ISSS NewsFlash Juli 2010



Editorial

Willkommen zum ISSS NewsFlash

Sie lesen die zweite Ausgabe des ISSS NewsFlash, welcher über die Aktivitäten der Information Security Society Switzerland (ISSS) und unserer Security Partner berichtet.

Sollten Sie die erste Ausgabe von Juni 2010 verpasst haben, so finden Sie diese auf www.isss.ch zum Download bereit.

Im Focus dieser Ausgabe berichten wir über die umfangreiche Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), zu welcher wir von ISSS aus eine Stellungnahme planen.

Der Vorstand hat für Sie den Inhalt der ISSS Zürcher Tagung 2010 „Data Leakage Prevention“ in einem Artikel in dieser Ausgabe zusammengefasst.

Verpassen Sie den Kick-off der SIG „Suisse-ID – benefits and risks for e-commerce“ am 12. Juli nicht. Details finden Sie in der Rubrik „ISSS Security Events“.

Falls Sie selbst einen Artikel für den ISSS NewsFlash schreiben wollen, schicken Sie diesen bitte an unser Sekretariat sekretariat@isss.ch.

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

Highlights in dieser Ausgabe

ISSS:

- ISSS offizieller Supporter von security4kids
- Neue Videos auf ISSSview
- Umzug auf neuen Webserver
- Reaktionen auf ISSS-NewsFlash

Focus:

- Revision Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)

Review:

- Zürcher Tagung 2010 „Data Leakage Prevention“

Agenda:

- Partnerevents
- ISSS Security Events
  - Einladung zum Kick-off der SIG „Suisse-ID – benefits and risks for e-commerce“ am 12.7.
  - Weitere SIGs in Gründung
  - Vorschau Berner Tagung 2010
  - Aufruf zur Mitwirkung bei der geplanten Stellungnahme zur Revision BÜPF

Information Security Society Switzerland

ISSS

ISSS neu offizieller Supporter von security4kids

Die ISSS ist seit Juli 2010 offizieller Supporter von securit4kids und erscheint mit Logo auf http://www.security4kids.ch/. Diese Security-Initiative vermittelt das Thema Online-Sicherheit auf anschauliche und stufengerechte Art an Kinder, Jugendliche, Eltern und Lehrpersonen. Schauen Sie mal vorbei.

Neue Videos auf ISSSview

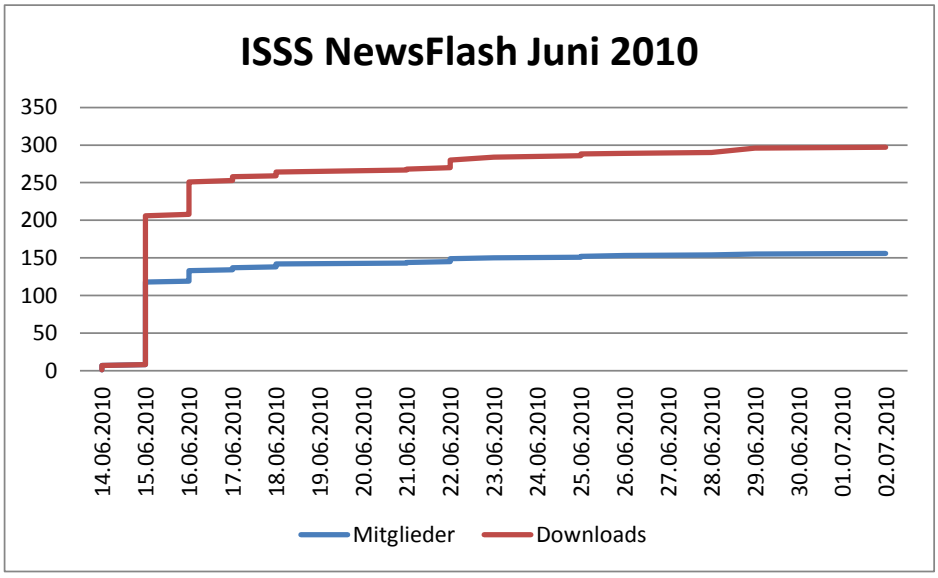
Auf unserem öffentlichen Videoportal http://www.youtube.com/ISSSview finden Sie die Videos zu den zwei ISSS Security Talks **„Business Continuity Management – Notwendigkeit und Chance für das Unternehmen“** von Wolfgang Mahr, der am 24.6.2010 in Zürich stattfand. sowie **„The rise (and fall?) of the CISO“** von Ed Gelbstein, der am 28.6.2010 in Lausanne stattfand. Die Slides sind auf den jeweiligen Eventwebsites verlinkt.

Umzug auf neuen Webserver

Am 14. Juni 2010 wurde isss.ch auf einen Webserver mit schnellerer Datenbankanbindung bei einem neuen Hoster migriert, wodurch die Antwortzeiten unserer Website www.isss.ch merklich von vorher durchschnittlich 1387 ms auf 231 ms verbessert werden konnte. Ein herzliches Dankeschön an unseren Webmaster Bernhard Tellenbach für seinen Wochenendeinsatz!

Reaktionen auf den ISSS-NewsFlash

Der im Juni neue lancierte PDF-Newsletter „NewsFlash“ stiess auf positive Resonanz. So schrieben ISSS-Mitglieder der Redaktion unter anderem *"Ich finde das Look & Feel einfach viel viel viel besser. Für mich und viele in meinem Umfeld ist es eine mega Erleichterung die News zu lesen"*. Die Anzahl Downloads in den ersten drei Wochen seit Versand per Email mit dem Link auf den Newsletter hielt sich mit 297 Downloads durch 156 Mitglieder (siehe auch untere Grafik) allerdings in Grenzen. Gewisse Personen haben ihren persönlichen Downloadlink auf den NewsFlash auch weitergereicht, was durchaus erwünscht ist.



Anzahl Downloads des ISSS NewsFlash Juni 2010 durch Anzahl angegebene ISSS-Mitglieder

Focus: Revision BÜPF – Erarbeitung einer Stellungnahme

Vorbereitung einer Vernehmlassung zur Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)

Autor: Fürsprech Beat Lehmann, ISSS Vorstand

Wir präsentieren hier eine erste Übersicht und Einschätzung über Bestimmungen in dem am 19. Mai 2010 vom Bundesrat in die Vernehmlassung gesetzten Vorentwurfes zur Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), welche für die Anbieterinnen von Fernmeldediensten und Internet Service Providern sowie für die durch Überwachungsmassnahmen betroffenen Personen von Bedeutung sein können und allenfalls bei der Ausarbeitung einer Vernehmlassung zu berücksichtigen wären. Die Bemerkungen zu den einzelnen als kritisch erachteten Bestimmungen sind in *Italics* beigefügt. Die ISSS wird auf dieser Basis bis 18. August 2010 eine Stellungnahme ausarbeiten. Wenn Sie an dieser Stellungnahme mitwirken wollen, melden Sie sich bitte umgehend bei beat.lehmann@isss.ch.

Als Hintergrundinformationen zu unserem Bericht empfehlen wir folgende Dokumente zur Lektüre:

- Vorlage der BÜPF-Revision
- Bericht zur BÜPF-Revision

Im Folgenden nun unsere Kommentare zu einzelnen Gestzesanpassungen.

Art. 2 / 31 Die Überwachung des Post- und Fernmeldeverkehrs wird im Auftrag des bereits bestehenden Überwachungsdienstes des Bundes (“zentraler Dienst“) ausgeführt durch

a) die Anbieterinnen von Post- und Fernmeldediensten, einschliesslich jene Internet-Anbieterinnen (“ISP“) , die ihre Tätigkeit berufsmässig ausüben, sowie durch

b) Personen, die berufsmässig für die Fernmeldedienstanbieterinnen und ISP Kommunikationsdaten verwalten, an Dritte Kommunikationsdaten weiterleiten oder die dafür notwendige Infrastruktur zur Verfügung stellen

Zunächst ist zu erwähnen, dass das Rev. BÜPF, ohne dies im Gesetz eindeutig zum Ausdruck zu bringen, den gesamten analogen und digitalisierten Kommunikationsverkehr erfasst, insbesondere alle Kommunkationen im Internet und die Internet-Telephone.

In Bezug auf die mit Überwachungsaufgaben betreuten Personen stellt sich die Frage, auf welche Stellen, welche Dienstleistungen im Zusammenhang mit dem Internet anbieten, das BÜPF ausgedehnt werden soll. Im Begleitbericht werden unter diesem Titel erwähnt: Reine Service-Provider, Web Hoster, Hosting Provider, Anbieterinnen von E-Mail und Mailbox-Diensten, von Speicherplatz oder externer Daten-Aufbewahrung.

Darüber hinaus stellt sich die Frage, ob und inwieweit den Fernmeldedienstanbieterinnen und ISP durch das neue BÜPF zusätzliche Pflichten auferlegt werden. Es ist darauf hinzuweisen, dass eine Missachtung der vom zentralen Dienst erlassenen Weisungen über die Durchführung von Überwachungsmass-nahmen neu mit Strafe bedroht ist.

Art. 6 f / 33 Der Bund betreibt ein zentrales Informationssystem zur Verarbeitung (d.h. Erfassung, Speicherung, Aufbewahrung und Gewährung des Online-Zugriffs) der durch die Überwachung des Fernmeldeverkehrs gewonnenen Daten (Kommunikations- und

Inhaltsdaten des Fernmelde- und Internet-Verkehrs der überwachten Personen)

Hier stellt sich die Frage der Kontrolle dieses grossen zentralen Informationssystems zur langfristigen Speicherung der Daten aus der Fernmelde- und Internet-Überwachung durch unabhängige politische und richterliche Instanzen im Hinblick auf die Gewährleistung der Grundrechte und zur Verhütung von Missbräuchen. Diesbezüglich enthält der Gesetzesentwurf nur die Bestimmung in Art. 33, dass der zentrale Dienst über die Einhaltung der Gesetzgebung betreffend die Überwachung des Post- und Fernmeldeverkehrs wacht; eine Bestimmung der korrekten Erfüllung der Aufgaben des zentralen Dienstes ist im BÜPF jedoch nicht enthalten. Im Begleitbericht wird zwar hervorgehoben, dass die Schaffung eines zentralen Systems unter dem Gesichtspunkt des Schutzes der Grundrechte einen Fortschritt bilde, weil die Daten dann besser kontrolliert und geschützt werden können. Andererseits schafft ein solches zentrales System mit der langfristigen Speicherung sämtlicher in der Schweiz aus den verschiedensten Gründen (nicht nur bei der Verfolgung qualifizierter Delikte) erfassten Daten aus dem privaten Kommunikations-verkehr aber auch offensichtliche Probleme für den Schutz der Privatsphäre und die Gefahr des Missbrauchs und verlangt eine Kontrolle durch eine unabhängige Instanz.

Art. 11 Es wird festgestellt, dass die Daten über den Fernmeldeverkehr der überwachten Personen im zentralen Informationssystem während sehr langer Dauer von 5 bis 30 Jahren gespeichert bleiben, wobei die Aufbewahrungsdauer durch unbestimmte Begriffe wie “so lange es für das verfolgte Ziel erforderlich ist“ bestimmt wird. Darüber hinaus kann die mit dem Verfahren befasste Behörde vom zentralen Dienst die Herausgabe der Daten (in elektronischer Form) nach Ablauf der Aufbewahrungsdauer im zentralen System verlangen, ohne dass bestimmt ist, zu welchem Zweck und wie lange die ersuchende Behörde die Daten dann weiterhin nutzen darf.

Hier wird sich vor allem die Frage der Bestimmung der Aufbewahrungsfrist im Einzelfall sowie das Vorgehen bei der Vernichtung der gespeicherten Daten nach Ablauf der Aufbewahrungsfrist und die Kontrolle der tatsächlichen Löschung stellen.

Art. 12 Sicherheit des zentralen Informationssystems sowie der Übertragung von Überwachungs-daten durch die Fernmeldedienstanbieter und ISP in das zentrale System

Hier wird sich vor allem die Frage stellen, welche Pflichten und Auflagen sowie damit verbundene Kosten die vom Bundesrat zu erlassende Verordnung über die technischen und organisatorischen Schutzmassnahmen für die in Art. 12 ebenfalls erwähnten Fernmeldedienstanbieter und ISP nach sich ziehen wird.

Art. 18/24 Setzt die Zertifizierung der Anbieterinnen von Fernmeldediensten auf deren eigene Kosten durch den zentralen Dienst im Hinblick auf ihre Befähigung zur “wirksamen Durchführung von Überwachungsmass-nahmen“ voraus

Der Gegenstand und Verfahren der Zertifizierung sind sehr unbestimmt formuliert; die daraus entspringenden Kosten für die Zertifizierung und die in solchen Fällen übliche Nachzertifizierung sind schwer abschätzbar. Auch ist nicht klar, ob sich auch ISP und die in Art. 2 abs. 1 (b) genannten weiteren Provider zertifizieren lassen müssen. Hinzuweisen ist auch auf die wesentliche Änderung im rev. BÜPF, dass die privaten Personen, welche mit der Durchführung der Überwachung betraut werden, dafür keine Entschädigung mehr erhalten, wie dies unter Art. 16 des geltenden Rechts noch vorgesehen war. Zusammen mit den an die privaten Provider delegierten erweiterten Aufgabe und die immer komplexer werdenden Überwachungs-massnahmen im elektronischen Kommunikationsverkehr könnte das rev. BÜPF daher eine nicht unerhebliche Belastung der Provider mit sich bringen. Der Hinweis im Begleitbericht, dass die zusätzlichen Kosten nur eine verhältnismässig geringfügige Belastung des Umsatzes (sic!) der Fernmeldedienstanbieter und ISP nach sich ziehen dürfte, erscheint etwas lebensfremd.

Art. 20/14 Auskünfte über Kommunikationsdaten (Personalien der TeilnehmerInnen am Fernmelde- und Internetverkehr, Adressierungselemente, Art der Anschlüsse) werden vom zentralen Dienst auf Gesuch auch den Polizeiorganen von Bund und Kantonen für allgemeine Polizeiaufgaben (also nicht nur für die Verfolgung der in Art. 269 StPO aufgeführten qualifizierten Delikte) sowie den Behörden von Bund und Kantonen zur Erledigung von Verwaltungsstrafsachen bekannt gegeben.

Damit stehen die Kommunikationsdaten, anders als die Inhaltsdaten, für eine sehr breit definierte Tätigkeit der Behörden von Bund und Kantonen zur Verfügung

Art. 20.3 Bei Straftaten, die über das Internet begangen werden, müssen die Fernmeldedienstanbieterinnen und ISP dem zentralen Dienst alle Angaben machen, die eine Identifikation des Urhebers oder der Urheberin ermöglichen.

Diese Bestimmung erfasst sämtliche Straftaten (z.B. Urheberrechtsverletzungen) die über das Internet begangen werden. Dadurch wird für alle Transaktionen, welche über das Internet abgewickelt werden, die Identifikation der Teilnehmenden für sämtliche Delikte des StGB, des Neben- und Verwaltungsstrafrechts (z.B. UWG wie die Abwerbung eines Mitarbeitenden, kartellwidrige Preisabsprachen, fiskalische Delikte usw.) sicher gestellt.

Art. 21.2 Fernmeldedienstanbieter und ISP müssen im Rahmen von Überwachungsverfahren die von ihnen angebrachte Verschlüsselungen an Daten vor deren Weiterleitung an den zentralen Dienst entfernen.

Der Aufwand der Dienstanbieter für die "Entschlüsselung" wäre zu prüfen. Es wäre zu prüfen, ob die Fernmeldedienstanbieterinnen und ISP ihre Kunden nicht darüber unterrichten sollten, dass die verwendete Verschlüsselung im Rahmen eines Überwachungsverfahrens nach BÜPF aufgehoben werden. Die "Entschlüsselung"

bezieht sich u.E. auch auf die offen zu legenden Telekommunikationsdaten nach Art. 14 und 20, d.h. auf einen sehr weiten Bereich der Fernmelde- und Internet Überwachung.

Art. 21.3 Auf dessen Verlangen sind die Fernmeldedienstanbieter und ISP verpflichtet, dem zentralen Dienst nur denn bezeichneten Typ oder bestimmte Typen von Daten aus dem Datenstrom zu liefern.

Eine solche Aussonderung der gewünschten Daten aus dem ungefilterten Datenstrom kann zu einem sehr erheblichen Triage-Aufwand führen, der von den Fernmeldedienstanbietern und ISP zu tragen ist; sie müssen auch die entsprechenden Triage-Systeme und Verfahren entwickeln.

Art. 21.4 Fernmeldedienstanbieterinnen und ISP sind verpflichtet, dem zentralen Dienst bei der Überwachung zu unterstützen, für welche Informatikprogramme nach Art. 270bis StPO zum Abfangen und Lesen von Daten erforderlich sind

Art. 270bis StGB schafft die Möglichkeit des Einsatzes von Spionageprogrammen ("Bundes-Trojaner"). Es ist nicht klar geregelt, ob die Fernmeldedienstanbieterinnen und ISP im Auftrag des zentralen Dienstes selber solche Spionageprogrammen entwickeln und einsetzen müssen, oder ob sie nur die Infrastruktur, Methoden und Verfahren für den Einsatz der vom Dienst entwickelten "Bundes Trojaner" bereit stellen müssen. Auf jeden Fall erscheint die Zusammenarbeit des zentralen Dienstes mit den Fernmeldedienst-anbieterinnen und ISP in Bezug auf den Einsatz von "Bundes-Trojanern" als ein kritischer Regelungsbereich des revidierten BÜPF.

Art. 22 Fernmeldedienstanbieterinnen und ISP müssen die notwendigen technischen Vorkehren treffen, um die Personen identifizieren zu können, die über ihre Vermittlung Zugang zum Internet erhalten.

Hier wäre zu prüfen, ob die Fernmeldedienstanbieterinnen und ISP zur Erfüllung dieser Rechtspflicht angesichts der voraussehbaren künftigen Entwicklung des Kommunikationsverkehrs über das Internet überhaupt in der Lage sind, bzw. welchen zusätzlichen Aufwand sie zur Identifizierung der TeilnehmerInnen auf eigene Kosten leisten müssen. Als kritische Anwendungsbeispiele für die Identifizierung werden im Begleitbericht erwähnt: (drahtlose) Internet-Zugänge in Schulen, Spitälern, Hotels, Restaurants, Internet-Cafés: Für diese Fälle muss der Access-Provider in Zukunft Vorkehrungen treffen, um die Identität des Benutzers des Internet-Zuganges sicher feststellen zu können: Keine leichte Aufgabe! Anonymes Surfen im Internet wird dadurch praktisch ausgeschlossen.

Art. 23/31 Die Kommunikationsdaten (nicht die Inhaltsdaten) über den Fernmeldeverkehr sind von den Fernmeldedienstanbieterinnen und ISP neu während zwölf Monaten aufzubewahren. Die vorsätzliche Verletzung dieser Aufbewahrungspflicht ist neu mit Strafe bedroht.

Diese Bestimmung bringt für die Fernmeldedienstanbieterinnen und ISP

zweifellos einen gewissen zusätzlichen Aufwand

Art. 25 Fernmeldedienstanbieterinnen und ISP müssen den zentralen Dienst auf dessen Anfrage jederzeit ausführlich über die Art und Merkmale von Technologien und Diensten unterrichten, welche sie der Öffentlichkeit zur Verfügung gestellt haben oder stellen werden.

Abgesehen von dem durch diesen Art. 25 geschaffenen zusätzlichen Aufwand ist auf das Risiko der Preisgabe von Geschäfts- und Betriebsgeheimnissen der Fernmeldedienstanbieterinnen und ISP beim Vollzug einer solchen Anfrage des zentralen Dienstes hinzuweisen.

Vorläufige Zusammenfassung

*A. Es dürfte unbestritten sein, dass die modernen Formen der Cyber-Kriminalität nach einer Erweiterung der Untersuchungsmittel der Strafverfolgungsbehörden verlangen. Die wesentlich erweiterten Verfahren zur Erfassung der Identität der Kommunikationspartner im Internet, die zusammenfassende langfristige Speicherung aller Daten aus der elektronischen Überwachung in einem zentralen System (mit den dadurch geschaffenen Auswertungsmöglichkeiten), Identifizierung sämtlicher Benützer des Internet; Einsatz von "Bundes-Trojanern", ruft nach entsprechenden Kontrollvorkehrungen**: Nicht nur die Spiesse der Strafverfolgungsbehörden und der Cyber-Kriminellen sollten gleich lang sein, sondern auch die Spiesse der Behörde und der in ihrer Privatsphäre und ihrer grundrechtlich geschützten Kommunikation betroffenen Bürger.***

B. Darüber hinaus dürfte die im revidierten BÜPF vorgesehene Übertragung der organisatorisch-technischen Überwachungsmassnahmen und der verschiedenen damit verbundenen zusätzlichen Aufgaben vom Gemeinwesen auf die Fernmeldedienstanbieter und ISP, wie z.B. die neu geschaffene Zertifizierungspflicht, die Qualitätskontrolle, die Verdoppelung der Aufbewahrungsdauer der Randdaten, die Identifizierung aller Internet-Benutzer an öffentlich zugänglichen Orten wie Hotels, Schulen, Restaurants, die Entfernung von privaten Schlüsseln, die Triage der bei der Überwachung erfassten Daten usw. ***eine nicht unerhebliche zusätzlichen Belastung der Privatwirtschaft*** *nach sich ziehen.*

Review: Zürcher Tagung 2010

ISSS Zürcher Tagung 2010 “Data Leakage Prevention”

Am 1. Juni 2010 strömten rund 117 Teilnehmende ins Widder Hotel am Rennweg in Zürich, um sich zu den neuesten juristischen und technischen Erkenntnissen zu „Data Leakage Prevention“ aus erster Hand zu informieren. Auf der nächsten Seite finden Sie einen Artikel zum Inhalt dieser ISSS-Tagung. Ein weiterer Artikel ist in der Netzwoche erschienen und kann wie auch die Unterlagen und Videos zur Tagung von unserer Event-Website heruntergeladen werden ab https://www.isss.ch/veranstaltungen/2010/zuercher-tagung/.

Fotoimpressionen

Keynote “The Future of Data Leakage Prevention" von Sandy Porter

Das Thema DLP stösst auf breites Interesse

Die weltweite Gesetzeslage zum Verhalten bei „Data Breaches“ ist sehr uneinheitlich.

USB Stick: Klein, praktisch und ein (potentielles) Datenleck.

Jürgen Wagner erläutert den Fall „LGT“.

Thomas Maxeiner, McAfee GmbH, Deutschland zur “Praxis von DLP”.

David Rosenthal erklärt „Datenklau“ aus juristischer Sicht

Beat Lehmann moderiert das erste Podium zur juristischen Sicht auf Data Leakage Prevention

Oliver Jäschke, Zurich Versicherungs-Gesellschaft AG, auf dem zweiten Podium zur technischen Sicht auf DLP.

Review: Zürcher Tagung 2010

ISSS Zürcher Tagung 2010 zum Thema Data Leakage Prevention

Spektakuläre Fälle von Datenpreisgabe an ausländische Stellen wie z.B. die Weitergabe von Daten der LGT Vaduz mit anschliessenden Schadenersatzansprüchen betroffener Personen gegen den Dateninhaber oder der Datendiebstahl bei HSBC Genf unterstreichen die wachsende Bedeutung von Data Leakage Prevention (DLP). An der DLP-Fachtagung der Information Security Society Switzerland (ISSS) im Widder Hotel in Zürich im Juni 2010 nahmen denn auch 117 Personen teil.

DLP dient dazu, die Risiken der Preisgabe von Daten an Unberechtigte durch verstärkte Kontrolle über die Nutzung der Daten zu kontrollieren. Mindestens soll sichergestellt werden, dass die Daten bei unbefugtem Zugriff, Verlieren oder Entwendung von Datenträgern, unsorgfältiger Entsorgung etc. nicht verwertet werden können.

Die ISSS Zürcher Tagung 2010 war wie jedes Jahr in zwei Teile unterteilt. Der erste Teil beschäftigte sich mit den Aspekten von Recht und Compliance der DLP und ging auf die Sanktionen gegen die Täter, Empfänger und Nutzer entwendeter Daten sowie auf die Verantwortung und Haftung von Unternehmen und Verwaltungsstellen bei ungenügenden Massnahmen zur DLP ein. In sehr spannenden Vorträgen legten die Referenten David Rosenthal, Konsulent für Informations- und Kommunikationsrecht, Kanzlei Homburger, Zürich, Karin Koç, juristische Beraterin in datenschutzrechtlichen Fragen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB), und Jürgen Wagner, Rechtsanwalt und Fachanwalt für Handels- und Gesellschaftsrecht, Wagner & Joos Rechtsanwälte, Konstanz/Zürich/Vaduz ihre Erfahrungen aus der Praxis dar.

David Rosenthal zeigte auf, dass es sich beim vielzitierten “Datenklau“ aus rechtlicher Sicht meistens nicht um Datendiebstahl handelt. Einer der Hauptgründe hierfür ist das gemäss dem Artikel 143 StGB erforderliche Tatbestandsmerkmal des unbefugten Zugriffs auf besonders gesicherte Daten. Diese Bestimmung erfasst meist nur externe Angreifer, da die Mitarbeitenden über eine Zugangsberechtigung zu den Daten verfügen. Da die Datendiebe aber meist etwas mit den gestohlenen Daten anfangen wollen, bietet sich trotzdem die Gelegenheit, rechtlich einzugreifen. Herr Rosenthal stellte die wichtigsten strafrechtlichen und zivilrechtlichen Ansatzpunkte wie z.B. der Tatbestand der Bekanntgabe "entwendeter" Geheimnisse an Dritte oder der Persönlichkeits- oder Vertragsverletzung kurz vor.

„Datenklau“ oft verwirrend

Mit der Frage „Vertrauen ist gut, Kontrolle ist besser?“ stellte Karin Koç die Teilnehmenden vor die nächste Herausforderung. Gleich zu Beginn betonte sie, dass aus Gründen des Persönlichkeitsschutzes die Überwachung der Mitarbeitenden immer die letzte aller möglichen Massnahmen sein sollte. Sie zeigte auf, welche rechtlichen Grundlagen und Voraussetzungen erfüllt sein müssen, damit eine Überwachung der eigenen Mitarbeitenden rechtmässig erfolgen kann.

Jürgen Wagner bezog sich in seinem Referat im Speziellen auf die LGT Treuhand, welcher im Jahre 2002 Kundendaten gestohlen worden sind. Auch aus seiner Sicht ist die Begriffsbezeichnung „Datenklau“ verwirrend oder gar zu harmlos formuliert. In Fällen wie dem vorliegenden gehe es vielmehr um Straftaten wie z.B. Betrug.

Schutzmechanismen als Teil der Daten

Der zweite Teil der Veranstaltung behandelte die Möglichkeiten der technischen Umsetzung von DLP. Sandy Porter, Head of Identity and Security bei Avoco Secure ging in seiner Keynote insbesondere auf die Zukunft von DLP ein. Ausgehend von den klassischen DLP-Massnahmen wie Verschlüsselung der Daten auf dem Übertragungsweg, Verschlüsselung der Datenträger und strikten Access-Control Mechanismen argumentierte Herr Porter, dass diese unter Berücksichtigung der immer stärkeren Auflösung der klassischen Security-Perimeter (Stichwort Cloud) und modernen Formen der Zusammenarbeit in Zukunft nicht mehr genügen. Seine Vision ist es deshalb, dass die Schutzmechanismen ein inhärenter Teil der Daten selbst sein müssen, wodurch die Daten selbst hinsichtlich Vertraulichkeit und Integrität konsequent geschützt sind und zwar unabhängig davon, wo sich die Daten gerade befinden oder über welchen Übertragungskanal sie gerade gesendet werden. Es gibt heute zwar bereits Rights-Management Systeme, die diesen Ansatz verfolgen, diese sind aber noch weit davon entfernt, einfach, universal (und damit auch über

Unternehmensgrenzen hinweg) und flexibel eingesetzt zu werden. Die Vision von Herr Porter geht entsprechend über heute gebräuchliche Systeme hinaus.

Daten finden, klassifizieren, überwachen

Johann Petschenka, Channel Manager für internationale Sales Partner bei SECUDE IT Security GmbH ging auf die goldenen Regeln der Data Loss Prevention ein. Diese 10 einfach verständlichen und prägnant formulierten Regeln sind eine praktische Hilfestellung, wenn man selbst an die Einführung von DLP-Massnahmen denkt oder die bestehenden Massnahmen optimieren möchte. Die Regeln decken nicht nur technische Aspekte (wie z.B. zentrale Benutzerverwaltung, Endpoint-Security, Datenträgerverschlüsselung und Access-Control) und organisatorische Aspekte (z.B. Risikoabschätzung, Identifikation der schützenswerten Daten), sondern behandeln auch „menschliche“ Aspekte. So empfiehlt eine Regel die Einführung einer Unternehmensethik bezüglich sicherem Verhalten und eine weitere Regel warnt vor zu starker Kontrolle, wodurch eine „Big Brother“-Mentalität entstehen und an die Öffentlichkeit gelangen könnte.

Oliver Jäschke von Group IT Risk der Zurich Financial Services präsentierte wie die Zurich Financial Services DLP in der Praxis umgesetzt haben. Der Ansatz folgt dem einfachen Prinzip: Daten finden, klassifizieren und überwachen. Die Eckpfeiler des Systems bestehen dabei aus:

- Dem Erkennen und Überwachen der Daten auf Client- und Server Systemen durch einen DLP Client
- Dem Überwachen der Daten bei deren Übermittlung
- Der Verschlüsselung der Daten beim Kopieren auf mobile Geräte
- Der Entfernung oder Anpassung von unsicheren Clients

Oliver Jäschke betont, dass die von Ihnen eingesetzten technischen Massnahmen nur eine Seite ihres DLP Konzepts sind. Die auf der organisatorischen Seite ergriffenen Massnahmen wie die Klassifizierung von Daten oder Abklärungen im Bezug auf regulatorische Anforderungen sowie der Definition eines Vorgehens im Falle eines Verlustereignisses, seien mindestens genauso wichtig.

In seinem Talk “Data Protection in der Praxis” betonte Thomas Maxeiner, Product Line Executive für Data Protection Central Europe bei McAfee GmbH Deutschland, dass Daten heute eine harte Währung sind: Daten wie Kreditkartennummern, PayPal Konten oder Sozialversicherungsnummern werden genauso im Internet gehandelt wie auch Software zur Ausspähung dieser Daten. Neben dem Fakt das Daten zur “New Age Currency“ wurden, motivierte Thomas Maxeiner den Einsatz von DLP auch durch regulatorische Gründe wie z.B. die in den USA, Deutschland und Österreich eingeführte Informationspflicht im Falle eines Verlustes von schützenswerten Daten sowie der zusätzlichen Flexibilität durch die sichere Nutzung von Daten auch ausserhalb speziell geschützter und vollständig kontrollierter Infrastrukturen.

Security-Vorfälle haupsächlich intern

Weiter unterstrich er, dass DLP vor allem auch einen Schutz gegen den Faktor Mensch ist und deshalb jeden betrifft. Mit Fragen wie „Haben Sie schon mal ein Email an die falsche Adresse geschickt?“ oder „Haben Sie schon mal vertrauliche Daten auf einen unverschlüsselten USB Stick kopiert und wissen Sie noch, wo all Ihre jemals gekauften/benutzten USB Sticks jetzt sind?“ verdeutlicht er diese Position und nennt einige Schlüsselergebnisse aus einem McAfee/ICM Research Survey. So geben z.B. 26% der Befragten an, dass Sie regelmässig vertrauliche Daten auf über USB anbindbare Datenträgern speichern und mit nach Hause nehmen. Erschreckend ist aber vor allem das Ergebnis, dass die Ursache von über 70% der Vorfälle mit schützenswerten Daten firmenintern zu suchen ist.

Teil der Veranstaltung waren auch zwei Podiums-diskussionen, die von Beat Lehmann und Bernhard Hämmerli moderiert wurden. Diese beiden Podiums-diskussionen boten die Gelegenheit, die vorgetragenen Themen zu vertiefen. Abgerundet wurde die Veranstaltung durch einen reichhaltigen Apéro, der den Teilnehmern die Gelegenheit zu einem intensiven Austausch untereinander und mit den Vortragenden ermöglichte.

Autoren: Frank Heinzmann, Liliane Mollet, Bernhard Tellenbach, Marc Rennhard, Lukas Ruf, alles Mitglieder des ISSS Vorstandes

Information Security Society Switzerland

Agenda: Partner Events mit Rabatt für ISSS Mitglieder

Security Events unserer Partner (Auswahl)

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

Do, 09.09.2010	08:30 - 17:00	Compass Security AG	**Compass Event 2010 - iPhone, Laptop & Co. unter Beschuss** ISSS Mitglieder erhalten 20% Rabatt	Rapperswil
Di, 14.09.2010	09:00 - 17:00	EBDI, IBCOL, OLOR	**Praktiker-Fachtagung „IT Risk Management & BCM“** ISSS Mitglieder erhalten 15% Rabatt (nicht kumulierbar)	Zürich
Mi - So, 03.11. - 06.11.2010	ganztags	DEFCON	**Hashdays Security & Risk Conference (#days)** ISSS Mitglieder erhalten den "reduced delegate" Tarif (255.- statt 300.- CHF). Anmeldung bis 30.06.2010 erforderlich. **Neu:** Management Sessions „Cyber Threat Roundtable“	Luzern

Security Kurse unserer Partner (Auswahl)

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

Mi. - Di. 14.07. - 20.07,2010	ganztags	ROMAN Consulting & Engineering	**Security Fachkurs: "CISSP (Certified Information Systems Security Professional)"** ISSS-Mitglieder zahlen CHF 4463.- statt CHF 5250.- (15% Rabatt)	Zürich
Mo - Fr, 06.09. - 10.09.2010	ganztags	ROMAN Consulting & Engineering	**Security Fachkurs: "Check Point Security Administrator R70 (CCSA R70)"** ISSS-Mitglieder zahlen CHF 3868.- statt CHF 4550.- (15% Rabatt)	Zürich
Mo - Fr, 27.09. - 01.10.2010	ganztags	ROMAN Consulting & Engineering	**Security Fachkurs: "EC-Council: Disaster Recovery and Business Continuity (EDRP)"** ISSS-Mitglieder zahlen CHF 4760.- statt CHF 5600.- (15% Rabatt)	Zürich
Di - Mi, 23.11. - 24.11.2010	8:30 - 17:00	Plattner Beratung und Schulung	**Kompaktkurs "Internet (In)Security Exposed" - Internetgefahren verstehen und Webapplikationen richtig schützen in Theorie und Praxis.** ISSS-Mitglieder zahlen CHF 1840.- statt CHF 2300.- (20% Rabatt).	Zürich

Beachten Sie bitte auch die Agenda mit wissenschaftlichen Konferenzen:
https://www.isss.ch/veranstaltungen/wiss-konferenzen/

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

Information Security Society Switzerland

Agenda: Hinweise zu ISSS Security Events

Einladung zum Kick-off der SIG „Suisse-ID – benefits and risks for e-commerce“

Die von Anthony Thorn initiierte SIG stösst auf grosses Interesse. Wenn auch Sie sich für das Thema „Suisse-ID – benefits and risks for e-commerce“ interessieren, melden Sie sich bitte umgehend beim SIG-Lead anthony.thorn@isss.ch an. Das Kick-off Meeting wird am **Montag 12. Juli 2010, 9:30 morgens in Zürich** stattfinden. Die vollständige Beschreibung zu dieser und weiteren in Gründung befindlicher SIGs finden Sie auf unserer Homepage im SIG-Teil: http://www.isss.ch/aktivitaeten/special-interest-groups/

Aufruf der zu gründenden SIG „Computerkriminalität und Schadprogramme“ an Interessierte

Marc Furner ruft alle Interessierten zum Thema „Computerkriminalität und Schadprogramme“ auf, sich bei ihm per Email an marc.furner@isss.ch bis 20.8.2010 zu melden. Wenn genügend Interesse besteht, wird eine SIG und eventuell später ein Forum zu diesem Thema gegründet. Die Detailausschreibung zu dieser SIG (PDF) finden Sie online.

Vorschau zur 13. ISSS Berner Tagung 2010 „Unbegrenzte Mobilität: Chancen und Risiken“

Donnerstag, 25. November 2010, 13.30 – 18.00 Uhr, Hotel Bellevue Palace, Bern.

Der spannende Titel der 13. Berner Tagung verspricht interessante Referate und Diskussionen über die Fragen der ständigen und jederzeit möglichen Erreichbarkeit. Wie gewährleisten wir als Personen und Unternehmen die Informationssicherheit in einer Zeit, in welcher immer mehr Mitarbeitende jederzeit und von überall her auf sensible Unternehmensdaten zugreifen können, sich aber gleichzeitig online in sozialen Netzwerken aufhalten. Freizeit und Arbeit verschmelzen immer mehr. Nicht nur meine Freunde finde ich in der virtuellen Welt auch viele Firmen machen mittlerweile Gebrauch von der Möglichkeit, ihre Geschäftsinformationen in diesen Netzwerken zu verbreiten. Expertinnen und Experten werden versuchen, die virtuelle Welt mit der realen Welt und den entsprechenden Sicherheitsanforderungen und -konzepten wieder etwas zusammenzubringen.

Das vollständige Programm wird bis im September auf www.isss.ch aufgeschaltet werden. Eine Anmeldung ist ab sofort möglich.

Geplante Stellungnahme der ISSS zur Überarbeitung der „BÜPF“

Beat Lehmann <beat.lehmann@isss.ch> plant zusammen mit dem ISSS-Vorstand und ISSS-Mitgliedern sowie weiteren Interessierten, eine Stellungnahme der ISSS zur Überarbeitung der „BÜPF“ bis 18. August 2010 zu verfassen und einzureichen. Interessierte melden sich bitte umgehend bei ihm. Im Focus dieser Ausgabe finden Sie dazu einen erläuternden Bericht.

Information Security Society Switzerland

Agenda: Events der Information Security Society Switzerland

Nächste ISSS Fachtagungen

26.10.2010	17:30 – 21:30	**ISSS/ISACA Abendseminar: „Innovative Alternativen zum Passwort“** (inkl. Apéro, kostenloser Anlass, Anmeldung erforderlich)	Zürich
25.11.2010	13:15 – 18:30	**13. Berner Tagung für Informationssicherheit: „Unbegrenzte Mobilität - Chancen und Risiken“** (Anmeldung erforderlich)	Bern

Nächste ISSS Security Lunches

Eintritt kostenlos, auch für Nichtmitglieder; Essen wird zu Selbskosten vom Restaurant vor Ort in bar eingezogen; Anmeldung erforderlich.

31.08.2010	12:00 – 14:00	**SuisseID - erste Erfahrungen aus der Praxis**	Bern
09.09.2010	12:00 – 14:00	**Cloud Computing - was ist aus rechtlicher Sicht zu beachten?**	Luzern
06.10.2010	12:00 – 14:00	**Kostengünstige Identifizierung bisher nicht erkannter Sicherheitslücken mit Threat Modeling, Static Analysis und Fuzzing**	Zürich

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

Impressum:
Information Security Society Switzerland
Wasserwerkgasse 37
3000 Bern 13
sekretariat@isss.ch
Tel. +41 31 311 5300
Auflage: Versand als PDF per Email an alle ISSS-Mitglieder und Publikation auf http://www.isss.ch/