DATENSCHUTZVERSTÖßE SICHER VERMEIDEN – KÖNIGSWEGE BEI NEUER INFORMATIONSPFLICHT

Die Bedrohungslage

Die Hauptursachen für Verstöße gegen den Datenschutz sind verbesserte Angriffsverfahren der Täter (G5.2, G5.23, G5.142 et al.), mangelndes Risikobewusstsein oder technische Kenntnis der Anwender (G3.1, G3.3, G3.44), aber auch vorsätzlicher Datendiebstahl (G5.4) von internen Mitarbeitern. Kriminelle verkaufen hochsensible Daten meistbietend, da lukrative Gewinne zu erzielen sind – Presseberichte sind fast täglich zu lesen. Die gestohlenen Daten gehen über schwarze Kanäle an illegale Märkte, dienen wie in Liechtenstein einem persönlichen Rachefeldzug oder werden sogar legalisiert weiter verkauft. Verstöße gegen das Datenschutzgesetz führen nach der Novellierung des Datenschutzgesetztes zu einer zwingenden Informationspflicht – diese vermeidet man am besten, indem man die Datenschutzgesetzte beweisbar einhält. Wir möchten in diesem Artikel also zuerst die potentiellen Verstöße und Angriffe, die zu diesen Verstößen führen können, entlang des Grundschutzkatalogs aufzeigen und dann Lösungsmöglichkeiten skizzieren.

Der Verfassungsschutzbericht 2009 meldet vermehrt Computerspionage-Angriffe auf Wirtschaftsunternehmen und Regierungsstellen. Dabei schleusen die Angreifer Schadcode verborgen in eigentlich erlaubten Dateiformaten über Email, Web oder auch USB-Sticks - vom Benutzer unbemerkt - in das Unternehmen ein. Aktuell bekannt geworden sind Angriffe über *.lnk Dateien. In 2010 sind auch Angriffe über infizierte pdf-Dateien, der direkte Angriff auf Schwachstellen von Applikationen, zum Beispiel dem Internet Explorer, mit erhöhtem Presseaufkommen dokumentiert. Beim Einschleusen von Schadcode können verschlüsselte Objekte nur von intelligenter Spezialsoftware sicher geprüft werden, welche die Verschlüsselung rechtlich korrekt – also mit Wissen und Zustimmung des Anwenders - in einer Quarantäne aufbricht. Natürlich muss das vor der Nutzung geprüft werden. Deshalb bergen verschlüsselte Objekte, geschachtelte Archive und in Standarddateien eingebettete Objekte besondere, verborgene Gefahren. Dass das beweisbare Einhalten der Sicherheitsvorgaben auch in diesem Fall nicht über organisatorische Lösungen erreicht werden kann erschließt sich von selbst, denn der Anwender kann ja in die Dateien nicht hineinsehen ohne sie eingelesen zu haben.

Sind diese schädlichen Anwendungen einmal in das Netzwerk importiert, dann nutzen sie die Rechte des angemeldeten Users, um ohne dessen Wissen über importierte DLLs, JAVA-Script oder eingebettete Executables Daten nach außen zu transportieren. Unter Benutzerrechten wird im Hintergrund, oft ohne Wissen des angemeldeten Anwenders, Datenmaterial – auch über Festplattenverschlüsselung vermeintlich gut geschützte Information – über verschiedene Kanäle nach draußen transportiert. Sensible Daten können dabei, zum Beispiel verschlüsselt (http-s), über den Standard-Browser auf gemieteten Plattenplatz im Internet hochgeladen werden, ohne dass das Firewallsystem aus rechtlichen Gründen wegen der Verschlüsselung davon etwas bemerken kann.

Aktive Funkverbindungen umgehen die zentralen Netzwerk-Schutzvorkehrungen. USB-Dumper (G5.141) kopieren verschlüsselte Daten von beliebigen USB-Sticks unbemerkt im Klartext an andere versteckte Lokationen. Sensible Daten liegen unverschlüsselt auf Laptops und mobilen Datenträgern und sind so bei Verlust oder Diebstahl ungeschützt oder bei vollständig transparenter Entschlüsselung in Echtzeit durch Dritte unerkannt abgreifbar.

Diese Bedrohungen zeigen deutlich, dass eine rein organisatorische Lösung nicht durchgesetzt werden kann, da es dem Anwender nicht möglich ist, *vor* dem Öffnen einer Word-Datei zu prüfen, ob ein eingebettetes Executable enthalten ist – nicht nur weil ihm die technische Expertise fehlt. Insofern gilt es auch in sehr offen eingestellten Umgebungen zumindest technisch gesteuerte Warnmeldungen auszugeben und eine geeignete Protokollierung sowie evtl. eine gute Quarantänelösung anzubieten.

Strategien zur Vermeidung von Datenschutzverstößen gemäß der vom BSI empfohlenen Maßnahmen im IT Grundschutzkatalog Datenschutz

Im folgenden wird eine Auswahl der Maßnahmen und deren technische Umsetzung aufgezeigt, die der IT Grundschutzkatalog am Endgerät ausweist.

M 7.1 Das Datenschutzmanagement ist ein Prozess und integrativer Bestandteil des IT Sicherheitsprozesses, bestehend aus den Phasen Definition der Datenschutzpolicy – Soll/Ist Abgleich – Umsetzung und Betrieb. Bewährt hat sich für den Soll/Ist Abgleich ein Software-gestütztes Risikomonitoring nach:

- Verwendung der Geräte, Devices, Schnittstellen und Ports
- Netzverbindungen, ob diese kabellos oder kabelgebunden sind
- Anwendungen: Welche Anwendungen sind wann und ggf. von wem im Einsatz
- Dateneingang und -Ausgang

Diese Ergebnisse fließen in das jeweils verfeinerte Datenschutzkonzept ein. Ebenso sollte ein interaktives Werkzeug zur Verfügung stehen, um rechtliche Änderungen direkt im Kontext der Verwendung von betroffenen Daten an den Anwender zu

kommunizieren und im besten Fall die Nutzung von dem nachgewiesenen Wissensstand des Anwenders abhängig machen.

M 7.2 Regelung der Verantwortlichkeiten im Bereich Datenschutz schreibt die explizite Zuweisung der Verantwortlichkeiten und Befugnisse an Rollen bzw. Organisationseinheiten bei allen datenschutzrelevanten Aufgaben vor. Auch die eingesetzte Lösung hat dieses Rollenkonzept abzubilden und unterschiedliche Rechte für unterschiedliche Rollen zu ermöglichen. So soll es nicht möglich sein, dass Systemadministratoren Zugriff auf die datenschutzrelevante Informationen bekommen, auch wenn sie die Systeme an sich warten müssen.

M 4.4 Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern und M 4.200 Umgang mit USB-Speichermedien. Diese Maßnahmen dienen dazu, unkontrolliertes Booten, unkontrolliertes Einspielen von Software und unberechtigtes Kopieren von Daten auf Wechselmedien zu verhindern. Dabei lassen sich über die USB-Schnittstelle eine Reihe von Zusatzgeräten mittels der Plug & Play-Funktionalität ohne die Installation eines Treibers an PCs anschließen. Neben den klassischen USB-Sticks können dies USB-Kameras, USB-Drucker und auch Smart-Phones sein. Allerdings kann die USB-Schnittstelle nicht komplett gesperrt werden, da andere Peripheriegeräte wie Maus und Tastatur ebenfalls über USB angeschlossen werden. Diesem Problem wird mit einer Port- und Device-Kontrolle begegnet. Sie definiert, wer, wann, welches Device, welche Schnittstelle unter welchen Umständen einsetzen darf (z.B. WLAN nur außerhalb des Firmen-Netzes, um einen Bypass der bestehenden IT Sicherheitsinfrastruktur zu vermeiden).

M 4.23 Sicherer Aufruf ausführbarer Dateien schreibt vor, dass nur freigegebene Versionen ausführbarer Dateien und keine eventuell eingebrachten modifizierten Versionen eingesetzt werden. Das bedeutet, dass die Applikationen kontrolliert werden müssen, dass alle eingesetzten Applikationen zu inventarisieren sind und dass deren Start und die kritischen Dateizugriffe überwacht werden müssen. Unerwünschte Anwendungen sind zu blockieren. Ein eigener Rechteraum für die Applikation trennt die Zugriffsrechte der Applikation von den Rechten des angemeldeten Benutzers (z.B. *Skype* darf nur auf die eigene Konfiguration zugreifen und kann deshalb keine unerwünschte Datenübertragung durchführen).

M 4.29 Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme und M 4.34 Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen um bei Abhandenkommen des Gerätes die darauf liegenden Nutzdaten vor unautorisiertem Zugriff zu schützen. Zudem dient die Verschlüsselung dem Integritätsschutz und dem Vertraulichkeitsschutz der Daten. Wenn die Daten an Dritte mittels mobilem Device (z.B. USB-Stick) übergeben werden, sind diese mit einem persönlichen Transportschlüssel zu schützen, und zwar pro Vertraulichkeitsstufe oder Empfänger mit einem eigenen Schlüssel, so kann auch sichergestellt werden, dass die nicht für den Empfänger bestimmten Daten, z.B.

durch einen USB-Dumper, ausgespäht werden können. Wenn die auf dem Device gespeicherten Daten das Unternehmen unter keinen Umständen verlassen sollen, so muss die Verschlüsselung zwangsweise und für den Anwender transparent mit einem Unternehmensschlüssel vorgenommen werden. Für den Anwender steigt die Akzeptanz, wenn er mehrere Schlüssel auf einem Device anwenden kann.

M 4.33 Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung bedeutet, dass das Device erst nach erfolgreichem Abschluss des Virenscan-Vorganges freigegeben wird, die Prüfung der Dateien also im Hintergrund stattfindet, ohne, dass der Anwender in den Prozess eingreifen kann.

M 4.81 Audit und Protokollierung der Aktivitäten im Netz. Die revisionssichere Protokollierung dient dazu, bestimmte Ereignisse für eine spätere Auswertung abzuspeichern, ohne dass diese Daten im Nachhinein modifiziert werden können. Die Audit-Funktionalität meldet in Echtzeit Sicherheitsvorfälle und ermöglicht so eine Alarmierung der Verantwortlichen aber auch das Abschließen individueller Verträge mit dem Anwender durch eine rechtssichere elektronische Willenserklärung.

M 4.199 Vermeidung gefährlicher Dateiformate. Eine Inhaltskontrolle stellt sicher, dass nur gewünschte Dateiformate übertragen werden, selbst wenn diese umbenannt wurden oder sich in verschlüsselten ZIP-Archiven befinden oder aber, wenn diese in erlaubte Formate eingebettet wurden. Die gefährlichen Dateiformate sind insbesondere ausführbare Inhalte, wie EXE und DLLs.

M 4.345 Schutz vor unerwünschten Informationsabflüssen. Ein Data Loss Prevention-System dient dazu, sicherzustellen, dass Daten nicht unerwünscht abfließen, indem der Datenfluss auf dem Endgerät kontrolliert wird, also dort wo die Daten entstehen und verarbeitet werden. Hierbei werden die Daten je nach Vertraulichkeit unterschiedlich behandelt. So kann es möglich sein, dass vollkommen unkritische Daten, beispielsweise eine Anfahrtsskizze, unverschlüsselt übertragen (exportiert) werden können, währenddessen vertrauliche Daten entweder zur Weitergabe vollkommen gesperrt werden oder aber nur verschlüsselt übertragen werden können. Um die Kritikalität der Daten festzustellen ist eine Inhaltskontrolle nötig. Bei Verstößen gegen die definierten Regeln bieten DLP-Tools ereignisabhängig abgestufte Reaktionsmöglichkeiten, dazu gehören beispielsweise:

- Anzeige eines Hinweises für den Benutzer, dass die geplante Transaktion gegen das Regelwerk verstoßen würde
- Abfrage einer expliziten Zustimmung des Benutzers
- Blockade der Aktion
- Protokollierung
- Information Dritter, z. B. eines Administrators oder Vorgesetzten

Datenschutzverstöße sicher vermeiden – Königswege bei neuer Informationspflicht

Die Erfahrung zeigt, dass die Anzeige von Warnhinweisen sehr wirkungsvoll ist, um die Mitarbeiter für den verantwortungsbewussten Umgang mit vertraulichen Informationen zu sensibilisieren. Zu starke Einschränkungen oder Kontrollen über DLP-Tools hingegen können sich negativ auf die Motivation der Mitarbeiter auswirken.

M 5.69 Schutz vor aktiven Inhalten, egal über welche Schnittstelle und in welchem Dateityp sich diese verbergen, um so das Einschleusen von Schadcode zu verhindern.

M 6.38 Sicherungskopie der übermittelten Daten gegen die Bedrohung des Verlustes der Verfügbarkeit (G1.9, G4.52, G4.7, G5.1 et al.), die natürlich auf mobilen Datenträgern durch deren physikalische Gefährdung besonders hoch ist, schützt ein automatisches „Shadowing“. Entsprechend GoBS, GoS, FAIT und vielen anderen Auflagen und Standards unterliegen bestimmte Daten - z.B. Daten zur Rechnungslegung - einer Archivierungspflicht. Die Archivierungspflicht ist nur erfüllt, wenn die archivierten Daten über den Verpflichtungszeitraum auch im Klartext zur Verfügung stehen. Hat nun ein Anwender die Möglichkeit die unter Archivierungspflicht liegenden Daten verschlüsselt abzulegen, dann sind die Daten zwar archiviert, aber die gesetzliche Auflage ist nicht erfüllt. Diese Herausforderung lässt sich nur durch eine geeignete Schlüsselhinterlegung lösen. Die Aufbewahrungspflicht der beteiligten Schlüssel UND des gesamten Verfahrens zur Entschlüsselung ist also ebenfalls an die gesetzlichen Auflagen gekoppelt. Damit der Wirtschaftsprüfer das Verfahren auch abnimmt, muss also nicht nur das Verfahren „transparent“ sein sondern auch jede Nutzung der optionalen Verschlüsselung daraufhin überprüft werden, ob archivierungspflichtige Daten betroffen sind und dann sofort eine geeignete Maßnahme getroffen werden.
Wesentlich ist hierbei, dass man die Berechtigung zur Einsichtnahme der Daten im „Shadow“ in das Gesamtkonzept aufnimmt, da hier insbesondere bei VIP-Anwendern häufig Daten verarbeitet werden, die nicht für die Augen anderer bestimmt sind.

Fazit

Die Umsetzung des Datenschutzes kann also proaktiv so organisiert werden, dass erst gar keine Informationspflicht entstehen kann, weil man die geeigneten technischen und organisatorischen Lösungen umgesetzt hat. Dieses sind beispielhaft:

- Verschlüsselung mit Unternehmensschlüssel auf mobilen Datenträgern und Notebooks – dadurch können die Daten nicht in falsche Hände gelangen.
- Überwachen der Import- und Export-Schnittstellen am Endgerät, denn dort liegen die Daten entweder im Klartext vor oder der zuständige Anwender kann per revisionssicher gespeicherter elektronischer Willenserklärung in Echtzeit zur Entschlüsselung in einer Quarantäne aufgefordert werden.

Datenschutzverstöße sicher vermeiden – Königswege bei neuer Informationspflicht

- Importiert und exportiert werden Daten nicht nur über mobile Datenträger an den Ports (USB, Firewire, Bluetooth ...) sondern auch durch kommunizierende Anwendungen heruntergeladen oder verschickt (Browser, E-Mail Client, ftp ...).
- Entpacken und Entschlüsseln von importierten Daten, um die Freiheit von Schadcode oder unerwünschten ausführbaren Programmen zu gewährleisten.
- Einschränkung der Rechte von Anwendungen mit hohem Angriffspotential (z.B. Browser).
- Kontrolle der aktiven Anwendungen, insbesonderer der portable Apps, die automatisch von mobilen Datenträgern starten, mittels Protokollierung und White- und Black-Listing.
- Umsetzen der Archivierungspflicht durch ein geeignetes Shadowing.
- Die Umsetzung empfiehlt sich natürlich durchgehend (360 Grad), d.h. auf Desktops, Fat Clients, Thin Clients, Notebooks, Citrix® und Terminalservern und Servern, deren physikalischer und technischer Schutz nicht ausreicht.

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