wave®
Simplifying Encryption and Authentication

Netzwerksicherheit: So verteidigen Sie eine Grenze, die sich ständig verschiebt

Da in Unternehmen immer häufiger Laptops oder Heimarbeitsmöglichkeiten genutzt werden, können immer mehr Benutzer, Daten, Geräte und Anwendungen nicht mehr durch eine herkömmliche Firewall für das Unternehmensnetzwerk geschützt werden. Gleichzeitig werden die Vorschriften immer strenger, nach denen sich die Unternehmen – und ihre IT-Administratoren – für Lücken in der Daten- und Netzwerksicherheit verantworten müssen. Bedauerlicherweise haben sich die herkömmlichen Tools für die Netzwerksicherheit nicht besonders gut an die rasante Dezentralisierung der Unternehmensnetzwerke angepasst. Mit den herkömmlichen, auf Kennwörtern und Software beruhenden Sicherheitsmethoden können die Benutzer und Computer im Netzwerk nicht effektiv authentifiziert, Daten auf abhanden gekommenen oder gestohlenen Laptops nicht effektiv gesichert und die Einhaltung von gesetzlichen Vorschriften zur Offenlegung verloren gegangener persönlicher Daten nicht gewährleistet werden.

In diesem Whitepaper wird die wahrscheinlich leistungsstärkste, kosteneffektivste und einfachste Lösung dargestellt, wie die weit verstreuten Endgeräte heutiger mobiler Netzwerke wieder in einer starken und zentralen Netzwerksicherheitsarchitektur vereint werden können. Sie beruht auf drei allgemein verfügbaren, bewährten, jedoch meist unterschätzten Technologien: Trusted Platform Modules (TPM, vertrauenswürdige Plattformmodule), Self-Encrypting Drives (SED, selbstverschlüsselnde Festplatten) und zentralisierte (Fern-) Verwaltung der Netzwerksicherheit. Mit diesem Whitepaper möchten wir Ihnen nicht nur dabei helfen, fiktive und reale Fakten über diese Technologien voneinander zu unterscheiden, sondern auch aufzeigen, dass Netzwerksicherheit nicht als bloße Strategie, sondern vielmehr als durchsetzbare Unternehmenspolitik etabliert werden kann, wenn diese drei Technologien in der richtigen Kombination miteinander eingesetzt werden.

Die Entwicklung der Datensicherheitslandschaft

Wohl kaum ein IT-Manager wird die Tatsache bestreiten, dass der Bereich Datensicherheit in den letzten zehn Jahren radikal gewachsen ist und dieses Wachstum nicht mehr rückgängig zu machen ist. Neben der Sicherheitsverwaltung von zentralen Netzwerken müssen sich IT-Manager heute außerdem um immer mehr mobile Mitarbeiter kümmern. Diese Mobilität hat dazu geführt, dass immer mehr Endbenutzer, Geräte, Softwareanwendungen und höchst vertrauliche Daten nicht mehr durch die Unternehmens-Firewall geschützt sind. Vor diesem Hintergrund ist die Durchsetzung von Datensicherheit vergleichbar mit der Verteidigung einer Grenze, die sich fortlaufend verschiebt, sodass Teile des Netzwerks praktisch auf unbekanntem Territorium geschützt werden müssen.

Mit der Zahl der potentiellen Angriffspunkte ist auch der Preis für einen tatsächlichen Datenverlust angestiegen. Laut einer Schätzung von Gartner Research können die Kosten, die aus dem Verlust eines einzigen Geräts oder aus einem einzigen unberechtigten Zugriff auf das Computernetzwerk eines Unternehmens entstehen[1], bis zu 1,32 Millionen Dollar betragen, selbst wenn die Sicherheitsverletzung keine weiteren Folgen nach sich zieht, wie z. B. den Missbrauch der verlorenen Daten. Ein Großteil dieser Kosten wird durch die Gesetze über die Bekanntgabe von Sicherheitsverletzungen verursacht, die bereits in 46 US-Bundesstaaten und dem District of Columbia verabschiedet wurden. Laut dieser Gesetze müssen Unternehmen Sicherheitsverletzungen öffentlich bekannt geben, es sei denn, das Unternehmen kann garantieren, dass die Sicherheit der Daten nicht kompromittiert wurde und kein Missbrauchsrisiko durch unberechtigte Personen besteht.

Erschwerend kommt hinzu, dass sich die herkömmlichen Sicherheitsmaßnahmen für Authentifizierung und Verschlüsselung nicht besonders gut an die gestiegene Mobilität und Dezentralisierung der Benutzer in Unternehmensnetzwerken angepasst haben. Bisher beruhte die Kontrolle über den Netzwerkzugriff für berechtigte Benutzer auf der Verwendung von Kennwörtern. Während diese Methode für die Authentifizierung von Benutzern an einem unternehmensinternen Endgerät recht effektiv ist, werden die Kennwörter jedoch häufig von den Benutzern schlicht und einfach vergessen, besonders wenn die Richtlinien zufällige Zeichenfolgen und regelmäßige Änderungen der Kennwörter erfordern. Anders ausgedrückt: Kennwörter können leicht kompromittiert werden und bieten nur wenig Schutz außerhalb der Unternehmens-Firewall.

Die Verlagerung von unternehmensinternen Computern und Benutzern in den Bereich außerhalb der Firewall machte die Entwicklung neuer Authentifizierungsmethoden erforderlich, z. B. digitale Zertifikate, Biometrie, OTP-Tokens (Einmalkennwörter) und Smartcards. All diese Verfahren sind weitaus besser als bloße Kennwörter. Außendienstmitarbeiter, die stark auf ihren Laptop angewiesen sind, können sich insbesondere auf Tokens und Smartcards verlassen. Doch während der Umfang der Nutzung von Laptops und die Zahl der Telearbeitsplätze zugenommen haben, sind auch die Kosten für Anschaffung, Bereitstellung und Austausch der Tokens und Smartcards sowie der dafür benötigten Soft- und Hardware gestiegen.

Die herkömmlichen Datenschutzmaßnahmen konnten mit der neuen Netzwerkumgebung ebenfalls nicht Schritt halten. Vor erfahrenen Hackern bieten Kennwörter, wie z. B. BIOS-, OS- und ATA-Kennwörter, kaum Schutz, und sie bieten keine Möglichkeit, die Daten zu verschlüsseln. Wenn Sie bei Google nach den Wörtern „unlock hard drive password“ (Festplattenkennwort entsperren) suchen, erhalten Sie mehrere Treffer (z. B. HDD Unlock und Password Crackers), bei denen eigenständige Softwareprodukte und Dienste für weniger als 100 $ angeboten werden.

Stattdessen ist die softwarebasierte Festplattenverschlüsselung (FDE) zum Standard für den Schutz von Daten auf Laptops avanciert, bei der jedes Datenbit auf der Festplatte oder dem Festplatten-Volume verschlüsselt wird und unberechtigte Benutzer somit keinen Zugriff auf den Computer erhalten.

[1] Gartner, „Pay for Mobile Data Encryption Up Front, or Pay More Later“, 2009.

Vor Kurzem hat Microsoft seine eigene FDE-Software mit dem Namen Bitlocker auf den Markt gebracht, das für bestimmte Ausgaben des Betriebssystems Windows VISTA und Windows 7 kostenlos angeboten wird. In Kombination mit anderen Sicherheitsmethoden (die noch genauer betrachten werden) stellt dies einen großen Fortschritt für die Sicherheit mobiler Geräte dar.

Während die Software-FDE einen guten Schutz vor Hackern bietet, bleibt sie ziemlich anfällig für Sicherheitsbedrohungen anderer Art, da mit „Cold Boot"- und „Evil Maid"-Angriffen Zugriff auf die Verschlüsselungsschlüssel erlangt werden kann. Außerdem nimmt die Software-FDE die Speicher- und Verarbeitungsressourcen der jeweiligen Laptops stark in Anspruch, was häufig zu einer merklichen Verschlechterung der Systemleistung, längeren Startzeiten und somit auch zu einer Verschlechterung der Gesamtproduktivität führt. Und die Installation und Konfiguration der Software-FDE dauert buchstäblich stundenlang – nichts für ohnehin bereits überlastete IT-Mitarbeiter.

Kurz gesagt stellen Authentifizierungskennwörter und softwarebasierte Verschlüsselung lediglich Versuche dar, mit herkömmlichen Maßnahmen auf Risiken und Herausforderungen zu reagieren, die sich rasend schnell verändern und immer einen Schritt voraus sind. Zu den bereits genannten Beschränkungen kommt hinzu, dass die Sicherheit der Daten im Fall eines verloren gegangenen Laptops oder einer anderen Sicherheitsverletzung bei einer softwarebasierten Sicherheitslösung nicht garantiert werden kann. Diese Sicherheitsmaßnahmen entsprechen also nicht den gesetzlichen Pflichten zur Veröffentlichung von Sicherheitsverletzungen, und somit ist das Unternehmen nicht vor kostspieligen juristischen Folgen geschützt.

Anders ausgedrückt: Ein Netzwerk, in dem die Sicherheit seiner Endgeräte nicht garantiert werden kann, ist kein sicheres Netzwerk. Die Grundprinzipien der Datensicherheit gelten jedoch weiterhin, auch wenn sich immer mehr Daten, Geräte, Benutzer und Anwendungen in den Bereich außerhalb der Firewall verlagern. Die Grundprinzipien für IT-Manager zur Wahrung der Netzwerkintegrität lauten wie folgt:

1. Vertrauliche Daten bei Speicherung und Übermittlung sichern
2. Identität aller Geräte und Benutzer sicherstellen, die auf das Netzwerk zugreifen
3. Netzwerksicherheitsprotokolle zentral steuern, damit die Einhaltung der gesetzlichen Sicherheitsbestimmungen nachgewiesen werden kann

Die meisten IT-Manager kennen diese Grundprinzipien bereits. Was viele jedoch nicht wissen: Es gibt Methoden, mit denen jedes dieser Grundprinzipien auch in äußerst mobilen und verteilten Netzwerken durchgesetzt werden kann, und zwar praktisch über Nacht und zu minimalen Kosten. Dazu gehören:

1. TPM-Sicherheitschips (Trusted Platform Module) zum Etablieren einer automatischen und transparenten Authentifizierung von autorisierten Netzwerkgeräten und -benutzern
2. SEDs (Self-Encrypting Drives) zum Aufstellen eines unüberwindbaren Datenschutzes immer und überall
3. Eine Software-Verwaltungsplattform, bei der Verschlüsselung und Geräteauthentifizierung über eine zentrale Stelle gesteuert werden, wodurch die Einhaltung der gesetzlichen Bestimmungen bei Sicherheitsverletzungen nachgewiesen werden kann

Von diesen drei Methoden sind die ersten beiden weit verbreitet, kosteneffektiv und auf den meisten Unternehmens-Laptops bereits installiert oder problemlos als Option verfügbar. Zudem können sie in wenigen Schritten aktiviert werden. Und wenn dieses Trio vollständig angewendet wird, können die grundlegenden Sicherheitsprinzipien moderner mobiler Netzwerke an ihrer empfindlichsten Stelle durchgesetzt werden – auf jedem Endgerät.

Trusted Platform Modules: Mythen und Methoden

Der Begriff „Trusted Platform Module“ (TPM) ist bislang nur wenigen IT-Mitarbeitern vertraut. Kurz gesagt, handelt es sich hierbei um einen Sicherheitschip, der sich auf der Hauptplatine des Computers befindet. Somit werden die Sicherheitsfunktionen direkt in die Gerätehardware integriert. Da der TPM-Chip einen physischen Bestandteil des Geräts darstellt, ist er optimal zur Erstellung und Überprüfung einer eindeutigen Geräteidentität geeignet. Auf diese Weise wird sichergestellt, dass ausschließlich autorisierte Zugriffe auf das entsprechende Netzwerk erfolgen können. Die Vorteile des TPM liegen also in der Möglichkeit einer eindeutigen und transparenten Authentifizierung sowohl der Geräte als auch der Benutzer im Unternehmensnetzwerk.

Bietet Ihr derzeitiges Authentifizierungsverfahren diese Funktionen auch?

- ☑ Starke Authentifizierung von Gerät und Benutzer
- ☑ Zwei-Faktor-Authentifizierung ohne proportional ansteigende Kosten für Hardware, Einsatz oder Pflege
- ☑ Vollständige Aktivierung und Betriebsbereitschaft innerhalb von Minuten
- ☑ Problemlose Integration in vorhandenes VPN bzw. vorhandene Drahtlos-Infrastruktur
- ☑ Einheitliches Anwendungsprinzip für den Benutzer sowohl innerhalb als auch außerhalb der Firewall

Leider sind wahrscheinlich die meisten IT-Manager, die sich schon einmal mit TPMs beschäftigt haben, den falschen Auffassungen über diese Technologie zum Opfer gefallen. Diese falschen Vorstellungen entstammen ausnahmslos einem grundlegenden Missverständnis darüber, was TPMs eigentlich sind, wie sie eingesetzt werden sollten oder was die Sicherheitsanforderungen eines modernen Unternehmensnetzwerks wirklich beinhalten.

Einer der häufigsten Mythen stellt TPMs als neue, noch nicht ausgereifte Technologie dar. In Wirklichkeit sind sie wahrscheinlich bereits in über 90 % des gesamten PC-Bestands eines Unternehmens vorhanden. Bei führenden Herstellern wie Dell, Lenovo und HP werden TPMs seit vielen Jahren als Standardkomponenten in alle Notebook- und Desktop-Computerserien für Unternehmen integriert. Das bedeutet, dass Laptops mit TPMs den überwiegenden Großteil aller Laptops bilden, die derzeit in Gebrauch sind. Bis Ende 2010 wird dieser Anteil fast bei 100 % liegen.

Weiterhin wird oft fälschlicherweise angenommen, dass Sicherheitsmaßnahmen, die in die Hardware integriert sind, bei ausreichend guten Softwarelösungen nicht notwendig sind. Trotz dieser Behauptung konnten andere hardwarebasierte Lösungen wie RSA SecurID®-Tokens in den letzten zehn Jahren ein rasantes Wachstum verzeichnen und werden nun von ca. 25.000 Unternehmen genutzt, die sich jeden Tag darauf verlassen. Die Kunden überzeugte die zusätzliche Sicherheit, die Hardware-Tokens bieten; diese ist besonders wichtig für die Sicherung des Remote-Benutzerzugriffs.

Ironischerweise sind durch diesen Erfolg jedoch auch die Nachteile von Token sichtbar geworden: Ihre Gesamtbetriebskosten steigen im Verhältnis zur Anzahl der Mitarbeiter an, die sie verwenden. Während die Lösung in einem Unternehmen mit wenigen Laptops gangbar ist, steigen die Kosten für Anschaffung, Bereitstellung und Austausch der Tokens mit steigender Laptop-Nutzung erheblich an. Hinzu kommt, dass Einmalkennwörter von Windows nicht nativ unterstützt werden. Benutzer, die sich beim Unternehmensnetzwerk anmelden möchten, müssen daher ein zweistufiges Verfahren durchlaufen: Für die Anmeldung über ein VPN (virtuelles privates Netzwerk) ist ein OTP-Token erforderlich, aber für die Anmeldung innerhalb der Firewall (drahtgebunden oder drahtlos) werden andere Anmeldedaten gefordert, z. B. ein Kennwort oder eine Smartcard. Üblicherweise bevorzugen Unternehmen ein einheitliches Verfahren zur Benutzerauthentifizierung, um Verwirrung zu verhindern und die damit verbundenen Kosten für IT-Wartung und den Help Desk zu reduzieren.

wave®

Im Gegensatz zu OTP-Tokens, mit denen nur die Benutzer verifiziert werden, werden mit TPMs automatisch alle Geräte authentifiziert, die auf das Netzwerk zugreifen. Sie sind praktisch integrierte Hardwaretokens. Und weil sie auf neuen Laptops meist schon vorinstalliert sind, fallen keine zusätzlichen Anschaffungskosten an. Im Gegenteil: Die „harten" Bereitstellungskosten, die Tokens mit sich bringen, werden überflüssig. Dadurch senken TPMs die Gesamtbetriebskosten. Darüber hinaus bieten sie den Endbenutzern Transparenz und den Komfort, sich nicht auch noch um zusätzliche Hardware kümmern zu müssen. Für die IT-Abteilung bedeutet dies geringere Kosten und weniger Help-Desk-Anrufe zu verlorenen oder vergessenen Tokens.

Ein weiterer Trugschluss über TPMs sind Bedenken hinsichtlich des Datenschutzes, da sie Unbefugten potentiell Einblick in den Nutzungsverlauf eines Laptops bieten. Bei diesen Bedenken werden jedoch die Anforderungen an den Datenschutz für Verbraucher mit den strikteren Anforderungen an den Schutz eines Unternehmensnetzwerks verwechselt. Unternehmen müssen notwendigerweise eine höhere Priorität auf Netzwerkintegrität und Compliance als auf den Schutz der Daten einzelner Benutzer legen. Viele Unternehmen sind sogar gesetzlich dazu verpflichtet, sicherzustellen, dass Hacker keinen Zugriff auf die im Netzwerk gespeicherten Kundendaten erhalten können. Dazu müssen die IT-Mitarbeiter PC-Nutzung und -Zugriff streng verwalten sowie bei Datenverlust Sofortmaßnahmen ergreifen und Berichte erstellen können.

In diesem Kontext gesehen erhöht sich ohne TPMs das Risiko einer Datenschutzverletzung. Die meisten Endbenutzer in Unternehmensnetzwerken verstehen dies und akzeptieren die integrierten Sicherheitslösungen, die für die Einhaltung der Sicherheitsrichtlinien sorgen, bereitwillig – von Web-Filtern bis hin zu Richtlinien über das Öffnen von E-Mail-Anhängen. Wenn die Nutzung eines durch das Unternehmen authentifizierten Geräts mit einem TPM als Voraussetzung für den Zugriff auf unternehmenswichtige Netzwerkressourcen festgelegt wird, wird dadurch automatisch ein Sicherheitsniveau etabliert, das nicht von den Gewohnheiten einzelner Benutzer abhängt.

Mit jedem ausgeräumten Mythos entsteht nun langsam ein schärferes Bild darüber, was ein TPM alles nicht ist. Aber die vielleicht größte Hürde, die TPMs überwinden müssen, ist das allgemein fehlende Verständnis darüber, was TPMs eigentlich sind und was sie in einem modernen Unternehmensnetzwerk bewirken können. Schauen Sie sich zum Beispiel an, wie Mobil-, Kabel- und Satellitennetzwerke aufgebaut sind, die heute zu den sichersten und am schnellsten wachsenden Netzwerken gehören. Grundlage der Sicherheit in all diesen Netzen ist die Ermittlung der Identität des Endgeräts. Die Netzwerke für iPod, iPhone und iPad von Apple® verwenden die Geräteidentität seit neuestem auch als Schlüsselelement für den Netzwerkzugriff und die Nutzung von Diensten. Bei all diesen Beispielen ist das Prinzip der Netzwerkstruktur relativ einfach: Der Zugriff auf sensible Netzwerkressourcen darf nur durch „bekannte" Geräte erfolgen. Ein weiteres Hauptmerkmal dieser Netzwerke ist die Tatsache, dass die Geräteidentität nicht in der Software, sondern in der Hardware gespeichert und geschützt wird. Die Identität des Geräts ist somit dauerhaft geschützt.

Bei TPMs handelt es sich ebenfalls um Hardware, die dafür ausgelegt ist, den Status eines PCs zu ermitteln und so die Sicherheit und den Datenschutz des Benutzers sicherzustellen und gleichzeitig die Netzwerkintegrität zu sichern. Daher ist die Authentifizierung im Allgemeinen die erste und intuitivste Anwendung eines TPMs, was außerdem einen erheblichen Einfluss auf die Sicherheit der Endgeräte hat. Ein Großteil der heute agierenden Unternehmen hat die Möglichkeit, die TPMs, die bereits im unternehmenseigenen Laptopbestand vorhanden sind, zu aktivieren und damit die Sicherheit sowohl der virtuellen privaten Netzwerke als auch des Zugriffs per Drahtlosnetzwerk zu erhöhen. Immer mehr Benutzer arbeiten von zu Hause aus oder greifen online auf Daten und Dienste zu. Hier können TPMs helfen, den Zugriff auf Daten zuverlässig einzuschränken, sodass es nur bekannten Geräten möglich ist, E-Mails, Informationen zu Finanzen oder geistigem Eigentum und andere sensible Daten herunterzuladen. Allein dieser Einsatz von TPMs wirkt sich überaus positiv auf die Sicherheit der Cyber-Infrastruktur aus.

Das TPM birgt auch vielversprechende Möglichkeiten im Hinblick auf das Cloud Computing – einer neuen Anwendungsplattform, die viele Fragen aufwirft: Wer hat Zugriff auf den Dienst? Welche Daten werden abgerufen, kopiert und verteilt? Können Unternehmen Cloud-Dienste nutzen und dabei die Datenschutzgesetze einhalten?

Ein TPM blockiert den Zugriff auf Webdienste und Inhalte nicht durch herkömmliche Sicherheitsmethoden. Es stellt vielmehr eine hardwarebasierte, vertrauenswürdige Verbindung zwischen dem PC und dem Server für den Austausch von Informationen unter strengster Geheimhaltung her und überprüft, ob die Gegenseite wirklich ist, wer sie zu sein behauptet. Das TPM ist ein Hardwaretoken, der verbessert und in die Hauptplatine des PCs integriert wurde.

Self-Encrypting Drives: Gespeicherte Daten sichern

Die Einrichtung einer starken Geräteauthentifizierung zur Verhinderung von nicht autorisierten Zugriffen auf das Netzwerk stellt nur eine Ebene einer für die heutige Landschaft geeigneten Datensicherheitsstrategie dar. Die zweite Ebene besteht darin, auch auf den mobilen Geräten des Unternehmens für einen absolut sicheren Datenschutz zu sorgen. Wie weiter oben bereits beschrieben reicht die potentielle Gefährdung von Daten aus, um dem betroffenen Unternehmen erhebliche Kosten zu verursachen. Laut einer vor Kurzem vom Ponemon Institute durchgeführten Studie[2] kann eine Sicherheitsverletzung, die durch einen verloren gegangenen Laptop entsteht, Kosten in Höhe von ca. 200 $ pro auf dem Laptop gespeicherten Datensatz verursachen. In der Studie wurde außerdem berichtet, dass die durchschnittlichen Kosten für Unternehmen infolge einer Verletzung des Datenschutzes 2008 ca. 6,5 Millionen Dollar betrugen, je nach Reaktion der Öffentlichkeit und den jeweils geltenden gesetzlichen Bestimmungen.

Kann Ihre derzeitige Verschlüsselungslösung das?

- ☑ Vollständige Aktivierung und Betriebsbereitschaft innerhalb von Minuten
- ☑ Einrichtung eines undurchdringlichen Schilds gegen Softwareangriffe
- ☑ Schutz der Verschlüsselungsschlüssel im Controllerchip des Laufwerks
- ☑ Kein IT-Aufwand für die Verwaltung der Schlüssel erforderlich
- ☑ Betrieb ohne Beeinträchtigung der Laufwerksleistung

Die Kosten für eine FDE-Lösung variieren, betragen aber durchschnittlich bei Volumenlizenzen ca. 100 $ pro Computer. Wie bereits erwähnt hat sich die Verschlüsselungssoftware nicht besonders gut an die Anforderungen heutiger, immer mobilerer Netzwerke angepasst. Im Vergleich dazu bieten SEDs (Self-Encrypting Drives) Schutz, der immer aktiv ist. Die Schlüssel befinden sich stets auf der Festplatte und sorgen somit dafür, dass die gesetzlichen Datenschutzbestimmungen eingehalten werden.

Die Funktionsweise von Self-Encrypting Drives ist schnell erläutert: Sie besitzen eine geschlossene und unabhängige Architektur, ihren eigenen Prozessor, Speicher und RAM, und es gibt bezüglich des auf diesen Laufwerken ausführbaren Codes strikte Einschränkungen. Die Ver- und Entschlüsselung der Daten geschieht im Controller des Laufwerks, sodass die CPU des Host-PCs entlastet wird.

In jedem SED ist ein kleiner Block des internen Speichers reserviert und vom restlichen Laufwerk isoliert. Diese geschützten Partitionen dienen zur sicheren Speicherung

[2] Ponemon Institute, Fourth Annual US Cost of Data Breach Study, 2009.

der Verschlüsselungsschlüssel und der Anmeldedaten der Benutzer. Wenn das Laufwerk entsperrt ist, können die Daten ungehindert auf das Laufwerk geschrieben und von dort abgerufen werden. Autorisierte Benutzer können auf die Daten zugreifen. Nicht autorisierten Benutzern gewährt das Laufwerk keinen Zugriff, und die Daten können auch nicht auf andere Weise abgerufen werden, z. B. durch herkömmliche softwarebasierte Malware- und Rootkit-Angriffe.

Da der Verschlüsselungsschlüssel während der Herstellung direkt auf der Festplatte erstellt wird und diese geschützte Hardwaregrenze auch nie verlässt, ist er gegen herkömmliche Softwareangriffe immun, und es ist unmöglich, ihn zu stehlen. Auf dem Computer kann keine Software – böswillig oder nicht – ausgeführt werden, bis die Festplatte entsperrt und das Betriebssystem gestartet ist.

Die fest integrierte Datenverschlüsselung bietet gegenüber Softwarelösungen auch logistische und wirtschaftliche Vorteile. Da die Verschlüsselungsschlüssel die Festplatte niemals verlassen, muss die IT-Abteilung kein Geld und keine Zeit für die Verwaltung der Schlüssel oder die Erstellung von Schlüsselhinterlegungs- und Sicherungsprogrammen aufwenden.

Außerdem nehmen die SEDs die Speicher- und Verarbeitungsressourcen des jeweiligen Computers überhaupt nicht in Anspruch. Es kommt also im Gegensatz zu vielen Softwarelösungen zu keiner merklichen Verschlechterung der Systemleistung. Wie eine Studie von Trusted Strategies LLC gezeigt hat, erbrachte eine handelsübliche SED die gleiche Leistung wie ein Standardlaufwerk und konnte Vorgänge mit großen Dateien beinahe doppelt so schnell wie drei Laufwerke mit aktiver softwarebasierter Verschlüsselung ausführen.[3]

Wie bei den TPMs wird auch bei SEDs oft fälschlicherweise angenommen, es sei eine neue, noch nicht ausgereifte Technologie, die nicht überall erhältlich ist. Auch hier ist jedoch das Gegenteil der Fall. SEDs werden bei führenden Festplattenherstellern wie Hitachi, Samsung, Seagate und Toshiba in der handelsüblichen Produktpalette angeboten. Zudem werden die SEDs bei diesen Herstellern gemäß dem Opal-Standard der Trusted Computing Group gefertigt – dem Branchenmaßstab für Interoperabilität und Zuverlässigkeit. Auch PC-Hersteller wie Dell und Hewlett-Packard bieten SEDs regulär als Speicherungsoption an. Im Durchschnitt kostet eine SED von Dell nur wenig mehr als ein vergleichbares, nicht-verschlüsselndes Laufwerk. Bei anderen führenden Computerherstellern wie Lenovo und Panasonic werden SEDs ebenfalls in ausgewählten Computern angeboten.

SEDs lassen sich auch problemlos implementieren. In der oben erwähnten Studie von Trusted Strategies[4] benötigten die untersuchten Software-Verschlüsselungsmethoden für die vollständige Verschlüsselung einer Festplatte 3½ bis 24 Stunden. Im Gegensatz dazu kann eine SED unmittelbar nach der Anschaffung eines neuen Computers in Betrieb genommen werden. Da das Laufwerk bereits integriert und die Verschlüsselung aktiviert ist, sind praktisch kein IT-Aufwand und keine Ausfallzeiten des Geräts zu verzeichnen, wenn der Datenschutz aktiviert wird.

SEDs und TPMs ergänzen sich perfekt. Bei beiden Technologien werden die grundlegenden Sicherheitsfunktionen von der Software in die Hardware verlagert. Dadurch werden nicht nur die Endgeräte des Netzwerks optimal geschützt, auch die Betriebskosten für Laptops mit hardwarebasiertem Schutz können gesenkt werden. Außerdem können Sie mit SEDs und TPMs alle Probleme umgehen, die eine Software im Bereich Logistik, Systemleistung und Compliance mit sich bringt.

[3] Trusted Strategies LLC, Hardware Versus Software Full Drive Encryption. 2010
[4] Trusted Strategies LLC, Hardware Versus Software Full Drive Encryption. 2010

Zur zentralisierten Netzwerksicherheit zurückkehren: Fernverwaltung

Mit TPMs und SEDs können Sie die Endgeräte eines Unternehmensnetzwerks optimal schützen. Sie sorgen dafür, dass die auf mobilen Geräten gespeicherten Daten selbst bei Verlust oder Diebstahl des Geräts sicher bleiben. Und sie garantieren, dass alle Geräte und Benutzer mit Zugriffswunsch autorisiert werden.

Aber es gibt ein weiteres Element der modernen Informationssicherheit, das diese beiden Elementen mit einer vollständigen Verwaltung und Verantwortung für alle Endgeräte im Netzwerk in einer zentralen Stelle im Unternehmen zusammenführt. Dieses dritte Element sorgt dafür, dass das Unternehmen seine Fähigkeit zurückerhält, den Datenschutz nicht als bloße Strategie, sondern vielmehr als durchsetzbare Unternehmenspolitik zu betrachten.

Kann Ihre derzeitige Sicherheits-verwaltungsplattform das?

- ☑ Zentrale Initialisierung der Sicherheitsfunktionen von SEDs, Sperrung und Zuweisung von Benutzern und Richtlinien in wenigen Minuten
- ☑ Automatische Aktivierung und Besitzübergabe von TPMs sowie Schlüsselverwaltung
- ☑ Keine Möglichkeit für Benutzer, die Verschlüsselung zu deaktivieren oder die SED-Sicherheitsrichtlinien zu ändern
- ☑ Bericht über SED-Sicherheitsprofile für Compliance-Nachweis
- ☑ Unmittelbare Deaktivierung von TPMs zur Blockierung von „gefährdeten“ Benutzern und Geräten

Eine ungefähre Beschreibung ist die „zentrale Sicherheitsverwaltung an den Endgeräten“. Lassen Sie sich nicht dadurch ablenken, dass dies in Form von Software und Remote-Servern erfolgt. Am besten lässt sich der Begriff durch drei Grundfunktionen erläutern, die jede Lösung besitzen muss: richtlinienbasierte Zugriffssteuerung, zentrale Verwaltung und Compliance-Nachweis.

Ungeachtet der vielen Probleme, die durch die stetig wachsende Anzahl an mobilen Mitarbeitern entstehen, müssen die IT-Manager eines Unternehmens dafür sorgen, dass die Sicherheitsrichtlinien von einer zentralen Stelle aus an alle Endgeräte im gesamten Unternehmen verteilt werden, der Zugriff auf verschlüsselte Informationen auf autorisierte Personen beschränkt wird und die Anmeldedaten der Benutzer aus der Ferne verwaltet werden. Außerdem, und dies ist vielleicht am wichtigsten, müssen Sie bei einer Sicherheitsverletzung den Nachweis führen können, dass das Unternehmen die gesetzlichen Datenschutzbestimmungen eingehalten hat und weiterhin einhält. Die bloße Einführung einer Datenschutzrichtlinie reicht nicht aus. Ein IT-Manager muss nachweisen können, dass diese Richtlinie implementiert und durchgesetzt wurde.

Wie zu erwarten gibt es inzwischen Clientanwendungen zur Unterstützung der hardwarebasierten Sicherheitslösungen. Diese Lösungen sind keine bloßen FDE-Produkte, die so „modifiziert“ wurden, dass sie Self-Encrypting Drives unterstützen. Bei ihrer Entwicklung lag der Schwerpunkt von Anfang an auf der Hardwaresicherheit. Dies bedeutet, beim „Anpassen“ des Codes an die Unterstützung von Hardware keine Hintertüren oder Sicherheitslücken entstanden sind.

Solche Anwendungen sind von Wave Systems erhältlich und dienen der Unterstützung aller integrierten Sicherheitsfunktionen von Self-Encrypting Drives und TPMs.

So ist überprüft z. B. die EMBASSY®-Software von Wave Systems als einzigem ISV die Pre-Boot-Anmeldedaten der Benutzer in den „sicheren Partitionen“ der Self-Encrypting Drives. Dadurch wird bei jeder Aktivierung eines mobilen Geräts die richtlinienbasierte Zugriffssteuerung durchgesetzt. Zudem unterstützt die Software ein sekundäres, externes (USB) Self-Encrypting Drive. Außerdem bietet die Software Unterstützung der Einmalanmeldung bei Windows®, wodurch die Anzahl der Kennwörter reduziert wird, die sich die Benutzer merken müssen (und damit die Anzahl der Help Desk-Anrufe). Darüber hinaus 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.

Mit der Wave-Software ist eine optimale Nutzung der TPM-Sicherheitsfunktionen möglich, beispielsweise die Fähigkeit, softwarebasierte digitale Zertifikate in die TPM-Umgebung zu verschieben und sie damit effektiv in Hardwarezertifikate umzuwandeln. Auf diese Weise ist in Unternehmen die Einrichtung von hardwarebasierten PKI-Umgebungen möglich. Die VPN-Server eines Unternehmens werden so konfiguriert, dass nur Computer mit hardwarebasierten Zertifikaten authentifiziert werden. Somit werden alle Benutzer, die die Anmeldedaten nicht auf ihrer lokalen Hardware verifizieren können, daran gehindert, sich an der Domäne oder am Netzwerk anzumelden.

Für TPM- bzw. SED-Bereitstellungen in einem Unternehmen bietet der EMBASSY Remote Administration Server (ERAS) von Wave die robuste, richtlinienbasierte Verwaltung von Benutzern, Anmeldedaten und Zugriffsrechten von einer zentralen Stelle aus. Durch die systemnahe Integration in vorhandene Verzeichnisstrukturen und Mechanismen zur Verteilung von Richtlinien kann das Zuweisen von Benutzern und entsprechenden Richtlinien im vorhandenen Verzeichnis-Framework ausgeführt werden, sodass die Bereitstellung immens vereinfacht wird.

Gemäß der aktuell geltenden Datenschutzbestimmungen sind die Unternehmen dazu verpflichtet, im Fall einer Sicherheitsverletzung nachzuweisen, dass angemessene Schutzmaßnahmen getroffen worden sind. Daher müssen die Fernverwaltungsserver Sicherheitsprotokolle erstellen und über robuste Berichterstellungsfunktionen verfügen.

ERAS unterstützt alle handelsüblichen TPMs, darunter auch Intel® vPro. Statt die TPMs auf jedem Gerät einzeln zu aktivieren, kann das IT-Team die TPM-Richtlinien mithilfe dieser Infrastrukturtools von einem zentralen Standort aus für das gesamte Unternehmen steuern und verwalten. Sobald TPMs im Netzwerk verfügbar sind, können mit jeder beliebigen standardkonformen Zertifizierungsstelle und der EMBASSY-Software von Wave hardwarebasierte digitale Zertifikate für die VPN-, Wireless- oder anderen PKI-fähigen Anwendungen eines Unternehmens erstellt werden. So werden die Funktionen für private Schlüssel und die Fähigkeit, eine Geräteidentität sicherzustellen, hochgradig geschützt.

Fazit

Während immer mehr Arbeitsplätze in Bereiche außerhalb der Unternehmens-Firewall verlagert werden, bleibt das grundlegende Ziel der IT-Administratoren gleich: Schutz der Netzwerkintegrität durch Absicherung aller Daten, Benutzer, Geräte und Anwendungen – von den zentralen Netzwerkservern bis hin zu entferntesten Endgerät. Viele Unternehmen verlassen sich auf ein kleines Arsenal von Lösungen, um in dieser immer komplizierter werdenden Landschaft bestehen zu können. Dabei ist hardwarebasierte Sicherheit nicht nur die leistungsstärkste, sondern auch die einfachste Lösung.

In der Frage, welche PCs in Unternehmensnetzwerken zugelassen werden sollen, sind sich die meisten IT-Unternehmen darüber einig, dass der erste Schritt die Nutzung von TPMs für die Computerauthentifizierung ist. Manche Unternehmen setzen TPMs auch zur Steigerung der Sicherheit für VPNs und Drahtloszugriff ein. Da immer mehr Benutzer per Fernzugriff arbeiten oder Daten und Dienste über das Internet abrufen, wird es auch immer wichtiger, diesen Zugriff so zu verwalten, dass nur bekannte Geräte mit bekannten Sicherheitsprofilen E-Mails, Informationen zu Finanzen oder geistigem Eigentum und andere vertrauliche Daten herunterladen können.

Bei der Datenverschlüsselung haben sich SEDs als beste Option erwiesen, um Daten „auf unbekanntem Territorium“ zu sichern und die Einhaltung der Datenschutzbestimmungen nachzuweisen. Diese eigenständigen Geräte, die von Anfang an mit ihrer eigenen sicheren Umgebung entwickelt wurden, bieten die sicherste und leistungsstärkste FDE-Lösung, die auf dem Markt erhältlich ist.

In der vernetzten Welt von heute ist für eine umfassende Datenschutzlösung mehr als nur eine robuste Authentifizierung und Verschlüsselung notwendig. Richtlinienbasierte Zugriffssteuerung, zentrale Verwaltung und Compliance-Nachweis sind ein Muss. Die Unternehmen müssen dafür sorgen, dass Sicherheitsrichtlinien von einer zentralen Stelle aus im gesamten Unternehmen bereitgestellt werden können, der Zugriff auf Informationen nur autorisierten Personen gewährt wird und, was vielleicht am wichtigsten ist, nachgewiesen werden kann, im Fall einer Sicherheitsverletzung die Sicherheitsmaßnahmen intakt waren. Mit ihrer hervorragenden SED- und TPM-Unterstützung bietet die EMBASSY-Software von Wave all die erwähnten Funktionen und mehr.

03-000273/Version1.02

Wave Systems Corp.
480 Pleasant Street, Lee, MA 01238, USA
+1-877-228-9283 • Fax +1-413-243-0045
www.wave.com