Data Leak Prevention

Der USB-Stick als Spionage-Tool

21.07.2016

Von  Michael Bauner (Experte)

USB-Sticks bergen im Unternehmenseinsatz nicht nur die Gefahr von Datenverlust. In Verbindung mit menschlicher Neugier werden sie zu einem idealen Instrument für Wirtschaftsspione. Mitarbeiter könnten so ohne ihr Wissen zu Mittätern werden. Während Verbote nur bedingt wirksam sind, lässt sich der Einsatz der Speichermedien mit technischer Unterstützung zielgerichtet regulieren.

Jetzt noch schnell das Angebot auf den Stick ziehen und ab ins Wochenende. Obwohl es deutlich sicherere Möglichkeiten zum Transport von Daten gibt, ist der USB-Stick (http://www.computerwoche.de/v/windows-10-von-usb-stick-installieren,959532) zu diesem Zweck der Deutschen liebstes Tool. Einer Umfrage von IronKey und Vanson Bourne (http://www.ironkey.com/en-US/resources/documents/IronKey-by-Imation-Commentary-Presentation.pdf) aus dem Jahr 2014 zufolge nutzen 40 Prozent der Arbeitnehmer den USB-Stick, wenn sie Dateien aus dem Büro mitnehmen. Woher sie das Speichermedium haben, wissen sie wahrscheinlich selbst nicht mehr so genau.

Das Einmaleins der IT-Security **1/35**

Sichere Passwörter

IT-Sicherheit beginnt mit Sensibilisierung und Schulung der Mitarbeiter sowie mit einer klaren Kommunikation der internen Verhaltensregeln zur Informationssicherheit:

Komplexe Passwörter aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen, mindestens achtstellig.

Foto: wk1003mike - www.shutterstock.com

USB-Sticks: Gefährliche Fundstücke

Laut Statista (http://de.statista.com/statistik/daten/studie/151613/umfrage/absatz-von-usb-sticks-seit-2004-in-deutschland/) kamen im Jahr 2015 knapp 16 Millionen USB-Sticks in den Handel, 75 Millionen innerhalb der letzten fünf Jahre. Rein numerisch hat also nahezu jeder deutsche Bürger einen USB-Stick in Besitz. In vielen Fällen dürften sich im Laufe der Jahre mehrere Schubladen im Büro oder Zuhause gefüllt haben. Die meisten USB-Sticks dürften dabei Werbegeschenke von Kunden und Dienstleistern sein, mit aufgedrucktem Firmenlogo und Produkt- oder Marketing-Infos.

Das ein oder andere USB-Device wurde vielleicht auch irgendwo gefunden und dann zuhause oder im Büro kurzerhand dem Rechner zugeführt. Wer so etwas tut, vermutet in der Regel Daten darauf, die dem Eigentümer wichtig sind und erhofft sich Angaben zu dessen Identität, um den Stick zurückgeben zu können. Natürlich müsste inzwischen jeder Computer-Nutzer wissen, dass ein solches Vorgehen aus IT-Security-Perspektive (http://www.computerwoche.de/a/wirkungslose-it-sicherheits-massnahmen,3229874) ein absolutes Unding ist. Trotzdem siegt bei nahezu der Hälfte der USB-Stick-Finder die Neugier über die Vernunft, wie eine aktuelle Untersuchung von Google und den Universitäten von Illinois und Michigan (https://zakird.com/papers/usb.pdf) zeigt.

Großbritannien: Cabinet Office

In Großbritannien gingen 2008 sicherheitspolitisch brisante Daten bezüglich Al-Qaida und den Irak aufgrund eines menschlichen Fehlers verloren. Ein Angestellter des Cabinet Office, welches direkt dem Premierminister und den Ministers of Cabinet untersteht, muss mit seinen Gedanken schon ganz im Feierabend gewesen sein, als er seine Arbeitsunterlagen in einem Pendelzug liegen ließ. Ein Fahrgast fand den Ordner mit den streng geheimen Dokumenten und übergab diesen der BBC, die ihn wiederum an die Polizei weiterleitete. Obwohl die Tagträumerei gerade noch einmal gut ging, wurde der Beamte daraufhin wegen Fahrlässigkeit suspendiert.
Mehr Infos (http://news.sky.com/story/611541/al-qaeda-data-blunder-official-suspended)

Foto: - shutterstock.com

Inside Job: Vom Mitarbeiter zum Hacker-Tool

Kriminelle Hacker sowie Industrie- und Wirtschaftsspione setzen gezielt auf dieses menschliche Verhalten (http://www.computerwoche.de/a/datenschutz-un-sicherheitsfaktor-mensch,3229132), um mit minimalem Aufwand in Unternehmensnetzwerke einzudringen und Daten zu stehlen. Dafür werden eigens präparierte Sticks - rein rechnerisch (siehe oben) genügen zwei bis drei - auf dem Parkplatz, vor dem Eingang, im Aufzug oder auf den Fluren abgelegt. Um nicht aufzufallen,

werden die USB-Köder meist nicht alle am selben Tag ausgelegt. Die Wahrscheinlichkeit, dass ein Finder das USB-Device in grenzenloser Naivität an seinen Rechner anschließt, statt ihn in der IT-Abteilung (http://www.computerwoche.de/a/it-abteilungen-sind-die-treiber-der-digitalisierung,3094502) abzugeben, ist äußerst hoch. Und selbst wenn nicht: Sollte der Finder zu der Gruppe derer gehören, die vorzugsweise per USB Dokumente transportiert, ist es nur eine Frage der Zeit, bis sich der Schadcode (http://www.computerwoche.de/a/die-gefaehrlichste-malware-2015,3221737) seinen Weg vom heimischen Rechner ins Unternehmensnetz gebahnt hat. Auch der schlagzeilenträchtige NSA-Spionage-Trojaner (http://www.computerwoche.de/a/cyberattacke-im-kanzleramt-wirft-weiter-fragen-auf,3091410) aus dem Jahr 2014 gelangte über einen privaten Rechner ins Bundeskanzleramt.

Das Auslegen manipulierter oder infizierter USB-Devices wird erst durch die menschliche Neugier zur effizientesten Methode der Industriespionage (http://www.computerwoche.de/a/spionage-im-cloud-zeitalter,3069427). In Sachen Aufwand und Erfolgsquote ist die Methode darüber hinaus auch jeder Social-Engineering-Kampagne (http://www.computerwoche.de/a/wie-sie-social-engineering-erkennen,3094016) oder dem klassischen Hack (http://www.computerwoche.de/a/die-groessten-cyberangriffe-auf-unternehmen,3214326) haushoch überlegen. Schließlich ist es deutlich einfacher einen Standort auszukundschaften und einen Stick abzulegen, als eine Firewall zu überwinden. USB-Sticks sind zudem inzwischen für wenig Geld zu haben, für die Modifizierung gibt es Bausätze, mit deren Hilfe auch mäßig begabte Anwender klarkommen dürften. Für die Spionage selbst bieten sich unterschiedliche Wege an: klassisch mittels Schadcode oder aber über die Manipulation der Firmware des Sticks.

Diese zielt darauf ab, dass sich der Stick dem PC gegenüber als ein anderes USB-Gerät ausgibt und sich beispielsweise als Tastatur am Rechner anmeldet. Dieses Verfahren ist auch als BadUSB (http://www.computerwoche.de/a/so-nutzen-sie-usb-weiter-sicher,3067048) bekannt. Der Stick kann dann - genauso wie ein menschlicher User - Befehle direkt an das Betriebssystem senden und beispielsweise Daten an einen Server übermitteln oder Schadsoftware von dort nachladen. So übernimmt ein unscheinbares USB-Device die Kontrolle über einen Rechner. Der Schadcode schützt sich dabei in der Regel mit unterschiedlichen Funktionen vor der Erkennung durch Virenscanner und lädt gegebenenfalls weitere Komponenten nach. Für den eigentlichen Diebstahl (http://www.computerwoche.de/a/5-4-millionen-dollar-kostet-ein-datendiebstahl,3090006) werden die Daten verschlüsselt und über erlaubte Protokolle an den externen Server versendet.

Die Top 15 Hacker-Angriffe auf Unternehmen

Unternehmen weltweit rücken seit Jahren in den Fokus von Hackern und Cyberkriminellen. Identitäts- und Datendiebstahl stehen bei den Anhängern der Computerkriminalität besonders hoch im Kurs - kein Wunder, dass Cyber-Risk-Versicherungen immer mehr in Mode kommen. Wir zeigen Ihnen 15 der größten Hacking-Attacken auf Unternehmen der letzten Jahre.

Foto: McIek - shutterstock.com

USB-Devices im Unternehmen: Ein Verbot ist nicht genug

Schulungen die über die Gefahren durch USB-Sticks aufklären und unternehmensinterne Regelungen zur Nutzung solcher Devices führen zwar dazu, dass weniger Mitarbeiter im Unternehmen nicht erwünschte Geräte nutzen. Allerdings zeigen zahlreiche Studien, dass sich ein beträchtlicher Teil der Mitarbeiter über solche Einschränkungen hinwegsetzt. Insbesondere dann, wenn die Mitarbeiter den Eindruck haben, dass die Regelungen ein effizientes Arbeiten (http://www.computerwoche.de/a/mit-itsm-kosten-sparen-und-effizient-arbeiten,3098383) be- oder verhindern. Und wenn der Baum dann brennt, wird die Präsentation eben doch schnell auf einen USB-Stick kopiert. Unternehmen, die bezüglich des Einsatzes von USB-Geräten ausschließlich auf Anweisungen beziehungsweise Verbote setzen, sollten damit rechnen, dass sie das Problem nicht aus der Welt schaffen können.

Da die Manipulation von Firmware nicht unmittelbar aufgedeckt werden kann und ein Schadcode leicht Antivirus-Software und Firewall (http://www.computerwoche.de/a/antivirus-ist-tot-die-security-trends-2016,3220280) austricksen kann, sollte die

Verwendung von USB-Sticks am Firmen-PC nicht nur durch Anweisungen geregelt werden, sondern zusätzlich durch eine technische Lösung überwacht und gegebenenfalls blockiert werden. Dafür sorgt die sogenannte Device-Control-Funktionalität (http://www.computerwoche.de/a/die-besten-loesungen-fuers-mobile-device-management,2547010). Sie ermöglicht als Kernkomponente - beispielsweise von Lösungen für Data Leak Prevention (http://www.computerwoche.de/a/sag-mir-wo-die-daten-sind,3228632) - die Identifizierung von USB-Geräten anhand Seriennummern und IDs und blockiert alle unbekannten und nicht eindeutig identifizierbaren Devices. Erst durch Device Control werden geschenkte, gefundene oder zugesteckte USB-Sticks aus dem Spiel genommen. Gute Systeme erkennen inzwischen auch BadUSB-Angriffe und blockieren die vermeintliche neue Tastatur, die ein manipulierter Stick zu sein vorgibt. Wenn USB-Sticks für spezielle Aufgaben erforderlich sein sollten, können diese im Rahmen eines White Listing über granulare Einstellmöglichkeiten für ausgewählte Rechner und Gruppen freigegeben werden. (fm)

Die Security-Trends 2016 **1/12**

Security-Trends 2016

Viren, Cyberkrime, Erpressung, Kreditkartenbetrug - die Liste der digitalen Gefahren im Internet ist mittlerweile langgeworden. Wir haben die Top-10-Bedrohungen für 2016 zusammengestellt.

Foto: wk1003mike - shutterstock.com