-05-28/

ISSS: News aus den Special Interest Groups

Kickoff-Telco der neuen ISSS Special Interest Group (SIG) „Smart Grid Security“:

Anlässlich der Kickoff-Telco, an welcher Vertreter der Akteure des Energiesektors teilnahmen (Industrie, Energieversorger, Anwender und Dienstleister aus der IT-Security Branche, Forschung und Lehre), wurden die für die Arbeitsgruppe massgeblichen Themen aus Optik der Akteure dargestellt. Als erste Schritte werden nun die für die Smart Grid Security massgeblichen, vorbestehenden Dokumente auf nationaler, europäischer und internationaler Ebene gesammelt und allen Teilnehmern auf einer gemeinsamen Plattform zur Verfügung gestellt. Es wird dann darum gehen, diese zu analysieren und deren Relevanz für die Schweiz festzulegen. Weiter wird sich die Arbeitsgruppe mit der Smart Grid Road Map für die Schweiz des Bundesamtes für Energie näher auseinandersetzen und sich durch die Einladung eines Referenten des BFE die weiteren Schritte erläutern lassen und die mögliche Kooperation von ISSS festlegen.

Teilen auch Sie Ihr Wissen mit und bringen Sie Ihre Expertise ein, indem Sie dieser neugegründeten Special Interest Group Smart Grid Security (SGS) beitreten. Bei Interesse melden Sie sich doch bitte bei Frau Dr. Ursula Widmer, Präsidentin ISSS, president@isss.ch.

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

Erste Arbeitssitzung der ISSS Special Interest Group (SIG) „Cloud Computing Security“: Arbeitsprogramm 2013 festgelegt

Beim ersten Treffen der SIG Cloud Computing Security (CCS) unter dem Lead von Bernhard Tellenbach, Vorstand ISSS, diskutierten die neun anwesenden SIG Mitglieder angeregt über die Ziele, welche die SIG verfolgen soll. Dabei kamen verschiedene Ideen zur Sprache, wie z.B. die Veröffentlichung eines White Papers zu einer konkreten Problemstellung, wo existierende Leitfäden bisher keine oder zu wenig Hilfestellung bieten oder die Publikation einer Übersicht zu bestehenden und zukünftigen Zertifizierungen.

Durchgesetzt hat sich schliesslich die Idee, dass die SIG eine standardisierte Präsentation zum Thema Cloud & Security zusammenstellt, die die relevanten Cloud Security Themen für die Zielgruppe “grössere KMUs” beinhaltet. Diese Präsentation soll dann von jedem SIG Mitglied jeweils mindestens dreimal gehalten werden und zwar insbesondere an Veranstaltungen anderer Organisationen (Handels- und Industrievereine, KMU-Verbände, Cloud Computing Gruppierungen etc.), welche die gewählte Zielgruppe als Mitglieder haben oder ansprechen.

Um das Rad nicht neu zu erfinden, wird die SIG CCS für die Erstellung der Präsentation als erster Schritt eine ausführliche Recherche bezüglich hierfür verwertbarer Materialien/Literatur durchführen. Anschliessend wird entschieden, welche Inhalte die Präsentation genau umfassen soll.

Gleichzeitig sucht die SIG CCS den Kontakt zu anderen Gruppierungen mit ähnlicher Zielsetzung, denn Doppelspurigkeiten sollen vermieden und vorhandenes Know-How optimal genutzt werden.

Das nächste Treffen der SIG CCS ist im Mai im HB Zürich geplant. Wer sich für eine Teilnahme interessiert, kann sich informieren oder anmelden bei bernhard.tellenbach@isss.ch

Bernhard Tellenbach, Vorstand ISSS
Lead ISSS SIG Cloud Computing Security
bernhard.tellenbach@isss.ch

Information Security Society Switzerland

ISSS: News

Bundesrat schlägt Einführung des Staatstrojaners vor

Der Bundesrat hat die Botschaft zu einer grundlegenden Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) verabschiedet und zur Beratung an das Parlament überwiesen.

Wie allgemein erwartet worden war, sieht die Revision auch eine ausdrückliche Regelung für den Einsatz von Software zur Überwachung von Computern, allgemein als Staatstrojaner bezeichnet, vor. Derartige Software wurde von den Strafverfolgungsbehörden verschiedentlich bereits eingesetzt, jedoch war bisher unklar, ob hierfür eine genügende Rechtsgrundlage besteht. Dies soll nun mit der Revision des BÜPF und einer damit verbundenen Anpassung der Strafprozessordnung geändert und klargestellt werden.

Gemäss Vorschlag des Bundesrates ist der Einsatz von Staatstrojanern ausschliesslich auf die Überwachung der Telekommunikation beschränkt. Mit dem Staatstrojaner sollen verschlüsselt über das Internet abgewickelte Kommunikationen (z.B. E-Mails und Internet-Telefonie) überwacht und deren Inhalt erkannt und die Randdaten (Absender, Empfänger, Zeitpunkt, Dauer der Kommunikation) aufgezeichnet werden können, indem die Trojaner-Software die entsprechenden Daten erfasst, bevor sie zum Versand verschlüsselt werden.

Nicht vorgesehen ist dagegen, dass Staatstrojaner, was technisch möglich wäre, generell für die Durchsuchung von Festplatten oder für die Überwachung von Räumen und Personen durch Aktivierung der in die Computer eingebauten Kameras und Mikrofone eingesetzt werden dürfen.

Der Einsatz eines Staatstrojaners ist nach dem Revisionsentwurf zudem nicht präventiv möglich, sondern nur im Rahmen der Aufklärung von besonders schweren Straftaten und unter der Voraussetzung, dass andere, weniger einschneidende Aufklärungsmittel erfolglos waren oder als aussichtslos oder unverhältnismässig erscheinen. Der Einsatz muss zudem durch die Staatsanwaltschaft angeordnet und von einem Gericht genehmigt werden.

Im Gesetzesentwurf ebenfalls vorgesehen ist eine Verlängerung der Aufbewahrungsdauer für die Kommunikationsranddaten, welche die Fernmeldedienstanbieter aufzeichnen müssen und welche für die rückwirkende Überwachungen ausgewertet werden können. Die Aufbewahrungsdauer soll neu 12 statt 6 Monate betragen.

Zudem soll der Geltungsbereich des Gesetzes, der bisher auf die Fernmeldedienstanbieter beschränkt war, erheblich ausgeweitet werden. Neu sollen auch Hosting-Provider, Chat-Betreiber und Betreiber von Plattformen zum Dokumentenaustausch, Betreiber von firmen- oder hausinternen Netzen, die Dritten den Zugang dazu zur Verfügung stellen (z.B. Hotels, Spitäler, Schulen) dem Gesetz unterstellt werden, wobei jedoch der Umfang der ihnen obliegenden Pflichten entsprechend der Art ihrer Tätigkeit abgestuft ist. Sie sind insbesondere verpflichtet, den Zugang zur ihren Anlagen zu gewähren, für die Überwachung erforderliche Auskünfte zu erteilen und Randdaten, soweit bei ihnen verfügbar, zu liefern.

Bemerkenswert ist schliesslich, dass der Bundesrat in seinem Entwurf am Grundsatz festhält, dass die Fernmeldedienstanbieter für den Aufwand, welcher ihnen die Durchführung von Überwachungen verursacht, entschädigt werden sollen. Im Rahmen einer früher durchgeführten Vernehmlassung über den Gesetzesentwurf bei den interessierten Kreisen, war dieser Punkt umstritten; teils wurde der vollständige Verzicht auf eine Entschädigung gefordert, teils eine Ausweitung in dem Sinn, dass nicht nur der Aufwand für Überwachungsmassnahmen, sondern auch die Kosten für die erforderlichen technischen Investitionen zu entschädigen seien.

Es ist zu erwarten, dass das Gesetz im Parlament zu kontroversen und umfangreichen Diskussionen Anlass geben wird, und man darf gespannt sein, in welcher Form das Gesetz am Ende vom Parlament beschlossen wird.

Rückblick: ISSS Security Lunches vom 9. und 10. April 2013

ISSS Security Lunches: „Verteidigung unter Angriff : Gemessene und getestete Limiten unserer Sicherheitstechnologien“

9. April 2013 in Bern und 10. April 2013 in Zürich

Rückblick verfasst von Prof. Dr. Marc Rennhard, Vorstand ISSS:

Wie effektiv schützen eigentlich die heute eingesetzten Sicherheitstechnologien wie Next Generation Firewalls (NGFW), Intrusion Prevention Systeme (IPS) und Anti-Malware Systeme wirklich vor Exploits? Antworten darauf wurden am ISSS Security Lunch vom 9. April im Hotel Kreuz in Bern und am 10. April im Zunfthaus zur Meisen in Zürich aus erster Hand von Dr. Stefan Frei, Research Director bei NSS Labs (http://www.nsslabs.com), geliefert.

Das Thema stiess auf sehr grossen Anklang und die ISSS bedankt sich bei den insgesamt rund 70 Teilnehmern.

Im ersten Teil informierte uns Stefan Frei darüber, wie sich in den letzten Jahren eine eigentliche Cybercrime Industrie entwickelt hat, die heute äusserst professionell vorgeht. Malware wird z.B. erst dann verwendet bzw. an Dritte verkauft, wenn sie von keinem der aktuellen Anti-Malware Programme detektiert werden kann.

Und der Verkauf von Malware in den einschlägigen Untergrund-Märkten erfolgt teilweise sogar mit einer Garantie, dass die Malware während einer bestimmten Zeit von den Sicherheitsprogrammen nicht detektiert werden kann.

Dieser Bedrohung wird typischerweise mit einem Layered-Defense Ansatz begegnet. Server und Benutzerrechner werden mit mehreren hintereinandergeschalteten Abwehrtechnologien wie NGFW, IPS und Anti-Malware System geschützt, in der Hoffnung, dass eine Attacke von mindestens einer dieser Komponenten erkannt und damit abgewehrt werden kann.

Wie gut dieser Ansatz aber wirklich funktioniert, bleibt unbekannt, so lange man keine Daten zur Effektivität dieser Sicherheitsprodukte unter realistischen Angriffsbedingungen hat. Seit 20 Jahren testet NSS Labs als unabhängiges Unternehmen Sicherheitstechnologien und schliesst diese Informationslücke mit Analysen und Services.

Zu diesem Zweck untersucht NSS Labs – unter anderem – die tatsächliche Leistungsfähigkeit der Security-Devices verschiedener Hersteller bezüglich der Erkennung von Exploits. Bei den Tests werden sowohl bereits bekannte Exploits, als auch sogenannte Zero-Day Exploits, die noch nicht öffentlich bekannt sind, verwendet.

Im Rahmen des Referats stellte Stefan Frei die Ergebnisse der 2012 und 2013 durchgeführten Tests von Intrusion Detection Systemen, Next Generation Firewalls und Enterprise Antivirus Protection mit bereits bekannten Exploits vor.

Die Exploits wurden anhand des Common Vulnerabilities and Exposures (CVE) Verzeichnis klassifiziert und die getesteten Geräte/Produkte decken jeweils mehr als 90% des Marktanteils im entsprechenden Bereich ab. Die Geräte wurden dabei in der Standardkonfiguration getestet und man würde eigentlich erwarten, dass alle Gerät,e vor allem auch die teils mehrere Jahre alten, die bereits bestens dokumentierten Exploits erkennen würden.

Die Realität sieht anders aus. Z.B. konnte keine der neun im Frühjahr 2013 getesteten Next Generation Firewalls sämtliche Exploits detektieren und nur etwa die Hälfte der rund 1'700 im Test verwendeten Exploits wurden von allen Geräten detektiert.

Rückblick: ISSS Security Lunches vom 9. und 10. April 2013

Zudem gab es einige Exploits, welche von überhaupt keinem der neun Geräte im Test entdeckt werden konnten. Die meisten der nicht detektierten Exploits richten sich an Microsoft-Systeme, was aber natürlich auch durch deren grossen relativen Anteil aller Exploits begründet ist.

Herr Frei wies auch darauf hin, dass die Verwendung von zwei verschiedenen dieser Geräte in Serie keinen sehr grossen Sicherheitsgewinn bietet, weil die Geräte bezüglich der Nichterkennung der spezifischen Exploits eine starke Korrelation aufweisen, sprich: Wenn ein Gerät einen Exploit nicht erkennt, so ist die Wahrscheinlichkeit relativ gross, dass dies auch bei einem anderen Gerät der Fall ist.

Daraus folgt auch, dass ein Layered-Defense Ansatz in der Realität häufig nicht so effektiv ist, wie er auf dem Papier erscheint.

Zum Abschluss fasste Stefan Frei die wichtigsten Erkenntnisse nochmals zusammen. Ganz wichtig ist die Tatsache, dass keine Produktkombination 100% Schutz liefert – nicht einmal gegen bereits öffentlich bekannte Exploits.

Entsprechend muss man beim Risk Management davon ausgehen, dass interne Systeme bereits kompromittiert sind und deshalb ist es sinnvoll, dass man nebst den reinen Abwehrmechanismen weitere Massnahmen implementiert, mit welchen man erkennen kann, ob ein System bereits kompromittiert ist, z.B. indem versucht wird, Command and Control Kommunikationskanäle zu detektieren.

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

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

ISSS St. Galler Tagung vom 12. März 2013 "Secure Unified Communication in der Praxis"

Rückblick verfasst von Dr. Lukas Ruf, Consecom, Vorstand ISSS

Am 12.03.2013 veranstaltete die Information Security Society Switzerland (ISSS) ihre dritte ISSS St. Galler Tagung. Das brandaktuelle Thema, Secure Unified Communication in der Praxis, wurde aus Anwender-, Anbieter- und Beratersicht durch erfahrene Referenten aus verschiedenen Blickwinkeln betrachtet.

Dr. Lukas Ruf, Consecom, Vorstand ISSS, Tagungsmoderator

48 Teilnehmer fanden sich am späteren Dienstagnachmittag in St. Gallen in der zentral beim Bahnhof SBB gelegenen Migros Klubschule im sehr schönen, historischen Saal ein, um einen Einblick in die moderne, integrierte und sichere Kommunikation mittels Unified Communication zu erhalten.

Dr. Ursula Widmer, Rechtsanwältin, Präsidentin ISSS

Ursula Widmer, unsere Präsidentin, stellte die ISSS den anwesenden Nichtmitgliedern kurz und unterhaltsam vor.

Reto Weber von der Consecom führte ins Thema ein. Dabei baute er auf seiner Erfahrung aus Mandaten bei Grossunternehmen auf, um auf mögliche Fallstricke bei der Einführung von Unified Communication hinzuweisen. Zentral ist dabei, dass nicht nur technologische sondern auch organisatorische und prozessbezogene Aspekte gesamtheitlich miteinbezogen werden.

Michael Binder von der Symantec präsentierte Bedrohungen und mögliche Schutzmassnahmen, die es auch für einen sicheren Betrieb von Unified Communication zu beachten gilt. Mechanismen werden dabei auch Unified Communication schützen. Aus dem mit dem Event zeitgleich publizierten Symantec Intelligence Report berichtete er den Teilnehmern von den neuesten Entwicklungen und Erkenntnissen.

Mark Lütz von der Swisscom zeigte auf, welche Themen bei einer Einführung von Unified Communication und Collaboration Schwerpunkte für einen Anbieter von Outsourcing Lösungen bilden. In seinem Referat führte er sowohl in die kritischen Erfolgsfaktoren beim Aufbau einer entsprechenden Infrastruktur als auch in die essentiellen Herausforderungen beim Betrieb einer Unified Communication und Collaboration Lösung ein. Insbesondere wies er darauf hin, dass eine End-to-End Service-Verantwortung entscheidend für den Erfolg ist, um aus Unified Communication eine Standard Kommunikationslösung zu etablieren, wie sie das klassische Telephon bereitstellt.

Mark Lütz, Swisscom

Markus Huwyler und Beat Suter von der Swiss Life stellten ihre Erfahrung bei der Einführung und dem Einsatz von Unified Communication und Collaboration vor. Aus Anwendersicht legten sie dar, wie zwei Erfolgsfaktoren zuvorderst stehen: die Flexibilisierung der Kommunikation in Relation zu den dafür eingegangen Risiken. Sie legten so die Basis für einen idealen Übergang zur Podiumsdiskussion, in welchem die Referenten diskutierten und die Publikumsfragen beantworteten. Abgerundet wurde die dritte ISSS St. Galler Tagung durch einen gemütlichen Apéro riche mit reger Diskussion unter den Teilnehmern.

Agenda: ISSS Events

Nächste ISSS Events

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

Datum	Zeit	Veranstalter	Titel und Details	Ort
Mi, 24.04.2013	16:00 - 21:00	ISSS	ISSS-Generalversammlung mit Keynote von Prof. Dr. Ueli Maurer Eintritt gratis. Nur für ISSS-Mittglieder. Details, Anmeldung	Glattbrugg
Do, 25.04.2013	18:00 - 20:00	ISSS	ISSS Security Talk für Studierende: "Hacking for Fun and Profit" Details, Anmeldung	Zürich
Di, 28.05.2013	12:00 - 14:00	ISSS	ISSS Security Lunch: "Sichere Verwendung von unsicherem Cloudspeicher mit SecureFolder Mobile" Details, Anmeldung	Zürich
Mi, 05.06.2013	09:00 - 17:00	ISSS	ISSS Zürcher Tagung 2013: "IT-Sicherheit im Finanzbereich - Der Umgang mit operationellen Risiken" Details	Zürich
Di, 01.10.2013	09:00 - 17:00	ISSS	1. ISSS Information Security Switzerland Conference Details	Lausanne
Do, 28.11.2013	13:00 - 18:00	ISSS	16. Berner Tagung für Informationssicherheit Details	Bern

Vorschau: Events unserer Partner

Swiss Cyber Storm 4 – International Conference on Cyber Defence vom 13. Juni 2013

08.30 – 17.45 Uhr im KKL Luzern

In der nun bereits vierten Ausgabe der Swiss Cyber Storm (SCS) Konferenz treffen sich nationale und internationale IT Offizielle, Entscheidungsträger und Cyber Security Spezialisten um neuste Erkenntnisse und Probleme bei der Verteidigung unserer (kritische) IT Infrastruktur und virtuellen Grenzen zu diskutieren. Die SCS Konferenz wird in dieser Mission von SPIK (Swiss Police ICT) und MELANI (Melde- und Analysestelle Informationssicherung) unterstütz.

Dem Plenum am Morgen folgen zwei unterschiedliche Tracks (Tech-Track und Management-Track) am Nachmittag wo führende Cyber Defence Experten technische, sozio-ökonomische und politische Aspekte von Cyber Defence diskutieren.
Experten wie z.B. Costin G. Raiu, Leiter des Kaspersky Lab's Global Research & Analysis Team, John Matherly, Entwickler der Computer Suchmaschine Shodan, Dr. Stefan Lüders, CSO vom CERN, Dr. Timo Steffens vom CERT Bund and Yaron Blachman, Security und Forensik Technology Leader von PwC Israel teilen ihre Erkenntnisse und ihr Wissen über die aktuelle Bedrohungslage und zeigen auf was wir tun können, um den aktuellen und zukünftigen Bedrohungen zu begegnen.

Nuten Sie auch die Gelegenheit Michael Anti, dem vielfach ausgezeichneten Journalisten und Blogger zuzuhören, dessen Blog zur Chinesischen Politik im Dezember 2005 auf Druck der Chinesischen Regierung von Microsoft entfernt wurde. Michael Anti wird aufzeigen, wieso Cyber Security und Zensur eng miteinander verbunden sind. Besuchen Sie auch die Vorträge der Experten von MELANI, EUROPOL EC3 (European Cybercrime Centre) und dem BMI (Bundesministerium des Inneren) um zu erfahren, was Regierungen und (Strafverfolgungs-)Organisationen über die nationale und internationale Entwicklung von Cybercrime und Cyber Defence zu sagen haben.

Die SCS ist aber mehr als nur zuhören, was die Vortragenden zu Themen wie Advanced Persistent Threats oder Cyber Intelligence zu sagen haben. Nach jedem Vortrag ist genügend Zeit um IHRE Fragen an die Experten zu richten.

Nicht zuletzt können Sie auch die 10 Schüler und 10 Studenten treffen, welche die Online-Qualifikation für den Halbfinal des “Security Alpen Cup” in der Schweiz gewonnen haben. Während der Konferenz werden diese um einen Platz in der Schweizer Delegation für die Finals im November 2013 in Linz, Österreich, kämpfen. Unterstützen Sie unsere Mission, Cyber Security unter den Schüler und Studenten bekannter zu machen und treffen Sie die Security Experten der Zukunft!

Wir würden uns freuen, Sie an der Swiss Cyber Storm 4 begrüssen zu dürfen.

ISSS Mittglieder erhalten 15% Rabatt. Um den Rabatt zu erhalten, geben Sie beim Kauf der Tickets auf www.swisscyberstorm.com/registration/ den Code **XXSCS4PARTNERXX** an.

Bernhard Tellenbach
ISSS Vorstandsmitglied
President Swiss Cyber Storm

Vorschau: Events unserer Partner

D•A•CH Security 2013 vom 17. und 18. September 2013

Das Konferenzsystem ist scharfgeschaltet, die Registrierung und das Hochladen von Abstracts sind somit bereits möglich.

Die D•A•CH Security 2013 findet am 17. und 18. September 2013 an der Georg-Simon-Ohm-Hochschule in Nürnberg statt.

Einreichung: Fachbeiträge und Überblicksarbeiten zum Themenbereich IT-Sicherheit und interdisziplinären und rechtlichen Aspekten 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. Themen und Call for Papers: http://www.syssec.at/ds13_cfp

Termine:

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

Weite Informationen zur D•A•CH Security 2013: www.syssec.at/dachsecurity2013/

Hacking Day 2013 vom 16. Mai 2013

Dieses Jahr hat Digicomp spannende Vorträge und Workshops der Schweizer Top-Security-Auditoren für Sie zusammengestellt. Seien Sie am Donnerstag, 16. Mai, dabei! ISSS Mitglieder erhalten 15% Rabatt.

Unter anderem werden Themen wie Application Security, Digital Forensics, Cyber Warfare, Kryptographie, iOS Security und Schwachstellentrends behandelt, wertvolle Tipps und Tricks vermittelt und eingefahrene Denkmuster hinterfragt. Wem dies zu theoretisch ist, der kann sich in zwei Hacking Challenges in den Bereichen Web Security und Penetration Testing messen.

Weitere Informationen zum Hackingday 2013: www.digicomp.ch/hackingday

TeleTrusT-Informationstag "IT-Sicherheit im Smart Grid" vom 13. Juni 2013

Datum: 13. Juni 2013, 9:30 - 16:30 Uhr
Ort: Thomas-Dehler-Haus, Reinhardtstraße 14, 10117 Berlin (Tagungs- und Kongresszentrum Reinhardtstraßenhöfe)

Das "intelligente Energienetz" (Smart Grid) benötigt eine IKT-Struktur, die als sog. kritische Infrastruktur angemessen gesichert sein muss, um die Zuverlässigkeit der technischen Prozesse für die Steuerung und Administration sicherzustellen - und das auch in Krisenzeiten. TeleTrusT richtet den inzwischen 3. IT-Sicherheitstag für Smart Grids aus. Experten von DKE, BTC, Landis+Gyr, AIT, KIT und Smartlabs stellen dabei den aktuellen Entwicklungsstand rund um die Themen Standards und Normen, Leitstellen und Elektromobilität mit Fokus auf IT-Sicherheit vor. Da auch Österreich und die Schweiz vor vergleichbaren Herausforderungen stehen, werden Referenten aus beiden Ländern berichten. Der Informationstag richtet sich an Vertreter aus Wirtschaft und Verwaltung, insbesondere aus den Bereichen IT-Sicherheit, Energieversorgung und Datenschutz.

ISSS-Mitglieder können zum Tarif für TeleTrust-Mitglieder teilnehmen und bezahlen €125.- statt €165.-. Bitte geben Sie unter Anmeldung „ISSS-Mitgliedschaft" an. Weitere Informationen/Anmeldung: http://www.teletrust.de/veranstaltungen/smart-grid/2013/

Agenda: Security Events unserer Partner

Nächste Security Events unserer Partner

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

Datum	Zeit	Veranstalter	Titel und Details	Ort
Do, 13.06.2013	ganztags	TeleTrusT	IT Sicherheit im Smart Grid ISSS Mitglieder erhalten 20% Rabatt Details	Berlin
Do, 13.06.2013	08:30 - 17:45	Swiss Cyber Storm	Swiss Cyber Storm 4 International IT Security Conference with focus on on Cyber Defense. Patronage: MELANI und SPIK. ISSS Mitglieder erhalten 15% Rabatt. Rabatt Code: XXSCS4PARTNERXX Details, Anmeldung	KKL, Luzern
Mo - Di, 17.06.-18.06.2013	ganztags	COMPUTAS	DuD 2013 - Datenschutz und Datensicherheit Spezialpreis (EUR 600.-) für ISSS-Mitglieder. Details, Anmeldung	Berlin
Mi, 26.06.2013	13:00 - 17:00	Swiss Infosec AG	MEET SWISS INFOSEC! Sichere Informationen aus erster Hand Event zu Informations- und IT-Sicherheit: Erleben Sie hochkarätige Referenten, lernen Sie uns und unser Partner kennen. kostenlos Details	Zürich-Flughafen

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, 22.04.-26.04.2013	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	Olten
Di - Mi, 23.04.-24.04.2013	ganztags	Compass Security AG	iPhone® & iPad® Security Seminar Neues Compass Seminar mit Hands-on Labs zum Thema iPhone, iPad, MDM und Secure Devices. CHF 2300 (CHF 1950 für ISSS-Mitglieder) Details, Anmeldung	Bern
Mi, 24.04.2013	09:15 - 17:15	Compass Security AG	Wireless & Mobile Security Seminar zum Thema Wireless Technologie mit Fokus Wi-Fi Angriffe und Abwehr. CHF 2300 (CHF 1950 für ISSS-Mitglieder) Details, Anmeldung	Jona
Di, 30.04.2013	09:00 - 17:00	Swiss Infosec AG	Elektronische Archivierung Rechtliche Anforderungen, tech. Grundlagen und praktische Umsetzung der Archivierung, CHF 870.- Details	Sursee
Mo - Fr, 03.06.-07.06.2013	09:00 - 17:00	Detecon (Schweiz) AG	Informationssicherheit – ISO/IEC 27001 Leitender Auditor IRCA-zertifizierter Lead Auditor Kurs inkl. Prüfungsgebühr und Zertifikat CHF 3980.- (abzüglich 15% ISSS Rabatt) Details	Zürich
Mo - Fr, 19.08.-23.08.2013	09:00 - 17:00	Detecon (Schweiz) AG	Informationssicherheit – ISO/IEC 27001 Leitender Auditor IRCA-zertifizierter Lead Auditor Kurs inkl. Prüfungsgebühr und Zertifikat CHF 3980.- (abzüglich 15% ISSS Rabatt) Details	Zürich

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