Link: http://www.computerwoche.de/a/identitaetsdiebstahl-schwer-gemacht,2557113

Access Management

Identitätsdiebstahl schwer gemacht

Datum: 22.04.2014
Autor(en): Stanislav Wittmann

Gehen Kundendaten, technisches Know-how oder Firmenstrategien verloren, bekommt jedes Unternehmen Schmerzen. Wie lässt sich Datendiebstahl, gerade im Bereich Nutzerzugänge und Identitäten, verhindern? Und was ist im Schadensfall zu tun?

Zunächst zu den möglichen Szenarien. Es gibt zwei mögliche Varianten des Identitätsdiebstahls - den ungezielten, der auf Masse abhebt und den gezielten, der es auf bestimmte, meist privilegierte Nutzer abgesehen hat.

Massenidentitätsdiebstahl

Seien es nun Wettbewerber, die der Reputation eines Unternehmens schaden wollen oder kriminelle Cybergangster, die es ausschließlich auf den Weiterverkauf von Kundendaten abgesehen haben: Datenklau im großen Stil ist kein Einzelphänomen, wie diverse Vorfälle der Vergangenheit zeigen. Ob **Sky**[1], der französische Telefonriese **Orange**[2] oder der Super-GAU bei **Sony**[3] vor drei Jahren - kaum jemand scheint vor Massenidentitätsdiebstahl sicher. Und jedes Mal sind tausende von Menschen betroffen.

Gezielter Identitätsdiebstahl

Stellen wir uns vor, es existieren zwei Konzerne, die weltweit den Markt bei Passagierflugzeugen dominieren. Da ist ein Zweikampf um größere Ausschreibungen geradezu vorprogrammiert. Denkbar sind Spionageattacken, um die Konkurrenz auszuspähen: Firma A schleust einen Mitarbeiter in Firma B ein - Firma B hingegen sucht sich direkt einen unzufriedenen Mitarbeiter von Firma A, der die "Arbeit" noch günstiger erledigt.

Nehmen wir an, dass sich besagte Mitarbeiter Zugang zu kritischen Unternehmensdaten wie Preislisten oder vergangene Angebote verschaffen. Und das ganz ohne das Telefon des Vorstands abzuhören. Denn im Idealfall arbeiten die Spione in der eigenständigen IT-Sicherheitsabteilung und besitzen entsprechende Zugangsberechtigungen. Sollte es sich "nur" um die IT-Abteilung handeln, sind clevere **Social-Engineering-Attacken**[4], um sich Passwörter und Zugangsdaten zu erschleichen, aber ebenfalls nahezu problemlos möglich.

Dieses konstruierte Beispiel ist durchaus realistisch, wie der Zweikampf der Flugzeugbauer Boeing und EADS zeigt, in dem es vor knapp zehn Jahren **entsprechende Verdachtsmomente, in den sogar Regierungsvertreter verwickelt schienen, gab**[5].

Der Schaden

Kommt eine solche Meldung an die Öffentlichkeit, entstehen Schäden für ein Unternehmen. Ob nun Kunden- oder Angebotsdaten verfälscht werden (Integrität), Server ausfallen (Verfügbarkeit) oder Daten in falsche Hände gelangen (Vertraulichkeit) - alle drei Grundwerte der Informationssicherheit wären gefährdet.

Beispiele für die verletzten Grundwerte in der Informationssicherheit in Fall eines Identitätsdiebstahls. Foto: Stanislav Wittmann

Der monetäre sowie der Reputationsschaden stehen in der Regel im Vordergrund. Außerdem kann bei großen Konzernen das Image durchaus eine bedeutende Rolle spielen. Gerade wenn diese an der Börse notiert sind, ist es für den **"Shareholder Value"**[6] nicht gerade förderlich, wenn sich Identitätsdiebstahl oder Spionageversuche aufgrund von möglichen Wettbewerbsvorteilen aufdecken lassen.

Für jedes Unternehmen sind fünf grundsätzliche Arten von Schäden denkbar, im Kontext Datendiebstahl zumeist nur drei (monetärer Schaden, Reputationsschaden, juristischer Schaden). Besonders der Reputationsschaden kann schnell zum Verhängnis werden. Je größer der mediale Auftritt, desto gravierender kann der Reputationsschaden für das Unternehmen sein.
Foto: Stanislav Wittmann

Nicht nur Unternehmen, sondern auch Privatanwender können von Sicherheitslücken im Access Management betroffen sein. So gab es kürzlich gleich zwei millionenfache Identitätsdiebstähle, wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) **berichtet**[7].

Vorgehen bei einem Datenleck

Wer als Unternehmen oder auch Verein von einem möglichen Angriff und Datenleck betroffen ist, muss schon nach dem Willen des Bundesdatenschutzgesetzes (BDSG) unverzüglich handeln. Schließlich heißt es unter §3 (7) über die so genannte **"verantwortliche Stelle"**[8]: "Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt." Sollte ein drittes, externes Unternehmen die Daten beispielsweise im Rahmen einer Website verarbeiten, gilt dieses ebenfalls als verantwortliche Stelle.

Wichtig ist, die von dem Identitätsdiebstahl Betroffenen zu informieren - idealerweise persönlich, was bei Massendiebstählen jedoch kaum machbar ist. Deshalb schreibt **§ 42 a des BDSG**[9] bei "unverhältnismäßigem Aufwand" die Benachrichtigung in der Öffentlichkeit vor. Das bedeutet beispielsweise eine Meldung über eine halbe Seite in mindestens zwei bundesweit erscheinenden Tageszeitungen oder ein Fernsehbeitrag oder Meldungen auf anderen Medienkanälen.

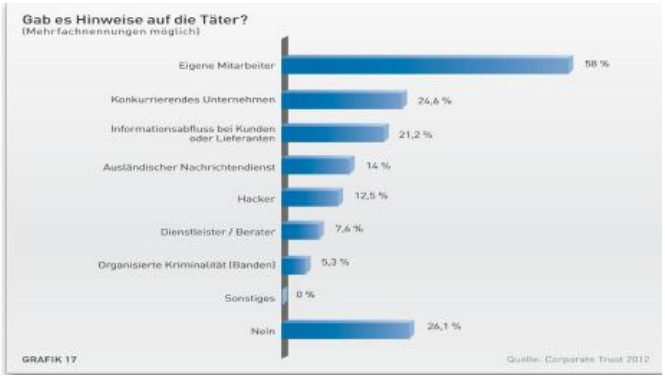
Ein Datenleck - ob im Unternehmen oder auch im Verein oder der Organisation - trifft meist verschiedene Interessensgruppen.
Foto: Stanislav Wittmann

"Anstatt sich um den eigenen Imageschaden zu sorgen, spricht das Aufzeigen einer Datenpanne für eine aktiv gelebte Sicherheitskultur", unterstreicht Datenschützer Michael Werner. Es helfe außerdem, drohende Bußgelder (§43 BDSG- Bußgelder) und mögliche Haftstrafen (§44 BDSG- Strafvorschriften) zu vermeiden. Überhaupt ist es eine sinnvolle Vorsichtsmaßnahme für Unternehmen, für solche Szenarien bereits im Vorfeld Notfallpläne zu erstellen. Nicht nur, um mögliche Schäden der Betroffenen zu reduzieren, sondern auch um das eigene Image aufrecht zu erhalten. Denn je schneller die Warnmeldungen an die Betroffenen rausgehen, desto eher können alle Parteien reagieren und als Konsequenz vorhandene Schäden versuchen zu mindern.

Täterprofile

Hacker, **Social Engineers**[10] oder eingeschleuste Mitarbeiter: Um Daten zu entwenden, bedarf es immer Menschen mit einer gewissen kriminellen Energie und bestimmten technischen Fertigkeiten. Zumeist sind es Insider, die für Sicherheitsvorfälle verantwortlich zeichnen - so zumindest das Ergebnis der **2012er-Studie von Corporate Trust**[11]. Demnach führt die Spur in mehr als der Hälfte aller Spionageattacken zu Innentätern. "Mitarbeiter, die sich ausgenutzt fühlen, sind nicht loyal. Der Schaden, der Unternehmen dadurch entsteht, geht in die Milliarden", erklärt Professor Wolfgang Berger, Leiter des **Business REFRAMING Instituts Karlsruhe**[12].

Die Studie „Industriespionage 2012“ von Corporate Trust macht deutlich, dass Innentäter am häufigsten Ursache sind.
Foto: Corporate Trust 2012



Nur jede achte Fall von Spionage ist laut Corporate Trust auf Hacker von außen zurückzuführen. Dazu kommen Attacken von Wettbewerbern und auch von Nachrichtendiensten. So berichtet der Whistleblower Edward Snowden **in einem Videobeitrag**[13], dass Nachrichtendienste teils sogar wissentlich nicht die "idealen Sicherheitslösungen für Unternehmen empfehlen", um deren potenzielle Schwachstellen bei Bedarf auszunutzen zu können. "Bei der Reduzierung des Sicherheitsniveaus in der Kommunikation, setzen Nachrichtendienste nicht nur die Welt, sondern auch Amerikaner Risiken aus", so Snowden.

Prävention

Wer den Schaden abwenden möchte, muss frühzeitig beginnen, ein Schutzpaket zu schnüren:

[Hinweis auf Bildergalerie: **Datenlecks vermeiden - Schutzmaßnahmen -**] gal1

Fazit

Ein ganzheitliches Sicherheitskonzept wie die **ISO 27001**[14] ist bestimmt ein passender Schlüssel zum Schutz vor Identitätsdiebstahl und Datenmissbrauch. Unternehmen sollten sich trotzdem Gedanken über das das Betriebsklima und eine eventuell hohe Personalfluktuation machen. Auf den ersten Blick sparen sie Geld, wenn sie kurzfristig beispielsweise Werkstudenten oder Praktikanten für kleinere (Sicherheits)-Projekte beauftragen. Möglicherweise machen diese auch einen guten Job. Jedoch es gibt auch eine Kehrseite: Mit jedem Mitarbeiter, der das Unternehmen verlässt, geht ein Stück Know-how verloren und das Risiko für Schäden durch die beschriebenen Angriffe steigt. Zudem erfreut sich das eigene Personal nicht gerade an einer hohen Fluktuation. Mitarbeiter spüren, wenn Unternehmen höhere Umsätze einem zufriedeneren Personal vorziehen.

Um das Betriebsklima zu wahren, sollen Unternehmen alle Mitarbeiter schätzen, aktiv wahrnehmen und auf ihre Bedürfnisse eingehen. Erfahrungsgemäß gehen die besten zuerst - und mit ihnen das wertvollste Know-how. Daher ist neben einem ganzheitlichen und individuell abgestimmten Sicherheitskonzept das Betriebsklima entscheidend. Berger macht deutlich: "Die härteste Realität in jedem Unternehmen ist nicht die ‚Hardware', sondern eine sehr spezielle Software: Das, was die Mitarbeiter über ihr eigenes Unternehmen denken." Genau diese Gedanken entscheiden letztlich über ihre Handlungen. Dagegen können manchmal selbst die besten Schutzmaßnahmen nichts ausrichten. Nicht einmal die der NSA. So konnte es beispielsweise **ein einziger Mann**[15] mit dem vielleicht mächtigsten Nachrichtendienst unseres Planeten aufnehmen. (sh)

Links im Artikel:

[1] **http://derstandard.at/1389859624885/Datenklau-bei-Sky-Auch-oesterreichische-Kunden-betroffen**
[2] **http://www.rga-online.de/rga_139_110515690-1-_Daten-von-800-000-Telefonkunden-in-Frankreich-gestohlen.html**
[3] **http://www.sueddeutsche.de/digital/datenklau-bei-sony-hacker-stehlen-millionen-geheime-kundendaten-1.1089569**
[4] **http://www.computerwoche.de/a/wie-sich-mitarbeiter-vor-social-engineering-schuetzen%2C2540578**
[5] **http://www.spiegel.de/wirtschaft/wirtschaftsspionage-verdacht-pentagon-prueft-ausschreibung-fuer-tankflugzeug-a-264272.html**
[6] **http://boersenlexikon.faz.net/sharehol.htm**
[7] **https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Mailtest_21012014.html**
[8] **http://www.gesetze-im-internet.de/bdsg_1990/__3.html**
[9] **http://www.gesetze-im-internet.de/bdsg_1990/__42a.html**
[10] **http://www.computerwoche.de/a/es-war-ein-spiel-und-ich-wollte-der-beste-sein%2C2516454**
[11] **http://www.corporate-trust.de/studie/studie-2012.html**
[12] **http://www.business-reframing.de/**
[13] **http://www.youtube.com/watch?v=-6QmwLpse3E**
[14] **http://www.computerwoche.de/a/iso-27001-stempel-mit-aussagekraft%2C2555531**
[15] **http://videokatalog.msn.de/Staat/video-US-Enth%C3%BCller-Snowden-packt-zu-%C3%9Cberwachungs-Aff%C3%A4re-aus-Sonderverwaltungszone-645714.html**

Bildergalerien im Artikel:

gal1 **Datenlecks vermeiden - Schutzmaßnahmen -**