

Risiko Management Strategie lässt Datendieben keine Chance

Ganzheitlicher Security-Ansatz gegen Datenabfluss und Industriespionage

Datendiebstahl hat Konjunktur: Nach Angaben des Identity Theft Resource Center in San Diego ist die Zahl der gemeldeten Datenverluste allein in den USA zwischen 2007 und 2008 um 47 Prozent gestiegen. Ursachen waren unter anderem, dass die personenbezogenen Informationen nur in 8,5 Prozent der Fälle zumindest durch Passwörter geschützt und in 2,4 Prozent der Pannen verschlüsselt gewesen sind. Auch hierzulande reißen die Meldungen über Datenpannen und Verluste von sensiblen Informationen nicht ab. In einer Vergleichsstudie hat das Ponemon Institute 18 Unternehmen befragt, die im Jahr 2008 Daten verloren haben. Die Gesamtkosten pro Datenpanne bezifferten sich durchschnittlich auf mehr als 2,4 Millionen Euro, ganz abgesehen vom Imageverlust. Bis zu acht Prozent der Kunden kehrten den betroffenen Unternehmen nach einem Datenunfall den Rücken. Aber nicht nur Kundendaten sind in Gefahr. Auch Forschungs- und Produktdaten sind für Wirtschaftskriminelle von großem Interesse. Für 2008 schätzte die Arbeitsgemeinschaft für Sicherheit und Wirtschaft (ASW) den Spionageschaden für die deutsche Wirtschaft durch ausländische Dienste und Konkurrenten auf bis zu 30 Milliarden Euro.

Auch wenn die genannten Zahlen und Fakten etwas Beängstigendes haben, die komplette Abschottung von Unternehmensinfrastrukturen von der externen Kommunikation und damit gegenpotenzielle Bedrohungen ist keine Lösung. Moderne, arbeitsteilige Geschäftsprozesse erfordern den schnellen Datenaustausch mit Partnern, Kunden und Zulieferern. Immer mehr Unternehmen planen deshalb die Einführung durchgängiger Risiko-Management-Strategien zum Schutz ihres Informationskapitals. Eine umfassende Sicherheitsstrategie schützt Geschäftsprozesse über Standorte und Unternehmensgrenzen hinweg, hilft Compliance-Regeln einzuhalten und fördert das Vertrauen der Kunden in das Unternehmen. Folglich ist IT-Sicherheit ein Thema mit strategischer Bedeutung, mit dem sich nicht nur IT-Administratoren, sondern vor allem die Geschäftsleitung befassen sollte. Angesichts der potenziellen Risiken und Kosten von Sicherheitslücken

relativieren sich Investitionen zum Schutz sensibler Informationen deutlich.

A wie Analyse

Was gilt es also zu tun, damit der Datenklau durch Externe oder eigene Mitarbeiter weitestgehend ausgeschlossen werden kann? Vor den ersten konkreten Maßnahmen steht immer eine umfassende Bestandsaufnahme der Sicherheitsanforderungen und individuellen Gegebenheiten im Unternehmen. Schon bei den zu schützenden Informationen gibt es stark schwankende Sicherheitsanforderungen: beispielsweise haben die SAP-Kundendaten in der Regel eine höhere Relevanz für den Geschäftserfolg als Informationen auf Testsystemen. Eine Klassifizierung der gesamten Unternehmensdaten ist also sinnvoll.

80 Prozent aller Fälle von Datenverlust oder -missbrauch sind auf Fehler oder Versäumnisse innerhalb der Firma zurückzuführen (Ponemon-Studie). Deshalb sollten die Mitarbeiter umfassend über Risiken aufgeklärt und für Sicherheitsthemen sensibilisiert werden. Wichtig ist dann außerdem die Einstufung der IT-Risiken individueller Geschäftsprozesse, um nachfolgende Maßnahmen entsprechend priorisieren zu können.

Modulare Sicherheitskonzepte

Der Analyse folgt die schrittweise Einführung von Sicherheitstechnologien auf Infrastruktur-, Client- und Anwendungsebene unter dem Dach eines unternehmensweiten Identitäts- und Zugriffsmanagements. Entsprechend ist Informationssicherheit längst nicht mehr die Betrachtung von einzelnen Komponenten, die abgesichert werden müssen. Hier entsteht über die Zeit ein schwer zu managender Flickenteppich, der durch seine Unübersichtlichkeit eher noch mehr Lücken in die Struktur bringt. Einen ganzheitlichen Ansatz liefert idealerweise ein IT-Dienstleister, der Erfahrungen in allen IT-Services hat.

IT Security spielt nicht mehr nur im Netzwerk eine Rolle, sondern in allen Disziplinen. Als Beispiel ist hier die Sicherheit der Clients im mobilen Umfeld zu nennen. Es reicht längst nicht mehr aus, einen Virenschanner zu implementieren

oder die Festplatte zu verschlüsseln. Unternehmen müssen sich Gedanken machen, wie sie die mobilen Geräte schützen und die entsprechenden Lösungen auf alle Clients ausrollen können. Weitere Themen in diesem Zusammenhang sind das Monitoring der Status sowie das Patchmanagement. Inzwischen gibt es zudem die Möglichkeit, sämtliche Sicherheitsmaßnahmen in Form von Managed Security Services oder ganzheitlichem Outsourcing komplett oder in Form einzelner Module an einen Dienstleister auszulagern. Dieser sollte nach Möglichkeit alle IT Disziplinen beherrschen, um umfassend schützen zu können. Standardisierung ist hier der Schlüssel zum Erfolg für die Unternehmen.

Bestehende infrastrukturelle Sicherheitsinstanzen wie Firewall- und Intrusion-Prevention-Systeme oder klassische VPN-Lösungen sind wichtig, denn sie halten Eindringlinge fern. Identity-Aware-Networks verschmelzen das Wissen der verteilten Dienste und Komponenten im Netzwerk und ermöglichen eine neue rollenbasierte Sicht auf den Datenverkehr im Netzwerk. Trotz aller Neuerungen sollten Unternehmen nicht auf ein automatisches Schwachstellen-Management verzichten, das die wirklichen Ursachen für Angriffe und Fehler erkennt. Zudem sorgen Log-Korrelationssysteme (Security-Information- und Security-Event-Management-Systeme) dafür, dass Anomalien, Gefahren und Angriffe in der Flut der Logs erkannt und in Bezug zueinander gesetzt werden.

Datenschutz für unterwegs

Knapp ein Drittel der Datenverluste resultieren aus dem Diebstahl oder Verlust von mobilen Endgeräten wie Notebooks. Die wirksamste Maßnahme dagegen ist – neben dem schlichten Aufpassen auf das Gerät – die Verschlüsselung der auf dem Notebook befindlichen Daten sowie eine wirksame Zugangskontrolle. Dazu kommen Standardmaßnahmen wie Anti-Virus, Anti-Spyware, Patch-Management oder spezielle Desktop-Firewalls. Zudem sollte der mobile Zugriff auf die Unternehmenssysteme durch VPN-Technologien und sichere Authentifizierungsverfahren abgesichert sein. Information-Rights-Management und Data-Loss-Prevention liefern zusätzlich neue Ansätze, um die Verarbeitung und den Verwendungszweck von Informationen genauer kontrollieren zu können.

Webbasierte Plattformen und Anwendungen sind gang und gäbe, um medienbruchfrei mit Kunden, Partnern und Mitarbeitern zu arbeiten. Mittlerweile ist allerdings davon auszugehen, dass bis zu 90 Prozent der Angriffe auf Unternehmensnetzwerke direkt auf Applikationen zielen. Sicherheitslücken lassen sich beispielsweise durch Web-Application-Firewalls schließen. Sie verstehen die Logik der Webapplikation und analysieren den entsprechenden Traffic. Auch die Überwachung der Kommunikation zwischen Datenbanksystemen und Applikationen kann unerlaubte Transaktionen aufspüren. Generell gilt: Die Entwicklung einer Anwendung sollte als Prozess verstanden werden, der nicht mit ihrer Inbetriebnahme endet. Vielmehr sollte die Lösung über ihren gesamten Lebenszeitraum hinweg auch unter Sicherheitsaspekten weiterentwickelt werden.

Straffes Management der digitalen Identität

Der Zugriff auf Unternehmensnetzwerke, Desktops und Datenträger muss automatisch in Einklang mit geltenden Sicherheitsregelungen erfolgen. Ziel sollte es sein, die Zahl der zu verwaltenden digitalen Identitäten und Passworte zu konsolidieren. Mit gezieltem Passwort-Management lässt sich etwa die Anzahl der Logins verringern (Single Sign On), der Bedienungskomfort erhöhen und die Helpdeskkosten beispielsweise durch Password-Self-Management senken. Digitale Zertifikate ermöglichen eine Authentifizierung mit standardisierten Verfahren, standardisierte Verschlüsselungslösungen oder digitale Signaturen. Auf Basis einer Public-Key-Infrastruktur können digitale Identitäten zentral verwaltet werden. Smartcards und USB-Token bilden die natürliche Identität in idealer Weise auf eine digitale Identität ab. Der Anwender benutzt seinen Ausweis als Schlüssel zu all seinen Anwendungen in seinem Unternehmen.

Natürlich eignen sich nicht alle vorgestellten Maßnahmen für jedes Unternehmen. Auch das blinde Hinzukaufen der neuesten Technologien ist nicht in jedem Fall die richtige Lösung. Der geeignete Technologiemix in Kombination mit dem entsprechenden Security-Know-how und vernünftigen, lebhaften Prozessen machen eine Infrastruktur weitgehend sicher. Hierbei ist

darauf zu achten, die vorhandenen Bordmittel zum Beispiel der Betriebssysteme auszuschöpfen.

So „sicher wie in Fort Knox“ sind die Unternehmensdaten allerdings nie. Böswillige Hacker, Wirtschaftskriminelle und auch illoyale Mitarbeiter werden immer Mittel und Wege finden, an sensible Informationen heranzukommen. Das oberste Ziel der Unternehmen sollte trotzdem immer sein, es Angreifern so schwer wie augenblicklich technologisch möglich zu machen. Der wesentliche Punkt dabei ist eine strategische und strukturierte Vorgehensweise bei der Umsetzung zuvor ermittelter Maßnahmen. Die immensen Kosten eines Datenverlustes, der Imageverlust beim Kunden, Bußgelder des Gesetzgebers beim Nichteinhalten von Sicherheitsvorgaben, Umsatzausfälle und langwierige Gerichtsverfahren liefern Argumente genug, um Unternehmensdaten professionell und ganzheitlich zu schützen.

((9.191 Zeichen))