Data Leakage in Deutschland

Drei typische Ursachen

28/08/2012, Securitymanager.de

Sergej Schlotthauer

EgoSecure GmbH
Sergej Schlotthauer entwickelt mit seinem Team neue Konzepte im Bereich der Endpoint-Security und organisiert als Geschäftsführer den Ausbau der EgoSecure GmbH

Nachdem InfoWatch vorvergangenen Monat den jährlichen Data Leakage Report vorgestellt hat, veröffentlicht das Security-Unternehmen nun eine Liste mit Datenpannen in Deutschland. Die Beispiele machen deutlich, dass viele solcher Pannen mit Datenverlust meist grob fahrlässig und nicht vorsätzlich geschehen.

Inhaltsverzeichnis

Data Leakage Report

Aus den zusammengetragenen Fällen geht hervor, dass die wirklich folgenschweren Vorfälle im Jahr 2011 eher im Ausland und nicht in Deutschland geschahen. Allerdings ist dies nicht sonderlich beruhigend, solange Daten von deutschen Unternehmen häufig auch von externen Dienstleistern im Ausland gehostet werden oder Dritte mit sensiblen Daten betraut werden. "Eine Unterschrift und die Versicherung Daten zu schützen, würden mir als Unternehmer allein nicht reichen. Denn selbst, wenn das Unternehmen den finanziellen Schaden durch Datenverluste erstattet bekommen würde, der Image-Verlust haftet anschließend doch an ihm. Fest installierte DLP-Software, nachvollziehbare und kontrollierte Sicherheits-Policies und transparente Sicherheitsmaßnahmen überzeugen hier mehr.

Das Motiv für die Veröffentlichung der von Data Leakage Vorfällen 2011 in Deutschland ist vorrangig, Unternehmen für das Thema Data Leakage Prevention zu sensibilisieren. Gerade Unternehmen, die nicht aus dem IT-Umfeld kommen, vertrauen oft blind wichtige Daten externen IT-Firmen an, ohne nachzuvollziehen, wo und wie diese die Daten speichern. Zudem sieht man häufig Gefahren von außen und wappnet sich dagegen, interne Anwendungsfehler, grobe Fahrlässigkeit und Bedrohungen von Innen werden hingegen immer wieder unterschätzt.

Die repräsentative Liste von Vorfällen in Deutschland wurde von InfoWatch erstellt, um beispielhaft zu illustrieren, welche Ursachen Data Leakages haben können und was man dagegen unternehmen kann. Es geht InfoWatch auch nicht darum, bestimmte Unternehmen vorzuführen. Alle Vorfälle, die veröffentlicht wurden, sind bereits publik geworden und dies nicht durch InfoWatch. Diese hatte eher die Qual der Wahl, welche Vorfälle exemplarisch herausgegriffen werden sollten, um die Problematik von mangelhafter Datensicherheit in der Praxis zu verdeutlichen.

Erster Fall: Anwenderfehler beim E-Mail-Versand

Zahlreiche Fälle 2011 ließen sich auf Anwenderfehler beim Umgang mit E-Mails zurückführen. Meist wurden versehentlich Empfänger statt in das BCC-Feld in die Empfängerleiste geschrieben oder bei einer weitergeleiteten E-Mail fanden sich weiter unten noch vertrauliche Informationen. Solche Fehler geschehen nicht absichtlich, sind leider aber auch keine Seltenheit. Aufwendige Sicherheitssoftware umfasst diese Art des Datenlecks meist nicht.

In der Regel ist Security-Software darauf ausgelegt, zu gewährleisten, dass nicht autorisierten Personen der Zugriff verwehrt wird. Haben Personen aber erst einmal Zugriff, so gibt es oft keinen effektiven Schutz vor größeren Problemen durch Anwendungsfehler und Unaufmerksamkeiten. DLP-Software erkennt die Art der Daten und analysiert das Benutzerverhalten, um Benutzer rechtzeitig zu warnen.

Folgende Fälle ereigneten sich 2011, die sich allesamt auf Anwenderfehler beim Versenden von E-Mails zurückführen lassen:

- Ein großer Lebensmittelkonzern suchte vergangenes Jahr Fachkräfte und schrieb diese Stellen öffentlich aus. Im Rahmen des Bewerbungsverfahrens wurden alle Bewerber in einer Sammelmail angeschrieben. Zynischerweise wurden die Bewerber in dieser Sammelmail über geänderte Datenschutzbestimmungen informiert. Der Datenschutz wird hier vor allem deshalb empfindlich verletzt, weil eventuell auch der bisherige Arbeitgeber auf diesem Weg von einer Bewerbung erfahren könnte, was letzten Endes die Kündigung des bestehenden Arbeitsverhältnisses zur Folge haben könnte. Insgesamt standen über 200 Empfängern in der Adress-Zeile dieser E-Mail.

- Ein fast identischer Fall ereignete sich auch bei einer Partei im Berliner Senat, die ebenfalls über 200 E-Mail-Adressen von Bewerbern in das CC-Feld anstelle des BCC-Feldes kopiert hatte, mit gleichen Konsequenzen.

- Auch ein baden-württembergischer Fußball-Verein sorgte für einen breiten Adress-Austausch unter den Fans durch E-Mails mit hunderten von Empfängern.

- Die Arbeitsagentur einer niedersächsischen Stadt verschickte ebenfalls auf diese Weise Informationen an insgesamt 650 Empfänger. Für alle Empfänger waren folglich die E-Mail-Adressen von hunderten weiterer Arbeitssuchender einsehbar.

- Ein besonders extremer Fall, der aber schon mit Standard-DLP-Software hätte verhindert werden können, ereignete sich bei einer Grazer Bank. Um Kunden von einem Kredit zu überzeugen schickte ein Mitarbeiter diesem Kunden die Daten von weiteren 150 Kunden um zu demonstrieren, welche Vorteile dieser Kredit auch anderen Kunden bereits gebracht hatte. Ein Fall der deutlich macht, dass nicht nur das Fehlverhalten eines einzelnen Mitarbeiters enorme Konsequenzen haben kann, sondern das auch die Bank selber ihrer Sorgfaltspflicht nur ungenügend nachgekommen ist. Ein Unternehmen wie eine Bank, das mit hochsensiblen Daten arbeitet, sollte gewährleisten können, dass bestimmte Daten weder absichtlich noch unabsichtlich an Unbefugte weitergeleitet werden können.

Zweiter Fall: Versehentliche Veröffentlichung im Internet

Websites werden zunehmend generisch erstellt, um es auch Laien zu ermöglichen, schnell und ohne große Vorkenntnisse Inhalte zu bearbeiten. So reicht es beispielsweise in vielen Fällen aus, Daten nur in ein bestimmtes Verzeichnis zu kopieren, damit das Web-System diese in die Homepage einbindet. Dies erklärt auch die hohe Zahl von fälschlicherweise online verfügbaren Datensätzen. In vielen Fällen wurden durch Copy und Paste oder durch fehlerhafte Lese-Schreib-Berechtigungen Daten online einsehbar, die teils mehrere Tage lang online verblieben, bis der Fehler bemerkt wurde.

DLP-Software ist in der Lage, zwischen sensiblen und unsensiblen Speicherbereichen zu unterscheiden. Ebenso kann DLP-Software sensible von unsensiblen Daten unterscheiden. In der einfachsten Form wäre

ein Pop-Up mit einem Warnhinweis, dass die folgende Aktion die Veröffentlichung im Internet zur Folge hätte, schon ein wirksamer Schutz vor Data Leakage.

Dennoch war auch dieser Daten-Kanal bei vielen Fällen von Data Leakage 2011 ursächlich:

- Ein rheinland-pfälzisches Ministerium veröffentlichte fälschlicherweise Dokumente zu einem laufenden Untersuchungsausschuss auf der Website. Neben Berater-Honoraren und Privatadressen waren somit für jeden auch anwaltliche Schreiben in diesem Zusammenhang einsehbar. Hintergrund war aller Wahrscheinlichkeit nach ebenfalls ein Anwenderfehler. - Eine besondere Ironie bekommt der Fall durch den Umstand, dass die sensibelsten Daten nicht im Internet zu finden waren, weil die Datenschutzbestimmungen vorsahen, dass diese gar nicht in elektronischer Form einsehbar sein sollten. Ein zweifelhafter Ansatz, Datensicherheit dadurch zu erlangen, indem Daten nur in Papierform existieren.

- Ein ähnlicher Fall ereignete sich auch bei einem bayerischen Web Hoster, bei dem nicht nur Namen, sondern auch Konto-Informationen, behördliche Schreiben mit der Polizei sowie Passwörter online zugänglich waren. Offenbar kann ein Anwenderfehler wie im rheinland-pfälzischen Ministerium auch professionellen Anwendern eines Internet-Dienstleisters unterlaufen.

- Ein weiterer Fall ereignete sich bei einem im Bau befindlichen Flughafen, wo Probe-Fluggäste über die Homepage gesucht wurden. Nach der Anmeldung war für jeden Probe-Fluggast eine vollständige Liste aller bisher angemeldeten Nutzer einsehbar. Offenbar fand ein Testlauf der Anmelde-Software nie statt.

- Ebenso veröffentliche ein Gericht in Dresden die Liste aller akkreditierten Journalisten online, inklusive Adresse, Ausweis- und Presseausweis-Nummern, Geburtsdaten und dem verhandelten Fall.

- Auch eine große deutsche Universität veröffentliche genauso versehentlich Namen, Adresse und Fachrichtung von insgesamt 20.000 Studenten. Jeder Prüfer konnte so Matrikelnummer und Namen abgleichen.

Dritter Fall: Mangelhafte Entsorgung von Altpapier

Seit Jahren ist das Altpapier eine der Hauptfundgruben für sensible und vertrauliche Daten. Weltweit wird etwa jeder fünfte verlorene Datensatz über das Altpapier entwendet. Die Situation sieht in Deutschland leicht besser aus, auch weil in dieser Hinsicht Deutschland schärfere rechtliche Bestimmungen hat. Dennoch ist Altpapier auch hier eine Quelle für sensible Daten. DLP-Software ist in solchen Fällen zwar nicht in der Lage, die korrekte Entsorgung des Altpapiers zu gewährleisten, allerdings kann DLP gewährleisten, dass Daten, die nicht notwendigerweise ausgedruckt werden müssen, gar nicht erst gedruckt werden können. Effektive DLP-Software kann zu diesem Zweck sogar das Druckersignal selbst nach bestimmten Keywords durchsuchen.

So hat ein Berliner Verein, der bis 2006 als Anlaufstelle für notleidende Berliner Bürger fungierte, fünf Jahre später noch einmal Schlagzeilen gemacht, als Bürger Unterlagen des Vereins im Müll fanden, die offenbar nach der Auflösung des Vereins weder akkurat gelagert noch ordnungsgemäß vernichtet worden waren. Diese Unterlagen enthielten neben Namen und behördlichen Schreiben auch Informationen über Krankheitsverlauf, psychische Gutachten bis hin zu Missbrauchsfällen und Betreuungsbedarf. Offenbar hat man sich nach der Auflösung des Vereins recht preisgünstig mittels Papiermüll der Aktenberge entledigt.

Situation in Deutschland vergleichsweise positiv zu bewerten

Generell scheint die Situation in Deutschland verglichen mit anderen Ländern eher positiv bis entspannt, allerdings ist diese Einschätzung mit Vorsicht zu genießen. Auf der einen Seite gibt es in Deutschland, im Gegensatz zu Großbritannien oder den USA, keine Veröffentlichungspflicht bei Fällen von Data Leakage. Vorfälle, die vor der Presse geheim gehalten werden konnten, tauchen demzufolge in keiner Statistik auf.

Ein Vergleich mit oben genannten Ländern ist daher schwierig. Allerdings muss man davon ausgehen, dass auch ohne Veröffentlichungspflicht Vorfälle, bei der mehr als eine Million Datensätze betroffen sind, bekannt werden.

Insofern ist die deutsche Situation vorsichtig positiv zu bewerten, wenn man oben erwähnten Vorfällen bestimmte internationale Vorfälle gegenüberstellt. So verlor eine britische Behörde 2011 insgesamt mehr als 10 Millionen Datensätze. Ein File Hoster gewährte jedermann vier Stunden lang Einsicht in 25 Millionen Kundendaten und ein koreanisches soziales Netzwerk erlaubte seinen 35 Millionen Mitgliedern Namen, Telefonnummern und E-Mail-Adressen der übrigen Mitglieder einzusehen. Vor solchen Fällen blieben wir im vergangenen Jahr in Deutschland verschont, vorausgesetzt man nutzte als Deutscher nicht die Dienste von betroffenen ausländischen Unternehmen.

Details, Namen und Quellen der Vorfälle können im Anhang zum DLP Report 2011 auf der Website von InfoWatch eingesehen werden.

http://www.securitymanager.de/magazin/data_leakage_in_deutschland.html