Sicher auf allen Kanälen

Das Risiko eines Datenverlusts im Unternehmen wächst mit der Zahl der genutzten Mobilgeräte. Eine Enterprise Information Defense Strategy kann helfen.

Von **Daniel Liebhart***

Die Mehrheit der zwei Milliarden Menschen, die heute weltweit online sind, verwendet mobile Geräte. In den kommenden fünf Jahren werden es laut Google noch einmal zwei Milliarden Nutzer mehr sein. Laut Schätzungen von IDC werden sie zu einem Gutteil auch mobil arbeiten können oder wollen. Im Jahr 2015 gibt es laut IDC voraussichtlich 1,3 Milliarden mobile Arbeitsplätze.

Wie Untersuchungen im Rahmen der Cisco-Studie „Workplace of the Future" aufzeigen, möchte der überwiegende Teil aller Unternehmen bis ins Jahr 2020 auch mobile Arbeitsplätze zur Verfügung stellen. Damit verbinden die Unternehmen hohe Erwartungen: mehr Produktivität durch Flexibilität, weniger Kosten für Immobilien und Reisen sowie eine höhere Anziehungskraft auf dringend benötigte Fachkräfte. Verbesserte Kommunikation und klügere Entscheidungen aufgrund aktueller Informationen vor Ort, beispielsweise beim Kunden, erhöhen die Produktivität zusätzlich.

Drei Typen von Mobil-Arbeitsplatz

Doch mobiler Arbeitsplatz ist nicht gleich mobiler Arbeitsplatz. Zum einen wird mit unterschiedlichen Arbeitsgeräten – etwa Notebooks, Smartphones, Tablets, Digitalkameras, Videobrillen, Fernseher oder Auto – auf Daten und Anwendungen des Unternehmens zugegriffen. Zum anderen erfolgt dieser Zugriff auf lokaler Client-Ebene sowie auch auf Remote-Basis. Manche Mitarbeiter verbringen zwar den Tag im Büro, arbeiten aber innerhalb des Firmengeländes ständig mobil. Andere sind von einem festen Home- oder Remote-Office aus tätig. Wieder andere arbeiten immer von unterwegs. Was die Sicherheit und den Schutz von unternehmenskritischen Daten betrifft, hat jede dieser Zugriffsarten ihre spezifischen Risiken, denen die jeweilige Firmen-IT begegnen muss.

Sicherheitsstandards

Die Marktforscher von IDC schätzen, dass gut die Hälfte der kritischen Datenverluste in den Unternehmen durch interne Mitarbeiter verschuldet sind. Die Gründe reichen von Unachtsamkeiten und Fehlern bis zu schlecht verwalteten Systemen. Der Verlust wichtiger Informationen kann Firmen jeder Größe empfindlich treffen. Ohne neue Standards werden solche Vorfälle in Zeiten des mobilen Wachstums rasant zunehmen.

Die Standards müssen allerdings den gesamten Bereich eines mobilen Arbeitsplatzes und sämtliche Zugriffsarten umfassen. Eine kluge „Enterprise Information Defense Strategy" für die Bereitstellung sicherer mobiler Arbeitsplätze beginnt beim Endgerät, umfasst die Kommunikationsplattformen zwischen Endgeräten und IT-Infrastruktur und endet bei der Bewertung unternehmenswichtiger Daten sowie Informationen. Sie stützt sich auf die traditionellen Ansätze der IT-Security und kombiniert zunächst einmal unterschiedliche Ausrichtungen der traditionellen Data Loss Prevention (DLP) miteinander.

Data Loss Prevention

DLP unterscheidet zwischen Bewegungsdaten (Data in Motion), gespeicherten Daten (Data in Rest) und Daten auf dem Endgerät (Data at the Endpoint). Darüber hinaus ist eine unternehmensweite Bewertung von Informationen sinnvoll. Zusätzlich muss die Strategie die sich durch Mobilität verändernden lokalen Rahmenbedingungen einbeziehen. Je nach Land sind die Zugriffsrechte auf bestimmte Daten zu definieren, gleichzeitig aber lokale gesetzliche Rahmenbedingungen zu berücksichtigen.

Das Ziel von DLP besteht darin, einen Verlust von unternehmenskritischen Daten zu vermeiden. Dieses Element der Enterprise Information Defense Strategy setzt sich folglich aus verschiedenen Maßnahmen zum Schutz der Bewegungsinformationen, zur Überwachung der gespeicherten Daten sowie der Absicherung unternehmenskritischer Informationen auf dem Endgerät zusammen.

Schutz von Bewegungsdaten

Im Fall der Bewegungsdaten geht es beispielsweise darum, die unkontrollierte Kommunikation über das Netz zu verhindern. Die erlaubte Kommunikation wird von

Die hauptsächlichen Datenklassen

- **Kritische Daten:** Zu dieser Kategorie zählen alle Daten, die das Unternehmen für die wichtigen Geschäftsprozesse benötigt und deren Verlust zu einer operativen Katastrophe führen kann (die Leistungserstellung ist massiv be-, wenn nicht verhindert). Ferner handelt es sich hier um Daten, die aus rechtlichen Gründen aufbewahrt werden müssen.
- **Business-Performance-Daten** sind dagegen solche Daten, die für die Steuerung und Planung eines Unternehmens relevant sind. Gehen sie verloren, kann das im Extremfall ebenfalls zu einer unternehmerischen Katastrophe führen.
- **Essenzielle Daten:** Darunter fallen alle diejenigen Daten, die für das tägliche Geschäft verwendet werden. Sie bilden einen Teil des Business-Know-hows des Unternehmens.
- **Sensible Daten** sind solche, die ebenfalls für das Daily Business verwendet werden, aber die sich entweder schnell wiederherstellen oder durch alternative Daten ersetzen lassen.
- **Nicht kritische Daten** schließlich lassen sich mit geringen Kosten wiederherstellen. Bisweilen handelt es sich bei dieser Datenklasse auch um Duplikate bestehender Daten.

Seiten der internen IT daher ständig überwacht und analysiert. Dies geschieht sinnvollerweise auf der Grundlage eines speziellen Regelwerks, das die unternehmensweiten Richtlinien für den Schutz sensitiver Daten abbilden muss.

Schutz gespeicherter Daten

Die gespeicherten Daten werden in drei Bereichen geschützt:

1. **Sichtbarkeit** (Wo sind überall Daten zu finden?),
2. **Zugriff** (Wer darf auf die Daten zugreifen?) und
3. **Sicherheit** (Wer greift eigentlich gerade auf die Daten zu?).

Schutz der Daten auf Endgeräten

Auch für die Absicherung der Daten auf dem jeweiligen Endgerät gibt es ein Maßnahmenpaket. Eine der größten Schwachstellen ist schließlich der Verlust von mobilen Geräten wie Smartphones oder Notebooks: Gelangen diese in falsche Hände, so wird dem Missbrauch quasi Tür und Tor geöffnet.

Ebenfalls wichtig sind exakte Kontrollen bei der Auslieferung sämtlicher Endgeräte und bei der Speicherung der Unternehmensdaten. Gewährleistet sein müssen auch eine sichere Verwaltung der Endgeräte einschließlich des Schutzes ihrer Software und Privilegien sowie die zentrale Überwachung verteilter IT-Infrastrukturen.

Unterscheidung der Datenklassen

Neben dem DLP basiert eine Enterprise Information Defense Strategy auch auf der Unterscheidung zwischen kritischen und unkritischen Informationen. Nur wenn ein Unternehmen diese Datenklassen unterschieden und festgelegt hat, lassen sich eine Strategie definieren sowie Sicherheitsmaßnahmen festlegen und umsetzen.

Bereits eine so simple Unterscheidung wie die zwischen kritischen Daten, Business-Performance-Daten, essenziellen Daten, sensiblen Daten und nichtkritischen Daten (siehe Kasten „Die hauptsächlichen Datenklassen“) ist hier sehr hilfreich und reicht für viele Unternehmen aus. Die einzelnen Datenklassen müssen dann entsprechend ihrem Unternehmenswert geschützt und sicher verwaltet werden.

Der lokale Kontext des Zugriffs

Das dritte Element einer guten Enterprise Information Defense Strategy besteht darin, den lokalen Kontext des Zugriffs auf die Daten zu berücksichtigen. Dies betrifft besonders den mobilen Arbeitsplatz. Denn je nach Aufenthaltsort des Mitarbeiters gelten für den Umgang mit kritischen Daten unterschiedliche Regeln.

So ist es beispielsweise in vielen Ländern nicht strafbar, geschützte Technologien, also das geistige Eigentum anderer, ohne Lizenzierung zu verwenden oder gar in eigene Produkte zu integrieren. Das wird insbesondere in forschungsintensiven Hochtechnologiesektoren schnell zu einem Problem, weil sich Konkurrenten auf diese Weise einen Vorteil verschaffen und wirtschaftlichen Schaden anrichten können.

In unterschiedlichen Ländern gelten außerdem unterschiedliche Datenschutzgesetze. Die lokalen gesetzlichen Vorgaben sind zu berücksichtigen und in die Strategie einzubeziehen.

Klassische Regeln reichen nicht

Die „mobile Explosion“ hat also weitreichende Konsequenzen für die IT-Infrastruktur von Unternehmen jeder Größe und damit auch für die Verwendung Business-relevanter Informationen. Klassische Sicherheitsregeln allein genügen nicht, um die neuen Risiken der globalen Mobilität von Arbeitsplätzen konsequent abzusichern.

Unternehmen, die mobile Arbeitsplätze anbieten wollen, sind also gut beraten, vor dem Start mögliche Konsequenzen beim Umgang mit unternehmenskritischen Daten genau zu analysieren. Komplettlösungen existieren noch nicht. Doch lassen sich kritische Daten mit einer konsequenten Sicherheitsstrategie, wie sie oben skizziert ist, bereits jetzt sehr gut schützen. *(sh/qua)*

***Daniel Liebhart** ist Dozent für Informatik an der Züricher Hochschule für Angewandte Wissenschaften und Solution Manager der Trivadis AG.