Peripherie

Gefährliche Mäuse

[22.11.2016] Um IT-Systeme abzusichern, genügt es nicht, lediglich aktuelle Anti-Viren-Programme zu installieren. Denn: Auch Peripheriegeräte sind Einfallstore für Schad-Software. Der Einsatz von speziellen Switches ist deshalb dringend zu empfehlen.

Hacker-Attacken auf Ämter und Behörden sind heute an der Tagesordnung. Zwar haben längst alle öffentlichen Institutionen in gewisser Weise darauf reagiert und auf den Servern und PCs sowie neueren Geräte-Klassen wie Tablets und Smartphones Anti-Viren-Software zum Schutz installiert. Firewalls und Software-Updates, Schulungen der Mitarbeiter und Zugangskontrollen ergänzen die Sicherheitsvorkehrungen.
Sind diese Mechanismen implementiert, ist alles gut – könnte man meinen. Doch dem ist bei Weitem nicht so. Die Bedrohungsszenarien sind mittlerweile so vielfältig, dass sich eine genauere Betrachtung eines normalen Büroarbeitsplatzes durchaus lohnt, um Schwachstellen zu erkennen, über die sich bisher vielleicht nicht jeder potenziell Betroffene ausreichend Gedanken gemacht hat. Denn für Hacker bietet sich eine Vielzahl weiterer Möglichkeiten, die Netzwerke zu infiltrieren. Peripheriegeräte wie Mäuse, Tastaturen, Drucker, Scanner, Multifunktionsgeräte und Monitore verfügen über interne Speicher. Versierte Hacker können sich dies zunutze machen, beispielsweise um möglichst wenig aufzufallen, wenn sie schädliche Software in scheinbar ungefährlichen Geräten platzieren.
Damit nicht nur die Netzwerk-Architektur sicher ist, sondern auch die andere Seite mit Maus, Tastatur, Monitoren und vielleicht noch einigen anderen Peripheriegeräten, ist der Einsatz sicherer KVM-Umschaltsysteme (Keyboard-, Video-, Maus-Switch) Pflicht. Geschieht das nicht, ist durch die Verbindung der unterschiedlichen Computer über gemeinsam genutzte Maus und Tastatur die Sicherheit plötzlich komplett ausgehebelt, denn auch USB-Geräte eignen sich als Einfallstore für Hacker.

Gefährlicher USB-Port

Entsprechend ist die Verbindung zwischen PC und Peripherie über den USB-Port ohne Überwachung extrem gefährlich. So geht die französische IT-Sicherheitsbehörde ANSSI davon aus, dass jedes zehnte persönliche Gerät, das an das Netzwerk des Arbeitgebers angeschlossen wird, durch Malware kompromittiert ist. Dabei sind das nur zufällige Attacken, die nicht per se auf eine Behörde zielen. Das Paradebeispiel sind USB-Speichersysteme, die aufgrund ihres geplanten Einsatzes geradezu prädestiniert sind, als Datenträger auch Malware in PC-Netzwerke zu tragen. Und dabei reicht es, dass nur ein einzelner Anwender eines Amtes oder einer Behörde sich keine Gedanken darüber macht, welche Schäden er unter Umständen anrichtet, wenn mal eben wichtige vertrauliche Daten mit dem USB-Stick von einem PC zum anderen transportiert werden, weil etwa der Server-Zugriff gerade nicht funktioniert oder der neue Kollege noch nicht alle Rechte im System hat.
Dabei sind schon heute genau dafür Switches verfügbar, die diese Schwachstellen beseitigen. So lassen sich über besondere Umschaltsysteme sichere Verbindungen zwischen PCs und Peripheriegeräten herstellen. Zu empfehlen sind dabei Switches, die zum einen über eine sehr feste Mechanik im USB-Port verfügen, sodass ein versehentliches Abstecken und dann ein Anschluss an einem nicht zugelassenen Port unmöglich sind.
Zum anderen müssen diese Switches besondere Konfigurationsmechanismen aufweisen. Beispielsweise sollten die IT-Administratoren sie so konfigurieren können, dass nur genau ein Typ Drucker, Tastatur und

Maus zugelassen ist. Darüber hinaus muss es möglich sein, bestimmte Geräteklassen wie USB-Speicher von der Nutzung auszuschließen, sodass diese direkt beim Einstecken in den USB-Port vom System zurückgewiesen werden.

Sicherheitsrichtlinien vorgeben

Um hier bestmögliche Ergebnisse zu erzielen, ist es unumgänglich, dass die IT-Verantwortlichen entsprechende Sicherheitsrichtlinien nicht nur vorgeben, sondern sich auch um deren korrekte Implementierung kümmern. Denn nur wenn der PC an sich sicher konfiguriert ist, können die Peripheriegeräte diese Sicherheit weiter ausbauen. Ist das jedoch nicht der Fall, so gleichen die sicheren Peripheriegeräte dies nicht aus, es fehlt schlicht die notwendige Basis.
Um all das noch ein bisschen komplizierter zu machen: Woher wissen die IT-Verantwortlichen nun, welche Systeme sie einsetzen sollen und welche besser nicht? Alle Lösungen, die verfügbar sind, selbst zu testen, übersteigt dann doch die Ressourcen nahezu aller IT-Abteilungen. Aber das ist auch gar nicht notwendig. Denn schon seit einigen Jahren können Anbieter ihre Hard- und Software ausführlich unter Sicherheitsaspekten testen und zertifizieren lassen. Wichtig ist dabei, dass es sich um eine unabhängige Zertifizierung handeln muss. Diese weist nach, dass es sich bei den Angaben der Hersteller nicht nur um eigene Marketing-Aussagen handelt, sondern dass die Lösungen Tests durchlaufen, und diese bestanden haben. Die bekannteste ist hierbei Common Criteria (CC), andere, zum Teil im Zusammenhang stehende, sind EAL (Evaluation Assurance Level) oder NIAP (National Information Assurance Partnership).
Bisher sind es vornehmlich Institutionen wie die NATO oder die Polizei, die hier die Vorreiter sind. Doch auch für Ämter und Behörden gilt, konsequent auf die vollumfängliche Sicherheit der Infrastruktur zu setzen. Die Konsequenz ist deshalb so wichtig, da für die Sicherheitsinfrastruktur genau das gleiche gilt, wie für eine Kette: Sie ist nur so stark, wie das schwächste Glied. Ist in der IT-Umgebung nur ein unsicherer Switch, so ist genau dieser ein lohnendes Ziel für Hacker. Das Einschleusen von Viren, Trojanern und dergleichen ins Netz kann dann verhältnismäßig einfach erfolgen. Und dieser eine Schwachpunkt macht – wie gezeigt – alle anderen Sicherheitsanstrengungen hinfällig und gefährdet nicht zuletzt die Sicherheit und Identität der Bürger.

()

Dieser Beitrag ist in der November-Ausgabe von Kommune21 im Schwerpunkt IT-Sicherheit erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Linksys, Peripheriegeräte