



Datenverschlüsselung auf Datenträgern

Das Husarenstück in der Client-Absicherung?

DI (FH) Stefan Bumerl

CRYPTAS it-Security & Media GmbH

Modecenterstrasse 22/B2
A-1030 Wien

www.cryptoshop.com
www.cryptas.com

Datenverschlüsselung auf Datenträgern

Das Husarenstück in der Client-Absicherung?

Virenschutz und Firewall gehören (zum Glück) mittlerer weile zur Standardausstattung der Unternehmen, aber wie werden die Unternehmenskritischen Informationen vor der Neugier etwa des Mitbewerbes geschützt? Das Stichwort ist „Verschlüsselung“ – viele Anbieter drängen sich auf den Lösungsmarkt, aber was ist für eine sinnvolle Festplattenverschlüsselung alles zu beachten? Welche Möglichkeiten existieren und wo liegen deren Gefahren? Dieser Exkurs soll etwas Licht in diese keinesfalls triviale Thematik bringen und wichtige Schlüsselfunktionen erläutern um Interessenten bei ihrer Entscheidung zu unterstützen.

Produktionsfaktor Information

Dass die Absicherung sensibler Daten ein sehr relevantes Thema ist, erkennt man schon an den immer häufiger erscheinenden Medienberichten über deren Diebstahl im großen Rahmen. Erst in jüngster Vergangenheit haben, nach Angaben von MasterCard selbst, Betrüger Zugang zu etwa 40 Millionen Kreditkarten-Informationen erlangt. Die Bank of America „verlor“ im Februar Daten von 1,2 Millionen Angestellten. Das sind natürlich die wirklich großen Brocken und nicht unbedingt auf fehlende Festplattenverschlüsselung zurückzuführen, zeigen aber dennoch sehr schön die Versäumnisse bei der Datenabsicherung auf. Im Normalfall geht es beim Datenklau um vertrauliche Unternehmensinformationen aus den Bereichen Vertrieb, Entwicklung oder Finanz. Preislisten, Kalkulationen, Angebote, Leads, Kundendatenbanken, Source Codes, Gehaltslisten, Passwörter ... sind nur einige der begehrtesten Informationen für Eindringlinge.

Es zahlt sich aus

ROSI (Return On Security Invest)-Berechnungen sind nicht immer ganz so leicht anzustellen, da einerseits einer Studie zufolge 95 % der Eindringlinge völlig unbemerkt bleiben und andererseits auch der Schaden schwer zu bewerten ist. In jedem Fall sollte man sich aber vor Augen halten, dass alleine in Taxis jeden Tag Tausende von Notebooks, PDAs und Handys liegen bleiben – das ergab eine internationale Umfrage des Sicherheitsunternehmens Pointsec unter 900 Taxifahrern in neun Großstädten. Im zweiten Halbjahr 2004 haben Fahrgäste 10.000 Notebooks, 30.000 PDAs und 200.000 Handys zurückgelassen und laut FBI werden in den Vereinigten Staaten jedes Jahr mehr als eine Million Notebooks gestohlen. Es ist zu vermuten, dass diese Zahlen nicht wesentlich von Europa abweichen werden.

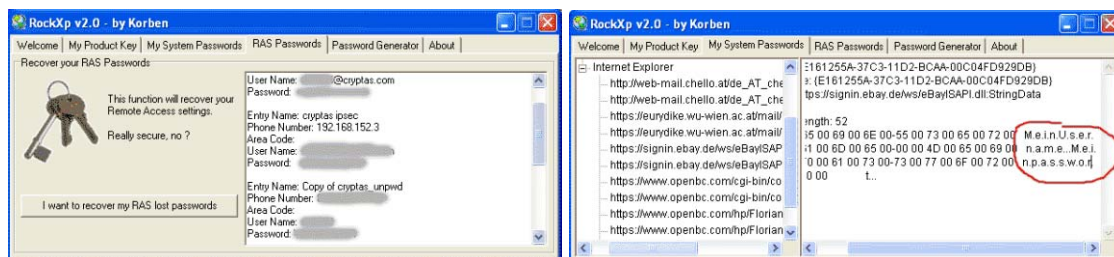
Aber was bedeutet das?

Der typische Vertriebs- und Außendienstmitarbeiter trägt alle für seine Arbeit nötigen Informationen inklusive der E-Mail Kommunikation (Stichwort Outlook-Offlinefähigkeit) mit sich herum. Muss er auch, um den immer schneller steigenden Anforderungen der Kunden bezüglich der Reaktionszeit gerecht werden zu können. Aber warum so ungesichert?

Datenklau ist keine Hexerei

Um Daten von einem Notebook abzusaugen braucht es in der Regel keinen Experten. Dazu muss man das Gerät ja nicht einmal entwenden – wenn es geschickt angestellt wird, ist alles im Handumdrehen erledigt und der rechtmäßige Eigentümer merkt nichts davon. Beliebte

Möglichkeiten dazu sind Mittagspausen bei Präsentationen, Verhandlungen, Konferenzen oder sonstige Veranstaltungen bei denen man sich scheinbar entspannt trifft und die Geräte nur kurz zum Beispiel im Besprechungsraum liegen lässt. Sie sind ja ohnehin durch das Systempasswort und NTFS abgesichert. Nur wissen die wenigsten, dass das nicht die geringste Hürde ist, man braucht auch kein mechanisches Werkzeug dazu. Die einfachste Variante ist eine bootbare CD (z.B. das kostenfreie Knoppix – <http://www.knopper.net/knoppix/>) zu benutzen und ohne Passwortabfrage alle gewünschten Daten von der Festplatte auf einen USB-Stick zu kopieren. Ebenfalls ohne Kenntnis des Kennwortes lassen sich mit dem kommerziellen (~150 US\$) Tool ERD Commander der Firma Winternals (<http://www.winternals.com/Products/ERDCommander/>) auch die Registry verändern und das Administrator Passwort des Zielsystems neu setzen. Wer soweit geht, nimmt dann wahrscheinlich auch gleich alle Zugangsdaten des Opfers mit (auch ohne das Admin-PWD zurückzusetzen). Man muss lediglich in der Registry [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] das Starten eines Stück Softwares nach dem Systemstart initiieren, welches die gespeicherten Systempasswörter (der Webseiten) und RAS Passwörter (der VPN und Terminal Server Zugänge) des Benutzers aus dem System ausliest und an eine beliebige E-Mail Adresse sendet (evtl. noch ein Key-Logger zusätzlich).



Eine Demonstration dazu findet man mit „RockXP“ bei www.korben.tk.

„Problemzonen“ von Verschlüsselungslösungen

Damit kommen wir auch schon zu den Problemzonen, denen wir unsere Aufmerksamkeit schenken sollten, denn sensitive Informationen finden sich nicht nur in der einen Excel-Kalkulation oder der anderen Word-Datei. Sie sind im System bewusst und unbewusst an zahlreichen Stellen hinterlegt. Die gängigsten Orte sind:

- **Temporäre Dateien**
Viele kommerzielle Softwarepakete erzeugen temporäre Dateien um entweder Zwischenergebnisse abzulegen oder darin eine Kopie des Originals mit den letzten Änderungen für den Fall eines unerwarteten Absturzes zu speichern. Diese Files sind zwar oft extrem nützlich, aber auch ein ebenso großes Sicherheitsrisiko.
- **Auslagerungsdateien**
Werden in modernen Betriebssystemen stark verwendet um die Knappheit von Arbeitsspeicher auszugleichen. Dabei werden Speicherinhalte auf die Festplatte geschrieben um Platz für andere Anwendungen zu schaffen. Sobald diese Inhalte wieder benötigt werden, kommen sie zurück an ihre alte Position.
- **„Mistkübel“ (Recycle Bin)**
Wenn eine Datei im System gelöscht wird, kommt sie zuerst in den Mistkübel. Bis dieser geleert wird, können die Daten jederzeit wieder hergestellt werden. Aber selbst dann verweilen die darin enthaltenen Informationen auf der Festplatte, solange sie nicht von einer anderen Datei überschrieben werden. Mit vielen Software Werkzeugen können Sie gefunden und gelesen werden.

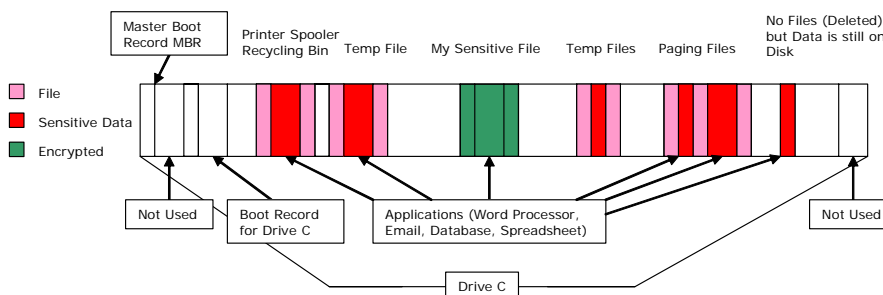
- **Windows Registry**
Viele Anwendungen legen wertvolle Information in der Registry ab, wie zum Beispiel Username/Passwort-Kombinationen für Websites. Aber auch deren unautorisierte Manipulation kann, wie wir ebenfalls bereits gesehen haben, zu erheblichen Sicherheitslöchern führen.
- **Hibernation und Sleep Mode**
Diese Modi werden oft bei Notebooks verwendet um Batterie zu sparen wenn der Computer noch eingeschaltet ist. Dabei wird der gesamte Inhalt des Arbeitsspeichers inklusive aller enthaltenen sensitiven Daten auf die Festplatte gespeichert. Dadurch lässt sich beim nächsten Hochfahren der exakte Zustand wiederherstellen.
- **File Slack**
Windows organisiert seine File Systeme in so genannten Clusters, die wiederum aus bis zu 64 Sektoren bestehen. Auch wenn eine Datei nur wenige Byte lang ist, belegt diese immer einen ganzen Cluster (meist viele Kilobyte). Der letzte von Nutzdaten angefangene Sektor ist mit willkürlichen Daten aus dem RAM aufgefüllt – das können selbstverständlich auch Passwörter oder Inhalte der gerade bearbeiteten E-Mail sein! Es gibt eigene Werkzeuge welche mit forensischen Methoden diese Daten auswerten können (<http://www.forensics-intl.com/getslack.html>).
- **Versteckte Partitionen**
Das sind Teile der Hard Disk, die das Betriebssystem nicht erkennt und anzeigt. Dennoch verwenden einige Anwendungen diesen Platz um Daten am System vorbei abzulegen.

Verschlüsselung ist nicht gleich Verschlüsselung

Man muss schon recht tief in die Materie eindringen um eine sinnvolle Verschlüsselungslösung anbieten zu können. Die zahlreichen Hersteller nähern sich somit der Thematik mit unterschiedlichen Lösungsansätzen – einige davon haben doch erhebliche Einschränkungen! Vergleichen lässt sich das mit einem Haus mit einer fünf Tonnen schweren Eingangstür, für welche sieben unterschiedliche Schlösser zu sperren sind, aber die daneben liegenden Fenster sind nicht abschließbar und gewähren jedem Zutritt.

Fileverschlüsselung (Manuell)

Bei dieser sehr einfachen Variante kann manuell eine Datei verschlüsselt werden. In der Regel erfolgt dies im Explorer mit der rechten Maustaste auf das gewünschte File und dann im Menü auf „Verschlüsseln“ gehen. Diese Methode ist als einzige auch dazu geeignet, eine verschlüsselte Datei zum Beispiel per Mail zu übertragen. Daher bieten gute Festplattenverschlüsselungshersteller auch zusätzlich diese Möglichkeit an (in diesem Fall ist diese Datei dann doppelt verschlüsselt). Aber alleine betrachtet bietet sie keinen hinreichenden Schutz und unterliegt allen oben beschriebenen „Problemzonen“. Darüber hinaus kommt noch der Fehlerfaktor Mensch hinzu, etwa wenn auf die Verschlüsselung vergessen wird.

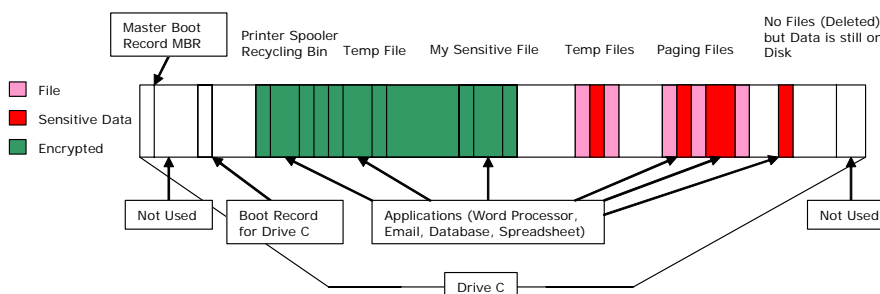


Folder Verschlüsselung

Im Gegensatz zur File Verschlüsselung werden die Dateien innerhalb des angegebenen Folders automatisch Ver- und Entschlüsselt. Durch die Integration in das Betriebssystem ist somit keine Benutzerinteraktion mehr nötig und die Verschlüsselung läuft für den Anwender transparent. Auf den ersten Blick klingt dieses System sehr vernünftig, jedoch können auch Produkte dieser Kategorie keinen Schutz für die genannten Schwachstellen bieten. Dazu ist auch noch zu bemerken, dass dieser Ansatz im Vergleich zur Festplattenverschlüsselung erheblich größere CPU und Festplatten-Ressourcen benötigt. Der Overhead liegt darin begründet, dass hier jede Datei des Folders einzeln verschlüsselt wird und dazu eine Schlüsselerzeugung und -Ablage (manchmal mehr als 2 kByte je File) nötig wird.

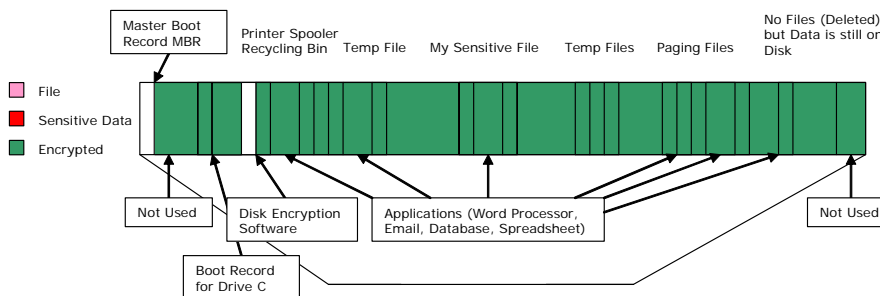
Container Verschlüsselung

In dieser Variante wird eine große versteckte Datei angelegt, in welche alle verschlüsselten Daten geschrieben werden. Für den Anwender erscheint dann ein Virtuelles Laufwerk, welches er wie eine Partition auf der Festplatte behandeln kann. Alle darin angezeigten Files liegen in verschlüsselter Form eben in dieser Datei auf der Platte. Manche Produkte unterstützen auch mehrere solcher Dateien und bieten eine Zugriffsverwaltung für unterschiedliche Benutzer an, in der auf Container-Ebene in sehr vereinfachter Form Berechtigungen vergeben werden können. Da die gesamte Implementation auf bestehenden Funktionalitäten des Betriebssystems aufsetzen kann, ist hier auch die Unterstützung von HW-Token wie Smart Cards mit und ohne Zertifikate recht komfortabel und umfangreich. Auch biometrische Authentifizierung ist, zusätzlich in Kombination mit einer Smart Card, erhältlich. Diese Lösungen lassen sich sehr einfach und unkompliziert umsetzen, bieten jedoch einige substantielle sicherheitstechnische Schwachstellen. Zum Beispiel behandelt das Betriebssystem dieses virtuelle Laufwerk nicht wie eine physikalische Disk, wodurch sich darauf keine Temporärverzeichnisse und Auslagerungsdateien anlegen lassen. Dies führt natürlich dazu, dass alle dort enthaltenen Informationen nach wie vor unverschlüsselt auf der Platte liegen. Darüber hinaus ist auch nach wie vor das Betriebssystem (speziell die Registry) ungeschützt.



Festplatten Verschlüsselung

Bei der Festplatten Verschlüsselung liegt der größte Unterschied zu den beiden voran genannten Varianten darin, dass sie Sektor für Sektor die gesamte Platte verschlüsselt und nicht jede Datei einzeln behandeln muss. Dadurch läuft die gesamte Ver- und Entschlüsselung für den Benutzer vollkommen im Hintergrund und er bemerkt keinen Unterschied zu einem unverschlüsselten System. Dadurch ist dieser Ansatz auch wesentlich performanter: der WinStone Benchmark ergibt nur eine Geschwindigkeitsreduktion von 3 %, was in annähernd allen Konfigurationen mit freiem Auge nicht mehr unterschieden werden kann. Da alle Schreib- und Lesezugriffe vom System über eine einzige Schnittstelle erfolgen, sind wirklich alle - also auch die nicht allozierten - Bereiche verschlüsselt. Nur mit diesem Ansatz lassen sich durch diesen Umstand alle der beschriebenen Gefahren eliminieren. Allerdings bringt die Verschlüsselung des Betriebssystems auch eine erhebliche Komplexitätsebene mit sich, da bereits vor dem eigentlichen Boot-Vorgang des Betriebssystems die Authentifizierung des Benutzers zu erfolgen hat um die Entschlüsselung zuzulassen. Dieser Boot-Schutz wird auch Pre-Boot Authentication bezeichnet. Da zu diesem Zeitpunkt keine HW-Treiber, also auch nicht jene für Kartenleser oder Netzwerkkarten zur Verfügung stehen, ist die Integration von den essentiell notwendigen Hardware Tokens als zusätzliches Authentifizierungsmedium für die Lösungshersteller sehr aufwändig. Als Folge dessen werden jeweils nur eine begrenzte Anzahl dieser Geräte unterstützt (je nach Qualität der Verschlüsselungslösung und der Erfahrung des Herstellers variiert deren Anzahl zum Teil erheblich – unbedingt darauf achten!).



Verschlüsselungs Matrix

Funktion	File	Folder	Container	Disk
Primärer Einsatz				
Primär designed für Desktop Security		x	x	x
Primär designed für das Verschicken über Netzwerke	x			
Sicherheit				
Schützt ein individuelles File	x	x	x	x
Schützt den Inhalt eines Folders		x	x	x
Schützt Temporary & Paging Files				x
Schützt den File Slack			x	x
Schutz für Datenbanken			x	x
Schutz für gelöschte Dateien			x	x
Schützt Back-Up & Auto-Save Files			x	x
Ermöglicht die Windows Un-Delete Funktionalität			x	x
Schützt Dateinamen			x	x
Schützt die Windows Registry				x
Schutz für alle Applikationen (OS, Software, etc.)				x
Schützt Dateien auf Wechseldatenträgern	x		x	x
Schutz durch Bildschirmschoner	*	*		x
Transparenz				
Echt-Zeit Verschlüsselung		x	x	x
Echt-Zeit Entschlüsselung		x	x	x
Menschliches Fehlverhalten minimiert				
E-mail				
Senden verschlüsselter Files als E-Mail	x	x		
Senden verschlüsselter E-Mail	x			

* Herstellerabhängig

Worauf sollte man nun bei der Auswahl achten?

Wenn wir die weiteren Betrachtungen auf jene Produkte einschränken, welche die gesamte Festplatte verschlüsseln und hier klar das Unternehmensumfeld mit vielen zu schützenden Computern fokussieren, so ist die zentrale Verwaltbarkeit des Systems an die erste Stelle zu setzen. Die Verschlüsselung der Daten selbst ist durchwegs mehr als ausreichend (jeder der das System an dieser Stelle anzugreifen versucht, wird graue Haare bekommen), die Geschwindigkeitseinbußen sind bei modernen Maschinen zu vernachlässigen, also bleiben die Funktionalitäten.

Unterstützung von Smart Cards

Passwörter sind wie man es dreht und wendet problematisch und sollten durch modernere Verfahren wie digitale Zertifikate abgelöst werden. Das ist zwar leider nicht in jedem Umfeld gleich möglich, allerdings sollte man sich den Weg dorthin nicht mit einer Lösung verbauen, die diese Technologie nicht ausreichend unterstützt. Damit lassen sich die Themen der niedergeschriebenen und vergessenen Zugangscodes und deren Synchronisation zwischen den unterschiedlichen Systemen endlich aus der Welt schaffen. Träger solcher Zertifikate ist in der Regel eine Smart Card oder ein USB-Token. Allerdings ist Smart Card nicht gleich Smart Card und es gibt viele Kriterien aus dem Single-Sign-On Bereich, welche hier herein spielen,

deshalb ist eine breite Unterstützung von Kartentypen von der Verschlüsselungssoftware sehr zu empfehlen.

Ausrollen der Lösung

Die Software sollte sich natürlich ohne jegliche Interaktion am Client mittels üblicher Werkzeuge a'la Microsoft SMS oder Novell ZENWorks inklusive der eigentlichen Plattenverschlüsselung ausrollen lassen. Dafür ist die Funktionalität eines „Silent Re-Boots“ ganz wesentlich, da das Betriebssystem ja nur dann startet, wenn im Pre-Boot Bereich die Authentifizierung erfolgreich ist. Gute Lösungen bieten hierfür einen interaktionsfreien Re-Boot an.

Da Benutzer- und Computerinformationen im Normalfall in einem X.500-Directory (Active Directory, NDS...) oder einer Datenbank verwaltet werden, sollte hierfür eine Integration angeboten werden – wer legt schon gerne alle Benutzer händisch noch einmal an?

Administrierbarkeit

Dabei sind natürlich der Komfort und die Möglichkeiten der Verwaltung von Benutzern, Computern und Verschlüsselungsschlüssel im Vordergrund. Aber auch die Bequemlichkeit der Standard-Abläufe bei Token-Verlust, vergessenem Passwort, neuen Benutzern etc. sind ganz wesentlich. Wie einfach kann ein weiterer Benutzer, eine Benutzergruppe zu einem Gerät hinzugefügt werden? Wie läuft ein Key-Recovery ab?

Last but not least die Features...

Interessant ist auch die Betrachtung der Interoperabilität mit bestehenden Systemen wie Bootmanagern und Disk Imaging Lösungen. Lassen sich Wechselmedien ebenfalls verschlüsseln und sind diese dann auch multi-user-fähig? Wie sieht es mit externen Prüfungen aus, existieren Zertifizierungen und große Referenzen?

Auf alle Fälle sollte man sich für die Evaluierung einer Verschlüsselungslösung etwas Zeit nehmen um nicht die Katze im Sack zu kaufen. Oft sind hier nämlich gerade die Lösungen, die anfangs sehr schnell Resultate zeigen auch jene, denen später die Luft ausgeht.

CRYPTAS it-Security & Media Gmbh
Modcenterstrasse 22/B2
A-1030 Wien, Austria
T +43 (1) 798 96 96 – 0
F +43 (1) 798 96 96 – 99
info@cryptas.com

www.cryptoshop.com
www.cryptas.com
www.croptomedia.com