Verbindliche Verschlüsselung

Februar 2011

Hintergrund

In den vergangenen Jahren haben eine Reihe von ungewollten Offenlegungen personenbezogener Daten sowie Sicherheitsverletzungen die Aufmerksamkeit der Öffentlichkeit und der Regierungen erregt. Im Jahr 2007 hat ein Regierungsbeamter zwei Computerfestplatten mit den unverschlüsselten Daten von rund 25 Millionen Bürgern in Großbritannien verloren. Im Jahr 2009 resultierte eine Datenschutzverletzung in den USA im Verlust von 100 Millionen Kreditkarteninformationen. Laut dem Microsoft Security Intelligence Report (SIR) ist gestohlenes Equipment in 30,6 Prozent aller Fälle die Ursache für Datenschutzverletzungen.

Staatliche Organisationen sowie die Industrie haben darauf reagiert und nutzen Verschlüsselungstechnologien, um die Datensicherheit zu erhöhen. Dank der Verschlüsselung sind die Daten nicht mehr lesbar. Es sei denn, man nutzt einen Code bzw. Algorithmus, um diese wieder zu entschlüsseln. Verschlüsselung sorgt für die Vertraulichkeit und Integrität der Daten. Bei der Verschlüsselung unterscheidet man zwischen gespeicherten Daten auf Platten, Bändern oder anderen Geräten (Data at Rest) sowie Daten bei der Übertragung über private Netzwerke oder das Internet (Data in Transit). Zudem lassen sich Daten danach klassifizieren, welchen Wert sie haben und welchem Zweck sie dienen. So identifizieren personenbezogene Daten wie der Name einen Menschen eindeutig. Als vertrauliche Daten gelten beispielsweise die Identifikationsnummern von Behörden oder auch Kreditkartennummern.

In den vergangenen Jahren haben Regierungsbehörden Gesetze erlassen oder Gesetze vorbereitet, die Organisationen dazu verpflichten, persönliche Daten zu verschlüsseln. Diese vorgeschlagene Gesetzgebung umfasst personenbezogene und vertrauliche Daten, Informationen, die übertragen werden, und in einigen Fällen auch Informationen, die übertragen und gespeichert werden.

Verschlüsselung spielt eine bedeutende Rolle für den Datenschutz, hat aber natürlich auch ihren Preis. Eine durchgängige und systemübergreifende Umsetzung von Verschlüsselungslösungen ist komplex und kostenintensiv – vor allem für kleine Unternehmen mit begrenzten Ressourcen für das IT-Management. In einigen Fällen ist Verschlüsselung auch nicht die geeignete Lösung, um Kundendaten zu schützen. Zudem sind viele moderne Endgeräte wie beispielsweise Smartphones nicht auf Verschlüsselung ausgelegt.

Immer mehr Gesetze verpflichten Unternehmen, Behörden und Institutionen dazu, Verstöße gegen die Datensicherheit anzuzeigen. Deshalb gehen immer mehr Organisationen dazu über, sichere Technologien einzusetzen, die beispielsweise auch Verschlüsselung umfassen. Viele Rechtsprechungen zu Verstößen gegen die Datensicherheit befreien Unternehmen davon, ihre Daten offen zu legen, wenn diese zum Zeitpunkt des Verlustes verschlüsselt waren. Diese „Ausnahmeregelung bei Verschlüsselung" ist ein starker Motivationsfaktor für Unternehmen, ihre sensiblen Daten zu verschlüsseln, um die schwerwiegenden Konsequenzen bei einer Datenschutzverletzung zu vermeiden.

Weiterführende Informationen:

www.microsoft.com/windows/windows-7/features/bitlocker.aspx
Microsoft Windows BitLocker

www.microsoft.com/online/exchange-email-encryption.aspx
Microsoft Exchange Hosted Encryption

www.microsoft.com/sir
Microsoft Security Intelligence Report

www.microsoft.com/security
Allgemeine Informationen zum Thema Sicherheit

Microsofts Lösungsansatz

Microsoft stellt Unternehmen, Regierungen und Privatpersonen nicht nur bewährte Sicherheitsverfahren, sondern auch Verschlüsselungstechnologien und -lösungen zur Verfügung.

- Microsoft BitLocker ermöglicht es Unternehmen und Privatpersonen, alle Festplatten von Computern mit Windows® 7 und Windows Vista® vollständig zu verschlüsseln. BitLocker To Go™ ermöglicht die Verschlüsselung von portablen Speichergeräten wie beispielsweise USB-Flash-Drives.
- Microsoft Exchange Hosted Encryption sorgt für eine richtlinienbasierende Verschlüsselung zwischen dem Sender und dem Empfänger einer Nachricht. Dabei benötigt der Anwender keine zusätzliche Software oder Schulung.
- Der Microsoft Security Intelligence Report (SIR) bietet umfassende Informationen über die sich ständig ändernde Bedrohungslage im Internet. Zudem berichtet der SIR auch über die aktuellsten Datenschutzverletzungen, Schwachstellen und Schadsoftware.

Grundsätzliche Betrachtungen

- Aufgrund der Komplexität und der Kosten für eine durchgängige und systemübergreifende Verschlüsselung, ist die Implementierung eines einzigen Standards für die Datenverschlüsselung nicht der beste Weg, um Daten umfassend zu schützen.
- Microsoft unterstützt Rechtsvorschriften und Richtlinien wie die Anzeigepflicht bei Verstößen gegen den Datenschutz. Sie bestärken Unternehmen darin, Verschlüsselungstechnologien einzusetzen, um sich vor der Offenlegung ihrer Daten zu schützen.
- Staatliche Behörden setzen sich verstärkt mit Sicherheitsfragestellungen und den damit verbundenen Technologien und Online-Services auseinander. Dabei ist es wichtig, dass sie im Rahmen dieses Prozesses die Innovationsfähigkeit fördern und den Technologieeinsatz nicht beschränken. Behörden und Wirtschaftsunternehmen sollten zusammenarbeiten, um geeignete Maßnahmen und Methoden zu definieren.

Die wichtigsten Punkte im Überblick

- Microsoft macht Verschlüsselungstechnologien für Unternehmen, staatliche Einrichtungen und Privatpersonen mit Produkten wie BitLocker, Festplattenverschlüsselung und Microsoft Exchange Hosted Encryption zugänglich.
- Aufgrund der Komplexität und des Kostenaufwands, den eine durchgängige und systemübergreifende Verschlüsselung verursachen würde, ist ein einziger Verschlüsselungsstandard unserer Ansicht nach nicht der beste Weg, Daten zu schützen.
- Microsoft unterstützt die gesetzlichen und politischen Bestrebungen, dass Unternehmen nicht verpflichtet werden können, ihre Daten offen zu legen, sofern sie Verschlüsselungstechnologien einsetzen.