ISSS NewsFlash

April 2012

Editorial

Die Information Security Society Switzerland (ISSS) hat etwas zu feiern: Wir haben an unserer St. Galler Tagung am 28.3.2012 das 1000. Mitglied begrüssen dürfen! Dank dieser Grösse wird die ISSS vermehrt aktiv von Behörden, Organisationen und der Presse zu Anliegen der Informationssicherheit in der Schweiz angefragt. Als abtretender Präsident ist es für mich eine grosse Freude, die ISSS an der Vereinsversammlung vom 17.4.2012 in dieser Stärke an den zukünftigen Vorstand zu übergeben.

Die Revision des ZertES, dem Gesetz zur digitalen Signatur, verdient eine fachliche Betrachtung durch Experten der ISSS. Daher suchen wir noch Mitglieder mit Kenntnissen zur digitalen Signatur und PKI, welche in unserer Task Force mitarbeiten wollen. Interessierte melden sich bitte umgehend bei sekretariat@isss.ch.

Kürzlich wurde das Programm der ISSS Zürcher Tagung 2012 zum spannenden Thema „Wie sicher sind ‚sichere' IT-Systeme" sowie der ISSS Security Lunch zur „Kreditkartensicherheit nach dem PCI DSS Standard" auf unserer Website www.isss.ch aufgeschaltet. Nutzen Sie diese Gelegenheiten zur Weiterbildung und fürs Networking mit Security Experten.

Das Schwerpunktthema „Webarchivierung" in dieser Ausgabe gibt die Kernpunkte des kürzlichen Security Lunches wieder.

Ich wünsche dem neuen Vorstand unter neuer Leitung alles Gute und viel Erfolg beim Meistern zukünftiger Security Herausforderungen.

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

Beste Grüsse,
i

Highlights in dieser Ausgabe

ISSS: Kurznews

Die Information Security Society Switzerland (ISSS) begrüsst ihr 1‘000. Mitglied!

Am 28.3.2012 hat die Information Security Society Switzerland (ISSS) an ihrer St. Galler Tagung 2012 mit Herrn Martin Möbes, IT Security Officer einer Bank, das 1’000. Mitglied aufgenommen.

Herr Möbes wurde durch den Leiter der St. Galler Tagung, Ivan Bütler, sowie ISSS-Vorstandsmitglied, Umberto Annino, herzlich in der ISSS begrüsst.

In den letzten fünf Jahren ist die ISSS somit von gut 400 Mitgliedern auf über 1’000 gewachsen. Mit ihrem attraktiven und vielfältigen Angebot an hochwertigen Security Tagungen, regionalen Security Lunches, Special Interest Groups, dem Videokanal http://youtube.com/ISSSview und dem Online Member Area verbindet die ISSS ein grosses und aktives Netzwerk von Security-Experten in der Schweiz miteinander. Mitglieder profitieren zudem von grosszügigen Vergünstigungen, z. B. bei Security-Kursen, die von den ISSS-Schulungspartnern organisiert werden.

ISSS at Geneva Security Forum 2012

ISSS will be represented by its president Dr. Thomas Dübendorfer, ISSS SIG Lead Mark Saxer and several members of the more than 50 expert strong ISSS SIG "Cyber Defense" at the Geneva Dialogue on Cybersecurity - Protecting Critical Infrastructure against Cyberattacks, on April 16-17, 2012. The event is organized by the Geneva Security Forum in cooperation with the Swiss Ministry of Defence and the East West Institute.

Countless meetings, international conferences and growing awareness of the challenges posed by increased cyber-vulnerability, have failed to deliver significant progress on developing cross-border agreements on key issues, in particular relating to Critical Infrastructure Protection. The nature of the challenges inherent in the development of cybersecurity policy at a national level have been so unwieldy and complex that addressing these issues with the goal of reaching some kind of international agreement has seemed close to impossible. The Geneva Dialogue 2012 will tackle some of the most critical issues related to developing international mechanisms to ensure cybersecurity, with a particular focus on Protecting Critical Infrastructure against Cyber-Attacks.

GENEVA SECURITY FORUM

http://genevasecurityforum.org/

Information Security Society Switzerland

ISSS: Kurznews

Security Lunch: Kreditkartensicherheit nach dem PCI DSS Standard am 26.4.2012 im Ristorante Certo, Zürich von 12.00 – 14.00 Uhr

Das Referat gibt einen Überblick zum gemeinsam von VISA, MasterCard und drei weiteren Kreditkartenfirmen entworfenen Kreditkartensicherheits-Standard PCI DSS. Es wird erklärt, welche Anforderungen für online Kreditkartenakzeptanzstellen gestellt werden und was bei einem Audit geprüft wird. Der Standard gibt diverse technische Vorgaben vor, deren Umsetzung an konkreten Szenarien erläutert wird.

Der Referent Peter Sakal ist IT-Security Consultant und PCI DSS Auditor bei der usd AG, einem Beratungshaus für IT-Security und Kreditkartensicherheit in Deutschland und in der Schweiz.

Das detaillierte Programm sowie das Anmeldeformular finden Sie auf hier.

Aufruf zur Mitwirkung an der ISSS-Stellungnahme zur Vernehmlassung „Totalrevision ZertES“, der Gesetzgebung über die digitale Signatur

Am 19. März 2012 hat das Bundesamt für Justiz die Vernehmlassung zur Totalrevision des Bundesgesetzes über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) eröffnet[1]. Die Revision wird damit begründet, dass sich die Erwartungen an die Schaffung einer Rechtsgrundlage für den elektronischen Verkehr in Wirtschaft und Verwaltung bisher nicht erfüllt haben. Die geltende Regelung wird insbesondere beim Massengeschäft als zu aufwändig erachtet. So fehlen beispielsweise einfache, praktikable Lösungen für elektronische Eingaben im Betreibungsverfahren sowie für maschinell lesbare Belege in der Mehrwertsteuer-Abrechnung. Nicht vorhanden ist auch die Möglichkeit der elektronischen Signatur für juristische Personen und Behörden. Durch die Gesetzesrevision soll mit der neu geschaffenen “**geregelten Signatur**“ die Nutzung im Tagesgeschäft ermöglicht, die digitale Signatur für juristische Personen und Behörden eingeführt, die Kombination der digitalen Signatur mit dem Zeitstempel geprüft und allgemein der Umgang mit elektronischen Dokumenten für die Anwender einfacher und sicherer gestaltet werden.

Die ISSS hat sich verschiedentlich mit der Anwendung der digitalen Signatur auseinandergesetzt, so an der Berner Tagung vom 20.11.2001 “PKI – quo vadis?“. Die ISSS hat zum Entwurf des heute geltenden Gesetzes am 27.03.2001 eine ausführliche Stellungnahme abgegeben, am 28.03.2001 zu diesem Thema eine Fachtagung in Zürich veranstaltet[2], und die Einführung des ZertES während mehrer Jahre mit einer “PKI Benutzergruppe“ begleitet. Wir gehen davon aus, dass der ISSS zahlreiche Mitglieder angehören, welche aus ihrer Tätigkeit konkrete Erfahrungen im Umgang mit elektronischen Signatur- und Authentisierungs-Verfahren verfügen. Diese aus der Praxis gewonnen Erfahrungen möchten wir in die Totalrevision der Gesetzgebung über digitales Signieren einbringen.

ISSS Mitglieder und weitere an der Revision ZertES interessierte Kreise werden daher eingeladen, ihr **Interesse an der Mitwirkung der vorgesehenen Task Force zur Prüfung der Totalrevision der Grundlagen der digitalen Signatur der ISSS Geschäftsstelle per E-Mail an sekretariat@isss.ch möglichst rasch bekannt** zu **geben**, so dass wir die neue Rechtsgrundlage kritisch und konstruktiv auf die Erfüllung der Anforderungen aus der Praxis prüfen können. Die Tätigkeit der Arbeitsgruppe soll mit der Einreichung einer Stellungnahme auf den 6. Juli 2012 abgeschlossen werden.

---

[1] Unterlagen verfügbar auf: http://www.ejpd.admin.ch/content/ejpd/de/home/dokumentation/mi/2012/2012-03-280.html
[2] Dokumentation auf der ISSS Webseite abrufbar:

- Unterlagen der FGSec Fachtagung PKI Infrastructure, 2001
- Stellungnahme zum Entwurf des "Bundesgesetz über die elektronische Signatur" (BGES), 2001

ISSS: Kurznews

Teilnehmer für Technologie-Gespräche am Alpbacher Forum gesucht

Congress Centrum Alpbach

Zum Thema **„Erwartungen – Die Zukunft der Jugend“** findet auch in diesem Jahr wieder das Europäische Forum Alpbach in Tirol statt. Seit 1945 treffen sich hier alljährlich im August renommierte Referenten und Referentinnen sowie Gäste aus allen Teilen der Welt. Fachleute und Studierende aus ganz unterschiedlichen Feldern der Wissenschaft, Wirtschaft und Politik kommen zusammen, um aktuelle Fragen der Zeit zu diskutieren und interdisziplinäre Lösungsansätze zu finden.

Vom **23.-25.08.2012** werden im Rahmen dieses Forums auch Technologiegespräche durchgeführt. Eine ganztägige Diskussionsrunde zum Thema **„Cyber-Sicherheit von Institutionen, Unternehmen und Individuen als kritischer Stabilitätsfaktor der modernen Gesellschaft“** wird angeboten. Alle Teilnehmer/innen haben die Möglichkeit, einen Vortrag zu halten. Die besprochenen Themen werden schriftlich festgehalten, um sie anschliessend allen Anwesenden zugänglich zu machen.

Teilnehmer/innen, die sich gerne auf europäischer Ebene zum Thema Security äussern möchten, sind zu diesen Technologiegesprächen herzlich eingeladen: Es werden noch Referenten und Referentinnen gesucht. Weitere Infos erhalten Sie von ISSS-Mitglied Thomas Bräuer (E-Mail: thomas.braeuer@nsn.com) sowie unter der Webadresse des Forums http://www.alpbach.org.

Reminder – ISSS Generalversammlung am 17. April 2012

Am Dienstag, den 17. April 2012, findet wie bereits angekündigt die Generalversammlung der ISSS im Auditorium der Swisscom in Worblaufen nahe Bern statt. Zudem erwartet Sie ein spannendes Referat über "**Sicherheit bei Swisscom (Schweiz) im Dienste der Kunden"** von Marcel Zumbühl, *Leiter Sicherheit von Swisscom (Schweiz) AG, Dozent ETH und* Remo Viscardi, *Leiter der ICT Security Services im Bereich Grosskunden der Swisscom (Schweiz) AG*
Da uns Ihre Meinung als Mitglied sehr am Herzen liegt, laden wir Sie ein, an dieser Veranstaltung teilzunehmen!
Die Anzahl der Plätze ist auf 100 begrenzt. Bei Interesse melden Sie sich bitte direkt hier an: Anmeldung

Weitere Informationen entnehmen Sie bitte unserer Website www.isss.ch

Event: ISSS Zürcher Tagung 2012

Sicherheitsprüfung von IT- Systemen – Lästige Pflicht oder zwingende Notwendigkeit?
ISSS Zürcher Tagung 2012, 12. Juni 2012, IBM Forum, Zürich Altstetten

Die Information Security Society Switzerland (ISSS) widmet sich an der diesjährigen Zürcher Tagung dem Thema Sicherheitsprüfung und gibt dabei nicht nur einen Überblick über die verschiedenen Typen von Sicherheitsprüfungen, sondern geht auch auf die entsprechenden Rahmenbedingungen ein. Eventuelle Schwachstellen zu kennen ist klarerweise ein erster Schritt in die richtige Richtung.

Ob Netzwerkschwachstellen oder andere sicherheitskritische Lücken, eine Prüfung sollte alle Verletzlichkeiten hervorbringen und den wahren Stand der Sicherheit offenlegen:

- Wie sicher sind Systeme, welche die Überprüfung erfolgreich abgelegt haben, wirklich?
- Was wird unternommen, wenn ein System die Überprüfung nicht besteht?
- Wie wird mit erkannten Risiken umgegangen?

Im Abschlussbericht einer Überprüfung werden nicht nur aufgezeigt, welche Methoden und Hilfsmittel verwendet wurden, sondern auch, welche Schwachstellen gefunden wurden. Es gibt jedoch viele Fragen, welche zusätzlich gestellt werden müssten, die jedoch meist ausgeklammert oder unzureichend beantwortet werden:

- Welche Testmethoden werden eingesetzt, um einzuschätzen, wie gross die Chancen eines Angriffes sind?
- Welche Massnahmen werden aufgrund der Prüfungsergebnisse ergriffen?
- Welche Lehren werden gezogen/kommuniziert?

Struktur der Zürcher Tagung 2012

Die Tagung beleuchtet in einem ersten Teil die technisch-organisatorischen Aspekte der Prüfungsmethoden und im zweiten Teil die rechtlichen Aspekte, welche es bei einer Prüfung zu beachten gilt. Im Anschluss gibt es ein offenes Panel mit den Referenten.

Technisch-organisatorische Prüfung

Verschiedene Typen von Sicherheitsprüfungen werden vorgestellt und die Aussagekraft der Ergebnisse analysiert. Insbesondere wird darauf eingegangen, wo die Grenzen der Tests sind und welche Aussagen nach einem Test zulässig sind.

Welches sind die Unterschiede zwischen Sicherheitsprüfung und Qualitätssicherung? Dieser Frage wird durch den Vergleich von einem im Entwicklungsprozess integrierten Security Audit und einer Überprüfung der IT-Infrastruktur, im Bereich „Systemüberprüfung“ auf den Grund gegangen.

Die Zürcher Tagung wird aufzeigen, was zu einem Systemcheck gehört, wie vollständig dieser durchgeführt werden kann und in welchen zeitlichen Abständen eine Wiederholung empfohlen wird.
Auch auf die „Personenüberprüfung“ wird eingegangen werden. Angesprochen werden hier Techniken wie Strafregisterauszug, Betreibungsregister, Erpressbarkeit, Backgroundchecks und Internetanalysen. Diskutiert werden sowohl die Zulässigkeit als auch die anzustrebenden Intervalle dieser der Öffentlichkeit nicht so bekannten Prüfung.

Rechtsgrundlagen und juristische Aspekte

Nicht alles, was technisch und organisatorisch möglich ist, ist auch rechtlich erlaubt: Dabei stellen sich folgende Fragen:

Wo beginnt die rechtliche Grauzone der Prüfungen und welche Prüfungen sind nicht einmal mit Einverständnis des Arbeitnehmenden zulässig?

- Wie viel Druck darf ausgeübt werden, um die Zustimmung eines Mitarbeitenden zu
- erhalten?
- Wie wird mit den Resultaten einer Prüfung umgegangen?

Zusätzlich steht die Haftungsfrage bei Unterlassung der Sicherheitsprüfungen immer im Raum:

- Wie geht man verantwortungsvoll und nachhaltig an diese Aufgabe heran und wie wird in Verdachtsfällen mit den Verantwortlichen umgegangen?

Wie wird mit Datendiebstahl umgegangen und welche Konsequenzen hat dieser für die Firma respektive für die Betroffenen?

- Wie kann aufgrund der Auswertung einer Sicherheitsprüfung das Sicherheitsbewusstsein des Personals erhöht werden?
- Wie werden bei Audits durch Dritte die Geschäftsgeheimnisse abgesichert?

Tagungsprogramm & Anmeldeformular

ISSS: CeBIT 2012: Rückblick

Genereller Eindruck [3]

Generell waren die typischen IT-Security-Hallen 11 und 12 nur zur Hälfte belegt. Dies lag daran, dass die absoluten Ausstellerzahlen zwar insgesamt gestiegen sind, jedoch die Aussteller mit vormals grossen Standflächen der Messe entweder gänzlich fernblieben oder sich einschränkten. Viele Unternehmen schlagen mittlerweile einen anderen Weg ein und verzichten auf Präsentationen ihrer Produkte während der Messe, um mit eigenen Roadshows ihre Kunden zu erreichen. Dass diese Entwicklung tatsächlich stattfindet, bestätigt schon die Tatsache, dass die Messe ohne Weiteres umdisponieren konnte: Wegen baulicher Schäden in einer stillgelegten Halle mussten die Aussteller kurzerhand in eine andere Halle verlegt werden. Dies wäre noch vor fünf Jahren logistisch unvorstellbar gewesen. Nichtsdestoweniger versucht jeder Anbieter dennoch irgendwie auf der Messe präsent zu sein, sei es mit Partnerständen oder Sales-Mitarbeitenden, die ihr Unternehmen vertreten und am Rande das informelle Gespräch mit Interessenten suchen.

Schwerpunkt „Cloud“

Das Schwerpunktthema dieser Messe war eindeutig Cloud-Computing. Hier versuchen alle, ein Stück vom Kuchen abzubekommen. Sei es, dass sie ihre Dienste in der Cloud anboten, oder ein Produkt zum Thema Cloud-Computing beizusteuern hatten.

Die SAP Aktiengesellschaft (in Zusammenarbeit mit der Deutschen Telekom) z. B. wirbt gross damit, dass sie ihre Leistungen in Zukunft auch als Cloud-Service bereitstellen können. Aber auch die Global Player Microsoft, IBM, Oracel und Datev bieten Anwendungen und Services im grossen Stil an. Im Endkundensegment geht die Entwicklung in Richtung Cloud.

http://www.areamobile.de/bilder/91401-original-cebit-2012

Von diesem Thema profitierte auch die CeBIT, da in diesem Jahr auch Anbieter wie Google, Facebook und Xing auf der Messe vertreten waren.

Alle grossen Anti-Malware-Anbieter haben ein Produkt, das letztendlich die transparente Verschlüsselung der Daten in der Cloud ermöglicht. Hierzu können herkömmliche Cloud-Storages oder Share-Services genutzt werden.

Mobile Security

Auch im Bereich Mobile Security haben die Anbieter aufgerüstet. So ist mittlerweile jeder Hersteller einer Security-Lösung mit einer Endpoint-Protection oder Mobile Device Management-Lösung (abgekürzt MDM) am Start – teilweise auch nur als Original-Equipment-Manufacturer (abgekürzt OEM).

[3] Dieses Dokument fasst die Eindrücke rund um die CeBIT zusammen. Die Messe für Informationstechnik fand im März 2012 statt. Der Artikel gibt die persönliche Meinung und Einschätzung des Autors wieder.

ISSS: CeBIT 2012: Rückblick (Fortsetzung)

Talentsuche

Interessant war, dass der Samstag, der eigentlich in der Vergangenheit durch Endkunden geprägt war, zum Recruiting-Day ausgerufen wurde. Viele Aussteller hatten hier ihre Recruiter am Stand, bei denen interessierte Personen nachfragen konnten. Das Konzept erscheint dem ersten Eindruck nach sehr vielversprechend zu sein.

Social Events

Letztendlich dient die CeBIT nach wie vor als Branchen-Treff, um zu sehen und gesehen zu werden. Die grossen Deals werden beim Networking am Abend besiegelt. Dennoch bietet die CeBIT nach wie vor eine wichtige Plattform, um interessierten Besuchern und Besucherinnen Informationen für das Daily Business bereitzustellen.

Schlussfolgerungen

Die Zeiten, in denen Hersteller ihre bahnbrechenden Innovationen punktgenau zur CeBIT präsentierten, sind leider vorbei. Ist ein IT-Verantwortlicher auf der Suche nach konkreten Lösungen (oder Informationen) für sein Unternehmen, ist er auf der CeBIT nach wie vor an der richtigen Adresse. Hier kann man sich einen konkreten Überblick verschaffen. Ist man hingegen auf der Suche nach neuen Impulsen oder tollen futuristischen Ideen, sollte man lieber Google bemühen.

Über den Autor

Marco Di Filippo, Regional Director Germany, Compass Security AG, Jona SG (Schweiz)

Als Regional Director Germany ist er für die Geschäftsentwicklung in Deutschland innerhalb der Compass verantwortlich. Auch in diesem Jahr war er mit zahlreichen Vorträgen auf der CeBIT zum Thema Cloud- u. Mobile-Security vertreten, unter anderem als Gastreferent beim Bundesministerium für Wirtschaft und Technologie, dem CeBIT Professional Data Center, dem Heise CeBIT Plaza sowie dem Gemeinschaftsstand von Sophos und Astaro.

E-Mail: marco.difilippo@csnc.ch

Swiss Crows / ISSS: Cyber Defense Conference

Die Swiss Crows und die ISSS laden Sie herzlich zur Cyber Defense Conference ein.
Mittwoch 25. April 2012, 14.00 Uhr in Aarau

Für ISSS-Mitglieder gilt ein Sonderpreis von CHF 30.-, wenn die Anmeldung bis zum 20. April 2012 erfolgt.

14.00	Begrüssung und Einleitung	**Richard Morva** President Swiss Crows Dipl. Ing. FH, IPMA CSPM, Senior Consultant
14.05	Keynote: Die Information als Waffe in der nationalen Unsicherheit	**Peter Regli** Div a.D. / Dipl. Ing. ETHZ Berater in sicherheitspolitischen Fragen
14.30	Cyber Bedrohungslage	**Riccardo Sibilia** Chef Cyber-Bedrohungsanalyse Zentrum elektronische Operationen, VBS
15.00	KOBIK, die gemeinsame Task Force der Kantone und des Bundes	**Tobias Bolliger** lic. iur., Fachsbereichsleiter Clearing&Analyse KOBIK, Bundes-kriminalpolizei, EJPD
15.30	Rechtliche Aspekte von Crime and De-fense im Cyberspace	**Beat Lehmann** lic. iur., Fürsprecher, Vorstand ISSS Dozent für jur. Aspekte der IT Security HS-LU
16.00	**Kaffee – Pause im Foyer**	
16.30	Die nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken: Akzente und weiteres Vorgehen	**Gérald Vernez** MAS ETH SPCM (Zürich) Projektleiter Stv. Cyber Defense , VBS
17.00	Engagement der Industrie im Bereich Cyber Defense	**Bruno Blumenthal** Dipl. Ing. FH, CISSP, Teamleader Information Security RUAG Defense
17.30	Podiumsdiskussion mit allen Referenten Moderation: Dr. Daniel Heller	**Dr. Daniel Heller** Dr. phil. I, UZH, Partner Farner Consulting AG, Militärpublizist
18.15	**Apéro riche im Foyer**	

Weitere Informationen und Anmeldung

Fokus: Webarchivierung

"Der Online-Kanal wächst rapide - welche Mittel gibt es zur Umsetzung von Rechtssicherheit im Internet?"

Anlässlich des ISSS Security Lunches vom 15.3.2012 trafen sich gut zwanzig Security Professionals in Zürich, um sich zum Thema Webarchivierung zu informieren und eine aktuelle Fallstudie der SBB zu hören. Neben dem im Folgenden dargelegten spannenden Thema bot der Anlass auch eine gute Gelegenheit zum persönlichen Networking.

Das Internet als Kommunikations- und Transaktionskanal wächst rasant und wird immer relevanter für die Unternehmen und Organisationen. Wie aber lassen sich die geschäftsrelevanten Informationen wie z. B. Internet-AGBs und E-Shop-Transaktionen rechtssicher verwalten? Und wie werden die Verbindlichkeitsanforderungen auf den Social Media-Kanälen wie Facebook umgesetzt?

Wie können Security Professionals aller Bereiche (Information, Compliance, Risk, Governance und Privacy) den Online-Kanal absichern und damit als kosteneffizientesten, flexibelsten und kundenfreundlichsten Kanal weiter stärken?

Der Einsatz von Web-Archivierung schafft hier Abhilfe: Web-Archivierung ist das Sammeln und dauerhafte Ablegen von Online-Informationen und –Transaktionen.[4]

Drei Methoden der Web-Archivierung

Es gibt drei unterschiedliche Methoden zur Archivierung von Web-Informationen:

- **Remote Harvesting** (oder client-seitige Archivierung): zum Erfassen der Web-Informationen nutz dieser Ansatz einen Web-Crawler. Dieser ruft die Inhalte einer Website von aussen ab und schreibt die Ergebnisse in ein Archivobjekt.
- **Database Archiving** (oder server-seitige Archivierung): bei diesem Ansatz werden die Datenbanken der auslieferndenWeb-Systeme archiviert.
- **Transactional Archiving**: Dieses Verfahren überwacht den gesamten Nutzungsprozess von Websites und –Applikationen und ermöglicht dadurch eine lückenlose Erfassung der Online-Informationen.

Interview mit Bruno Spicher (SBB, Leiter Kanalentwicklung E-Business):

1. Weshalb hat die SBB sich für eine Web-Archivierungslösung entschieden?

SBB.ch ist seit Jahren unter den top 10 der meistbesuchten Webseiten der Schweiz. Als im Jahr 2011 der grosse Relaunch vor der Tür stand, war klar, dass der alte Auftritt nicht einfach abgeschaltet werden konnte. Genau, wie bei alten Kursbüchern oder wichtigen Werbekampagnen sollten auch hier ein Stück kulturelles Erbe aufbewahrt werden. Mit www.sbb-archive.ch haben wir das weltweit erste interaktive Bahnmuseum der Welt realisiert. Als mehrfacher Gewinner des Best-of-Swiss-Web-Awards war es für das E-Business der SBB klar, dass diese Leistungen auch weiterhin sichtbar sein sollen.

2. Gab es weitere Gründe?

Sicher. Die Projektrisiken beim Relaunch waren hoch. Über 13'000 Seiten in vier Sprachen mussten vom alten Content Management System auf das neue CMS mit einer total neuen Technologie migriert werden. Durch die Archivierungslösung von qumram hatten wir die Sicherheit, dass keine Inhalte verloren gehen und das alte System nach dem Relaunch trotzdem sofort abgestellt werden konnte. Dies senkte die Risiken und die Betriebskosten deutlich.

[4] Die in diesem Artikel verwendeten Definitionen sind in Anlehnung an Wikipedia formuliert: DE: http://de.wikipedia.org/wiki/Web-Archivierung, resp. ENG: http://en.wikipedia.org/wiki/Web_archiving

Fokus: Webarchivierung (Fortsetzung)

3. Noch ein Grund?

Klar, aller guter Gründe sind drei. Da wir nebst dem statischen Content auch Use Cases des „Online-Fahrplans“ und des „Ticket Shops“ archivieren, stellen wir eine Art Proof-of-Concept für zukünftige Compliance Anforderungen sicher.

4. Bitte erklären Sie dies kurz?

Der E-Kanal (Online und v.a. Mobile) wächst seit einiger Zeit exponentiell. Damit werden nebst der Relevanz auch die Sicherheitsanforderungen an diesen Kanal immer grösser. Dabei muss die Frage nach der lückenlosen Aufzeichnung der Verkäufe – also der eigentlichen Transaktionen - und der Aufbewahrung der Verkaufsbelege beantwortet werden. Die Archivierung der für den Kunden sichtbaren Web-Inhalte ist sicherlich eine sich aufdrängende Option in dieser Fragestellung.

Herzlichen Dank für diese interessanten Ausführungen und viel Erfolg mit dem E-Business @SBB!

Abbildung 1: Bruno Spicher anlässlich des ISSS Security Lunches vom 15. März 2012 in Zürich.

Sieben exemplarische Anwendungsfälle der Web-Archivierung

1. Kontrollierte Publikation von Weisungen, Empfehlungen und Informationen

Immer mehr Informationen werden von den klassischen Kanälen und Formaten aufs Web verschoben, auch Informationen mit hoher Verbindlichkeit. Während früher beispielsweise Weisungen ausgedruckt und verschickt oder in Form von PDF-Dateien via E-Mail versandt und im Anschluss archiviert wurden, stehen diese Informationen mittlerweile auf Websites oder in Intranets zur Verfügung. Die Gründe dafür sind unter anderem die diversen Möglichkeiten zur effizienteren und kostengünstigeren Publikation und Distribution der Information. Informationen, die Weisungscharakter haben, unterliegen jedoch in der Regel den Vorgaben bezüglich Nachweisbarkeit. Unter regulierten Rahmenbedingungen muss eine Firma auf Anfrage genau belegen können, zu welchem Zeitpunkt welche Version der Weisung publiziert und damit gültig war, auch auf dem Online-Kanal. Die Frage „Welche Inhalte wurden wann und wie publiziert?“ kann dank einem Web-Archivierungssystem beantwortet werden
Die Schweizer Unfallversicherung (Suva) stellt die Nachvollziehbarkeit der Online-Informationen denn auch mittels Web-Archivierung sicher.

2. Sichere Kommunikation von Produkt- und Finanzinformationen

Finanzinstitute kommunizieren ihre Zinssätze und Konditionen genauso auf ihren Webplattformen, wie Telekommunikationsfirmen ihre Produktinformationen und die verschiedenen Abonnementskonditionen. All diese Preise sind starken Schwankungen unterworfen und führen immer wieder zu Diskussionen zwischen Anbietern und Endkunden. Durch die Web-Archivierung können diese Diskussionen auf einer zuverlässigen und rechtssicheren Faktenlage geführt werden. Denn der **Anbieter ist damit in der Lage eindeutig zu belegen, welche Preise und Konditionen auf seiner Web-Plattform zu jedem beliebigen Zeitpunkt in der Vergangenheit publik waren**. Nicht nur steigt damit die Beweiskraft

Fokus: Webarchivierung (Fortsetzung)

der Online-Informationen massiv an, eine starke Entlastung für jeden Kundendienst ist ebenfalls eine direkte Folge davon.

3. Kontrollierte Verwaltung von AGBs und Disclaimers

Wer kennt es nicht aus persönlicher Erfahrung, wie vor jedem Online-Einkauf noch das Häkchen gesetzt werden muss, dass die AGBs gelesen und akzeptiert wurden. Dank iTunes von Apple wissen auch die Meisten, wie häufig diese AGBs wechseln und wie wenig sie wirklich gelesen werden. Mittels Web-Archivierung kann ein Anbieter jederzeit nachweisen, welche ABGs zu welchem Zeitpunkt in seinem E-Shop aktuell waren und er weiss sogar genau, welche spezifische Version der AGBs von den einzelnen Kunden akzeptiert wurden und diesen gegenüber entsprechend gültig sind. **Die Web-Archivierung erlaubt damit, den Online-Kanal nahtlos in das Vertragsmanagement einer Organisation zu integrieren.**

4. Schlankere und sicherere Prozesse im E-Shopping, E-Offering und E-Government

Heute werden viele webbasierte Bestellprozesse, gerade im Versicherungs- und E-Government-Umfeld, aber auch bei E-Shop Bestellungen mittels Medienbrüchen unnötig verkompliziert. Der verbindliche Beleg ist dann jeweils nicht mehr eine Webseite, sondern eine E-Mail oder betreffend Medienbrüchen noch schlimmer eine PDF-Datei, die ausgedruckt, händisch unterschrieben und per Post verschickt wird.
Durch die Einführung der Web-Archivierung wird die Abschaffung von heute angewandten *„Workarounds“ und die Reduktion von unnötigen Medienbrüchen möglich*. Damit wird Benutzerfreundlichkeit und Sicherheit dieser Abläufe signifikant erhöht und gleichzeitig werden aufgrund deren Verschlankung die Prozesskosten reduziert. Die Attraktivität des E-Kanals steigt damit für alle involvierten Stakeholder massiv.

5. Zuweisung und Ergänzung des Kunden-, Patienten- resp. Bürgerdossiers mit Web-Aktivitäten

Nicht nur im E-Health Umfeld ist das E-Dossier seit Jahren ein Buzzword. Dank der Web-Archivierung wird es möglich sein, diese persönlichen Dossiers mit persönlichen Web-Aktivitäten und Web-Informationen zu ergänzen, resp. selber zu pflegen und gleichzeitig eine vollständige Historie über sämtliche Dossier-relevanten Informationen zu erhalten. **In diesem Anwendungsfall wird es wohl vermehrt zu notwendigen und heissen Diskussionen mit dem Datenschutz kommen.**

6. Absicherung von Inhalten, die auf externen Plattformen laufen

Die Auslagerung von internen Web-Plattformen und –Applikationen in die Cloud ist ein aktueller Megatrend der IT. Die Security Professionals weisen aber zu recht auf den damit einhergehenden Kontrollverlust hin. **Durch die Web-Archivierung wird es möglich, den Auslagerungstrend voll mitzumachen und die geschäftsrelevanten Informationen und Transaktionen aus der Cloud aufzuzeichnen** und in die von der eigenen revisionssicheren Recordsmanagemt- und Archiv-Systeme zu transferieren. Die Nachvollziehbarkeit über die Informationsflüsse kann damit realisiert werden, unabhängig davon, wer die Systeme betreut und wo diese lokalisiert sind.

7. Kontrolle von Inhalten, die das Unternehmen nicht selber erstellt hat

Das rapide Aktivitätswachstum auf den Social Media Plattformen wie Facebook oder Twitter führt dazu, dass immer mehr Inhalte zu Firmen und Organisationen durch Kunden, Mitarbeiter, Mitbewerber, etc. auf externen Web-Plattformen geschrieben und über diese verbreitet werden. **D.h. die technologie-gestützte Kontrolle über die Kommunikation ist den Firmen und Organisationen längst entglitten.** Die Web-Archivierung wird im Bereich der E-Discovery und des Social Media Monitorings eine wesentliche Rolle spielen, weil die kritischen Kanäle gezielt aufgezeichnet die darüber publizierten Informationen auf diese Weise ebenfalls aufbewahrt werden können.

Fokus: Webarchivierung (Fortsetzung)

Die eingesetzte Archivierungsmethode (siehe oben „Drei Methoden der Web-Archivierung“) bestimmt unmittelbar, welche Anwendungsfälle (siehe oben „Sieben exemplarische Anwendungsfälle der Web-Archivierung“) eine Lösung bzw. ein Anbieter zu adressieren in der Lage ist. Dies ist in der folgenden Tabelle illustriert:

	Archivierungsmethode		
Anwendungsfälle	Remote Harvesting (client-seitig)	Database Archiving (server-seitig)	Transaktionale Archivierung
1. Kontrollierte Publikation von Weisungen, Empfehlungen und Informationen	teilweise	teilweise	✓
2. Sichere Kommunikation von Produkt- und Finanzinformationen	teilweise	teilweise	✓
3. Kontrollierte Verwaltung von AGBs und Disclaimers	teilweise	teilweise	✓
4. Schlankere und sicherere Prozesse im E-Shopping, E-Offering und E-Government		teilweise	✓
5. Zuweisung und Ergänzung des Kunden-, Patienten- resp. Bürgerdossiers mit Web-Aktivitäten		teilweise	✓
6. Absicherung von Inhalten, die auf externen Plattformen laufen	teilweise		✓
7. Kontrolle von Inhalten, die das Unternehmen nicht selber erstellt hat	✓		teilweise

Tabelle 1: Geeignete Archivierungsmethode pro Anwendungsfall

Das Symbol ✓ bedeutet, dass der jeweilige Lösungsansatz in der Lage ist, die aktuellen Anforderungen der Anwendungsfälle zu erfüllen. Wenn “teilweise“ steht, heisst das, dass der Lösungsansatz einen Teil der aktuellen Anforderungen nicht abdeckt und auch nicht in der Lage sein wird, diese abzudecken (gerade aufgrund systeminhärenter Design-Ansätze).

Das bedeutet, dass zur umfassenden Erzielung von Compliance bzw. der Realisierung der allermeisten Anwendungsfälle zur Geschäftsoptimierung die transaktionale Methode zur Web-Archivierung eine Grundvoraussetzung darstellt.

Fokus: Webarchivierung (Fortsetzung)

Fünf Mehrwerte der Web-Archivierung

a. Die Web-Archivierung ist **ein Profilierungsfeld für die Security Professionals**. Die Web-Archivierung gibt Antworten zu den Risiken und Unsicherheiten betreffend der neuen IT Trends, wie der Auslagerung in die Cloud oder die unkontrollierte Kommunikation in den Social Media Kanälen. **Die Sicherheit und die Compliance werden erhöht.**

b. Sie optimiert bestehende Geschäftsprozesse, indem z.B. Medienbrüche reduziert werden oder neue Geschäftsfälle ermöglicht werden, bei gleichzeitiger vollständiger Abdeckung der Vorgaben zur Informationssicherheit. **Dies führt zu verschiedensten effizient realisierbaren Optimierungsmöglichkeiten und Innovationen.**

c. Da die Web-Plattform immer nur eine Schnittstelle zum Kunden hat – nämlich den Web-Browser - muss auch nur eine Schnittstelle im Projekt angepasst werden. Da die „Web-Ein-und-Ausgänge“ (Webserver, Web-Entry-Server und Web-Proxy-Server) der Firmen und Organisationen auf eine überschaubare Anzahl an Technologien und Produkten limitiert ist, ist eine **Web-Archivierungs-Lösung einfach implementiert**.

d. Die Bedienung der Web-Archivierung erfolgt durch den Benutzer ohne Schulungsaufwand. Das Surfen auf der archivierten Web-Plattform unterscheidet sich nicht von Surfen auf der aktuellen. **Das Bedienungs-Cockpit, mit dem Zeitstrang und der Volltextsuche ist ebenfalls intuitiv verständlich und einfach**. Zusätzlich lassen sich archivierte Web-Informationen nahtlos in bestehende Drittlösungen und Fachapplikationen wie beispielsweise ein ECM- oder ERP-System integrieren.

e. Durch die Implementierung am „Web-Ein-Aus-Gang“ und das Aufzeichnen des HTML Outputs gibt es **keinerlei Abhängigkeiten von bestimmten Produkten oder Technologien**. Dies gilt sowohl für das Aufzeichnen der Web-Inhalte und –Transaktionen aus WCM-Systemen, Portalen, E-Banking- oder E-Shop-Lösungen, wie für die Archivierung in RM-Systemen. Die eigentliche Information wird von den auslieferndenden Systemen entkoppelt, womit der „ Vendor Lock-in“ gegenüber diesen Technologieanbietern massiv reduziert wird und Systemmigrationen und –konsolidierungen signifikant vereinfacht werden.

Über den Autor

Der Autor Mathias Wegmüller ist Inhaber und Geschäftsführer der qumram AG, die kommerzielle Web-Archivierungslösungen anbietet.

Langjährige Berufserfahrung als Berater und Projektleiter von grossen internetbasierten Vorhaben an der Schnittstelle zwischen Geschäftsanwendungen und Technologie.

www.qumram.ch

wegmueller@qumram.ch

Mathias Wegmüller, Dipl. Natw. ETH, CEO qumram AG

Information Security Society Switzerland

Agenda: Security Kurse unserer Partner

Datum	Zeit	Veranstalter	Titel und Details	Ort
Mo - Fr, 16.04.- 20.04.2012	09:00 - 17:00	Swiss Infosec AG	**Managing Consultant** Wir vermitteln Ihnen unser grosses Know-How kompakt und praxisnah. Zielgerichtet, kompetent und gewinnbringend. 4200.- Details	Zürich
Mo - Fr, 23.04.- 27.04.2012	09:00 - 17:00	Swiss Infosec AG	**IT-SIBE Vertiefung** Erweitern Sie Ihr Fachwissen! Praktischer Vertiefungslehrgang für Informations- und IT-Sicherheitsbeauftragte. 4500.- Details	Sursee
Mo - Fr, 23.04.- 27.04.2012	09:00 - 17:30	OneConsult GmbH	**OPST, inkl. Einführung Protokolle und Scanning Tools** (1. Kurstag) Kurssprache: Deutsch (Unterlagen: Englisch) EUR 3450 (abzüglich 15% ISSS Rabatt) Details, Anmeldung	Salzburg (AT)
Di - Fr, 24.04.- 27.04.2012	09:00 - 17:30	OneConsult GmbH	**OPST (OSSTMM Professional Security Tester)** Kurssprache: Deutsch (Unterlagen: Englisch) EUR 2950 (abzüglich 15% ISSS Rabatt) Details, Anmeldung	Salzburg (AT)
Do - Fr, 03.05.- 04.05.2012	09:00 - 17:30	OneConsult GmbH	**Web-Security Awareness für Entwickler und Administratoren** Kurssprache und Unterlagen: Deutsch Die Kursteilnehmer lernen aktuelle Angriffsmethoden in Theorie und Praxis kennen. CHF 1850 (abzüglich 15% ISSS Rabatt) Details, Anmeldung	Thalwil
Do - Fr, 03.05.- 04.05.2012	17:30 - 18:30	OneConsult GmbH	**Practical Security Scanning** Praxisorientierte Schulung der Mitarbeiter mit dem Ziel, eigenständig Security Scans durchführen und interpretieren zu EUR 1450 (abzüglich 15% ISSS Rabatt) Details, Anmeldung	Wien (AT)
Mo - Do, 07.05.- 10.05.2012	09:00 - 17:00	Swiss Infosec AG	**Sicherheitsmanagement im IT-Umfeld** Mehr Sicherheit dank sicherer Technik! Der Lehrgang vermittelt Ihnen technisches Grundwissen im Bereich IT-Sicherheit. 3500.- Details	Chur
Mo - Do, 07.05.- 10.05.2012	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	Chur

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

Agenda: Security Events von ISSS & Partnern

Security Events von unseren Partnern

Datum	Zeit	Veranstalter	Titel und Details	Ort
Mi, 23.05.2012	09:00 - 12:00	First Security Technology	**FIRST SECURITY EXECUTIVE SUMMIT 2012** Die Teilnahme ist gratis. Details, Anmeldung	Zürich
Mo - Di, 18.06.- 19.06.2012	ganztags	COMPUTAS	**Fachkonferenz "DuD - Datenschutz und Datensicherheit"** Spezialpreis (EUR 1195 statt 1695) für ISSS-Mitglieder Details, Anmeldung	Berlin
Do, 28.06.2012	13:00 - 17:00	Swiss Infosec AG	**20. MEET SWISS INFOSEC!** Event zu Informations- und IT-Sicherheit: Erleben Sie hochkarätige Referenten, lernen Sie uns und unser Partner kennen. Kostenlos Details	Zürich-Flughafen

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

Security Events von ISSS

Datum	Zeit	Veranstalter	Titel und Details	Ort
Mi, 25.04.2012	14:00 - 18:15	Swiss Crows / ISSS	**Cyber Defense Conference** ISSS-Spezialpreis von CHF 30.00 mit Anmeldung bis 20.4.2012. Details, Anmeldung	Aarau
Do, 26.04.2012	12:00 - 14:00	ISSS	**ISSS Security Lunch: "Kreditkartensicherheit nach dem PCI DSS Standard"** Details, Anmeldung	Zürich
Di, 12.06.2012	13:30 - 18:00	ISSS	**ISSS Zürcher Tagung 2012 - Wie sicher sind "sichere" IT-Systeme?** Details, Anmeldung	Zürich
Do, 28.06.2012	12:00 - 14:00	ISSS	**ISSS Security Lunch: "Smart Grid – Intelligente Stromnetze: Chancen und Risiken für die Sicherheit"** Details, Anmeldung	Bern
Di, 27.11.2012	13:00 - 17:30	ISSS	**15. Berner Tagung für Informationssicherheit "Bring your own device: Chancen und Risiken"** Details, Anmeldung	Bern

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

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