Security Insider

Best Practice für IT-Leiter und Geschäftsführer

An Patch-Management führt kein Weg vorbei

09.11.16 | Autor / Redakteur: Robert Korherr / Peter Schmitz

Jede Woche werden neue Sicherheitslücken entdeckt und Patches veröffentlicht, um sie zu schließen. Doch Hacker haben insbesondere bei längst bekannten Schwachstellen oft großen Erfolg. Denn viele IT-Verantwortliche vernachlässigen das Patch-Management – ein schwerwiegender Fehler.

2799 Sicherheitslücken wurden dieses Jahr bis Ende Juni alleine in den Top 50 der meist verwendeten Softwareprodukte verifiziert (Quelle: CVEdetails.com). Entsprechend müsste die zeitnahe Installation von Patches gegen bekannte Sicherheitslücken, in der Prioritätsliste von IT-Administratoren und CSOs eigentlich ganz oben stehen. Müsste! Denn die Realität, zumindest bei kleinen und mittleren Unternehmen, zeichnet ein anderes Bild. Wie sonst ist es beispielsweise zu erklären, dass für die im Jahr 2014 am häufigsten attackierten Sicherheitslücken jeweils bereits seit über einem Jahr ein Patch verfügbar gewesen wäre.

Allein in den Betriebssystemen und Applikationen der Top-5-Hersteller - gemessen an der Anzahl der bekannten Sicherheits-lücken - wurden im Jahr 2015 pro Arbeitstag durchschnittlich mehr als zwölf Schwachstellen erkannt, bei Einsatz von Produkten der Top-50 Hersteller sogar 23 pro Arbeitstag. Solch imposante Statistiken sind wahrscheinlich ein Grund dafür, das Thema Patch-Management vor lauter Resignation erst gar nicht anzupacken. Fast in jeder IT fehlt es schließlich an Zeit, Personal und häufig auch an geeigneten Werkzeugen für die Verteilung von Security-Patches und Updates. a

Zudem haben viele IT-Verantwortliche bereits die Erfahrung gemacht, dass Patch-Management per „Turnschuh-Administration“ langwierig, ineffizient und im Endeffekt zu teuer ist. Denn zu allem Übel ist für die Wirkungsweise von Sicherheits-Updates auch noch ganz entscheidend, wann sie eingespielt werden. (Standardapplikationen von Adobe, Apple, Oracle Java, Mozilla Firefox und Co sind für 86 % der Sicherheitslücken verantwortlich, Microsoft-Produkte sind längst weniger vertreten). Impfungen helfen auch nicht mehr, wenn der Erreger sich bereits im Körper ausgebreitet hat. Und so kann man mit einem verspäteten Sicherheitsupdate auch nur noch die multiple Infektion weiterer Systeme durch die identische Sicherheitslücke verhindern, nicht mehr aber den ursprünglichen Ausbruch der Krankheit. Und Angreifer benötigen in der Regel lediglich wenige Wochen oder maximal Monate, um einen Großteil der Sicherheitslücken auszunutzen.

Hacker lieben Oldies

Für Hacker sind gerade „Oldies“ besonders einfach anzugreifende und damit attraktive „Goldies“, denn „alte“ Lücken sind umfassend dokumentiert und Malware-Bausätze leicht verfügbar. Den Cyber-Kriminellen kommt zudem zugute, dass viele Unternehmen beim Patch-Management offenbar nach dem Motto „Aus den Augen, aus dem Sinn“ verfahren. Damit ist auch der Umstand erklärbar, dass nur wenige CVEs (Common Vulnerabilities and Exposures: Industriestandard für eindeutige Sicherheitslücken) für den weitaus größten Anteil der ausgenutzten Sicherheitsschwächen verantwortlich sind. 2014 waren zehn bekannte Sicherheitslücken für 97 % der Angriffe verantwortlich, obwohl Patches dafür längst verfügbar waren.

Letztendlich ist aber fast jede Sicherheitslücke vor einer Patch-Freigabe bereits ein Oldie. Denn die wichtigsten Anbieter benötigen durchschnittlich drei Monate ab Bekanntwerden der Sicherheitslücke, bis sie überhaupt eine entsprechende Problemlösung liefern können.

Das Risiko bis zur Patch-Veröffentlichung liegt nicht in der Verantwortung der IT. Ab der Freigabe von Patches lebt die potenzielle Haftung wegen möglicher „Fahrlässigkeit“ bei IT-Verantwortlichen oder der Geschäftsleitung aber durchaus auf. Wer kann schon behaupten, von der Notwendigkeit von Patch-Management nichts gewusst zu haben?

Anti-Malware alleine reicht nicht aus

Anti-Viren Lösungen versuchen schädliche Software fernzuhalten, um damit eine Infektion bereits im Vorfeld zu verhindern. Patches schließen die bekannten Angriffsziele von Mal- und Ransomware, indem die betroffenen Sicherheitslücken geschlossen werden und damit von Schadsoftware nicht mehr kompromittiert werden können. Bei über 60 % aller Angriffe öffnen die eigenen Mitarbeiter dem Schädling meist aus Unwissenheit oder Neugier die Tür und unterziehen nicht nur die FrontendIT, sondern das gesamte Netzwerk durch USB-Malware oder Phishing-Attachments einem Stresstest. Sehr ungünstig dann, wenn die aktuelle Malware-Signatur den Virus noch nicht erkennt und die Sicherheitslücke noch besteht.

Patchen gegen Phishing

Früher war alles besser, zumindest bei Phishing-E-Mails. Schlecht getarnte Absenderadressen, auffällig viele orthografische und grammatikalische Fehler, die selbst simpelste Online-Übersetzungstools besser umsetzen hätten können oder eine steinreiche Verwandtschaft in Kenia, die man beerbt hat, deuteten schon auf den ersten Blick auf betrügerische E-Mails mit schlechten Absichten hin. Wie viele Anwender aber vermutlich selbst bestätigen können, reicht der erste Blick auf potenzielle Phishing-Mails seit einiger Zeit oft nicht mehr aus. Phishing wird immer professioneller und dementsprechend steigt die Anzahl der Empfänger, die die betrügerischen Absichten hinter der E-Mail nicht sofort erkennen. Dabei ist das reine Öffnen der Phishing-Mails meist ungefährlich –

doch auch die Zahl der Anwender, die ein Attachment öffnen, nimmt durch die steigende Professionalisierung der „Phisher“ stetig zu. Die bösartigen Anhänge in den Mails können nur dann den größtmöglichen Schaden erreichen, wenn sie sich auf bekannte Sicherheitslücken in Standard Betriebssystemen und -Applikationen stürzen.

Richtig patchen!

Häufig existiert noch die Meinung, dass Betriebssysteme und Applikationen von Microsoft mit Abstand am meisten attackiert werden und es deshalb reicht, die Security Bulletins von Microsoft zu verteilen. Aber: Hacker lernen schnell. Inzwischen entfällt ein Großteil der ausgenutzten Schwachstellen auf früher eher wenig beachtete Standardapplikationen von Herstellern wie Apple, Adobe, Mozilla, Oracle, Google usw. Die Verteilung von Microsoft Patches kurz nach dem Patch-Tuesday ist natürlich sehr wichtig – sie allein ist aber unzureichend. Die am meisten gefährdeten Applikationen sind in der Regel die verschiedenen Internet-Browser aller Hersteller sowie die dort eingesetzten Player und Reader. Bei den Betriebssystemen ist seit kurzem auch Mac OS besonders gefährdet.

Server und Business-kritische Applikationen

Bei kritischen Servern und Applikationen kommt die schöne Welt der Patch-Automatisierung in einigen Fällen ins Stocken. Durch die individuelle Konfiguration jedes Servers ist nicht immer eindeutig klar, ob das Patchen am Ende erfolgreich sein wird oder zum temporären Ausfall und damit zu Unproduktivität führt. Hier helfen Testumgebungen mit Kopien aller wichtigen produktiven Systeme und die Unterstützung von Power-Usern während der Patch-Evaluierung. Bei geschäftskritischen Applikationen wie zum Beispiel dem zentralen CRM geben die Hersteller vor, welche aktuellen Sicherheitsupdates installiert werden dürfen. Manchmal ist zunächst ein Patch des CRM-Herstellers erforderlich, bevor das eigentliche Sicherheitsupdate eingespielt werden kann. Immer wieder gibt es aber auch Szenarien,

in denen kritische Server teilweise „ungepatcht“ bleiben müssen. Diese Systeme stellen damit bis auf absehbare Zeit ein Sicherheitsrisiko dar und müssen engmaschig überwacht oder zusätzlich anderweitig geschützt werden. In diesem Fall kann beispielsweise die Aufteilung von Applikations-Komponenten wie zum Beispiel der Datenbank-Software auf andere Serversysteme das entstehende Risiko reduzieren, da einige Bestandteile für sich unter Umständen gepatcht werden können. Hilfreich ist zudem eine Gruppierung der Workstations und Server nach Funktionen, Bereichen und Standorten, um jederzeit den Überblick zu bewahren und nicht durch versehentliche Patch-Installation „Downtime“ zu verursachen. Bei virtualisierten Servern kann ein Angriff auf das Host-System auch Folgen für die Gast-Systeme haben, indem es sich innerhalb der physikalischen Hardware mehrfach repliziert. Das Patch-Management darf also virtuelle Server-Instanzen nicht ausklammern und muss Host, Gast und Templates aktiv patchen können - egal ob diese gerade online oder offline sind. Bei allen oben erwähnten Systemen stellt das noch verfügbare Zeitfenster für die Patch-Verteilung ein grundlegendes Problem dar. Scheduler, Power-Management und Scripting zur weitgehenden Automatisierung getesteter Workflows sind bei kritischen Systemen und Applikationen essenziell.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) rät: „Grundsätzlich ist eine unverzügliche Einspielung von Sicherheits-updates direkt nach Verfügbarkeit zwingend, um das Zeitfenster, in dem die Systeme verwundbar sind, so klein wie möglich zu halten“ (BSI: Lage der IT-Sicherheit in Deutschland 2015).

Viele Infektionskrankheiten lassen sich durch wirkungsvolle Maßnahmen wie Impfungen vermeiden. Auch beim Schutz der IT zählt Patch-Management zu den wichtigsten Basics für einen funktionierenden IT-Grundschutz. Anhand der obigen Fakten kann man erkennen, dass Patch-Management kein Nebenjob sein kann.