Creditreform Das Unternehmermagazin aus der Verlagsgruppe Handelsblatt
SecurITy made in Germany
TeleTrusT Pioneers in IT security.

Beitrag von Thorsten Urbanski, Leiter der TeleTrusT-AG "ITSMIG" in creditreform Magazin, 01.08.2013

http://www.creditreform-magazin.de/content/news/it-security-made-in-germany;215995

"IT Security made in Germany"

Der Schutz der IT-Infrastruktur vor Spionageangriffen ist für Unternehmen überlebensnotwendig. Denn wertvolle Konstruktionspläne, Kundendaten oder Business-Pläne sind bei Online-Kriminellen und ausländischen Geheimdiensten äußerst begehrt. Wir sprachen mit Thorsten Urbanski, der die Unternehmenskommunikation der G Data Software AG verantwortet. Außerdem leitet er die TeleTrusT-Arbeitsgruppe "IT Security made in Germany" und ist Mitglied im wissenschaftlichen Beirat der Deutsche-Messe-Initiative "CeBIT against Cybercrime".

Ausländische Behörden haben starke Unterstützer: Viele amerikanische Firmen arbeiten mit NSA, CIA & Co zusammen und halten in ihrer Software und in ihren Diensten Hintertüren offen, um die Angriffe zu ermöglichen. Zu einer Kooperation sind amerikanische Unternehmen per Gesetz seit Einführung des USA Patriot Acts (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) 2001 sogar verpflichtet.

Anders sieht die Situation bei deutschen IT Security-Herstellern aus. Diese unterliegen einer anderen Gesetzgebung und sind dazu verpflichtet, den hohen Anforderungen des deutschen Datenschutzgesetzes zu entsprechen. Das umfasst auch deutsche Anbieter von Cloud-Diensten, die den gesetzlichen Bestimmungen in Deutschland entsprechen müssen.

German Engineering

40 Prozent aller Unternehmen verzeichneten laut BKA bereits Angriffe auf ihre Netzwerke. Doch welchen Sicherheitslösungen können Unternehmen vertrauen? Die TeleTrusT Arbeitsgruppe "IT Security made in Germany" (ITSMIG) hat bereits 2011 eine Initiative auf den Weg gebracht, die u.a. in der Festlegung von Kriterien zur Zeichenverwendung des Qualitätssiegels "IT Security made in Germany" mündeten.

Unternehmen, die das TeleTrusT-Qualitätssiegels "IT Security made in Germany" tragen, verpflichten sich folgende fünf Kriterien zu erfüllen:

1. Der Unternehmenshauptsitz muss in Deutschland sein.
2. Das Unternehmen muss vertrauenswürdige IT-Sicherheitslösungen anbieten.
3. Die angebotenen Produkte dürfen keine versteckten Zugänge enthalten (keine "Backdoors").
4. Die IT-Sicherheitsforschung und -entwicklung des Unternehmens muss in Deutschland stattfinden.
5. Das Unternehmen muss sich verpflichten, den Anforderungen des deutschen Datenschutzrechtes zu genügen.

Im Kontext der aktuellen Diskussion um Prism, Tempora und Co zeigt Experte Thorsten Urbanski drei aktuelle IT Security-Problemfelder auf und gibt Ihnen entsprechende und Handlungsempfehlungen.

Beachten Sie folgende Hinweise: Cloud-Nutzung vorab regeln

Bei der Auslagerung von Daten sollten Unternehmen vorab Richtlinien entwickeln, welche Daten ausgelagert werden sollen und dürfen. Hier gilt es generell abzuwägen, ob beispielsweise sensible Unternehmensdaten die firmeneigene IT-Infrastruktur verlassen sollten. Neben den Sicherheitsvorkehrungen des jeweiligen Cloud-Anbieters, können Unternehmen selbst aktiv werden und wichtige Daten ausschließlich verschlüsselt auslagern. Der Einsatz leistungsstarker Verschlüsselungsprogramme ist dabei mit einem geringen Aufwand verbunden.

Cyberspionage von innen vermeiden

Die Angriffe auf Unternehmen erfolgen nicht ausschließlich über das Internet. Nicht selten gelangt Spionagesoftware mit Hilfe infizierter USB-Sticks in das firmeninterne Netzwerk. Ermittlungsbehörden

konnten in einzelnen Fällen von Betriebsspionage nachweisen, dass die Angreifer präparierte USB-Sticks auf Parkplätzen oder in Fahrstühlen von Unternehmen als "Fundsache" innerhalb des Zielobjekts platzierten. Bei diesem Konzept setzen die Täter auf die Neugier des Finders, der diesen ohne weitere Gedanken zu verschwenden, in seinen Arbeitsplatz-PC steckt, um zu überprüfen ob sich vielleicht interessante Daten darauf befinden.

Der installierte Schädling könnte, wie auch bei Angriffen über das Internet, nicht geschlossene Lücken in der installierten Software auszunutzen, um sich im Netzwerk zu verbreiten. Letztendlich könnten so auch Industrierechner erreicht werden, die nicht direkt mit dem Internet verbunden sind. Um Angriffe mit USB-Sticks zu vermeiden, sollten Unternehmen generell den Gebrauch privater Speichermedien in einer IT Policy fixieren und Mitarbeiter für das Thema Datensicherheit und Cyber-Spionage sensibilisieren. Zusätzlichen Schutz schaffen Sicherheitslösungen mit integriertem Policy Management, die den Gebrauch von USB-Speichermedien oder externen Festplatten technisch verhindern.

Software-Sicherheitslücken als Einfallstor

Gefahren, die durch Malware wie Trojaner und Würmer entstehen, sind hinlänglich bekannt und im Bewusstsein der IT-Verantwortlichen längst angekommen. Der Einsatz entsprechender IT-Sicherheitslösungen ist bei Unternehmen verpflichtend. Laut Microsoft werden am Tag durchschnittlich 22 Sicherheitslücken bekannt, pro Jahr kommen so über 8.000 Schwachstellen zusammen. Angreifer werten diese Lücken aus. Gut 70% aller Exploits werden aktiv für Cyber-Attacken ausgenutzt – und das, obwohl zum Zeitpunkt des jeweiligen Angriffs für 90 Prozent der Schwachstellen bereits ein Patch durch den jeweiligen Hersteller verfügbar war. 2013 wird daher nicht von ungefähr erwartet, dass Schadprogramme, welche diese Sicherheitslücken nutzen, die Spitze des Gefahren-Rankings bilden.

Patch-Management in den Grundschutz-Katalogen

Diese Ansicht teilt auch das BSI, das dem Patch-Management zusammen mit dem Änderungsmanagement unter der Überschrift "Übergreifende Aspekte" den Baustein B 1.14 in den Grundschutzkatalogen widmet Die Autoren legen den Wert der systematischen Aktualisierung für die Sicherheit ausführlich dar und beschreiben unter M. 2.421 detailliert den zugehörigen Planungs- und Durchführungsprozess. Dessen Darstellung samt Ablaufgrafik ist aber auch unmittelbar anzusehen, welch hohen Zeit- und Ressourcenaufwand das Verfahren nach sich zieht, wenn es nicht durch benutzerfreundliche Tools unterstützt wird.

Vor allem das Durchführen von Patch-Tests stellt sich bei manueller Vorgehensweise als ein zeitraubender Faktor dar. Die BSI-Autoren merken wohl aus diesen Gründen selbst an, dass Patch-Management eine Aufgabe darstellt, die vor allem kleine Organisationen stark fordert , und legen nahe, dass sich diese gegebenenfalls auf ein reines Änderungsmanagement beschränken sollten. Für größere Einheiten allerdings erklären sie Patch-Management quasi zur Pflicht.

Hintergrund: TeleTrusT-Initiative "IT Security made in Germany"

"ITSMIG" ("IT Security made in Germany") wurde 2005 auf Initiative des Bundesministeriums des Innern (BMI), des Bundesministeriums für Wirtschaft und Technologie (BMWi) sowie Vertretern der deutschen IT-Sicherheitswirtschaft etabliert und 2008 in einen eingetragenen Verein überführt. Sowohl BMI als auch BMWi hatten eine Schirmherrschaft übernommen. Nach intensiven Erörterungen sind TeleTrusT und "IT Security Made in Germany" (ITSMIG) im Jahr 2011 übereingekommen, dass sich auf ihren Handlungsfeldern Synergien erschließen lassen. Seitdem werden die ITSMIG-Aktivitäten unter dem Dach des TeleTrusT als eigenständige TeleTrusT-Arbeitsgruppe "ITSMIG" fortgeführt.