Information Security Society Switzerland

ISSS NewsFlash

Juli 2012



Editorial

Liebe ISSS-Mitglieder

In diesem Juli Newsflash finden Sie als Schwerpunkt das Thema Kreditkartensicherheit, betrachtet unter dem Aspekt der Zertifizierung nach dem Industrie-Standard PCI DSS.

In seinem Artikel gibt Peter Sakal einen Überblick über die Implementierung des Payment Card Industry Data Security Standard (PCI DSS) bei Händlern und Dienstleistungsanbietern. Von besonderem Interesse sind die Hinweise betreffend Vorbereitung und Durchführung von Zertifizierungen und Audits sowie betreffend technische und organisatorische Massnahmen zur Reduktion von Zertifizierungskosten.

Als weiteren Schwerpunkt informieren wir Sie über die von der ISSS Task Force erarbeitete Stellungnahme zum geplanten Bundesgesetz über die elektronische Signatur (ZertES), welche wir im Rahmen des Vernehmlassungsverfahrens fristgerecht beim Bundesamt für Justiz einreichen konnten.

Ich wünsche Ihnen eine interessante Lektüre und einen nicht allzu nassen Sommer

Dr. Ursula Widmer
Präsidentin ISSS
president@isss.ch

Highlights in dieser Ausgabe

ISSS: Kurznews

- Autor für Lehrbuch gesucht
- Publikationen im Eventkalender

Vorschau: ISSS Berner Tagung vom 27.11.2012

Fokus: Kreditkarten-Kriminalität ausbremsen

ISSS: Neues aus der Special Interest Group Revision ZertES

- ISSS hat Vernehmlassung eingereicht

ISSS: Rückblick

- ISSS Zürcher Tagung vom 12.6.2012
- ISSS Security Lunch vom 28.6.2012
- Swiss Crows Cyber Defence Conference vom 25.4.2012

Partnerevents: Rabatte für ISSS-Mitglieder

- 17. Symposium on Privacy and Security vom 29.8.2012
- Security Events
- Security Kurse

Information Security Society Switzerland

ISSS: Kurznews

Autor für Lehrbuch "Informations-sicherheit gewährleisten" gesucht!

Zur Minimierung des Risiko der fehlenden ICT-Fachkräfte in der Schweiz ist solide Grund- und Weiterbildung notwendig. Die berufliche Weiterbildung über eidgenössische Zertifizierungen und Diplome geniesst in der Schweiz einen hohen Stellenwert.

Die Handlungsziele der Fächer zur Weiterbildung zum "Informatiker mit Fachausweis" wurde von der Stiftung "ICT Berufsbildung Schweiz" kürzlich überarbeitet. In diesem Zusammenhang sucht ein renommierter Lehrmittelverlag nach einem Autor für ein Lehrbuch zu "Informationssicherheit gewährleisten" für das Fachmodul M176.

Die Autorenschaft wird vergütet, von den verkauften Buchexemplaren hat der Autor Anspruch auf Tantiemen und das Buch wird öffentlich publiziert (ISBN Nummer, zu beziehen über den Verlag oder im Fachhandel). Gesucht wird ein Autor, der die zum Teil bestehenden Inhalte redigiert und weitere Inhalte erstellt. Das Buch wird im Namen des Autors publiziert.

Die fachlichen Inhalte des Lehrbuches entsprechen den Handlungszielen für das Fach, siehe
http://www.ict-berufsbildung.ch/infobox-rechts/neu-modulbaukasten/176-informationssicherheit-gewaehrleisten/

Bei Interesse melden Sie sich bitte bis Ende September 2012 bei Umberto Annino, Vizepräsident ISSS, vicepresident@isss.ch

Möchten auch Sie in unserem Eventkalender erscheinen?

Sehr gerne bieten wir Ihnen die Möglichkeit, auf Ihre Veranstaltung auf der ISSS-Website und im ISSS-NewsFlash, welcher an über 1‘000 Mitglieder versandt wird, hinzuweisen. Hierfür erbitten wir lediglich einen Rabatt von 15% bis 20% auf Ihren regulären Veranstaltungspreis für unsere Mitglieder.

Sollten Sie noch weitere Fragen hierzu haben oder an einer Zusammenarbeit interessiert sein, steht Ihnen Frau Martina Ehrlich vom ISSS Sekretariat sehr gerne zur Verfügung.

Sie erreichen Sie wie folgt: Martina Ehrlich, sekretariat@isss.ch

Vorschau: ISSS Berner Tagung für Informationssicherheit

15. ISSS Berner Tagung “Bring your own device: Chancen und Risiken" vom 27. November 2012

Dienstag, 27. November 2012, 13.00 – 18.00 Uhr, Kursaal Bern, Bern

Das Thema beschäftigt Unternehmen, Behörden aber auch Mitarbeitende zunehmend. Aber worin können die Vorteile liegen, wenn die Mitarbeitenden ihre eigenen Geräte mitbringen? Bessere Identifikation mit dem Arbeitsmittel, weil es ‚meins‘ ist oder mit dem Arbeitgeber, weil er mir erlaubt, meine neuesten Errungenschaften mitzubringen? Geringere Kosten für das Unternehmen? Sicherheit versus grössere Flexibilität? Es sind viele Fragen, die in diesem Themenkreis gestellt werden (müssen). Einen Teil davon versuchen Experten im Rahmen der Tagung aufzugreifen, zu diskutieren und zu beantworten.

Hier finden Sie einen ersten Programmentwurf der diesjährigen Berner Tagung, welche durch **Kurt Aeschbacher**, Schweizer Fernsehen DRS, moderiert wird.

13.00 Uhr	**Begrüssung** Peter Fischer, Delegierter für die Informatiksteuerung des Bundes Informatiksteuerungsorganorgan des Bundes ISB
	Keynote Referent angefragt
	Referat SBB Referent angefragt
	Referat Swisscom Referent angefragt
14.30 Uhr	**Pause**
15.00 Uhr	**ISSS – Information Security Society Switzerland** Dr. Ursula Widmer, Präsidentin ISSS
	Referat Symantec Herr Frank Thonüs, Managing Director Symantec Switzerland AG
	United Security Providers AG / EMMI Referent angefragt
	Rechtliche Aspekte von BYOD Nicole Beranek Zanon, SWITCH
	Podiumsdiskussion Moderierte Diskussion mit den Referenten
17.00 Uhr	**Sichere Higgs-Teilchen?** Dr. Stefan Lüders, CERN Computer Security Officer
17.45 h	**Apéro**
19.00 h	**Ende der Veranstaltung**

Fokus: Kreditkarten-Kriminalität ausbremsen

Payment Card Industry Data Security Standard (PCI DSS)

Autor: Peter Sakal

Diebstahl von Kreditkartendaten ist ein florierendes Geschäft. In regelmäßigen Abständen werden neue Sicherheitsvorfälle in der Presse veröffentlicht. Zudem existiert eine hohe Dunkelziffer erfolgreicher Angriffe. 2006 etablierten die Kreditkartenorganisationen einen einheitlichen, internationalen Sicherheitsstandard zum Schutz von Unternehmen sowie deren Kunden: den Payment Card Industry Data Security Standard (PCI DSS).

Aktuelle Schadensquoten zeigen, dass die Umsetzung des Standards effektiv gegen Hacker und Kreditkartenkriminelle wirkt.

Wer ist zur PCI DSS Compliance verpflichtet und wie wird die Compliance nachgewiesen?
Handelsunternehmen (Merchants) und Dienstleister (Service Provider), die Kreditkartendaten speichern, verarbeiten oder übertragen müssen ihre PCI DSS Compliance nachweisen. Mögliche Nachweise sind:

- Vierteljährlich durchzuführende externe Vulnerability Scans durch ein zertifiziertes Unternehmen (Approved Scanning Vendor).
- Ein jährlich auszufüllender Fragebogen - Self Assessment Questionnaire (SAQ).
- Ein jährlich durchzuführendes Onsite-Audit, mit den dazugehörigen Abschlussberichten, das durch einen zertifizierten PCI DSS Auditor (Qualified Security Assessor bzw. Internal Security Assessor) durchgeführt wird.

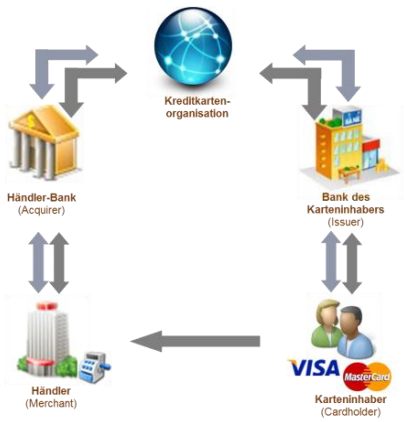


Abbildung 1: Kreditkarten Transaktionsprozess

Welche dieser drei Optionen gewählt werden muss, wird von den jeweiligen Kreditkartenorganisationen vorgegeben und ist insbesondere von der Transaktionsmenge abhängig. Die Händler-Banken (Acquirer) müssen sicherstellen, dass deren Händler ihre PCI DSS Compliance nachweisen. Die Kreditkartenorganisationen fordern von allen Dienstanbietern die PCI Compliance ein.

Wie lassen sich Strafzahlungen vermeiden?
Die Nichteinhaltung des PCI DSS Standards kann zu Strafzahlungen, dem Untersagen der Akzeptanz von Kreditkarten oder anderen Reglementierungen führen. Beispielsweise kann die Kreditkartenorganisation MasterCard derzeit Strafzahlungen bis zu USD 100.000 für jede Nichteinhaltung der PCI Standards erheben. Zusätzlich können zur Durchführung (computer-) forensischer Untersuchungen Gebühren erhoben werden, wenn ein eingetroffener Kreditkartenmissbrauchsfall untersucht wird.Wird ein Unternehmen kompromittiert, welches zum Zeitpunkt der Kompromittierung nachweislich PCI DSS compliant war, gilt die „Safe Harbour Regel“. Diese besagt, dass das betroffene Unternehmen nicht mit Forderungen seitens der Händler-Bank oder der Kreditkartenorganisationen konfrontiert wird.

Gibt es Möglichkeiten, die Zertifizierungskosten zu reduzieren?
Alle IT-Systeme, die Kreditkartendaten speichern, verarbeiten oder weiterleiten, befinden sich im „PCI DSS Scope“. Das bedeutet, dass diese Systeme die Anforderungen des PCI DSS Standards erfüllen müssen. Je größer der PCI DSS Scope ist, umso größer ist der Zertifizierungsaufwand, der wiederum mit Kosten verbunden ist. Deshalb sollte das Ziel sein, den PCI DSS Scope zu minimieren. Der PCI DSS Scope lässt sich reduzieren, indem die IT-Systeme, die mit Kreditkartendaten in Berührung kommen von allen anderen Systemen (z. B. der Büroumgebung) abgeschottet werden; z. B. durch netzwerktechnische Segmentierung mittels einer Firewall. Neben solchen technischen Aspekten können auch organisatorische Aspekte dazu beitragen den PCI DSS Scope zu reduzieren. Beispielsweise können Geschäftsprozesse so umstrukturiert werden, dass die Verarbeitung von Zahlungsdaten überflüssig wird oder die Zahlungsprozesse an externe Dienstleister ausgelagert werden.

Um alle auf die individuelle Situation zutreffenden Optionen zur Scope-Reduktion zu beleuchten und somit eine Entscheidungsgrundlage zu erhalten, sollte ein erfahrener PCI DSS Berater / Auditor zurate gezogen werden. Wenn er

Information Security Society Switzerland

Fokus: Kreditkarten-Kriminalität ausbremsen

das Geschäftsmodell des zu zertifizierenden Unternehmens versteht und einen Einblick in die relevanten Dokumente, Prozesse und auf die IT-Systeme erhält, kann er maßgeblich dazu beitragen, den Zertifizierungsaufwand zu reduzieren und somit Kosten zu sparen.

Welche Anforderungen gibt es und wo sind die Fallstricke?
Der PCI DSS Standard deckt technische und organisatorische Aspekte ab. Es existieren 12 Hauptanforderungen, die jeweils in mehrere Unteranforderungen gegliedert sind.

Kontrollziel	Nr	Anforderung
Erstellung und Wartung eines sicheren Netzwerks	1.	Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten
	2.	Keine vom Anbieter gelieferte Standardeinstellung für Systemkennwörter und andere Sicherheitsparameter verwenden
Schutz von Karteninhaberdaten	3.	Schutz gespeicherter Karteninhaberdaten
	4.	Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze
Wartung eines Anfälligkeitsmanagement-programms	5.	Verwendung und regelmäßige Aktualisierung von Antivirensoftware
	6.	Entwicklung und Wartung sicherer Systeme und Anwendungen
Implementierung starker Zugriffskontrollmaßnahmen	7.	Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf
	8.	Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff
	9.	Physischen Zugriff auf Karteninhaberdaten beschränken
Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken	10.	Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten
	11.	Regelmäßiges Testen der Sicherheitssysteme und -prozesse
Befolgung einer Informationssicherheits-Richtlinie	12.	Befolgung einer Informationssicherheits-Richtlinie für das gesamte Personal

Abbildung 2: Überblick über den PCI-Datensicherheitsstandard (Quelle: PCI Standards Council 2010)

Ein häufiger Fallstrick ist der Aufbau eines zentralen Logservers, um alle Aktivitäten auf der Kreditkartenumgebung lückenlos nachvollziehen zu können. Ferner wird ein restriktives Rechtemanagement gefordert – nur die unbedingt notwendigen Rechte sind zu gewähren und Zugriffe auf die Kartenumgebung auf ein Minimum zu reduzieren. Ein häufiges Problem ist auch die Bereitstellung der geforderten Dokumentation, die sich über alle Anforderungen erstreckt. PCI DSS Dokumentvorlagen sind dabei nur bedingt nützlich, da sie zu allgemeingültig sind, um konkrete Handlungsoptionen zu liefern. Ferner muss die Dokumentation mit den reellen Gegebenheiten übereinstimmen, was beim Einsatz von Dokumentvorlagen häufig außer Acht gelassen wird.

Wie wird mein Unternehmen schneller PCI DSS Compliant?
Um das Ziel der erfolgreichen PCI DSS Zertifizierung zu erreichen, empfiehlt sich folgendes systematisches Vorgehen, wobei nur das Onsite-Audit obligatorisch ist:

1. Scope Workshop: Dient der Orientierung und dem Überblick über die Inhalte des PCI DSS Standards, der Identifizierung des Scopes und von Möglichkeiten zur Reduktion des Scopes.
2. GAP-Analyse: Abgleich der bereits umgesetzten Maßnahmen mit den Anforderungen des Standards, wodurch Abweichungen zum Standard identifiziert werden.

Fokus: Kreditkarten-Kriminalität ausbremsen

3. Remediation: Mit der Hilfe von sachkundigen Beratern lassen sich Maßnahmen ableiten und die Abweichungen zum Standard im Rahmen eines systematischen Vorgehens beheben.
4. Jährlich durchzuführendes Onsite-Audit: Überprüfung durch einen zertifizierten PCI DSS Auditor – Qualified Security Assessor (QSA) bzw. Internal Security Assessor (ISA) – ob alle Anforderungen des Standards umgesetzt sind.
5. Vergabe des Zertifikats und ggf. Listing auf der Webseite der Kreditkartenorganisationen wie z.B. bei Visa Europe: http://www.visaeurope.com/en/businesses__retailers/payment_security/service_providers.aspx

Was wird im Onsite-Audit überprüft?
Die im Rahmen eines Onsite-Audits zu prüfenden und im Abschlussbericht zu dokumentierenden Aspekte sind in Form von „Testing Procedures“ zu jeder Anforderung definiert. Darüber hinaus existieren spezifische Anforderungen an den Abschlussbericht des PCI DSS Onsite-Audits (Report on Compliance - ROC), die in den „Reporting Instructions“ des PCI Security Standards Council definiert sind.
Der PCI DSS Auditor prüft mittels folgender Methoden, ob die Anforderungen erfüllt sind:

- Prüfung der Systemkonfiguration
- Prüfung der erforderlichen Dokumentation
- Durchführung von Interviews
- Beobachtung von Prozessen und Aktionen

Es existieren Anforderungen, bei denen die Möglichkeit der Identifizierung von „Samples“ besteht; das bedeutet, dass die geforderten Prüfungen anhand einer repräsentativen Stichprobe von IT-Systemen, Personen oder Prozessen durchgeführt werden können.

Wie finde ich einen Zertifizierer, Berater oderApproved Scanning Vendor?
Das PCI Security Standards Council (PCI SSC) verwaltet eine Liste der Unternehmen, die nach PCI DSS zertifizieren dürfen: https://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php
Viele Unternehmen, die zertifizieren, beraten auch. Es ist hilfreich, einen möglichst intensiven Informationsaustausch mit Beratern und Zertifizierern zu pflegen, um die Compliance möglichst optimal und kostensparend zu erreichen. Überflüssige Aufwände, z. B. durch falsch interpretierte Anforderungen, lassen sich dadurch vermeiden.

Ferner existiert eine Liste der Approved Scanning Vendors, die externe Vulnerability Scans durchführen dürfen:
https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php

Weiterführende Links
[1] www.pcisecuritystandards.org
[2] www.mastercard.com/us/merchant/pdf/SPME-Entire_Manual_public.pdf
[3] www.isss.ch/veranstaltungen/2012/security-lunch-2012-04-26
[4] www.compliancemagazin.de/compliancefachbeitraege/hintergrund/usdde110608.html
[5] www.compliancemagazin.de/compliancefachbeitraege/hintergrund/novell170807.html

Über den Autor
Peter Sakal ist IT-Security Consultant bei der usd AG, einem unabhängigen, europaweit agierenden Beratungshaus für IT-Security und Kreditkartensicherheit.

Fokus seiner Tätigkeit sind Sicherheitsmanagement sowie Risiko- und Sicherheitsanalysen. Als zertifizierter PCI DSS Auditor (QSA) sammelte er bereits umfangreiche Erfahrungen in der Finanz- und eCommerce-Branche, der Telekommunikationsindustrie und der Hotellerie. Seinen Master in Computer Science absolvierte er an der Hochschule Bonn-Rhein-Sieg (DE). Auch heute gilt sein Engagement weiter der Förderung des Themas IT-Sicherheit, so z.B. als Forschungsleiter für Informationssicherheit, Autor für Fachzeitschriften und als Lehrbeauftragter an verschiedenen Hochschulen.
Web: www.usd.de E-Mail: Peter.Sakal@usd.de

Information Security Society Switzerland

ISSS: Neues aus der Special Interest Group Revision ZertES

Stellungnahme der ISSS zur Totalrevision des Bundesgesetzes über die elektronische Signatur (ZertES)

ISSS hat im Juli 2012 in der Vernehmlassung zur Totalrevision des Bundesgesetzes über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) Stellung genommen (publiziert auf der ISSS Website http://www.isss.ch/fileadmin/publ/tf-zertes/Stellungnahme_ZertEs.pdf

ISSS befürwortet die Revision und deren Ziel, die praktische Verwendung von Zertifikaten, die in gesetzlich geordneten Verfahren ausgestellt werden, zu fördern. Dies soll vor allem mit einem neuen Typ von Zertifikaten, dem geregelten Zertifikat, erreicht werden. Dieses kann nicht nur auf Einzelpersonen, sondern auch auf Unternehmen und Organisationen ausgestellt werden und ist ausser für elektronische Signaturen auch für Zwecke der Authentifizierung verwendbar.

ISSS hat jedoch auch darauf hingewiesen, dass die Revision des ZertES allein nicht ausreichend ist. Wie das bisherige, regelt auch das neue ZertES die rechtliche Wirkung elektronischer Signaturen selbst nicht. Dies ist jeweils anderen Gesetzen vorbehalten, wie dem Obligationenrecht, welches die qualifizierte digitale Signatur rechtlich der eigenhändigen Unterschrift gleichstellt. Auch in anderen Gesetzen, z.B. betreffend den elektronischen Geschäftsverkehr mit Behörden und Gerichten, werden die Anforderungen festgelegt, welche die elektronische Signatur zu erfüllen hat, damit elektronische Sendungen und Dokumente gültig signiert werden können. Auch hier werden den praktischen Anforderungen entsprechende Regelungen festgelegt werden müssen. Dazu gehört vor allem auch, dass dort, wo die elektronische Kommunikation gesetzlich grundsätzlich anerkannt ist, diese auch tatsächlich eingesetzt werden kann. ISSS hat daher die Forderung gestellt, dass Private ein Recht haben, mit Behörden elektronisch zu kommunizieren und die Behörden verpflichtet sind, die ihrerseits hierfür erforderlichen technischen Einrichtungen vorzunehmen.

ISSS sieht ferner in verschiedenen Einzelpunkten Optimierungsbedarf im Hinblick auf die Vermeidung unnötiger Hindernisse und Unklarheiten bei der Ausstellung von Zertifikaten. Dazu gehört etwa, dass bei der Ausstellung von Zertifikaten auf im Handelsregister eingetragene Unternehmen deren Vertreter nicht mehr persönlich beim Zertifizierungsdiensteanbieter erscheinen müssen, oder eine Regelung bezüglich der Ungültigerklärung von Zertifikaten mit Berufs- und ähnlichen Attributen, wenn der Inhaber die Voraussetzungen für das Attribut verloren hat. ISSS beantragt zudem, dass auf eine besondere, verschärfte Haftung der Inhaber im Fall des Missbrauchs von geheimen kryptographischen Schlüsseln verzichtet wird. Dies im Hinblick darauf, dass das Risiko einer speziellen Haftung abschreckend für die Verwendung elektronischer Signaturen wirken könnte.

Das weitere Vorgehen nach der Vernehmlassung ist im Einzelnen noch nicht bekannt. Der Bundesrat hat jedoch vom Eidgenössischen Justizdepartement bis Ende 2012 einen Bericht bezüglich einer umfassenden Regelung von elektronischen Signaturverfahren verlangt. Es ist davon auszugehen, dass der Bundesrat basierend auf diesem Bericht auch über das weitere Vorgehen der ZertES Revision entscheiden wird.

An dieser Stelle möchte ich mich, als Lead der ISSS Task Force „Revision ZertES“, ganz herzlich bei den Mitgliedern der Task Force für ihre wertvolle und effiziente Mitarbeit bedanken. Es war eine grosse Herausforderung, den sportlichen Zeitplan einzuhalten und gleichzeitig eine grosse Freude, mit den folgenden qualifizierten Experten arbeiten zu dürfen:
Konrad Bähler, Markus Brütsch, Daniel Büttiker, Marcel Eberle, Walter Gygli, Ralf Hauser, Thomas Kessler, Martin Kurmann, Beat Lehmann, Doron Moritz, Carl Rosenast, Anthony Thorn, Reto Weber und Marc Zweiacker.

Dr. Ursula Widmer, Präsidentin ISSS, Lead ISSS Task Force Revision ZertEs, president@isss.ch

Information Security Society Switzerland

ISSS: Rückblick

Erfolgreiche ISSS Zürcher Tagung vom 12. Juni 2012
Experten diskutieren über: Wie sicher sind „sichere“ IT-Systeme?

Dr. R. Zergenyi, IT Audit Director bei der ZURICH Insurance Group (ZIG) zeigte auf, wie die IT Prüfungs-Herausforderungen in einem globalen Konzern meistert. Die ZIG ist in 170 Ländern aktiv und braucht pro Land eine Lizenz, um Versicherungen zu verkaufen - entsprechend viele Compliance-Anforderungen sind zu erfüllen. Ein globaler Audit-Plan mit lokalem Fokus ist Basis für die Planung, welche 5 Quartale im Voraus mit quartalsweiser Anpassung erfolgt. Mit einem Datacenter auf dem San Andreas Graben in San Francisco stehen aber auch Risiken ins Haus. Dr. Zergenyi informierte über das risikobasierte Audit in einer komplexen Welt, verschiedene Anforderungen an die Revisoren und die Abstimmung des Audit-Plans mit dem Business. Die gute Beziehung wird über Aktivitäten und gegenseitige Unterstützung zwischen Business und Audit auch ausserhalb des regulären Audits gefördert, welche letztlich auch ein qualitativ besseres Prüfresultat zur Folge hat.

Ivan Bütler von Compass Security zeigte in unterhaltsamer Weise auf, welche Erfahrungen in der Praxis im „Hacking“ von Systemen im Auftrag von Kunden gemacht werden. Penetration-Tests mit Nebeneffekten wurden beschrieben sowie Methoden und Werkzeuge des Testings erklärt. Die Internationalisierung, Zeitzonen sowie verschiedene Sprachen der involvierten Parteien bei Security-Tests stellen die heutigen Herausforderungen dar und auch ständig den aktuellsten Entwicklungen und Angriffen voraus zu sein oder zumindest zu wissen, was und wie „in der Wildnis des Internet“ passiert. Ein innovativer Ansatz, um fehlende Fachkräfte zu rekrutieren, rundete den Vortrag von Ivan Bütler ab.
Klaus Krohmann, Head E&Y Legal, erklärte die regulatorischen Grundlagen des IT-Audits und verschiedene Kontrollen, die durchgeführt werden können. Die meisten gesetzlichen Vorgaben implizieren eine Prüfung von IT-Systemen, ohne konkrete Vorgaben zu machen. In anderen Ländern gibt es eine steigende Tendenz zur gesetzlichen bzw. regulatorischen Forderung von z.B. Penetration-Tests von IT-Systemen. Freiwillige Prüfungen ausserhalb der regulären Jahresberichterstattung (financial audit) sind selten durch Vorschriften gefordert. Die Wesentlichkeit der Risiken wurde erläutert, anhand derer die zu prüfenden Systeme im Rahmen des regulären Audits ausgewählt werden.

Christoph Stocker, Rechtsanwalt bei UBS, erläuterte dem interessierten Publikum die Sicherheit von Systemen im Finanzbereich. Die Fokuspunkte sind dabei vor allem Datensicherheit und Vertraulichkeit, aus den gesetzlichen Anforderungen kommen der Gläubigerschutz, Aufbau von Risikomanagementsystemen und die Berücksichtigung von technischen Entwicklungen dazu. FINMA konformes Vorgehen bei allfälligen Outsourcing-Vorhaben und ein Business Continuity Management werden von der Finanzmarktaufsicht FINMA gefordert, um eine Betriebsbewilligung als Bank zu erhalten resp. nicht zu gefährden. Das rasche Reagieren und die Zusammenarbeit mit Behörden im Falle von Angriffen wurden anhand von Beispielen erläutert, aber auch die Pflicht der Kunden, sich in einem Verdachtsfall korrekt zu verhalten und Vorfälle oder Verdachtsmomente der Bank zu melden, wurden hervorgehoben.

Vor dem Panel mit den Referenten, welches von der Tagungs-OK-Vorsteherin Dr. Sonja Hof, ISSS Vorstandsmitglied, unterhaltsam moderiert wurde, gab es ein Abschlussreferat von Lukas Faessler, Rechtsanwalt, zu den Stolpersteinen bei der praktischen Durchsetzung von Rechten. Anhand eines realen Beispiels von Datendiebstahl und der damit verbundenen Durchsetzung von Schutzrechten wurde das Publikum auf eine interessante Reise durch die vielschichtigen praktischen Aspekte des Rechts geführt.

Die Slides der Tagung finden Sie unter: https://www.isss.ch/veranstaltungen/2012/zuercher-tagung/
Umberto Annino, Vizepräsident ISSS, vicepresident@isss.ch

Information Security Society Switzerland

ISSS: Rückblick

ISSS Security Lunch vom 28. Juni 2012
Smart Grid - Intelligente Stromnetze: Chancen und Risiken für die Sicherheit

Bereits zum fünften Mal in diesem Jahr veranstaltete ISSS in Bern einen Security Lunch zu einem topaktuellen Thema aus dem Bereich ICT-Security: „Smart Grid − Intelligente Stromnetze: Chancen und Risiken für die Sicherheit“.

Trotz schwülheissen Sommerwetters fanden sich pünktlich zur Mittagszeit rund 30 Interessierte im Restaurant Schmiedstube ein, um von den zwei ausgewiesenen Experten im Elektrizitätssektor, Herrn Dr. Maurus Bachmann und Herrn Christian Meier, aus erster Hand mehr über diese im Zusammenhang mit der aktuellen Atomausstiegsdebatte an zusätzlicher Dynamik gewonnenen Entwicklung in Richtung eines „Smart Grids“ zu erfahren.

Nach einer kurzen Begrüssungsrede von Frau Dr. Ursula Widmer, Präsidentin der ISSS, eröffnete Dr. Maurus Bachmann, Geschäftsführer des im August letzten Jahres aus elf Elektrizitätsunternehmen (EVUs) gegründeten Vereins „Smart Grid Schweiz (VSGS)“ den Fachteil und beleuchtete dabei aus Sicht der grossen EVUs die aufgrund der geplanten Energiewende bevorstehenden tiefgreifenden Veränderungen des Energieversorgungsnetzes in der Schweiz.

Der Trend gehe dabei eindeutig weg vom heute zentralen System mit wenigen grossen Stromproduzenten in Richtung eines hochgradig vernetzten Smart Grids mit zusätzlich tausenden von dezentralen kleinen bis sehr kleinen Strom-Einspeiseanlagen (Photovoltaik auf Hausdächern, Mikro-Wasserkraftwerke etc.), wobei diese sich durch eine stark fluktuierende und schlecht planbare Produktion auszeichneten, die möglichst zeitnah gemanaged werden müsse.

Am Beispiel der Photovoltaik erklärte Herr Bachmann, wie es im Stromnetz bei Sonnenschein angesichts der dezentralen Produktion zeitweise sogar zu einer Umkehr der Energieflussrichtung im Stromnetz kommen könne und dass eine zentrale Abschaltung der Stromzufuhr im Smart Grid, z.B. für die sichere Durchführung von Wartungsarbeiten, nicht mehr so einfach wie in den althergebrachten, hierarchisch gegliederten Stromnetzen zu bewerkstelligen sei. Dass der gute alte Stromzähler diesen neuen Anforderungen nicht mehr genüge und die Zukunft den Smart Metern gehöre, liege auf der Hand.

Gleichzeitig aber warnte Herr Bachmann davor, im Smart Grid die Lösung aller Energieprobleme zu sehen und strich in diesem Zusammenhang das Hauptziel des Vereins „Smart Grid Schweiz“ heraus: es gelte, die Politik und die Gesellschaft auf einen realistischeren Informationsstand zu bringen.

Dafür werde in einer ersten Etappe bis Ende Jahr ein Weissbuch erstellt, das ein gemeinsames Verständnis für die intelligenten Stromnetze mit dezentraler Stromproduktion, auch aus der Kundensicht, schaffe und die ersten Schritte zu einem Schweizer Smart Grid aufzeige.

Die Relevanz des Datenschutzes und der Datensicherheit im Smart Grid und insbesondere beim Smart Metering seien ebenfalls erkannt worden, stünden derzeit aber (noch) nicht im Zentrum der Arbeiten.

Christian Meier, Produkt Manager und EMEA Sicherheits-Strategie-Verantwortlicher bei Landis+Gyr, eines weltweit führenden Anbieters von Smart Metering Lösungen und seit der Übernahme im Jahr 2011 durch Toshiba auch von umfassenden Smart Grid Lösungen, ging in seinem Vortrag vertieft auf die Thematik des Datenschutzes und der Datensicherheit bei Smart Metern ein.

Bei ca. 5 Millionen in der Schweiz in Zukunft mit Smart Metern auszurüstenden Zählpunkten sei es unverzichtbar, die Datensicherheit bereits „by design“ in die Lösung zu integrieren und beim ersten Rollout zu realisieren, ansonsten könne es ganz schön teuer werden. Ein Elektrizitätsunternehmen in Puerto Rico, dessen Smart Meter gehackt wurden, wurde beispielsweise um 400 Mio. Dollar jährlich betrogen. Aber auch Nachlässigkeiten im Bereich Daten-

Information Security Society Switzerland

ISSS: Rückblick

schutz könne man sich in der Schweiz, wo wie in Deutschland der Datenschutz sehr gut gesetzlich verankert sei, nicht leisten, ansonsten drohten langwierige Streitereien mit Verbraucherorganisationen und Zeitverlust bei der Einführung.

Laut Herrn Meier sollte die Schweiz denselben Weg wie der Vorreiter Deutschland einschlagen. Dort sei nicht nur der Kernenergieausstieg aufgrund eines Bundestagsbeschlusses im Juni 2011 beschlossene Sache, sondern es würden seit kurzem auch der Datenschutz und die Datensicherheit und somit „security by design“ für Smart Grids bereits auf legislativer Ebene eingefordert.

Der Regulator in der Schweiz solle diese Entwicklung ebenfalls proaktiv mitgestalten und Mindestanforderungen bezüglich Sicherheit definieren, ansonsten hätten Kosten gegenüber Sicherheit Priorität und dies könne fatal sein − immerhin handle es sich ja beim Schweizer Stromnetz um die volkswirtschaftlich wohl relevanteste Infrastruktur, die bei ihrem Wandel in Richtung eines „Internets der Energie“ des entsprechenden Schutzes bedürfe.

Zum Abschluss der hochkarätigen Veranstaltung regte Frau Dr. Widmer die Bildung einer ISSS Special Interest Group (SIG) zum Thema „Smart Grid“ an, um frühzeitig das breite Expertenwissen der innerhalb der ISSS vernetzten Security-Professionals in dieses topaktuelle Thema einfliessen zu lassen und die verschiedenen Stakeholder in dieser hochspannenden Entwicklung zu unterstützen.

Interessenten an einer SIG zu diesem Thema melden sich bitte direkt bei Frau Dr. Widmer unter president@isss.ch.

Hanspeter Christ, Vorstand ISSS,
hanspeter.christ@isss.ch

Wo finden Sie Informationen zu ISSS-Special Interest Groups?

Auf unserer Website www.isss.ch finden Sie eine Auflistung aller ISSS Special Interest Groups (SIGs), geordnet nach SIGs in Gründung, aktiven SIGs und abgeschlossenen SIGs.

Wenn Sie spezifische Fragen zu SIGs haben, z.B. wie man eine SIG initiieren kann, welche Themen sich dafür eignen und welche Rechte und Pflichten eine SIG hat, so finden Sie Antworten unter Häufige Fragen.

Ihr Interesse am Mitmachen oder Initiieren einer SIG würde uns sehr freuen.

ISSS: Rückblick

Swiss Crows und ISSS: Cyber Defense Conference vom 25.04. 2012

Am 25.04.2012 führte die Swiss Crows (Swiss Chapter der Association of Old Crows) im Co-Sharing mit ISSS einen äusserst erfolgreichen Anlass zum Thema Cyber Defense im Kultur- und Kongresshaus in Aarau durch.Gegen 100 Konferenzgäste liessen es sich nicht nehmen, sich aus erster Hand von hochkarätigen Experten informieren zu lassen.

Ziel der Konferenz war, das Thema Cyber Defense von der Analyse der Bedrohungslage, über das Engagement der Kantone und des Bundes bis hin zur nationalen Strategie, den rechtlichen Aspekten im Cyberspace wie auch im Engagement der Wirtschaftsunternehmen zu beleuchten.

Die Präsentationen der Cyber Defense Conference waren alle sehr spannend (siehe https://www.isss.ch/veranstaltungen/2012/swiss_crows_cyber_defense/). Speziell sei auf das höchst interessante Referat des ISSS Vorstandsmitglieds lic.iur. Fürsprech Beat Lehmann hingewiesen, welcher einen fundierten Überblick über die Rechtslage gab.Cyber Defense Conference: Podiumsgespräch unter der Leitung von Dr. Daniel Heller mit den Referenten Richard P. Morva, Präsident Swiss Crows, president@crows.ch

Wer ist Swiss Crows?

Die Swiss Crows (www.crows.ch) sind ein Chapter der Association of Old Crows (AOC). AOC ist eine internationale Non-Profit-Organisation mit über 13'500 Mitgliedern, welche in über 47 Ländern in 69 Chaptern organisiert sind.

Die Swiss Crows sind eine Plattform-Organisation, welche zum Ziel haben, im Bereich Elektronischer Operationen und Informations Operationen die Wissenschaft und Forschung, die Industrie sowie die Anwenderbereiche zusammenzuführen und auf diese Weise Synergien zu bilden. Die ursprünglichen Bereiche der Elektronischen Kriegführung wie Funkaufklärung (Communication Intelligence, COMINT) und Elektronischer Kampf (Electronic Warfare, EW) werden ergänzt mit weiteren Themenbereichen wie Informationssicherheit, Kryptologie und Computer Netzwerk Operationen.

Sie setzen sich aktiv dafür ein, Forschung zu begünstigen, neues Wissen aufzubauen, zugänglich zu machen und zu verbreiten sowie das allgemeine Verständnis zu fördern.

Zudem engagieren sie sich auch für die Schulung in entsprechenden wissenschaftlichen Disziplinen und die historische Dokumentation der diesbezüglichen Entwicklungen.

Agenda: Partner Events mit Rabatt für ISSS Mitglieder

17. Symposium on Privacy and Security vom 29. August 2012 in Zürich, ETHZ

«Wo sind die Daten? Auslagerung von Datenbearbeitungen: Outsourcing und Cloud Computing. Die Verantwortung von Unternehmen und Verwaltung für Sicherheit und Datenschutz»

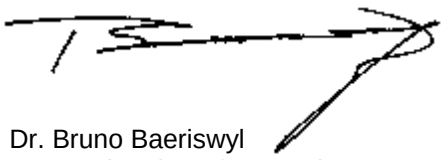
Bei Datenbearbeitungen in Unternehmen und Verwaltung werden zunehmend Dritte mit einbezogen. Dabei werden einzelne Dienstleistungen ausgelagert oder die gesamte Datenbearbeitung wird von Dritten erbracht. Die technologische Entwicklung hin zur virtualisierten Infrastruktur bringt neue Möglichkeiten. Das klassische «Outsourcing» wird abgelöst von «Cloud Computing» – ein Begriff, der auch bei näherer Betrachtung nebulös bleibt. Das neue technologische Umfeld bringt aber zusätzliche Herausforderungen. Auf der einen Seite locken neue Business-Modelle, die grosse Kosteneinsparungen versprechen. Auf der anderen Seite wächst die Sorge um den Schutz und die Sicherheit der eigenen Daten.

Die Auslagerung der Datenbearbeitungen an Dritte wirft zahlreiche organisatorische und technische Fragen zur Sicherheit und zum Datenschutz auf. Können rechtliche, organisatorische und technische Massnahmen die Vorgaben ausreichend gewährleisten und damit Vertrauen in die Datenbearbeitung durch Dritte schaffen? Oder ist Vertrauen nicht möglich und die Nutzung der neuen Möglichkeiten der Auslagerung von Datenbearbeitungen – insbesondere bei sensitiven Daten – nicht verantwortbar?

Das SPS 2012 geht diesen Fragen vertieft nach. Chancen und Risiken der neuen technologischen Möglichkeiten werden analysiert. Ist «Trusted Computing» möglich? Welche rechtlichen Rahmenbedingungen sind zu schaffen und wie kann die «Compliance» hergestellt werden? Dies alles in einem Umfeld, wo Daten immer umfassender erhoben werden und der Zugriff (auch unbefugter) Dritter immer häufiger ist. Dazu bringt das Symposium Vertreter(innen) aus den verschiedenen Bereichen miteinander ins Gespräch.

Wir würden uns sehr freuen, Sie oder jemanden aus Ihrem Unternehmen oder Ihrer Verwaltung aus den Bereichen Technik, Informatik, IT-Sicherheit, Compliance, Datenschutz, Recht oder Risk Management am diesjährigen Symposium begrüssen zu dürfen.

Mit freundlichen Grüssen
Für die Stiftung für Datenschutz und Informationssicherheit



Dr. Bruno Baeriswyl
Datenschutzbeauftragter des Kantons Zürich
Präsident privatim

Dr. Beat Rudin
Datenschutzbeauftragter des Kantons Basel-Stadt
Lehrbeauftragter an der Universität Basel

Als ISSS-Mitglied erhalten Sie 20% Rabatt auf die Ticketpreise. Bei der Online-Anmeldung das Feld «ISSS» ankreuzen!

Weitere Informationen finden Sie unter: http://www.privacy-security.ch/2012/default.htm

Information Security Society Switzerland

Agenda: Security Events unserer Partner

Nächste Security Events unserer Partner

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

Datum	Zeit	Veranstalter	Titel und Details	Ort
Do, 12.07.2012	18:00 - 21:00	swisssecurity.org	swisssecurity.org Stamm Der Anlass ist kostenlos für Mitglieder einer der 12 Sicherheitsorganisationen in swisssecurity.org. Jeder zahlt seine konsumierten Getränke selbst. Details, Anmeldung	Zürich, Amber Bar&Club
Di, 14.08.2012	16:00 - 18:30	OWASP	OWASP Switzerland Meeting Die Teilnahme ist kostenlos. Details	Zürich
Di, 14.08.2012	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
Mi, 29.08.2012	ganztags	sdi, privatim	17. Symposium on Privacy and Security ISSS Mitglieder erhalten 20% Rabatt. Details, Anmeldung	Zürich
Di, 11.09.2012	18:30 - 23:30	DEFCON Switzerland	DEFCON Switzerland Beer on Tuesday Ort: Blues Bar, Speichergasse 29, 3000 Bern Die Teilnahme ist kostenlos. Details	Bern
Di, 09.10.2012	16:00 - 18:30	OWASP	OWASP Switzerland Meeting Die Teilnahme ist kostenlos. Details	Zürich
Di, 09.10.2012	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

Information Security Society Switzerland

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
Fr - Di, 27.07.-31.07.2012	08:30 - 17:00	Swiss Infosec AG	Vorbereitung CISSP Erfolgreiche CISSP-Zertifizierung dank seriöser Vorbereitung! Die Certified Information Systems Security Professional (CISS Details	Zürich
Mo - Di, 20.08.-02.10.2012	09:00 - 17:00	Swiss Infosec AG	Certified IT Process and Quality Manager - Foundation Level Aufbau und Weiterentwicklung eines prozessorientierten Qualitätsmanagementsystems. Details	Olten
Mo - Di, 20.08.-21.08.2012	09:15 - 17:15	Compass Security AG	Web Security Basic Bei diesem Seminar erlernen Sie anhand von Theorie und praktischen Laborübungen im Hacking-Lab die OWASP TOP 10 kennen. Details, Anmeldung	Jona
Mi - Fr, 22.08.-24.08.2012	09:00 - 17:00	Swiss Infosec AG	Sicher entscheiden und umsetzen Grundkurs für Krisenorganisationsmitglieder und Entscheidungsträger Details	Olten
Mi - Do, 22.08.-23.08.2012	09:15 - 17:15	Compass Security AG	Web Security Advanced Dieser Kurs richtet sich an erfahrene Web Security Spezialisten die sich im Thema vertiefen wollen. Details, Anmeldung	Jona
Do, 23.08.2012	09:00 - 17:00	Swiss Infosec AG	Einführung ISO 27001/27002 Einführung und Überblick über die Norm ISO 27001 und den Standard ISO 27002. Details	Chur

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

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 www.isss.ch