



Charles Kolodgy
Research Director, Security Products

Verbesserung von Benutzerfreundlichkeit und technischer Handhabbarkeit durch Festplattenverschlüsselung

Februar 2010

Durch den explosionsartigen Anstieg der Datenmenge sind Informationen zu einer neuen Währung geworden. Informations-Bits haben einen erheblichen Wert. Informationen können mit geringem Aufwand erstellt, kopiert, geändert, vervielfältigt und verbreitet werden. Sie sind auch sehr anfällig für Verluste und Diebstahl und müssen deshalb aufgrund ihres Werts geschützt werden. Die Konsequenzen einer Datenverletzung sind real und bringen Organisationen in Gefahr. IDC ist der Ansicht, dass Organisationen Datenschutzlösungen einrichten sollten, um den Wert ihrer proprietären Daten zu erhalten, Informationen zu schützen, die ihnen von anderen anvertraut wurden und um Unternehmens-, Industrie und Regierungsrichtlinien und -bestimmungen einzuhalten. Verschlüsselung, insbesondere eine Endgeräteverschlüsselung ist eine der effektivsten Methoden, um Geschäftsinformationen, Personendaten und geistiges Eigentum zu schützen.

Die folgenden Fragen wurden von Safend an Charles Kolodgy, Research Director der IDC-Sparte Security Products, im Auftrag der Kunden von Safend gestellt.

F. Es gibt viele Bestimmungen, die den Schutz von personenbezogenen Daten erfordern. Was sind das für Bestimmungen, wie sollte man am besten dabei vorgehen und sind am Horizont bereits Änderungen ersichtlich?

A. Als Folge einer Reihe von Datendiebstählen und Sorgen über den Datenschutz haben Regierungen viele verschiedene Richtlinien beschlossen, die den Schutz von Personendaten zum Ziel haben. Um den Umfang der Diskussion zu begrenzen, konzentriere ich mich auf einige der wichtigsten Bestimmungen in den USA. Der amerikanische Health Insurance Portability and Accountability Act (HIPAA) erfordert, dass elektronische Patientendaten und Informationen vor Missbrauch und unberechtigtem Zugriff auf diese Informationen geschützt werden sollen. Durch den Health Information Technology for Economic and Clinical Health (HITECH) Act wurde das HIPAA aktualisiert, indem eine Verletzung als Form von „Aneignung, Zugriff, Verwendung oder Offenlegung“ geschützter Gesundheitsinformationen definiert wird, die ohne Befugnis erfolgt. Der Gramm-Leach-Bliley Act (GLBA) erfordert, dass die Finanzindustrie entsprechende Standards definiert, um die Vertraulichkeit der Kundendaten und den Schutz der Daten vor unbefugtem Zugriff oder unbefugter Benutzung zu gewährleisten. Darüber hinaus haben 45 Bundesstaaten Gesetze verabschiedet, die die Offenlegung von Informationen bei einem unberechtigten Zugriff betreffen und in denen auf verschiedenen Ebenen festgelegt wird, dass bei Offenlegung oder Verlust von personenbezogenen Daten die Kunden von der Verletzung in Kenntnis gesetzt werden

müssen. In den Bundesstaaten setzt sich dabei die Meinung durch, dass nicht nur eine Offenlegung der Informationen erforderlich ist, sondern ein Schutz der Daten. Im Datenschutzgesetz von Massachusetts (201 CMR 17), das am 1. März 2010 in Kraft getreten ist, wird genau festgelegt, welche Datenklassen geschützt werden müssen und welche Technologien sich für den Schutz eignen.

Dabei handelt es sich um staatliche Vorschriften, aber es gibt auch private Verfahren, bei denen der Datenschutz erforderlich ist; am bekanntesten ist in diesem Zusammenhang der Payment Card Industry Data Security Standard (PCI DSS). Dieser Standard wurde entwickelt, um Kreditkartendaten vor einer Offenlegung zu schützen, die zu Identitätsdiebstahl und Betrug führen würde. Unter PCI DSS müssen gespeicherte Daten des Karteninhabers geschützt werden.

Die tatsächliche Frage besteht allerdings darin, wie man denn diese personenbezogenen Daten schützt sollte? In einem Wort – Verschlüsselung. Diese Bestimmungen haben etwas gemeinsam: Sie bieten einen „sicheren Hafen“, der es ermöglicht, dass ein Verlust, Diebstahl oder Zugriff auf personenbezogene Daten, die durch einen Einsatz von Verschlüsselung „nicht brauchbar, nicht lesbar oder unentzifferbar“ sind, nicht als Verletzung eingestuft wird. Durch eine Verschlüsselung der entsprechenden Daten können Organisationen viel Geld sparen und Schwierigkeiten vermeiden. Das Ziel aller Inhaber von vertraulichen Daten sollte darin bestehen, jetzt durch den Einsatz geringer Investitionen sicherzustellen, dass nicht später sehr viel höhere Kosten auf das Unternehmen zukommen.

F. Sie haben erwähnt, dass es sich bei der Verschlüsselung im Zusammenhang mit der Einhaltung von Bestimmungen um einen „sicheren Hafen“ und in der Folge um eine Best-Practice für den Informationsschutz handelt. Für viele Benutzer ist es aber dabei überhaupt nicht klar, welche Endgeräteverschlüsselung am effektivsten ist. Zwei konkurrierende Endgeräteverschlüsselungsverfahren sind die sektorbasierte Verschlüsselung des gesamten Datenträgers (full disk encryption = FDE) und die Verschlüsselung von Dateien und Ordnern (file/folder encryption = FFE). Wie unterscheiden sich diese beiden Verfahren und gibt es noch andere Möglichkeiten?

A. Bei den zwei Möglichkeiten, Daten zu schützen, die auf einem Endgerät gespeichert sind, handelt es sich um FDE und FFE. Bei einer Verschlüsselung des vollständigen Datenträgers wird – wie der Name vermuten lässt, alles verschlüsselt, was sich auf der Festplatte des Computers befindet, inklusive Betriebssystemdateien, Bootsektor, Anwendungen und Benutzerdaten. Da bei FDE alles verschlüsselt wird, ist ein Authentifizierungsmechanismus vor dem Bootvorgang erforderlich, der sich außerhalb der herkömmlichen PC-Authentifizierung befindet. Diese Maßnahme ist sehr effektiv, um die auf dem Computer gespeicherten Daten zu schützen, solange dieser heruntergefahren ist, sobald sich jedoch ein autorisierter Benutzer beim Computer angemeldet hat, bietet dieses System überhaupt keinen Schutz mehr für die Daten. Der Zugriff auf alle Daten ist dann jedem möglich, dem es gelingt, auf den Computer zuzugreifen. Die Verschlüsselung von Dateien und Ordnern ist dagegen jederzeit effektiv, weil bei diesem Verfahren bestimmte Ordner oder Dateien oder virtuelle Datenträger verschlüsselt werden. Mit FFE können mehrere Benutzer am selben Computer arbeiten und ihre spezifischen Daten schützen. Dabei ist jedoch vom Benutzer ein beträchtlicher Aufwand erforderlich, um sicherzustellen, dass die betreffenden Dateien in den verschlüsselten Ordnern gespeichert werden und dass verborgene Dateien, wie die Dateien für die automatische Datensicherung, geschützt werden. FDE wird im Allgemeinen als eine Lösung für den ausgeschalteten und FFE für den eingeschalteten Zustand eingestuft. Eine wirklich umfassende Endgeräte-Lösung würde aus einer Kombination der besten Elemente von FDE und FFE bestehen. Diese Option gibt es bereits und sie wird als Festplattenverschlüsselung bezeichnet. Tatsächlich handelt es sich um eine Fusion aus den

beiden anderen Lösungen. Der Schwerpunkt der Lösung besteht im Schutz von vertraulichen Daten durch eine Verschlüsselung von Inhalten auf einer Festplatte, jedoch nicht der System- und Programmdateien. Indem die Festplattenverschlüsselung dateibasiert erfolgt, ist es möglich, eine Verschlüsselung aufrecht zu erhalten, während der Computer eingeschaltet ist. Dabei wird die Struktur der Festplatte nicht verändert, und es werden die herkömmlichen PC-Authentifizierungsverfahren verwendet und die Standardarbeitsabläufe beibehalten. Dabei sind für die Verschlüsselung auch keine Benutzerinteraktionen erforderlich. Die Festplattenverschlüsselung wird dabei so konfiguriert, dass alle Datendateien verschlüsselt werden, egal wo sie sich auf der Festplatte befinden.

F. Wie sieht es mit der Sicherheit der Festplattenverschlüsselung und FDE aus? Ist die eine besser als die andere oder bietet eine Lösung Verbesserungen bezüglich der Sicherheitsfunktionen?

- A. Es steht außer Frage, dass eine Verschlüsselung (wenn Algorithmen von einem namhaften Anbieter integriert werden, die auf Standards basieren) sowohl bei der Festplattenverschlüsselung als auch FDE einen ausreichenden Datenschutz bereitstellen. Die Installation eines dieser Mechanismen auf einem Computer reicht in vollem Umfang aus, um die zuvor erwähnten Bestimmungen zu erfüllen, besonders, wenn der Computer am Flughafen verloren geht oder aus einem Hotelzimmer gestohlen wird. Wie zuvor erwähnt, bietet FDE keinen Schutz der Daten, wenn der Computer eingeschaltet ist. Wenn ein durch FDE geschützter Computer in den Windows-Standby-Modus (oder Ruhemodus) versetzt wird, werden auch Sicherheitslücken geöffnet. In diesem Modus ist der Datenträger nicht verschlüsselt und der Verschlüsselungsschlüssel ist für den Angreifer weiterhin verfügbar. Wenn jemand Zugang zum Computer erhält, kann dieser den Datenträger herausziehen oder eine andere Technik einsetzen, wie Cold Boot- oder FireWire-Angriffe, mit denen Schlüssel potenziell wiederhergestellt werden können, die im Speicher gesichert sind.

Bei der Festplattenverschlüsselung kommt es auf der anderen Seite nicht zu denselben Problemen wie bei FDE. Zum Einsatz kommt dabei der herkömmliche Windows-Authentifizierungsmechanismus, d. h., es wird kein neuer Code in den Boot-Mechanismus eingeführt. Auf diese Weise können Organisationen, die eine zweifache Authentifizierung, wie Token oder Biometrik, implementiert haben, diese Sicherheitssysteme ohne Änderungen weiter verwenden. Dank der Windows-Authentifizierung ist es auch möglich, verschlüsselte Daten von verschiedenen Benutzern auf demselben Computer zu segmentieren. Dabei haben Benutzer nur auf die Daten Zugriff, die sie erstellt, geändert oder empfangen haben. Eine Segmentierung der Daten für autorisierte Benutzer verbessert die Sicherheit. Computer, die mit Festplattenverschlüsselung geschützt wurden, können sicher in den Standby-Modus versetzt werden, weil sich der Verschlüsselungsschlüssel nicht im Arbeitsspeicher befindet. Durch dieses Verfahren wird der Computer auch gegen Cold-Boot-Angriffe immunisiert. Im Endeffekt wird es dadurch dem Angreifer erschwert, Zugriff auf die Daten zu erlangen.

F. In Bezug auf Endgeräte in Unternehmen werden Geräte zunehmend zentral verwaltet. Wirkt sich der Einsatz der Verschlüsselung auf die Fähigkeit aus, ein zentrales Management durchzuführen?

- A. Das größte Unterscheidungsmerkmal zwischen einer Festplattenverschlüsselung und FDE bezieht sich auf das Endgeräte-Management im Unternehmen. Wie bereits erwähnt, kommt es zu Problemen mit den grundlegenden Verwaltungsfunktionen, weil FDE einen proprietären Authentifizierungsmechanismus vor dem eigentlichen Boot-Vorgang einsetzt. Patch-Aufspielung, Prüfungen und Softwareinstallationen können unterbrochen werden, weil der Administrator ohne die Anmeldedaten des Benutzers das verschlüsselte System nicht entsperren kann. Eine dezentrale Verwaltung von ausgeschalteten Geräten, z. B. in den Abendstunden, um die Auswirkungen auf die Benutzer so gering wie möglich zu halten, ist

bei Geräten mit FDE und Authentifizierung vor dem Boot-Vorgang nicht möglich, es sei denn, es gibt eine Umgehung (d. h. Back-Door), die es dem Administrator ermöglicht, ein System remote zu booten. Diese zusätzlichen Zugriffsmechanismen haben weitere Sicherheitslücken zur Folge, die dazu missbraucht werden können, um auf die Daten des Systems zuzugreifen. Durch die Notwendigkeit, dass die Administratoren Anmeldedaten haben, können weitere Probleme entstehen, weil der Administrator nun auf die Daten zugreifen kann. Schließlich ist es bei auftretenden Fehlern schwierig, Datenträger oder Software zu reparieren, weil die Betriebssystemdateien, das Verzeichnissystem und die Anwendungen verschlüsselt sind.

Zu diesen Komplikationen für das Endgerätemanagement in Unternehmen kommt es nicht, wenn ein System – z. B. eine Festplattenverschlüsselung – verwendet wird, bei dem alle Daten verschlüsselt werden, während sich gleichzeitig der Administrator anmelden kann. Patch-Aufspielung, Prüfungen und Aktualisierungen können ganz normal, wie auf Systemen ohne Festplattenverschlüsselung remote durchgeführt werden. Endbenutzer müssen nicht in den Prozess integriert werden. Administratoren und Helpdesk-Mitarbeiter müssen ihre Arbeitsabläufe nicht abhängig davon ändern, ob die Verschlüsselung auf einem Computer installiert ist oder nicht. Da außerdem bei der Festplattenverschlüsselung die Betriebssystemdateien und Anwendungen nicht verschlüsselt sind, können die Daten nach einem Systemausfall leichter wiederhergestellt werden.

- F. Wir haben darüber gesprochen, wie sich die Verschlüsselung des vollständigen Datenträgers und die Festplattenverschlüsselung in Hinblick auf Funktionalität, Sicherheit und Handhabbarkeit unterscheiden; aber wie sieht es mit der Gebrauchstauglichkeit aus? Gibt es eine Auswirkung auf Funktionen und Arbeitsabläufe für Endbenutzer?**
- A. Damit eine Verschlüsselung von Endgeräten besonders effektiv ist, müssen die Auswirkungen für die Endbenutzer so gering wie möglich sein. Die meisten Benutzer werden durch Verschlüsselung eingeschüchtert. Sie verstehen die Technologie nicht sehr gut und machen sich Sorgen, was sie mit ihren Computern macht. Sie möchten ihre Arbeit in der ihnen vertrauten Weise erledigen und sich keine Gedanken über die Sicherheit machen müssen. Im Allgemeinen betrachten sie Sicherheit, insbesondere Verschlüsselung, als Behinderung. Am besten geht man damit um, indem sichergestellt wird, dass alle die Sicherheit betreffenden Prozesse für die Endbenutzer transparent sind. Eine Festplattenverschlüsselung erfüllt diese Anforderungen. Der Anmeldevorgang ändert sich für den Benutzer nicht, das Desktop-Management bleibt dasselbe und die Systemleistung wird nicht beeinträchtigt, weil nur Benutzerdaten und nicht alles verschlüsselt und entschlüsselt werden. Benutzer müssen nicht entscheiden, welche Dateien verschlüsselt werden müssen. Eine Verschlüsselung von Endgeräten ist besonders akzeptabel, wenn die Auswirkungen auf die Benutzer minimal sind. Weil sich Funktionen und Vorgänge nicht für den Benutzer ändern, ist es für die Benutzer viel schwieriger, alle auftretenden Systemprobleme auf die Verschlüsselung zu schieben. Die Transparenz der Festplattenverschlüsselung für Benutzer wird durch die Verwendung der herkömmlichen Anmeldemechanismen verkörpert.

ÜBER DIESEN ANALYSTEN

Charles Kolodgy ist Research Director für die IDC-Sparte Security Products. Innerhalb der Sparte Security Products ist er für Hardware- und Software-Sicherheitsprodukte verantwortlich. Zu den Schwerpunktproduktbereichen gehören Firewalls, Intrusion Detection und Prevention, Gefährdungsanalyse und Management, Hardware-Authentifizierung (Token und Smartcards) und Verschlüsselung. Produktmärkte übergreifenden Untersuchungsbereiche umfassen Produktzertifizierung, Webseiten-Sicherheit und Sicherheitsrichtlinien.

ÜBER DIESE VERÖFFENTLICHUNG

Diese Veröffentlichung wurde von IDC Go-to-Market Services herausgegeben. Die darin dargestellten Meinungen, Analysen und Forschungsergebnisse wurden aus ausführlicheren Untersuchungen und Analysen extrahiert, die von IDC unabhängig durchgeführt und veröffentlicht wurden, es sei denn, eine Finanzierung durch ein spezielles Unternehmen wurde angemerkt. IDC-Go-to-Market-Services macht IDC-Inhalte in vielen verschiedenen Formaten verfügbar, damit diese von verschiedenen Unternehmen verteilt werden können. Eine Lizenz zur Verteilung von IDC-Inhalten impliziert weder eine Billigung des oder Meinung über den Lizenznehmer.

COPYRIGHT UND EINSCHRÄNKUNGEN

Alle IDC-Informationen oder Referenzen auf IDC, die in Werbungen, Presseveröffentlichungen oder Werbematerialien verwendet werden, müssen im Voraus schriftlich durch IDC genehmigt werden. Wenden Sie sich bei derartigen Anfragen an die GMS-Informationen-Hotline unter 001-508-988-7610 oder gms@idc.com.

Die Übersetzung und/oder Lokalisierung dieses Dokuments erfordert eine zusätzliche Lizenz von IDC.

Weitere Informationen über IDC finden Sie im Internet unter www.idc.com. Weitere Informationen über IDC GMS finden Sie im Internet unter www.idc.com/gms.

Internationaler Hauptsitz: 5 Speen Street Framingham, MA 01701 USA Tel.: 001-508 872 8200 Fax.001-508 935 4015, www.idc.com