
Foto: NASA – www.nasa.gov

Wirtschaftsspionage heute

Unverzichtbarer Schutzschirm

Spionage ist eine reale Bedrohung unserer Wirtschaft. IT-Verantwortliche sollten auf die notwendigen Sicherheitstechniken setzen, um ihre Unternehmen zu schützen.

TEXT: BEATRICE LANGE

Wir kennen Spionage noch aus der Zeit des kalten Krieges und lassen uns nur all zu gern von dem Gedanken trösten und ablenken, dass diese Zeit ja nun vorbei ist. Fälle wie der aufgeflogene Spionagering im Juni in den USA lassen aber aufhorchen und mahnen zur Obacht. Nicht nur für den russischen Geheimdienst ist Wirtschaftsspionage Teil des Aufgabengebiets.

Es ist uns häufig nicht bewusst, dass nicht nur sogenannte Schurkenstaaten ihre Aufklärungsdienste zur Beobachtung unserer Wirtschaft einsetzen. Es sind auch unsere europäischen Nachbarn, die gern Informationen aus deutschen Unternehmen abziehen, um sie für eigene Unternehmen in ihrem Land zu nutzen. Nachzulesen ist dies im Verfassungsschutzbericht 2010, vorgestellt im Juni in Berlin.

Nach diesen Berichten verwundert es, dass auf Nachfrage 60 Prozent der Unternehmen angaben, keinen Schutz für die sensiblen Daten zu haben. 30 Prozent schützen sich mit absonderlichen Maßnahmen wie Heißkleber in der USB-Schnittstelle. Nur 10 Prozent der gefragten Unternehmen schützen ihre wichtigen Daten durch Verschlüsselung. Dabei ist es sehr einfach, mit einem handelsüblichen USB-Stick in Sekunden den kompletten Datenbestand eines Unternehmens abzugreifen und so den Fortbestand des Unternehmen zu gefährden. Dazu ein Artikel: www.ln-online.de, Artikel 2775931 vom 25.04.2010.

Unternehmen, die bereits einmal von Datenverlust betroffen waren finden sich hier: www.projekt-datenschutz.de. Dabei trifft es aber nicht nur die großen Unternehmen, das Know-how und die Innovationen finden wir im Mittelstand. Und hier wächst die Bedrohung. Laut Statistik war in den letzten fünf Jahren jedes dritte Unternehmen Opfer von Datendiebstahl. Nach der Novellierung des Datenschutzgesetzes und der damit verbundenen Veröffentlichungspflicht im Falle eines Datenverlustes rechnen Experten mit einem sprunghaften Ansteigen der Zahlen seit September 2009.

Was sind außer Profitgier die Motive für Datendiebstahl? Das kann die innere Kündigung ebenso sein wie Erpressung oder allgemeine Verärgerung über das Unternehmen. Aber auch ein ganz profaner Grund: Die Mitarbeiter halten die von ihnen erstellten Daten für ihr Eigentum und haben kein Unrechtsbewusstsein, wenn sie diese mitnehmen. Hier ist Aufklärung ein ganz wichtiges Stichwort.

Denn Sicherheit ist nicht statisch. Sicherheit muss gelebt werden und die Mitarbeiter müssen in den Prozess eingebunden werden. Sie müssen verstehen, wozu diese Sicherheit dem Unternehmen und damit letztlich ihnen selbst, nutzt. Es

ist wichtig, die Mitarbeiter von Anfang an in die Sicherheitsmaßnahmen einzubinden. Denn wer den Mitarbeitern die »Datentür« vor der Nase zuschlägt, darf sich nicht wundern, dass die Mitarbeiter versuchen werden, Schutzsysteme zu umgehen. Abgesehen von einem eventuellen Datenverlust spielt die wertvolle Arbeitszeit, die vergeudet wird, eine Rolle. Also sind Unternehmen immer gut beraten, die Mitarbeiter von Anfang an mit in die Konzepte einzubinden. Diese sollten die Nutzung von Handys, den Umgang mit Besuchern und Besprechungen auf dem Flur ebenso behandeln wie den Schutz der Daten.

Verschlüsselung ist unverzichtbar

Es stellt sich die Frage, welches System helfen kann und geeignet ist. – Nur Verschlüsselung kann Daten sicher bewahren und Unternehmen wirkungsvoll schützen. Verschlüsselung ist die Veränderung von Informationen dahingehend, dass sie durch die Veränderung nur von berechtigten Personen gelesen werden kann. Verschlüsselung gibt es schon einige Tausend Jahre und sie wurde beispielsweise von den Ägyptern verwendet, um die heiligen Schriften den Priestern vorzubehalten. Ziele von Datenverschlüsselung ist die Vertraulichkeit zu erhalten, das heißt nur berechtigte Personen dürfen Einsicht in die Informationen nehmen. Ein weiteres Ziel ist die Integrität: Es muss ersichtlich sein, ob eine Manipulation der Daten stattgefunden hat. Authentizität beschreibt die eindeutige Identifizierbarkeit des Urhebers und die Verbindlichkeit weist die Urheberschaft der Daten gegenüber Dritten nach.

Anforderungen an Sicherheitssoftware

Daten müssen automatisch geschützt werden. Dies erreicht die Verschlüsselungstechnologie, die automatisch im Hintergrund arbeitet. Im Hintergrund, um die Nutzer nicht zu Aktionen oder Maßnahmen zu zwingen, die entweder vergessen oder missachtet werden könnten. Die Verschlüsselungssoftware erkennt selbsttätig nach vorgegebenen Richtlinien sensible Daten und verschlüsselt diese dann automatisch.

Eine solche Software sollte von einer zentralen Instanz aus bedient werden. Es muss sichergestellt werden, dass die notwendigen Installationen und die Deinstallation, die Vergabe von Rechten oder die Vornahme von Einstellungen nur von berechtigten Personen ausgeführt werden darf. Dies lässt sich am sichersten dadurch erreichen, dass die berechtigte Person sich durch eine Hardware wie einen USB-Token ausweisen muss. Es gibt Software, die in ihren Einstellungen die Möglichkeit gibt, die Daten vor jedermann, auch vor der EDV, zu schützen. Dies führt bei den Mitarbeitern der EDV regelmäßig zum Aufatmen, denn es wird als Entlastung in der Verantwortung empfunden. Ein weiterer wichtiger Punkt ist die Möglichkeit, Daten wieder herzustellen. Es werden Produkte angeboten, die durch die Vergabe eines persönlichen kryptografischen Codes sicherstellen, dass Daten immer wieder hergestellt werden können. Die EDV darf nicht überlastet werden. Sicherheit darf nicht an der Administration scheitern. Eine einmal installierte und eingerichtete Sicherheitslösung darf die EDV nicht belasten und muss im Hintergrund ohne weiteren Aufwand funktionieren. Schnittstellen müssen für einen reibungslosen Arbeitsablauf Signale von Tastatur, Maus aber auch Drucker und Scanner ohne Einschränkung passieren lassen. Andererseits dürfen Daten weder ungeschützt aus dem Unternehmen heraus oder in das Unternehmen hinein gelangen. An dieser Stelle hilft wieder Verschlüsselung, denn nur autorisierte Daten gelangen hinein oder auch hinaus. Diese werden am firmeneigenen Kryptocode erkannt.

Arbeitsabläufe dürfen nicht eingeschränkt werden, die Produktivität darf nicht leiden. Die durch Verschlüsselung geschützten Daten können von Systemen mit dem passenden Schlüssel gelesen werden. Die Eingabe eines Passwortes ist nicht erforderlich. Eine Sicherheitslösung muss manipulationssicher sein. Bereits bei der Auswahl sollte darauf geachtet werden, dass die

Lösung nicht durch das Löschen eines Treibers oder Änderungen in der Registry deaktiviert werden kann. Auf dem Markt finden sich leider viele Lösungen, die keine hohen Sicherheitsanforderungen an sich selbst stellen. Sichere Software ist mit einem Deinstallationsschutz versehen. Nur berechtigte Personen dürfen die Software deinstallieren. Selbst Usern mit Administratorenrechten auf dem eigenen Gerät muss dieses verwehrt werden.

Schutz ohne Hintertüren

Dabei gibt es aber für Unternehmen noch einen ganz wichtigen Punkt, den sie unbedingt beachten sollten: Nur in Deutschland nach deutschem Recht erstellte Software macht sie auch wirklich sicher. Es ist Entwicklern in Deutschland möglich, Software ohne Hintertüren, die sogenannten Backdoors, zu erstellen. Nur Verschlüsselungssoftware ohne die Möglichkeit der ungewollten Entschlüsselung bringt auch die gewünschte Sicherheit für Unternehmen. Ein weiterer wichtiger Aspekt bei der Auswahl einer passenden Lösung sollte die Entwicklung aller Komponenten von einem Hersteller sein. Oft kommt es bei Lösungen, bei denen verschiedene gekaufte Komponenten zusammengestellt werden, zu Kollisionen untereinander.

Neutrale Informationen

Bei der Suche nach der richtigen Lösung für Unternehmen findet sich beispielsweise hier Hilfe: Arbeitskreis 27001 beim www.ruhr-networker.de. Neben Veranstaltungen zum Thema finden Interessierte einen kurzen Fragebogen, nach dessen Ausfüllen sie einen Überblick über ihre eigene Bedrohungssituation erhalten und geeignete Maßnahmen zu ihrem Schutz finden.

Vorteile der tetraguard-Lösung

tetraguard systems schützt Firmennetze effektiv vor Informationsdiebstahl und Informationsverlust. Die unberechtigte oder fahrlässige Herausgabe oder Mitnahme von Daten wird unterbunden.

- Sicherheitszone(n) im Unternehmen: Das Besondere an dem tetraguard-Ansatz ist, dass innerhalb des Unternehmens keine Einschränkungen im Informationsaustausch entstehen. Definiert werden eine oder mehrere Sicherheitszonen. Innerhalb einer Sicherheitszone können Daten wie gewohnt ausgetauscht werden. Für den Im- und Export von Daten in eine Sicherheitszone wird eine Autorisierung benötigt.
- Einfache Handhabung: Über die Oberfläche des tetraguard-Sicherheitsmanagers werden alle Sicherheitskomponenten und Einstellungen zentral auf Serverebene verwaltet, Benutzerrechte vergeben und neue Clients eingerichtet. Die Installation und Konfiguration ist einfach gehalten. Tooltips bei jeder Einstellungsmöglichkeit sowie ein ausführliches Handbuch ergänzen dies. Mitarbeiter müssen nicht extra geschult werden und können ihre gewohnte Arbeitsweise beibehalten. Für das Arbeiten innerhalb einer Sicherheitszone sind keine neuen Arbeitsschritte erforderlich. Die Sicherheit ist dennoch jederzeit gewährleistet. Auch für Ausnahmefälle wie die Herausgabe von Dokumenten an einen Kunden wird nur ein einziger Arbeitsschritt benötigt. Das Anschließen eines Autorisierungsschlüssels genügt. Datensicherheit, die nicht manipuliert werden kann, ist nur durch Verschlüsselung zu erreichen. Die tetraguard-Verschlüsselung wird vom Benutzer durch ihre Schnelligkeit nicht wahrgenommen und stört durch die Arbeitsweise im Hintergrund die gewohnte Arbeitsweise nicht.
- Wartungsarm: Nach der Installation und Konfiguration muss die Konfigurationssoftware nur noch in Ausnahmefällen wie für das Einlesen eines neuen Autorisierungsschlüssels gestartet werden. Aktualisierungen werden auf dem Server durchgeführt. Die Client-Rechner werden dann automatisch aktualisiert.
- Flexibilität: Obwohl die Software einfach zu konfigurieren ist können auch komplexere Anforderungen an den Datenschutz erfüllt werden. Der Import von Daten und der Export von Daten sind getrennt konfigurierbar. So kann bei-

spielsweise ein Rechner oder eine Rechnergruppe für den Import von Daten zugelassen werden, für den Export jedoch nicht.

- Schutz vor Manipulation: Die tetraguard-Client-Installationen sind vor Manipulationen geschützt. Eine Implementierung auf Systemebene sowie verschiedene zusätzliche Sicherheitsvorkehrungen verhindern das manuelle Entfernen oder Anhalten der Client-Software. Sogar die Deinstallation durch angemeldete Administratoren wird unterbunden. Zur Deinstallation wird zusätzlich ein Administrationsschlüssel benötigt. Die Konfigurations-Software kann nur bei angeschlossenem Administrationsschlüssel auf dem Server gestartet werden. Die Datenbank ist komplett verschlüsselt und somit vor Manipulation geschützt. Diese Sicherheitsvorkehrungen ermöglichen die Trennung von Administration und Datensicherheit. Alle Administratoren können den Server warten. Bei tetraguard kann dies aber nur der Zuständige für die Datensicherheit. Nur dieser hat Zugriff auf die Richtlinien der tetraguard-Software.
- Geringe Systemanforderungen: Auf Grund der effizienten und performanten Umsetzung werden sowohl auf der Server- als auch auf der Client-Seite nur minimale Ressourcen für den Einsatz der tetraguard-Software benötigt. Auch ältere Hardware kann verwendet werden und es muss kein zusätzlicher Server bereit gestellt werden.

Kernkomponenten

- Kernfunktion tetraguard disk: tetraguard disk verschlüsselt automatisch auf mobilen und festen Datenträgern eine Partition oder ein oder mehrere selbst bestimmte Verzeichnisse. Dies ist insbesondere für die Datensicherheit auf Notebooks interessant, die von verschiedenen Personen genutzt werden, da nur die sensiblen Daten und nicht die gesamte Festplatte verschlüsselt wird. Die Vertraulichkeit der Daten bleibt bei Verlust des Gerätes erhalten. Die unkomplizierte Installation von Software-Updates und Patches, sowie auch die Wiederherstellung nach einem Systemcrash (Plattenschaden) sind gewährleistet. Als besonderen Vorteil empfinden die Anwender die Tatsache, dass Geräte ohne Verlust der Vertraulichkeit in den Service gegeben werden können, denn das Arbeiten am Gerät ist möglich. Die Daten sind verschlüsselt und damit nicht zugänglich. Auch Temp-Dateien werden durch Verschlüsselung geschützt. tetraguard arbeitet ohne Backdoors, wobei dem autorisierten Besitzer der Daten jederzeit ein Restore möglich ist. Dabei ist sichergestellt, dass diese Funktion nur durch berechtigte Personen durchgeführt werden kann. Es ist möglich, sensible Daten nur einer berechtigen Person oder einem Personenkreis zugänglich zu machen. Einer oft genannte Anforderung von EDV-Mitarbeitern wurde dadurch Rechnung getra-

Über tetraguard

tetraguard systems GmbH ist ein führender Anbieter im Bereich IT-Security. Bekannt wurde das Unternehmen (vormals tetraguard GmbH) durch die Entwicklung von Datensicherheitssystemen für die Microsoft Windows Plattformen. Im Laufe der jungen Firmengeschichte haben wir uns zu einem führenden Hersteller für Endpoint Security entwickelt und arbeiten mit Partnern und Kunden in mehr als 15 Ländern zusammen. Mit der zum Patent angemeldeten Softwarereihe »tetraguard« und deren innovativen Funktionen werden Firmennetze und Einzelplatzsysteme gezielt vor Informationsdiebstahl geschützt.
Die innovative Softwarelösung »tetraguard« wurde in den Jahren 2005 und 2006 von der Landesinitiative »secure-it.nrw« und im Jahr 2008 mit einer Auszeichnung der Initiative des deutschen Mittelstandes sowie durch die renommierte nationale und internationale Presse ausgezeichnet.

gen, dass Daten auch für die EDV nicht lesbar sind und damit die absolute Sicherheit vor fremden Blicken gewährleistet ist.

■ Kernfunktion tetraguard device & more: Die Komponente tetraguard device & more dient zum Schutz vor unberechtigtem Kopieren und Lesen von internen und externen Daten auf verschiedenste Wechseldatenträger wie CD/DVDs, USB-Sticks oder MP3-Player. Beim Einsatz von tetraguard device & more bleiben Schnittstellen wie IDE, USB oder Firewire offen, damit angeschlossene Geräte wie Tastatur, Maus, Drucker oder Scanner reibungslos funktionieren. Datenströme nach außen werden jedoch verschlüsselt. Für einen Datentransfer aus und in das Unternehmensnetz kann durch den Einsatz von Autorisierungsschlüsseln diese Funktion individuell auf den Arbeitsplätzen für eine bestimmte Zeit freigeschaltet werden. Wechselt ein Datenträger im Unternehmen von einem Mitarbeiter zum anderen, werden die verschlüsselten Daten automatisch erkannt und entschlüsselt. Erst wenn die Daten mit speziell eingesetzten Autorisierungsschlüsseln auf einem eingesteckten USB-Token geschrieben werden, sind sie außerhalb des Unternehmens lesbar. Der Vorteil der tetraguard Technologie ist, dass sie keine Computerschnittstellen wie IDE, USB oder Firewire verschließt, sondern den Datenstrom analysiert, beim Kopieren verschlüsselt und beim Lesen entschlüsselt, ohne auf administrativ aufwändige Whitelists zugreifen zu müssen. Tastatur, Maus, Drucker, Scanner und andere Geräte können so weiterhin funktionieren, da ihr Datenstrom von dem eines USB-Stick von tetraguard unterschieden wird.

Weitere Komponenten

■ tetraguard Sicherheitsmanager: Über die benutzerfreundliche Oberfläche des tetraguard-Sicherheitsmanagers, dem Herzstück der tetraguard-Technologien, werden alle Funktionen und Einstellungen zentral auf Server-Ebene verwaltet und neue Clients eingerichtet. Im Rahmen der Rechtevergaben können Arbeitsplätze zentral administriert und Rechte vergeben werden. Des Weiteren werden hier die verschiedenen Schlüssel verwaltet.

■ tetraguard lock: Mit der tetraguard lock-Funktion wird das Lesen und/oder Schreiben verschiedenster Wechseldatenträger wie CD/DVDs, USB-Sticks oder MP3-Player am Arbeitsplatz gesperrt. Hiervon unberührt bleiben Geräte wie Tastatur, Maus, Drucker oder Scanner.

■ tetraguard unit control: Diese Funktion sorgt für mehr Flexibilität im Einsatz von Wechseldatenträgern wie USB-Sticks oder Kameras. Zusätzlich zur Freigabe per Autorisierungsschlüssel bietet die Funktion tetraguard unit control die Möglichkeit, vordefinierte Wechseldatenträger im Unternehmen mit speziellen Berechtigungen zu versehen. So lässt sich beispielsweise definieren, ob unverschlüsselt geschrieben oder die Daten nur gelesen werden dürfen.

■ tetraguard crypt & go: Für den sicheren Transport außerhalb des Unternehmens verschlüsselt tetraguard crypt & go Dateien als Paket. So können diese sicher auf einem Wechseldatenträger wie USB-Stick oder CD/DVD gespeichert oder per E-Mail verschickt werden. Zum Anlegen und Öffnen der verschlüsselten Pakete kann wahlweise ein Passwort und/oder Autorisierungsschlüssel verwendet werden. Das verschlüsselte Paket kann entweder als selbstextrahierendes Archiv oder im speziellen tetraguard crypt & go Format gespeichert werden. Für Letzteres wird zum Entschlüsseln eine Software benötigt, die auf der tetraguard systems-Website kostenlos erhältlich ist.

■ tetraguard Suiten: Die tetraguard-Komponenten werden in Suiten optimal auf verschiedenste Anforderungen der Unternehmenssicherheit angepasst. Ab sofort stehen die neuen tetraguard-Sicherheitssuiten zur Verfügung. tetraguard basic 2011, tetraguard professional 2011 und tetraguard premium 2011 schützen Firmennetze effektiv vor Informationsdiebstahl.

Beatrice Lange,
Management tetraguard systems