



Datenschutz für eine mobile Welt

Lücken in der Datensicherheit: ein immer gravierenderes Problem im privaten und öffentlichen Bereich

Nahezu wöchentlich gelangen Nachrichten über Datenlecks weltweit in die Schlagzeilen. Hier berichtet das Krankenhaus einer Großstadt, dass Kranken- und Personalakten versehentlich öffentlich zugänglich waren. Dort gibt eine Universität zu, dass Daten von Absolventen verloren gegangen sind. Und immer wieder kommen diesem oder jenem Ministerium Personaldaten abhanden.

Das Problem verschlimmert sich zusehends, nicht nur hinsichtlich der Menge der offengelegten Daten, sondern auch bezüglich der Anzahl der betroffenen Institutionen. Haben Sie sich schon einmal gefragt, was das kostet? Neben den negativen Auswirkungen auf den Ruf und die Glaubwürdigkeit eines Unternehmens führen solche Vorkommnisse auch oft zu Haftungsansprüchen, die empfindliche finanzielle Strafen mit sich bringen. Unter Berücksichtigung der Kosten für Rechtsbeistand, verstärkte Öffentlichkeitsarbeit und Benachrichtigung der Kunden (einschließlich der Überwachung der Konten betroffener Personen) können bei Datenlecks bis zu 200 \$ pro Kundendatensatz fällig werden.

Immer häufiger lässt sich ein solches Leck auf einen verloren gegangenen oder gestohlenen Laptop zurückverfolgen. Angesichts dieser Zahlen ist das kein Wunder: Laut dem Ponemon Institute werden allein auf US-amerikanischen und europäischen Flughäfen pro Jahr durchschnittlich 834.000 Laptops als verloren oder gestohlen gemeldet.

Oft gehören diese abhanden gekommenen Laptops Personen, die oft fliegen und häufig Zugriff auf sensible und vertrauliche Daten haben, z. B. Führungskräfte, Anwälte, Berater oder Außendienstmitarbeiter. Da sich die Zahl der europäischen und US-amerikanischen Arbeitnehmer, die für ihre computerbezogene Arbeit hauptsächlich Laptops nutzen, innerhalb der nächsten fünf Jahre von derzeit schätzungsweise 30 auf 60 Prozent erhöhen wird, ist daher auch ein rapider Anstieg der Anzahl verlorener bzw. gestohlener Laptops absehbar. Durch die steigende Anzahl mobiler Mitarbeiter und die stark zunehmende Menge an Bestimmungen, die die Veröffentlichung von vermutlichen Datenmissbrauchsfällen vorschreiben, sind Unternehmen gezwungen, über mögliche Schutzmaßnahmen hinsichtlich ihrer mobilen Daten nachzudenken. Oft fällt dann eine Entscheidung für ein Verschlüsselungsverfahren.

Softwareverschlüsselung: besser als nichts, aber bei weitem nicht optimal

Mit der ersten Generation der Festplattenverschlüsselung wurde ein erheblicher Fortschritt erzielt. Bei der Festplattenverschlüsselung kann ein Zugriff auf die Daten im Laufwerk nur dann erfolgen, wenn das Betriebssystem geladen und die Verschlüsselungsschlüssel entsperrt wurden. Diese Verschlüsselungsart hat gegenüber anderen Systemen wie der Verschlüsselung einzelner Dateien oder Verzeichnisse den Vorteil, dass der gesamte Inhalt des Laufwerks geschützt wird, einschließlich aller Auslagerungs- und temporären Dateien. Der Benutzer muss sich auf diese Weise nicht mehr aktiv entscheiden, ob Dateien geschützt werden sollen.

Die softwarebasierte Festplattenverschlüsselung hat jedoch auch ihre Nachteile. Der Rückgriff auf die Speicher- und Verarbeitungsressourcen des Computers bringt oft merkliche Einbußen der allgemeinen Systemleistung mit sich. Der Benutzer muss längere Lade- und Reaktionszeiten in Kauf nehmen, was nicht nur frustrierend ist, sondern auch die Produktivität einschränkt. Speicherintensive Anwendungen, beispielsweise Virenskans, können bei Computern mit softwarebasierter Festplattenverschlüsselung durchaus doppelt so viel Zeit in Anspruch nehmen wie bei Computern ohne diese Verschlüsselung. Hinzu kommen Zweifel an der tatsächlichen Sicherheit dieser Systeme, da ein Zugriff auf die Schlüssel zur Softwareverschlüsselung immerhin möglich ist. Es gibt beispielsweise „Cold Boot“-Angriffe, bei denen die beim Herunterfahren aus dem Speicher entfernten Daten abgefangen werden, oder auch die etwas neuere Gefahr der „Evil Maid“ (ein Programm, das mittels eines Wechseldatenträgers das Passwort der Festplatte ausspäht). Aufgrund dieser Risiken wächst bei Unternehmen die Sorge, dass der Schutz durch softwarebasierte Festplattenverschlüsselung möglicherweise nicht ausreicht.

Das bei weitem größte Problem ist jedoch der Aufwand, den eine IT-Abteilung betreiben muss, um diese Verschlüsselungssoftware einzurichten und zu warten. Allein das Installieren und Konfigurieren dieser Software nimmt schon mehrere Stunden in Anspruch. Einer aktuellen Studie zufolge kann der Verschlüsselungsprozess einer Festplatte mit 500 GB von 3½ bis zu 24 Stunden dauern.

Zwar kann die Verschlüsselung im Hintergrund ablaufen, jedoch kann sich dies so negativ auf die Systemleistung auswirken, dass der Computer während dieser Zeit praktisch nicht nutzbar ist. Für große Unternehmen mit zehntausenden Mitarbeitern kann ein solcher mit dem Einsatz softwarebasierter Festplattenverschlüsselung einhergehender Kosten- und Ressourcenaufwand bereits ein Ausschlusskriterium sein.



Die bessere Lösung: Hardwareverschlüsselung

Vor einigen Jahren brachte der führende Laufwerkshersteller Seagate Technology das erste Festplattenlaufwerk mit „eingebauter“ Verschlüsselung auf den Markt. Diese Laufwerke mit hardwarebasierter Verschlüsselung, auch als Self-Encrypting Drives (selbstverschlüsselnde Laufwerke) bezeichnet, hatten einen großen Vorteil: Sie ermöglichten sowohl ein höheres Maß an Sicherheit als auch eine höhere Systemleistung.

Festplattenlaufwerke bieten schon vom Prinzip her eine sicherere Umgebung: Sie verfügen über einen eigenen Prozessor und dynamischen Arbeitsspeicher sowie eine eigene Preboot-Umgebung. Im Gegensatz zu gewöhnlichen Geräten gibt es bezüglich des auf diesen Laufwerken ausführbaren Codes strikte Einschränkungen, sodass sie gegenüber herkömmlichen Softwareangriffen geschützt sind. Hinzu kommt, dass die Verschlüsselungsschlüssel im Controller des Laufwerks und keinesfalls im Speicher des Systems abgelegt werden. Auf diese Weise ist kein unbefugter Zugriff möglich.

Self-Encrypting Drives haben außerdem keinen negativen Einfluss auf die Systemleistung. Da für das Ausführen von Befehlen eigens dafür vorgesehene Prozessoren genutzt werden, muss hierfür nicht auf Systemressourcen zurückgegriffen werden.

Darüber hinaus ist die Laufwerksverschlüsselung bereits ab Werk aktiv. Es werden also alle auf das Festplattenlaufwerk geschriebenen Daten verschlüsselt und alle ausgelesenen Daten wieder entschlüsselt. Durch dieses Prinzip entfällt der für die softwarebasierte Festplattenverschlüsselung notwendige Schritt der „Verschlüsselung auf einen Schlag“ – und damit auch das zeitaufwändige Einrichten. Eine ständig aktive Verschlüsselung ist gerade dann wichtig, wenn nachgewiesen werden muss, dass ein abhanden gekommener Computer verlässlich geschützt ist. Die Gesetzgebung zum Datenschutz schreibt diesen Nachweis vor, um Unternehmen auf diese Weise vor Strafzahlungen bezüglich der Meldung von Datenverlust zu bewahren.

PC-OEMs machen SEDs allgemein verfügbar

Nachdem die Trusted Computing Group im Januar 2009 Herstellungsstandards für Self-Encrypting Drives veröffentlicht hatte (auch als „Opal“ bezeichnet), fand die Hardwareverschlüsselung verstärkt Beachtung. Diese großflächig unterstützte Vorlage veranlasste Toshiba, Hitachi und Samsung dazu, sich mit diesem Gebiet zu befassen und selbst Laufwerke mit hardwarebasierter Verschlüsselung anzukündigen. Neben Laufwerksanbietern taten sich auch Lenovo, Panasonic und HP mit Dell zusammen und boten viele ihrer Business-Laptops mit diesen Laufwerken an.

Strikte Zugriffskontrolle ist ein Muss für die Sicherheit

Entsprechend den bewährten Vorgehensweisen hinsichtlich Datensicherheit (und auch entsprechend den meisten Datenschutzbestimmungen) sind sowohl Verschlüsselung als auch strikte Zugriffskontrollen notwendig. Aus diesem Grund verfügen Self-Encrypting Drives über eine eigene Preboot-Umgebung auf Laufwerksebene. Dieser Bereich ist somit vor Eingriffen geschützt und bietet eine sichere Authentifizierung. Bei der Verifizierung auf Laufwerksebene werden alle Lese- und Schreibfunktionen gesperrt, bis der Benutzer die korrekten Anmeldedaten eingegeben hat. Dieses Verfahren ist wesentlich sicherer als die Verwendung von OS-, BIOS- oder ATA-Passwörtern, da diese vergleichsweise einfach auszuspähen sind und nicht den speziellen Ausnahmeregelungen entsprechen, die in den Gesetzen zur Veröffentlichung von Sicherheitsverletzungen in 45 Bundesstaaten der USA festgelegt sind.

Die Lösung: Self-Encrypting Drives und die EMBASSY®-Software von Wave

Eine umfassende Lösung für den Datenschutz erfordert mehr als nur Verschlüsselung. Ebenso unerlässlich sind richtlinienbasierte Zugriffsteuerung, zentrale Verwaltung und Nachweis der Konformität. In einem Unternehmen muss es möglich sein, Sicherheitsrichtlinien zentral gesteuert im gesamten Unternehmen umzusetzen, nur autorisierten Personen den Zugriff auf verschlüsselte Informationen zu gestatten, Kennwörter für Benutzer per Fernzugriff zurückzusetzen und, was wahrscheinlich am wichtigsten ist, nachzuweisen, ob die Daten eines Laptops zum Zeitpunkt seines Verschwindens verschlüsselt waren oder nicht. Die EMBASSY®-Software von Wave bietet diese unverzichtbaren Funktionen und mehr.

Trusted Drive Manager von Wave ist eine Clientanwendung, die die Sicherheitsfunktionen der Self-Encrypting Drives aktiviert. Dies umfasst unter anderem die Preboot-Authentifizierung sowie eine Funktion zum sicheren Löschen von Daten, die es ermöglicht, Laptops und Laufwerke auf sichere Weise außer Betrieb zu nehmen und zu entsorgen. Die Clientsoftware erzwingt unmittelbar beim Einschalten des PCs die richtlinienbasierte Zugriffsteuerung. Durch die Unterstützung von Windows® Single Sign-On muss der Benutzer sich weniger Kennwörter merken, was die Anzahl der Anrufe beim Help Desk verringert. Zudem ermöglicht die Integration in die Kennwortaktualisierung von Windows, dass Richtlinien für den Zugriff auf Laufwerke automatisch mit dem Betriebssystem aktualisiert werden. Dies stellt die Konformität mit den Kennwortrichtlinien des Unternehmens sicher.

Bei einem Einsatz in großen Unternehmen bietet EMBASSY Remote Administration Server von Wave den IT-Abteilungen die Möglichkeit, Richtlinien, Anmeldedaten und Zugriffsrechte von einem zentralen Standort aus zu verwalten. Durch die systemnahe Integration in vorhandene Verzeichnisstrukturen und Mechanismen zur Verteilung von Richtlinien kann das Zuweisen von Benutzern und Richtlinien im vorhandenen Verzeichnis-Framework ausgeführt werden, sodass die Bereitstellung immens vereinfacht und der Zeit- und Kostenaufwand reduziert wird.