



Datenverluste sind existenzgefährdend

Je wertvoller Daten sind, desto höher ist die Wahrscheinlichkeit, dass sie irgendwann »abhanden kommen«. Schlampelei allerorten macht den Datenklau oft zum Kinderspiel. Technische Barrieren können hier einiges verhindern, letztlich ist Datensicherheit aber eine organisatorische Frage.

von **jürgen höfling** |
juergen.hoefling@informationweek.de

Unternehmen müssen in Zeiten der digitalen Ökonomie offener denn je sein, bereit zu schnellem und komfortablem Datenaustausch mit Lieferanten und Kunden und zuweilen sogar mit dem Wettbewerb. Diese Offenheit hat natürlich ihren Preis. Vertrauliche Daten müssen umso penibler klassifiziert und geschützt werden, je offener ein Unternehmen im digitalen Kommunikationsverbund agiert. Undichte Stellen gibt es bekanntlich genug, vom banalen USB-Stick bis hin zu P2P-Netzwerken, über die sich Unbekannte unerkannt in unabsichtlich freigegebenen Ordnern bedienen können.

E-Mail im sicheren Datenraum

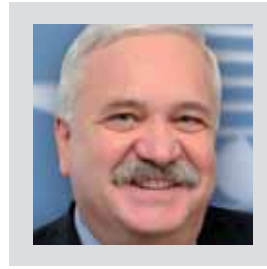
An technischen Tools zur Absicherung von vertraulichen Daten fehlt es wahrhaftig nicht. Von Microsoft bis Adobe, von Ironport bis McAfee, von Workshare bis Trend Micro: Verfahren und Techniken en masse und für (fast) jedes Budget. Trotzdem: das Verhindern des unerwünschten Abfließens vertraulicher Daten ist zunächst einmal ein Führungsproblem beziehungsweise eine organisatorische Angelegenheit. Gegen den Missbrauch von bestehenden Rechten oder den schlampigen Umgang damit ist jedes Tool machtlos. Da hilft nur ein Vier-Augen-Prinzip oder vielleicht das Konzept des sicheren Datenraums, bei dem ein auf Mark und Knochen geprüfter und gebriefter Vorstandsassistent die Rechte an bestimmten Dokumenten vergibt. Und auch das hilft nicht immer.

Der »Secure Dataroom« des Münchner Unternehmens Brainloop integriert die gängigen Sicherheitsmechanismen wie Verschlüsselung und Rechtevergabe auf einem speziellen Richtlinienserver, der von einem nicht-technischen Administrator kontrolliert wird und der die entsprechenden Rechte erst einbindet, wenn ein Dokument auf den Client geladen werden soll. Mit diesem sicher recht aufwändigen System lässt sich auch sicherer E-Mail-Verkehr fahren. Dabei findet der Empfänger zunächst eine Stellvertreter-E-Mail im elektronischen Postkorb, welche auf das Vorhandensein der echten Mail im Datenraum hinweist. »Eine Stellvertreter-E-Mail im Postfach schien uns zunächst doch sehr aufwändig für den täglichen Gebrauch zu sein. Nach dem ersten Ausprobieren sind wir aller-



»Drei Viertel aller deutschen Unternehmen testen ihre Software mit echten Kundendaten.«

Marcus Nohl, Senior Technical Consultant bei Compuware



»Informationssicherheit ist ein ganzheitlicher, unternehmensweiter Zustand.«

Josef Villa, Director Business Development bei S&T

dings von dem Nutzen dieser Vorgehensweise überzeugt und gebrauchen das Tool als tägliches Arbeitsinstrument«, sagt Stefan Groß, Certified Information System Auditor bei der Steuerberatungsgesellschaft Peters, Schönberger & Partner.

Probleme von dokumentenzentrierten Verfahren

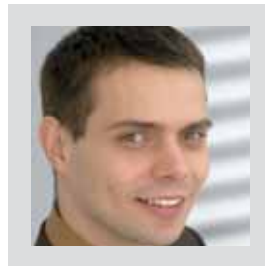
Brainloop hat die Windows Rights Management Services von Microsoft in sein System eingebaut, sodass Office-, Sharepoint und Exchange-Nutzer ihre diesbezüglichen Dokumente über den Brainloop-Server laufen lassen können, beispielsweise auch als Online-Service. Ebenso wie Adobe setzt ja Microsoft auf dokumentenzentrierte Systeme zum Schutz vertraulicher Daten. Dabei wird im Dokument selbst festgelegt, wer was wann mit diesem machen darf. Solche Systeme sind einerseits sehr präzise einstellbar, andererseits gibt es »immer wieder Hemmnisse bei den nur schwer erfüllbaren Kompatibilitätsanforderungen zwischen den Kommunikationspartnern«, gibt Stefan Strobel, Geschäftsführer des Heilbronner Sicherheitsspezialisten Cirosec zu bedenken. Darüber hinaus weist Strobel auf die vielfältigen Fehlerquellen hin, die sich »dadurch ergeben, dass bei diesem Verfahren die zu schützenden Daten und Dateien verändert werden«.

Die meisten Mechanismen, die dafür sorgen sollen, dass vertrauliche Daten nur im Kreis der Berechtigten bleiben, kennzeichnen vertrauliche Dateien deshalb rein äußerlich. »Rein äußerlich« soll dabei lediglich heißen, dass das Dokument nicht selbst verändert wird, die Klassifizierungsmethode bezieht aber in aller Regel die Inhalte, die in einem Dokument transportiert werden, in die Sicherheitsmaßnahme ein. Einige Tools wie das des Kaspersky-Ablegers InfoWatch betreiben eine umfangreiche linguistische Analyse, um vertrauliche Dokumente zu orten. Andere Tools wie beispielsweise Workshare kommen ursprünglich aus der Detektion von vergessenen Metadaten innerhalb von Office-Dokumenten, die ja oft nur scheinbar gelöscht sind. Workshare zeigt solche Schwachstellen an, über die vertrauliche Informationen unbewusst abfließen können. Nicht immer muss dabei die große Verbotskeule geschwungen werden. »Wir informieren unsere Mitarbeiter, dass es heikle Metadaten in ihren Dokumenten geben kann und dass sie mit Workshare Protect ein Werkzeug haben, mit dem sie ihre Dokumente reinigen können. Bei welchen Dokumenten sie dies tun, bleibt ihnen selbst überlassen«, erläutert Oli-

ver Müller, IT-Projektleiter bei der KfW Bankengruppe, die dortige Vorgehensweise.

Agentenbasierte Lösungen

Im Prinzip wird heute alles Mögliche als Schutzmechanismus gegen Datenverluste verkauft: Das Spektrum reicht von allen Arten von Verschlüsselungslösungen (weil sie die Daten ja schützen, wenn das Notebook oder der Handheld verloren geht oder gestohlen wird) über aufgemotzte Endgeräte-Blocker (USB-Sticks, Firewire, Bluetooth) bis hin zu Lösungen, die Dateien und Verzeichnisse durch ein umfassendes Rechte management steuern. De facto haben alle Hersteller, die noch vor zwei, drei Jahren ihre Softwarepakete als Kontrollinstrumente für externe Devices verkauften, mittlerweile



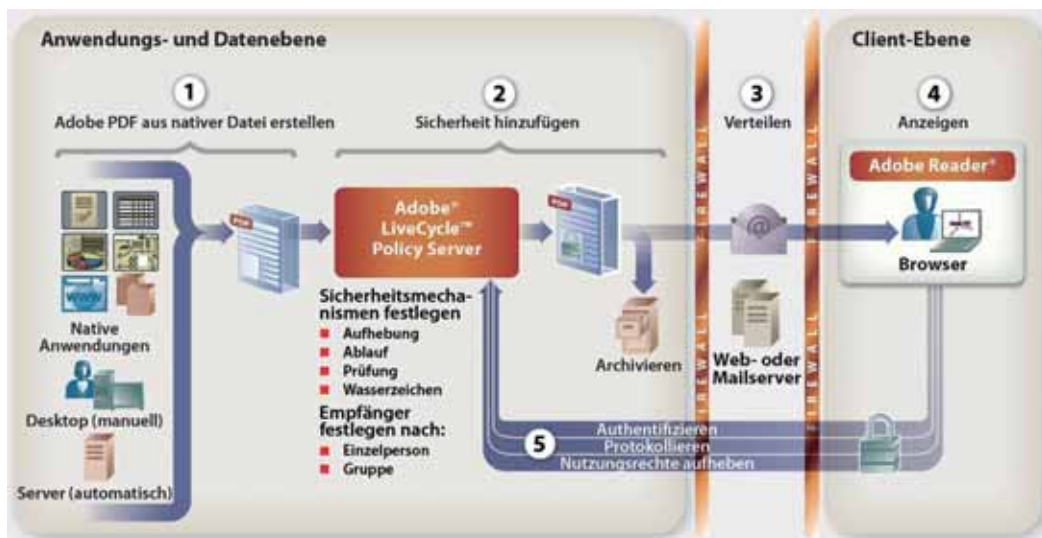
»Ein IT-Dienstleister muss vertraglich zusichern, dass seine Dienstleistung die üblichen Sicherheitsstandards erfüllt.«

Rainer Link, Senior Security Specialist bei Trend Micro

das Etikett gewechselt und segeln unter »Data Loss Prevention«. Sicher irgendwie zu Recht, denn die technische Basis ist ja die gleiche. Die Dateien und Verzeichnisse werden mit Kennzeichnungen (Tags) versehen, welche die Klassifizierungsstufen und die Nutzerrechte für vertrauliche Informationen innerhalb eines Unternehmens widerspiegeln. Diese Informationen werden durch einen Richtlinienserver verwaltet und den Agenten (falls es sich um eine agentenbasierte Lösung handelt, was aus Effizienzgründen fast unabdingbar ist) als Informationen zur Verfügung gestellt.

Im Detail gibt es bei den einzelnen Lösungen natürlich Unterschiede. So baut Lumension Security (früher Securewave) in erster Linie auf seinem Positivlisten-Verfahren (»alles, was nicht erlaubt ist, das ist verboten«) auf, Spezialisten für Schadsoftware-Bekämpfung wie Trend Micro setzen Schwerpunkte beim Perimeter-Schutz, E-Mail-Spezialisten wie Ironport heben ihre Stärken bei der Verschlüsselung von Mails heraus und Netzwerk-Schwergewichte wie Cisco konzentrieren die Prävention auf Tools wie den hauseigenen »Security-Agent«.

Auch Fingerprint-Verfahren sind in vielen Lösungen



Mit Richtlinien-
servern à la Adobe
lässt sich steuern,
wer was wann
mit bestimmten
Dokumenten
machen darf.

implementiert, so beispielsweise bei Workshare oder bei Trend Micro, dessen Produkt LeakProof übrigens auch von Utimaco innerhalb seiner Data Security Suite verkauft wird. Bei Fingerprint-Verfahren wird eine Art elektronischer Fingerabdruck der Daten erzeugt, wodurch verdächtige Teilstücke beziehungsweise veränderte Passagen erkannt werden können. Aber auch die Erkennung mittels Schlüsselwörter und sogenannter »regulärer Ausdrücke« ist gängige Praxis in vielen Produkten. Für derart klassifizierte Dokumente werden regelbasiert erlaubte und nicht erlaubte Aktionen definiert. Alle befragten Spezialisten geben zu Protokoll, dass die überwiegende Mehrzahl der Datenlecks durch Leichtsinn und Unwissenheit entstehen. Gezieltes Absaugen findet nach der Meinung der Herstellervertreter eher selten statt. Bei dieser Einschätzung ist sicher auch viel Zweckoptimismus im Spiel. Denn das bewusste und gezielte Abgreifen von Informationen kann durch keines der Tools wirklich verhindert werden. Dieses gezielte Abgreifen geschieht in aller Regel durch das missbräuchliche Ausnutzen von bestehenden Rechten.

Risikospiegel »Testen mit Echtdateien«

Auf eine meist wenig beachtete offene Flanke der ungewollten Datenoffenlegung weisen Rainer Link, Senior Security Specialist bei Trend Micro, und Marcus Nohl, Senior Technical Consultant bei Compuware, hin. Rund drei Viertel aller deutschen Unternehmen benutzen für ihre Softwaretests (die sehr oft von Externen durchgeführt werden) echte Kundendaten, hat das Ponemon-Institut bei einer Umfrage im Auftrag von Compuware herausgefunden. Und weiter: Fast die Hälfte der Befragten hat bereits Daten durch Leichtsinn oder Diebstahl verloren. Anscheinend sind die Anforderungen einer IT-Entwicklungsabteilung so weit von der Vorstellungswelt der Geschäftsleitung, aber auch der Sicherheitsbeauftragten entfernt, dass

diese gar nicht darauf kommen, dass hier Daten- und Personenschutz-Probleme vorhanden sein könnten. Die Fahrlässigkeit, die in diesem Bereich offenbar herrscht, ist umso unverständlicher, als es am Markt Verfahren gibt, die Echtdateien so zu anonymisieren, dass sie einerseits für Datenspione keinerlei Wert mehr haben, andererseits das Beziehungsgeflecht echter Daten haargenau simulieren.

Wie steht es um den Schutz vertraulicher Daten, wenn nicht nur die Programmentwicklung, sondern der halbe oder ganze IT-Betrieb ausgelagert wird? Die Antwort ist eigentlich klar: Gerade hier ist höchste Vorsicht geboten. »Es sollte kein Outsourcing-Partner unter Vertrag genommen werden, der hinsichtlich des Dokumentenschutzes nicht gemäß den Vorgaben seines Auftraggebers arbeiten kann. Andernfalls würde der Unternehmensleitung des Auftraggebers ein Organverschulden vorzuwerfen sein, das im Prüfbericht moniert werden müsste und zur persönlichen Haftung führen könnte«, gibt Rainer Link von Trend Micro zu bedenken.

Grenzen der Technik

Technische Maßnahmen zum Schutz vertraulicher Informationen sind also immer nur ein Mittel zum Zweck. Sie sind oft eine notwendige, aber nie eine hinreichende Bedingung dafür, dass die Informationssicherheit im Unternehmen gewährleistet ist. »Informationssicherheit ist nicht nur die Folge von Produkteigenschaften, sondern ein ganzheitlicher, unternehmensweiter Zustand«, sagt Josef Villa, Director Business Development beim Sicherheitsspezialisten S&T. Dass jemand seine Rechte missbräuchlich verwendet oder seine Rechte (oder auch die Gesetze) ignoriert, können technische Instrumentarien letztlich nicht verhindern. Allenfalls können sie die Latte, die zu überwinden ist, etwas höher setzen. ■