



Link: <https://www.cio.de/a/mobile-daten-effektiv-schuetzen,2948375>

Schutz unternehmensrelevanter Daten Mobile Daten effektiv schützen

Datum: 03.03.2014
Autor(en): Uwe Wöhler

Die meisten Daten sind heute mobil. Trotzdem müssen sie vor unberechtigten Zugriffen und Manipulationen geschützt werden. Das erfordert eine Sicherheitsstrategie, die an den Daten ansetzt und sowohl organisatorische als auch technische Maßnahmen umfasst.

Unternehmen stehen heute vor einem Dilemma: Einerseits wollen sie selbstverständlich ihre Daten schützen. Andererseits sind Daten, die sicher im Tresor liegen, heute im Grunde nichts mehr wert. Vielmehr gewinnen sie ihren Wert erst dadurch, dass sie zwischen den verschiedenen internen und externen Beteiligten eines Wertschöpfungsnetzes transportiert, immer wieder gelesen, verändert oder angereichert werden. Das Tresor-Modell funktioniert ganz einfach nicht mehr.

Ein gutes Beispiel dafür ist die Automobilindustrie, in der alle Akteure der vielgliedrigen, globalen Zulieferketten auf permanenten Informationsaustausch angewiesen sind. Die Entwicklung eines neuen Automodells - von den ersten Ideenskizzen bis zur finalen Produktionsfreigabe - durchläuft viele Stufen mit unterschiedlichen Akteuren im In- und Ausland, die jeweils mit zahlreichen Dokumenten unterlegt sind. Das erhöht die Wahrscheinlichkeit von Informationslecks. Das gilt besonders, wenn den Schutz- und Sicherheitsmaßnahmen das alte Paradigma der Edge-Security, also vom Schutz der Netzwerkgrenzen, zugrunde liegt. Denn in einem derart vernetzten Ökosystem ist schlicht nicht mehr feststellbar, wo die zu sichernden Grenzen verlaufen.

Ein Beleg für die aktuellen Probleme beim Datenschutz sind die jährlichen Automobilsalons. Dort treffen deutsche Qualitäts-Automobilbauer heute regelmäßig auf Aussteller aus Fernost. Deren Exponate setzen oft genug brandneue Ideen um, die ein hiesiger Autobauer in seinen Laboren entwickelt hat und jetzt zur gewohnten Qualität verfeinert, um sie in der übernächsten Fahrzeuggeneration auf den Markt zu bringen. Doch wenn die Idee schon anderweitig vermarktet wurde - und sei es in einer höchst imperfekten Weise - ist der Neuheiten-Effekt, auf den der etablierte Hersteller hoffen durfte, bereits verpufft. Kommt er mit seinem mit derselben, aber zur vollen technischen Funktionsreife entwickelten Innovation endlich auf den Markt, wird er bestenfalls als Nachahmer wahrgenommen und daher um den Lohn seiner Mühen gebracht. Gerade für die hiesige Automobilindustrie, aber auch für andere High-Tech-Industrien in den industrialisierten Ländern ist ein effektiver Schutz von Daten und Informationen deshalb überlebenswichtig.

Datenschutz braucht Rückendeckung des obersten Managements

Doch wie dafür sorgen? Nur eine holistische Perspektive verspricht Erfolg: Effektiver Datenschutz umfasst organisatorisch- politische und technische Maßnahmen. Als erstes muss das Thema ganz oben in der Unternehmenshierarchie als Priorität verankert werden. Sonst wird der hoffentlich vorhandene CISO (Corporate Information Security Officer) kaum die nötigen Mittel erhalten, um effektive organisatorische Strukturen und technische Maßnahmen in diesem Bereich umzusetzen.

Hat die oberste Geschäftsleitung die Notwendigkeit moderner und durchgreifender Schutzmaßnahmen erkannt und stellt deshalb entsprechende Budgets bereit, folgt der nächste Schritt: Man analysiert alle Daten auf ihren Wert und teilt ihnen und je nach der Werthaltigkeit ein entsprechendes Schutzniveau zu.

Das ist ein letztlich kaum automatisierbarer Vorgang, für den tiefgehendes Wissen über die einzelnen Prozesse nötig ist, in deren Verlauf Daten von immer anderen Beteiligten bearbeitet oder weitergegeben werden. Dieses Wissen besitzen am ehesten die Mitarbeiter aus dem jeweiligen Fachbereich, die die Prozesse gestalten und für ihren Ablauf verantwortlich sind. Sie sollten auch für den Schutz der ihnen unterstehenden Daten zuständig sein.

Deshalb hat es sich bewährt, das Unternehmen zunächst in Fachbereiche wie Design, Einkauf, Vertrieb etc. mit jeweils eigenem Datenbestand und eigener Datenzuständigkeit zu unterteilen. Anschließend analysieren die Fachbereichsverantwortlichen die Daten und weisen sie einer Schutzklassen zu.

Meist reichen drei Schutzklassen aus: weniger wichtig, durchschnittlich wichtig und höchst wichtig. Am wichtigsten sind selbstverständlich die Daten, deren Verlust dem Unternehmen den größten Schaden zufügen könnte. Dabei gilt: Der Wert eines Dokuments steigt mit dem Fortschreiten der Wertschöpfungskette. Während der Verlust der Konstruktionspläne des Gesamtfahrzeugs kurz vor der Produktionsreife der größtmögliche Schadensfall ist, ist der Verlust der ersten Konstruktionsskizzen oder der Verlust der Pläne für eine einzelne Standard-Komponente leichter zu verkraften. Beide Güter müssen daher unterschiedlich geschützt werden.

Die Bereichsverantwortlichen sollten sich auch nach der Implementierung effektiver Schutzmechanismen regelmäßig mit dem CISO und gegebenenfalls anderen Beteiligten über das Thema Datenschutz austauschen, da die Datenbestände, Prozesse und Technologien sich ständig verändern. Außerdem müssen alle an datensensiblen Prozessen Beteiligten auch über die Unternehmensgrenzen hinaus auf das Thema eingeschworen werden - beispielsweise durch Schulungen, Informationsmaßnahmen, Sanktionen bei Verletzung von Datenschutzregeln oder die Aufnahme entsprechender Vereinbarungen in die Verträge mit Zulieferern.

Daten und Dokumente statt Netzwerkgrenzen in den Mittelpunkt

Bei der nun folgenden Implementierung geeigneter technischer Maßnahmen rücken die einzelnen Dokumente in den Mittelpunkt. Denn dokumentenbezogene Schutzmaßnahmen wandern mit dem Dokument mit, egal, wo es sich befindet - auch dann, wenn es in unbefugte Hände gerät. Effektiven Schutz bietet eine Kombination von Enterprise Rights Management, Data Leakage Prevention und Verschlüsselung.

Enterprise Rights Management bedeutet, jedes einzelne Dokument mit Informationen darüber zu versehen, wer wie auf das Dokument zugreifen darf. So kann beispielsweise ein Mitarbeiter des externen Serviceteams auf einen Teileplan lediglich schreibenden Zugriff erhalten, während das Designteam diesen Plan im Rahmen der Weiterentwicklung des Fahrzeugs auch verändern darf. Weil die Zugriffsberechtigungen mit dem Dokument verbunden sind, sehen Unbefugte schlicht nichts, da sie keine Zugriffsrechte haben und können deshalb mit gestohlenen Dokumenten nichts anfangen.

Die Zugriffsrechte werden dabei durch Verschlüsselung durchgesetzt. Verschlüsselte Daten sind für alle nicht lesbar, die nicht über den gewünschten Schlüssel verfügen weil entsprechenden Rechte fehlen. Gerade in Zeiten forciertes Datenspionage gewinnen im allgemeinen Verschlüsselungsmechanismen erhöhte Bedeutung und sollten in keiner Datenschutzinfrastruktur fehlen.

Data Leakage Prevention schließlich sorgt dafür, dass Daten und Dokumente erst gar nicht an Orte kommen, an die sie nicht gehören. Dabei werden an verschiedenen Stellen der IT-Infrastruktur Clients implementiert, die alle dort befindlichen oder "durchreisenden" Dokumente nach bestimmten, vom Anwender vorgegebenen Stichworten untersuchen und dann je nach dem vermuteten Inhalt bestimmten Regeln unterwerfen. Beispielsweise könnte eine solche Regel lauten, dass Dokumente mit der Überschrift Vertrag niemals auf USB-Medien gespeichert oder nur an eine vordefinierte Liste von E-Mail-Empfängern versendet werden dürfen. Durch die Kombination aller drei Methoden wird dem Datenklau ein wirksamer technischer Riegel vorgeschoben.

Situationsangepasste Schutzmechanismen

Der Aufbau eines effektiven Datenschutzsystems erfordert die Berücksichtigung der divergierenden Interessen vieler und sehr unterschiedlichen Partner, die in ein Wertschöpfungsnetz eingebunden sind. So kann es einem großen Zulieferbetrieb mit einer eigenen IT-Mannschaft durchaus zugemutet werden, ein umfassendes Enterprise Rights Management aufzubauen. Einem hochqualifizierten Ingenieurbüro mit einer Handvoll Mitarbeitern, aber ohne interne IT, oder einem kleinen Offshore-Zulieferer ist dies schwerlich abzuverlangen. Hier müssen situationsangepasste Lösungen gefunden werden. Eine Möglichkeit sind dabei sichere, in der Regel projektbezogene Online-Datenräume, wo Daten unter Ausschluss unbefugter Dritter sicher und schnell global ausgetauscht werden können.

Wegen der Komplexität des Themas sind viele auch große Unternehmen überfordert damit, eine differenzierte Schutzinfrastruktur im Alleingang zu errichten. Bewährt hat sich hier die Zusammenarbeit mit Unternehmen, die Produkte für alle Schutzniveaus im Portfolio haben. Gleichzeitig sollten sie auch über das nötige, langjährige Implementierungs-Know-how verfügen, ihre Zuverlässigkeit bewiesen haben und möglichst Branchenerfahrungen mitbringen. Mit vereinten Kräften ist es so möglich, am Ende selbst von den guten eigener Ideen zu profitieren, statt den Gewinn unfreiwillig anderen zu überlassen.

Uwe Wöhler ist Senior Security Consultant - HP Enterprise Security Services