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 anschliessendem Schadenersatzansprüchen betroffener Personen gegen den Dateninhaber oder der Datendiebstahl bei HSBC Genf sowie Berichte über einen möglicher Datenverlust bei der CS, unterstreichen die wachsende Bedeutung des Themas Data Leakage Prevention (DLP). An der DLP-Fachtagung der Information Security Society Switzerland (ISSS) in Zürich 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 zeigt 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. Rosenthal stellte die wichtigsten strafrechtlichen und zivilrechtlichen Ansatzpunkte kurz vor, beispielsweise den Tatbestand der Bekanntgabe «entwendeter» Geheimnisse an Dritte oder der Persönlichkeits- oder Vertragsverletzung.

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

«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 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 Überragungsweg, Verschlüsselung der Datenträger und strikten Access-Control Mechanismen argumentierte Porter, dass diese unter Berücksichtigung der immer stärkeren Auflösung der klassischen Security-Perimeter (Stichwort Cloud) und modernen Formen der Zusam-

menarbeit 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 Überragungskanal 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 Sandy 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 zehn 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 zentrale Benutzerverwaltung, Endpoint-Security, Datenträgerverschlusselung und Access-Control) und organisatorische Aspekte (zum Beispiel 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

Keynote von Sandy Porter zu „The Future of Data Leakage Prevention".

Oliver Jäschke betonte, dass die eingesetzten technischen Massnahmen nur eine Seite des 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.

Das Thema DLP stösst auf breites Interesse.

In seinem Talk «Data Protection in der Praxis» betont 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, dass Daten zur "New Age Currency" wurden, motiviert Thomas Maxeiner den Einsatz von DLP auch durch regulatorische Gründe wie 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 hauptsächlich 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 E-Mail 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?» verdeutlichte er diese Position und nannte einige Schlüsselergebnisse aus einem McAfee/ICM Research Survey. So geben beispielsweise 26 Prozent 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 Prozent der Vorfälle mit schützenswerten Daten firmenintern zu suchen ist.

Frank Heinzmann, Liliane Mollet, Bernhard Tellenbach, Marc Rennhard und Lukas Ruf, Mitglieder des ISSS Vorstandes