VERSCHLÜSSELUNG – UNTERWEGS, LOKAL UND IM NETZ

Das neue Bundesdatenschutzgesetz stellt erhöhte Anforderungen an den Schutz personenbezogener Daten. Der Verfassungsschutzbericht 2009 des Bundesinnenministeriums meldet vermehrt Computerspionage-Angriffe auf Wirtschaftsunternehmen und Regierungsstellen. Die meisten Abwehrmaßnahmen basieren auf Bedrohungen von außen. Interne Risiken werden häufig vernachlässigt. Dabei sind die Folgen bei einem Missbrauch vertraulicher Unternehmensdaten immer verheerend, ganz gleich, wo das Datenleck seinen Ursprung hatte.

Verschlüsselung ist daher das Stichwort, wenn es um den Schutz vertraulicher Informationen geht, sei es für die lokale Ablage, bei der Speicherung von Daten im Netz (LAN oder WAN) oder unterwegs beim Transport. Welche Daten sensibel sind, kann häufig der Benutzer selbst einschätzen, jedoch hat er weder die technische Expertise für den gezielten Umgang mit Verschlüsselungstechnologien noch die Zeit, um sich um die Verschlüsselung der Daten zu kümmern. Einzelne Benutzer brauchen unterschiedliche Freiräume in der Behandlung der Daten. Daher muss eine Verschlüsselungslösung über zentrale Richtlinien die notwendige Vertraulichkeit steuern und wesentliche Aktivitäten revisionssicher protokollieren. Entscheidungskriterien müssen hier die jeweiligen Benutzerrechte, die verwendeten Datenträger bzw. Speicherorte und die Dateninhalte sein. Die Verschlüsselung muss für den Anwender einfach sein, weil sie sonst nicht verwendet wird. Zudem sollte sich der administrative Aufwand in Grenzen halten und im besten Fall keine Administration im Tagesbetrieb erfordern.

Verschlüsselung der Dateien im Netz

Arbeitsgruppen müssen gemeinsam vertrauliche Dateien nutzen, z.B. können dies die Personalabteilung, der Betriebsrat oder auch die Entwicklungs- und Konstruktionsabteilung sein. Meist werden gruppenvertrauliche Daten nur unter dem Schutz von „Bordmitteln“ auf zentralen Fileservern in eigene Arbeitsgruppen-Verzeichnisse gespeichert. Sind die Dateien einmal an einen anderen Ort kopiert worden, geht auch der Bordmittelschutz mittels ACL etc. verloren und die Dateien

können verändert, woanders abspeichert, per Email versendet oder mitgenommen (z.B. auf USB-Stick gespeichert) werden. Dieser Gefahr kann nur begegnet werden, wenn mit einer Inhaltskontrolle die weitere Verarbeitung dieser Dateien geregelt wird, wie zum Beispiel: Datei darf nur verschlüsselt auf USB-Stick geschrieben werden. Den Lebenslauf der sensiblen Daten kann man auf Knopfdruck abrufen, wenn man geeignete Protokollierungswerkzeuge zur Verfügung hat, die nicht nur die Daten unter dem Minimalitätsprinzip sammeln, sondern auch geschickt auswerten.

Die inhaltsbasierende Ver- und Entschlüsselung der Dateien anhand des Containers, in dem sie liegen, ist die einzig wirksame Methode Datenverluste an den Clientschnittstellen durch unberechtigten Zugriff zu vermeiden. Damit der Benutzer zwar durchaus über die Sensibilität der Dateien ein Sicherheitsbewusstsein erhält, dennoch nicht durch komplizierte Verfahren von der Verschlüsselung abgehalten wird, sollte pro Benutzersession und Container nur einmal ein Schlüssel eingegeben werden müssen. Danach muss die Verschlüsselung so automatisiert wie möglich und für den Anwender so sichtbar wie nötig in Windows integriert sein, wobei auch alle Standard-Windows Mechanismen für das Dateimanagement, wie „Drag & Drop“, „Cut & Paste“ und andere Kontext-Menüoperationen genauso unterstützt sein müssen, wie das „Speichern unter“ aus Anwendungen heraus.

Im WAN unter schmalbandigen Bedingungen gilt es besondere Anforderungen zu berücksichtigen: Die Verschlüsselung findet lokal auf dem Client statt, um Angriffe auf dem Netz zu verhindern. Verschlüsselte Dateien erlauben keine sinnvolle Komprimierung und die WAN-Optimierer, die Sektoren-basiert optimieren, greifen nicht; das heißt, der Traffic im Netz ist signifikant höher als ohne Verschlüsselung. Achten Sie deshalb darauf, dass Sie für den WAN-Betrieb eine Bandbreiten-basierte Verzögerung beim Durchschreiben administrieren können.

Verschlüsselung der Festplatte

Die meisten Festplattenverschlüsselungssysteme bieten heute eine Pre-Boot-Authentication; diese stellt sicher, dass sich ein Anwender noch vor dem Starten des Betriebssystems - gegebenenfalls sogar mit einem starken zwei-Faktor-Verfahren - authentisieren muss. So ist sichergestellt, dass nur von einem autorisierten Benutzer auf die Festplatte zugegriffen werden kann. Dieses Verfahren bietet einen wirksamen Schutz der Daten bei Diebstahl oder Verlust des gesamten Gerätes oder dessen Festplatte, solange das System ruht und sich der Benutzer noch nicht angemeldet hat. Sobald der Anwender angemeldet ist, erfolgt die Ver- und Entschlüsselung der Daten vollkommen transparent im Hintergrund. Nach dem *Microsoft Security Intelligence Report* [1] geht jedoch mehr als die Hälfte aller Gefährdungen von PCs und Notebooks von laufenden Anwendungen, die durch Schadcode infiltriert sind, von Malware im laufenden Betrieb aus dem Internet und von infizierten Dokumenten aus. Zudem weist dieser Report aus, dass Schadsoftware immer komplexer und leistungsfähiger wird. In ähnlichem Maße

wie der Leistungsumfang von legaler Software wächst, ziehen auch Online-Kriminelle nach, die rein kommerzielle Ziele bei ihren Angriffen verfolgen.

Gerade die vollkommene Transparenz der Ver- und Entschlüsselung wird zur Gefahr für die sensiblen Daten auf der Festplatte, da der Anwender gar nicht merkt, wenn Schadcode im Hintergrund mit seinen Rechten auf sensible Daten zugreift und diese unbemerkt ins Internet hoch lädt oder anderweitig nutzt.

Ein besserer Ansatz ist es, zum einen durch eine Applikationskontrolle sicherzustellen, dass die Anwendung integer ist und nicht durch Schadcode infiltriert wurde. Zum anderen sollte jeder Applikation ein eigener Rechteraum zugewiesen werden können, so dass z.B. der Browser (die Applikation explorer.exe) gar nicht erst auf verschlüsselte Dateien in einem automatisch entschlüsselnden Modus lesend zugreifen kann. So wird Sicherheit geschaffen ohne dabei Wake Up on LAN und weitere Systemsmanagementfunktionen wie Patch- und Softwareverteilung zu behindern.

Verschlüsselung beim Transport

Zum Transport sensibler Daten, wie zum Beispiel geplante Firmenübernahmen oder auch Kundenangebote, werden häufig Hardware-verschlüsselte USB-Sticks eingesetzt. Nach dem Anstecken und der erfolgreichen Authentisierung gegenüber dem Stick durch Eingabe der PIN oder anderer Mechanismen erfolgt die transparente Entschlüsselung des kompletten Speichermediums – für jeden der fragt. Normalerweise hat ein Anwender nur einen solchen Stick, weshalb Dateien mit unterschiedlichen Vertraulichkeitsstufen und unterschiedlichen Verwendungszwecken auf einem Stick gespeichert werden. Ein USB-Dumper [2] – oder jede andere Anwendung, die auf dem PC oder Notebook läuft, kann den gesamten Inhalt des Sticks im Klartext auslesen, ohne dass der Anwender das merkt.

Daten werden nicht nur auf USB-Sticks sondern auch auf anderen Speichermedien wie CD/DVD (Steuersünder-CDs aus der Schweiz und aus Liechtenstein), der Speicherkarte des Smartphones oder der Kamera sowie per Email transportiert. Auch hier muss sichergestellt sein, dass die vertraulichen Daten nicht in falsche Hände geraten. Daher ist es wichtig, dass die Verschlüsselung unabhängig vom jeweiligen Speichermedium nach dem Grad der Sensitivität der Daten erfolgt.
Eine geeignete Methode ist daher die Ziel- und Inhaltsbasierte Verschlüsselung, so dass Firmenvertrauliche Informationen auch intern bleiben, indem sie mit einem Firmenschlüssel, der weder dem Anwender noch dem Administrator bekannt ist, automatisch ohne Benutzeraktion verschlüsselt werden. Hingegen ist bei der Auslagerung von Bilddaten und lokalen Anwendungen auf digitale Fotoapparate, Bilddrucker oder andere Geräte eine unverschlüsselte Auslagerung zwingend erforderlich, da sonst das Gerät nicht mehr booten oder nicht arbeiten kann. Die Verschlüsselung ist also durch eine zentrale Vorgabe je nach Zielgerät und Inhalt zu steuern. Es darf aber nicht passieren, dass die Verschlüsselung genutzt wird, um verbotene Inhalte in die Hausnetze zu bringen – die Inhaltskontrolle muss also vollautomatisch und zwangsweise nach der Entschlüsselung durchgeführt werden – unabhängig davon wo die Entschlüsselung passiert, bei applikatorischer Entschlüsselung, also beim Schreiben des Klartextes.

Verschlüsselung – unterwegs, lokal und im Netz

Daten, die zur Weitergabe genehmigt sind, können protokolliert und durch einen persönlichen Schlüssel vor Missbrauch geschützt werden. Mit der Möglichkeit unterschiedliche Schlüssel für ein Speichermedium zu nutzen, besteht wirksamer Schutz vor USB-Dumpern auf unsicheren Rechnern. Dabei können unterschiedliche Schutzstufen auf einem Datenträger gemeinsam sicher gespeichert werden.

Da die meisten Anwender keine Administrationsrechte besitzen, darf keine Installation einer Software für die Entschlüsselung nötig sein. Das Entschlüsselungswerkzeug muss schon beim Verschlüsselungsvorgang automatisch auf jeden Datenträger aufgebracht werden, damit die Daten nach Eingabe des richtigen Schlüssels sofort zur Verfügung stehen und ohne Zeitaufwand oder besondere Rechte entschlüsselt bzw. verfügbar gemacht werden.

Schlüsselverwaltung

Die Verwaltung der Schlüssel sollte getrennt von der Systemadministration erfolgen, um dem Bestreben nach Vertraulichkeit und Compliance zu folgen. Die Schlüsseleigenschaften eines starken Schlüssels sind zentral zu definieren. Auch Key Escrow-Verfahren müssen berücksichtigt werden. Key-Verwaltungswerkzeuge stellen sicher, dass, auch wenn ein Anwender eigene persönliche Schlüssel generiert hat, die so verschlüsselten Daten dem Unternehmen auch nach dessen Ausscheiden, oder falls er den Schlüssel vergessen hat, weiterhin zur Verfügung stehen.

Die Anforderungen an ein geeignetes Verschlüsselungsprodukt und Fazit

Lösungen, die einen einzigen Schlüssel für eine ganze Partition bieten, sind nicht flexibel genug für eine Kommunikation mit verschiedenen Empfängern oder für unterschiedliche Vertraulichkeitslevel. Ein geeignetes Produkt besitzt ein zentrales, Compliance-konformes Management, die Möglichkeit die gewünschte Vertraulichkeit zentral zu steuern, ist einfach anzuwenden und bietet richtlinienkonforme Individualisierung sowie eine revisionssichere Protokollierung.

Ein Agent bildet alle Anforderungen an die Verschlüsselung benutzerfreundlich und sicher ab, der Administrationsaufwand wird somit minimiert, die Vertraulichkeit sensibler Daten und die Integrität der verarbeitenden Anwendungen ist somit jederzeit gewährleistet.

Literaturverzeichnis:

[1] Microsoft, Microsoft Security Intelligence Report Volume 8, S.81
[2] BSI, IT-Grundschutzkatalog, G5.142

Informieren Sie sich im Detail über unsere Innovationen und kontaktieren Sie uns unter:

Info@itWatch.de oder 089/ 620 30 100.

itWatch GmbH
Aschauer Str. 30
D-81549 München