

26.07.11

Schwerpunktthema: Cyber Attacken

Brainloop AG: Hacker müssen draußen bleiben



Nicole Dietrich

Warum gehen Informationen verloren? Häufige Fehleinschätzungen zum Thema Datensicherheit

Wie und wo geistiges Eigentum bei der Zusammenarbeit von Vertrauensgemeinschaften geschützt werden kann

In der modernen Arbeitswelt wechselt dokumentiertes Know-How meist per E-Mail-Anhang den Besitzer. Führungsverantwortliche vertrauten bisher auf die Loyalität ihrer Angestellten und gingen davon aus, dass schon nichts Wichtiges verloren geht. Diese Denkmodelle sind inzwischen überholt. Bedrohungen des Wissenskapitals durch Cyberkriminalität gehören zum Alltag und können täglich in der Presse nachgelesen werden. Das Bewusstsein wandelt sich und der Ruf nach Lösungen für den Schutz von so genannter Intellectual Property wird lauter. Das führende Marktforschungsunternehmen Gartner beispielsweise sieht eine rapide wachsende Nachfrage nach Möglichkeiten, „den Kommunikations- und Sicherheits-Anforderungen für den fortlaufenden Austausch sensibler Daten zwischen verschiedenen Organisationen über das Internet gerecht zu werden.“ Dieser Trend wird sich noch verstärken, wenn sich die Zusammenarbeit zwischen Innovationsnetzwerken, die weltweit an weit verstreuten Orten tätig sind, weiter intensiviert. Prozesse zum Austausch müssen einerseits sicher sein, sie dürfen aber andererseits auch nicht durch eine schwerfällige IT-Infrastruktur behindert werden, die die Ausführung anstehenden Aufgaben unnötig verzögert oder in die Länge zieht. Wie also können vertrauliche Inhalte hier schnell und sicher den Empfänger wechseln, ohne dass Andere mitlesen?

Warum gehen Informationen verloren?

Die Gründe, warum Informationen verloren gehen, sind vielfältig. Keine Seltenheit ist der vorsätzliche Diebstahl von Daten sowohl innerhalb eines Unternehmens als auch von

außen. Doch auch durch Unachtsamkeit kommt es zu Sicherheitslücken. Sie werden begünstigt durch unzureichende Datensicherungsmaßnahmen, Bedienungsfehler oder beides. Der über allem stehende Leitsatz, dass „die Arbeit getan werden muss“, veranlasst die Mitarbeiter nicht selten dazu, sensible Informationen unabhängig davon weiterzuleiten, ob Sicherheitsmaßnahmen getroffen wurden oder nicht. Die Kosten, die durch derartige Sicherheitslücken entstehen, können in allen Fällen enorm sein.

Nach Angaben der US-amerikanischen Chamber of Commerce führt Diebstahl geistigen Eigentums pro Jahr allein in den USA zu Verlusten in Höhe von 200 bis 250 Milliarden US-\$ sowie von etwa 750,000 Arbeitsplätzen. Nach Schätzungen von Forrester Research kann eine Sicherheitslücke Kosten zwischen 90 und 305 US-Dollar je Datensatz verursachen. Das heißt, dass die Kosten für eine einzige entscheidende Sicherheitslücke ohne weiteres in die Millionen oder gar Milliarden Dollar gehen können. Forrester Research befragte dazu 28 Unternehmen, bei denen es in letzter Zeit zu Sicherheitsproblemen gekommen war. Zu den direkten Kosten gehören Anwaltshonorare, Kosten für Benachrichtigungen und Gegenmaßnahmen, Produktivitätseinbußen des Personals, Marketing- und PR-Aufwendungen sowie Preisnachlässe auf Produkte. Doch warnte Forrester vor weiteren direkten Kosten, die nicht in der Schätzung enthalten waren, wie z. B. Strafen, Entschädigungszahlungen oder Mehrkosten durch Sicherheitsmaßnahmen.

Zusätzlich ergeben sich für ein Unternehmen durch jede Sicherheitslücke erhebliche weitere, nicht genau quantifizierbare indirekte Mehrkosten. Dazu gehört die ungewollte Offenlegung wichtiger Fakten und Daten, der potenzielle Verlust von Kunden, negative Auswirkungen auf den Aktienkurs, rechtliche Schritte von Aktionären, eine schlechte Presse durch den Imageschaden und dergleichen mehr. Diese Kosten können sogar noch höher sein als die unmittelbaren Kosten und sich auf zweistellige Millionenbeträge belaufen.

Häufige Fehleinschätzungen zum Thema Datensicherheit

Die Sicherheit der Daten zu gewährleisten ist in unserem modernen und dezentralisierten Umfeld wesentlich schwieriger als in der Vergangenheit. Teil des Problems ist, dass weitverbreitete Meinungen über Datensicherheit falsch sind. Nachfolgend sind drei der häufigsten Fehleinschätzungen aufgeführt, die Unternehmen bei der Umsetzung einer wirklich sicheren Lösung behindern.

Fehleinschätzung Nr. 1: Datensicherheit ist ein Problem der IT-Abteilung

Die meisten Führungskräfte möchten sicher sein, dass vertrauliche Dokumente vor Sicherheitslücken geschützt sind. Mit welchen Mitteln dies bewerkstelligt wird, ist ihnen gleichgültig. So delegieren sie das Thema Datensicherheit an die IT-Abteilung. Diese Betriebsblindheit kann jedoch in vielerlei Hinsicht problematisch sein.

Die Zuständigkeit der IT-Abteilungen für die Datensicherheit bezieht sich nämlich in erster Linie auf die Infrastruktur, und ihre Lösungen zielen daher primär auf die Computer interner Mitarbeiter als auf externe Partner. Hinzu kommt, dass Konsequenzen für den Endanwender häufig nicht genügend berücksichtigt werden, so dass beispielsweise viel Zeit und Ressourcen in die Ausarbeitung einer Infrastruktur investiert werden, die sich letztendlich für den Benutzer als umständlich erweist. Die Verschlüsselung von E-Mails oder Festplatten, die die Produktivität der Endanwender vermindern, dabei aber Dokumente nicht wirksam schützen, sobald sie an externe Partner verschickt wurden, sind Beispiele dafür. Häufig entwickeln sie eine firmenweite Lösung, die jeden Computer einbezieht, nicht auf externe Rechner übertragen werden und zudem Jahre dauern kann. Das andere Extrem sind nicht ausreichend wirksame IT-Lösungen, die wiederum neue Sicherheitslücken aufweisen.

Endanwender sehen sich daher häufig gezwungen, selbst eine effiziente Möglichkeit zur Abwicklung vertraulicher Geschäftsvorgänge zu finden, die auch vertrauenswürdig eingestufte externe Beteiligte einbezieht und strengsten Sicherheits-Anforderungen gerecht werden, ohne auf umständliche IT-Lösungen angewiesen zu sein. **Dabei betrifft das Thema Datensicherheit vor allem das Management, denn schließlich ist die Führungsetage haftbar, wenn es zu Sicherheitslücken kommt.**

Fehleinschätzung Nr. 2: Was sich hinter der Firewall befindet, ist sicher

Vertrauliche Dokumente sind auch hinter der Firewall verwundbar. Dabei kann die Datensicherheit von unzufriedenen Mitarbeitern oder von ‚Super-Usern‘ mit hohen Zugangs-Privilegien verletzt werden. Auch Personen, die aus dem Unternehmen ausgeschieden sind oder in eine andere Position versetzt wurden, deren Zugangs-Berechtigungen aber noch nicht aktualisiert wurden, können ein Sicherheitsrisiko darstellen.

Eine Firewall berücksichtigt zudem nicht den an kooperationsintensiven Geschäftsprozessen beteiligten Personenkreis. Der Zugang zu sensiblen Dokumenten sollte einer handverlesenen Gruppe weniger Personen vorbehalten bleiben. Aus diesem Grund sind Fileserver, Dokumentenmanagement-Systeme und E-Mail-Systeme äußerst unsicher, um vertrauliche Dokumente abzulegen und zu verwalten.

Die beste und zugleich sicherste Lösung zeichnet sich dadurch aus, dass sie einen reibungslosen Kontakt zwischen Anwendern auf beiden Seiten der Firewall ermöglicht. Gleichzeitig sollten unberechtigte Zugriffe durch Personen sowohl innerhalb als auch außerhalb des jeweiligen Unternehmens unterbunden werden. Von großem Vorteil ist die Ablage vertraulicher Dokumente auf Servern eines zertifizierten Rechenzentrums, da sie dort sowohl vor dem Zugriff durch unternehmensinterne Unbefugte als auch vor dem Betreiber selbst geschützt sind (Betreiberabschirmung).

Fehleinschätzung Nr. 3: Die traditionellen Sicherheitsmaßnahmen sind ausreichend

Manager, die mit hohem Termindruck an wichtigen Projekten arbeiten, vertrauen in der Regel darauf, dass die vorhandenen Sicherheitsmaßnahmen ausreichen, um die zu bearbeitenden Dokumente zu schützen. Allerdings sind - wie oben geschildert - viele Sicherheitsmaßnahmen der IT-Abteilungen in Wirklichkeit nicht wasserdicht. Gefährlich ist besonders die Auffassung, jede Sicherheitsmaßnahme sei besser als gar keine. **In Wahrheit ist halbe Sicherheit gleichbedeutend mit gar keiner Sicherheit.**

Nehmen wir als Beispiel die gängige Praxis, E-Mails mit einem Disclaimer zu versehen. Natürlich schützt solch ein Hinweis weder die E-Mail selbst noch die Daten in den Anhängen vor unbefugtem Zugriff. Genauso könnte man versuchen, sein Haus mit einem Schild „Einbrechen verboten!“ vor Dieben zu schützen.

Ein weiteres Beispiel für partielle Sicherheit sind verschlüsselte E-Mails, deren Informationen und Anhänge nur wirklich sicher sind, solange die Mail chiffriert ist. Sobald die Informationen auf dem Desktop in unverschlüsselter Form vorliegen, sind sie verwundbar. Auch die Festplatten-Verschlüsselung ist nur teilweise von Nutzen. Sie schützt nämlich nur die „ruhenden“ Daten. Sobald die Dokumente versandt werden, sind sie anfällig, denn die Verschlüsselung wird nicht mit übertragen.

Ein neues Paradigma

An diesen Fehleinschätzungen wird die Notwendigkeit eines tiefgreifenden Paradigmenwechsels in Bezug darauf deutlich, wie Unternehmen das Thema

Datensicherheit betrachten. Traditionelle Datensicherheitskonzepte wie etwa Firewalls (zur Absicherung der Außengrenzen) oder die Verschlüsselung von Daten auf dem Server oder während der Übertragung per E-Mail reichen nicht aus, denn sie gehen davon aus, dass die äußerst vertraulichen geschäftlichen Informationen in einer genau kontrollierten, definierten Umgebung bleiben. Diese Annahme ist aber falsch. Die Wahrheit ist, dass Dokumente in Bewegung sein müssen, damit man sie nutzen kann. Datensicherheit funktioniert deshalb nur, wenn sie mit dem betreffenden Dokument verknüpft ist und dem Dokument folgt, wohin auch immer es übertragen wird. **Nur dann kann man von durchgehender Dokumentensicherheit sprechen.**

Das neue Paradigma sieht Dokumente nur dann als sicher an, wenn sie sich an einem Ort außerhalb der Firewall befinden, der absolut sicher und dennoch für einen genau definierten Personenkreis jederzeit und von überall aus zugänglich ist. Anwender haben dabei die Möglichkeit, präzise zu kontrollieren, welche Dokumente eingesehen, genutzt und aktualisiert werden. Gemäß diesem Paradigma werden Dokumente in einem bestens geschützten, verschlüsselten Server außerhalb der Firewall abgelegt. Die Arbeitsabläufe werden nicht von der IT-Abteilung, sondern von autorisierten Endanwendern organisiert, so dass sensible Dokumente auch von internem Personal und Mitarbeitern der IT-Abteilung ferngehalten werden. Ein Zugriff auf die Dokumente ist nur mit Hilfe leistungsfähiger Authentifizierungs-Methoden möglich, die nur befugten Personen die Berechtigung erteilen. Zugriffsrechte lassen sich überdies auf Gruppen-Ebene oder für Einzelpersonen vergeben. Mit diesen Methoden sind Dokumente außerhalb der Firewall tatsächlich besser geschützt. Obwohl sie jederzeit und von überall zugänglich sind, erfasst ein lückenloser Audit Trail sämtliche Aktivitäten. Dank dieser Maßnahmen können die Geschäftspartner ungestört kooperieren und Informationen in der Gewissheit austauschen, dass die Dokumente in ihrem Reservoir absolut sicher sind.

Erfolgsstrategien in Sachen Datensicherheit

Je weiter sich wichtige Informationen von den physischen Grenzen eines Unternehmens entfernen, um so bedeutender wird die Technologie, die für die Sicherheit dieser Informationen sorgt. Gartner drückt es unmissverständlich aus: „Die traditionellen Sicherheitsmechanismen des Betriebssystems oder des Netzwerks werden diesen Anforderungen einfach nicht gerecht. Es gibt jedoch effektive Lösungen in Form von Sicherheitstechnologie, die auf der existierenden Infrastruktur aufsetzt, anstatt von ihr abhängig zu sein.“ Netzwerk-basierte Lösungen für die Datensicherung wie z. B. Fileserver oder die Firmen-Firewall sind für Dokumente, die mit externen Partnern geteilt werden müssen, nicht geeignet. Traditionelle Verschlüsselungsmethoden sind umständlich und können kooperative Geschäftsvorgänge behindern, während sie Datensicherheit nur bis zu dem Zeitpunkt gewährleisten, an dem die Dokumente entschlüsselt werden.

Nachfolgend wird eine Strategie zur lückenlosen Datensicherheit innerhalb dezentraler Unternehmen skizziert, die heute zur Verfügung stehen, um alle vertraulichen Dokumente zu schützen.

Die sichere Plattform für Document Compliance

Lösungen für Document Compliance sind web-basierte Anwendungen, die außerhalb der Firewall eines Unternehmens operieren. Sie bieten hochsichere Zugangs- und Sichtungskontrollen auf der Daten-Ebene (durchgängige Sicherheit) und kommen dennoch sowohl im Server als auch auf dem Client ohne proprietäre Software aus. Sie fungieren als Tresor für vertrauliche Dokumente außerhalb der firmeneigenen IT-Infrastruktur. Führungskräfte erhalten durch diese Lösungen die gewünschte und benötigte Kontrolle über hochsensible Dokumente, gleich wo sich diese befinden.

Um auf dieser Plattform hochvertrauliche Dokumente zu hinterlegen, sind höchste Sicherheitsstandards ein Muss: Dazu zählen der mehrstufige Login-Prozess mit Benutzernamen, Passwort und SMS-PIN, die Verschlüsselung der Inhalte während Download und Ablage auf dem Server und das manipulationsgeschützte Audit Trail (Protokollierung aller Aktivitäten auf der Plattform). Ein äußerst wichtiges Kriterium, auf das großer Wert zu legen ist, ist die Abschirmung des Betreibers, bei der durch Software und betriebliche Prozesse sichergestellt ist, dass die Betreiber der Document Compliance-Lösung keinen Einblick in Kundendaten nehmen können. Lösungen für Document Compliance kombinieren diese Sicherheits-Funktionen mit Kommunikations- und Administrations-Tools. Der Anwender kann mit deren Hilfe problemlos Zugriffsrechte festlegen und Arbeitsabläufe organisieren. Außerdem bekommt er die vollständige Kontrolle über alles, was von der Einrichtung bis zum Ende seiner Nutzung im web-basierten Arbeitsbereich vor sich geht. All dies geschieht auf eine Weise, die die Geschäftsabläufe vereinfacht anstatt sie zu behindern. Prozesse werden effizienter, und es bleibt Zeit für andere Aufgaben.

Zusammenfassung

In kritischen Geschäftsprozessen spielen stets hochvertrauliche, wichtige Dokumente eine Rolle, auf die jederzeit und von überall sicher zugegriffen werden kann. Gravierende Sicherheitslücken sind Folge unzureichender Sicherheitsmaßnahmen, die auf der traditionellen Sichtweise zum Thema Datensicherheit beruhen.

Das Geschäft geht weiter – ob mit oder ohne geeignete Kontrollmaßnahmen. Dokumente werden auch künftig übertragen. Je weiter sie sich dabei von den Grenzen des jeweiligen Unternehmens entfernen, umso wichtiger wird ihre Sicherheit, gleichgültig, wo sie sich im Einzelfall befinden. Es ist nicht hinnehmbar, dass wichtige Informationen angreifbar sind. Die Kosten, die sowohl direkt als auch durch Nichteinhaltung einschlägiger Vorschriften oder durch geschäftliche Risiken entstehen können, sind einfach zu hoch. Das Unternehmen selbst ist gefordert, dafür zu sorgen, dass seine wichtigsten Daten sicher und dennoch für alle relevanten Personen zugänglich sind. Es ist nicht verantwortbar, dass die Beschleunigung von Geschäftsabläufen zu Lasten der Sicherheit geht.

Die Technologie, die zur Gewährleistung der Sicherheit implementiert wird, ändert sich. Gefragt ist insbesondere ein Paradigmenwechsel in Bezug auf die Denkweise zum Thema Datensicherheit. So paradox es zunächst klingen mag: Vertrauliche Informationen sind sicherer aufbewahrt und für alle Beteiligten besser zugänglich, wenn sie außerhalb der Firewall eines Unternehmens gespeichert werden. Glücklicherweise gibt es heute bereits Lösungen, die diesem neuen Paradigma Rechnung tragen. Sie bieten neue Möglichkeiten, wichtige Geschäftsabläufe sicher und ungehindert durch komplexe IT-Aspekte abzuwickeln.

Siehe auch: <http://www.brainloop.de/loesungen/document-compliance-management.html>

Nicole Dietrich, Senior Director Marketing, Brainloop AG

[📺 Video von Brainloop ansehen](#)

Copyright All-About-Security.de / www.all-about-security.de Alle Rechte vorbehalten
Vervielfältigung nur mit Genehmigung von [All-About-Security.de](http://www.all-about-security.de)