Februar 2013

Datendiebstahl

Die wichtigsten Punkte im Überblick

- Der Diebstahl von Daten setzt Anwender einem erhöhten Betrugsrisiko und wahrscheinlicheren Identitätsmissbrauch aus. Zusätzlich wird das meist jahrelang gewachsene Vertrauensverhältnis zwischen Anwendern sowie Unternehmen und Regierungen empfindlich gestört.

- Microsoft will eine sichere und vertrauenswürdige Rechnernutzung aufbauen. Dazu gehört der Schutz vertraulicher Daten und persönlicher Informationen. Wir empfehlen für die Datenverwaltung einen Ansatz, der Richtlinien, Anwenderverhalten, Prozesse und Technologien berücksichtigt. Diese Empfehlung basiert auf unserer langjährigen Erfahrung bei Aufbau und Verwaltung sicherer Infrastrukturen und bei der Entwicklung ausgefeilter Systeme für die Identitäts- und Zugriffsverwaltung. Dazu gehört auch der Schutz von Informationen mit Überwachungs- und Berichtssystemen.

- Microsoft unterstützt Meldegesetze über Datendiebstahl, die mit einem risikoabhängigen Hinweissystem Nachrichten versenden, wenn eine nicht autorisierte Person auf geschützte Daten zugreift. Dies sollte nur geschehen, wenn ein erhöhtes Risiko für Betrug und Identitätsmissbrauch besteht, nicht bei einem minimalen Risiko. Dieses Gesetz sollte Anwender möglichst zeitnah informieren, es sei denn, eine Strafverfolgungsbehörde übernimmt dies im Zuge bereits eingeleiteter Ermittlungen.

HINTERGRUND

In den vergangenen Jahren berichteten Medien immer wieder von Datendiebstählen in öffentlichen Organisationen und Unternehmen der Privatwirtschaft. Weil dies auch Millionen vertraulicher persönlicher Daten und finanzieller Informationen betraf, war die öffentliche Aufmerksamkeit sehr hoch. Datendiebstahl bedroht nicht nur Anwender durch Betrug und Identitätsmissbrauch. Meistens wird auch das jahrelang gewachsene Vertrauensverhältnis zwischen ihnen und Unternehmen und Regierungen empfindlich gestört.

Viele Regierungen prüfen und überarbeiten derzeit die Meldegesetze über Datendiebstahl. Die vorhandenen Gesetze verpflichten normalerweise Unternehmen oder Behörden dazu, Anwender zu informieren, wenn ihre persönlichen Daten einem Risiko ausgesetzt sind oder missbraucht wurden. Dies geschieht entweder, wenn ein unbefugter Zugriff erkannt wird, oder mit einem risikoabhängigen Hinweissystem.

Im erstgenannten Fall müssen Unternehmen, die einen unbefugten Zugriff erkennen, die betroffenen Personen darüber informieren, dass ein nicht autorisierter Anwender auf ihre persönlichen Daten zugreifen wollte. Diese Informationspflicht ist unabhängig davon, ob der nicht autorisierte Anwender tatsächlich Daten entwendet hat oder der Versuch des Datendiebstahls erfolglos war. Im Gegensatz dazu müssen beim Einsatz eines risikoabhängigen Hinweissystems Unternehmen Anwender immer informieren, wenn ein potenzielles Risiko entdeckt wurde.

Obwohl Regierungen neue Richtlinien über die Hinweispflicht von Datendiebstählen entwickeln, ist ein Punkt besonders bemerkenswert: Es gibt in einigen Rechtsordnungen Unternehmen, die von einer Meldepflicht ausgenommen sind, wenn die Daten zum Zeitpunkt des Diebstahls verschlüsselt waren. Diese Ausnahmen sind für viele Unternehmen ein motivierender Faktor, Methoden zur Datenverschlüsselung einzusetzen und damit vertrauliche Daten besonders zu schützen. Unternehmen, die ausgefeilte Konzepte für die Datenverwaltung verwenden, reduzieren zusätzlich das Risiko eines Datendiebstahls. Denn sie machen dabei normalerweise effiziente Vorgaben für das Vorgehen im Falle entdeckter Sicherheitsrisiken.

DER MICROSOFT-ANSATZ

Wir empfehlen einen vielschichtigen Ansatz für die Datenverwaltung, der Richtlinien, Anwenderverhalten, Prozesse und Technologien berücksichtigt. Dieser Ansatz setzt auf:

- Eine mit Sicherheitsmechanismen verstärkte Infrastruktur, die Systeme vor Malware, Eindringlingen und nicht autorisierten Zugriffen auf vertrauliche Informationen schützt.
- Eine Identitäts- und Zugriffskontrolle, die vertrauliche Informationen vor unbefugten Zugriffen und Missbrauch schützt und eine ausgefeilte Verwaltung von Identitäten sowie deren Bereitstellung ermöglicht.
- Eine Speicherung vertraulicher, persönlicher Informationen in strukturierten Datenbanken, mit Schutzfunktionen wie einer Verschlüsselung von unstrukturierten Dokumenten, Nachrichten und Datensätzen.
- Ein Überwachungs- und Berichtssystem für die Systemintegrität, das zudem prüft, ob die Daten den unternehmensinternen Richtlinien entsprechen.

STRATEGISCHE ÜBERLEGUNGEN

- Sich widersprechende Gesetze können eine einheitliche regionale, nationale oder internationale Auslegung erschweren. Die große Vielfalt vorhandener Gesetze, Regeln, Verordnungen und Vorgaben verhindert oft den volkswirtschaftlichen Fortschritt und Innovationen. Ein gutes Beispiel hierfür sind die Vereinigten Staaten von Amerika mit ihren vielen verschiedenen Gesetzen in den einzelnen US-Bundesstaaten. Dort unterstützen wir eine breit angelegte, föderale Vorgehensweise für eine umfassende und einheitliche Gesetzgebung hinsichtlich der Privatsphäre. Gesetzgeber, Unternehmen und Organisationen müssen gemeinsam eine allseits anerkannte Lösung entwickeln, die sowohl die Privatsphäre als auch Innovationen schützt.
- Wir unterstützen Meldegesetze über Datendiebstahl, die Folgendes beinhalten:
  - » Ein risikoabhängiges Hinweissystem, das Anwender immer dann informiert, wenn eine nicht autorisierte Person auf vertrauliche Daten zugreift und wenn ein ernsthafter Verdacht auf einen Betrugsversuch oder Identitätsmissbrauch besteht.
  - » Wenn das potenzielle Risiko einer Schädigung oder eines Datendiebstahls sehr gering ist, soll keine Benachrichtigung des Anwenders erfolgen. Das ist beispielsweise dann der Fall, wenn die Informationen verschlüsselt oder auf andere Art und Weise für nicht autorisierte Personen unlesbar sind.
  - » Anwender sollen möglichst zeitnah informiert werden, es sei denn, eine Strafverfolgungsbehörde übernimmt dies im Zuge bereits eingeleiteter Ermittlungen.
- Obwohl wir eine obligatorische Information der Anwender über einen Datendiebstahl befürworten, sollte diese Hinweispflicht so ausgelegt werden, dass eine zeitnahe Benachrichtigung mit einer aussagekräftigen Beschreibung des Sachverhalts erfolgt. Werden Anwender zu schnell informiert, sind die gelieferten Informationen aufgrund der kurzen Zeit wahrscheinlich nicht genau genug oder nicht vollständig. Werden andererseits umfangreiche Hinweise auch bei einem vergleichsweise geringen Risiko auf einen Datendiebstahl versendet, werden Anwender höchstwahrscheinlich die vielen Meldungen recht schnell ignorieren.

Hilfreiche Ressourcen

Ein Überblick über die Microsoft-Richtlinien und -Initiative hinsichtlich der Privatsphäre
www.microsoft.com/privacy