Windows Update im Griff

Warum regelmäßige Patches so wichtig sind

Ein Windows ohne aktuelle Updates ist wie Autobahn fahren ohne Sicherheitsgurte und Airbags: Wenn etwas passiert, ist der Schaden groß. Die automatische Update-Suche ist eine der wichtigsten Maßnahmen, um den eigenen Rechner vor Angreifern zu schützen.

Von Ronald Eikenberg und Hajo Schulz

Windows-Updates kommen immer zur Unzeit und bremsen den Rechner aus, manche schleusen gar neue Fehler ins System ein. Sie nicht regelmäßig einzuspielen, ist aber auch keine Lösung: Die Patches, die Microsoft traditionell allmonatlich am zweiten Dienstagabend herausgibt, beseitigen nicht nur nervige Bugs und installieren neue Funktionen, sie stopfen in der Regel auch Sicherheitslücken. Ist Ihr System nicht auf dem aktuellen Patch-Stand, sind Sie leichte Beute für Online-Ganoven. Bereits der Aufruf einer Webseite kann dann fatale Folgen haben und etwa dazu führen, dass Spione und Botnetz-Betreiber beliebigen Schadcode auf Ihrem Rechner ausführen können.

Dass Windows Update regelmäßig nach neuen Patches Ausschau hält, ist also unverzichtbar. Dass es die normale Rechnernutzung dabei so wenig wie möglich stört, ist gut für den Blutdruck und sorgt dafür, dass man die automatischen Updates nicht doch irgendwann entnervt abschaltet. Die folgenden Artikel verraten die wichtigsten Handgriffe für einen reibungslosen Betrieb: Ab Seite 102 gehen wir der Frage nach, warum die Update-Suche in Windows 7 und 8.1 manchmal selbst nach Stunden noch nicht am Ziel ist und wie man ihr auf die Sprünge hilft.

Wo die älteren Windows-Versionen gelegentlich zu lange für die Updates brauchen, geht Windows 10 eher zu forsch ans Werk und lädt mehr als nötig oder startet den Rechner neu, wenn er eigentlich noch mit anderen Dingen beschäftigt ist. Wie man hier eingreifen kann, erklären wir ab Seite 106.

Einen Blick hinter die Kulissen von Windows Update wirft der Artikel auf Seite 112: Er erläutert die wichtigsten Fachbegriffe und klärt, wie sie zusammenhängen.

Grundschutz

Zugegeben: Für Anwender, die Wert auf Sicherheit legen, ist es mit dem regelmäßigen Einspielen von Windows-Patches nicht getan. Auch alle anderen Anwendungen, Plug-ins und Browser-Erweiterungen sollten auf dem aktuellen Stand sein. Windows Update kümmert sich lediglich um Windows und Zubehör sowie auf Wunsch um weitere Microsoft-Programme wie Office. Seit Windows 8 hält der Update-Prozess zudem die von den MS-Browsern (Internet Explorer und Edge) genutzte Flash-Installation auf dem aktuellen Stand.

Ist Ihr System nicht auf dem aktuellen Patch-Stand, sind Sie leichte Beute für Online-Ganoven.

Alles andere liegt in der Verantwortung des Nutzers. Insbesondere Programme, die häufig Kontakt mit Daten aus dem Netz haben, sollte man regelmäßig auf den aktuellen und somit sichersten Stand bringen. Dazu zählen Browser wie Chrome und Firefox, Adobe Reader, Flash und Java – sofern Sie letzteres immer noch installiert haben. Grundsätzlich gilt: Je weniger Komponenten installiert sind, desto weniger potenzielle Schlupflöcher gibt es. Zudem sollten Sie ein Virenschutzprogramm mit aktuellen Signaturen einsetzen. Einen ausreichenden Grundschutz liefert bereits der seit Windows 8 vorinstallierte Windows Defender.

Gegen die gegenwärtig größte Gefahr aus dem Netz helfen vor allem Backups: Erpressungs-Trojaner verschlüsseln die Dateien des Anwenders und geben sie erst nach Zahlung eines Lösegelds wieder frei. Macht sich so ein Programm trotz aller Vorsichtsmaßnahmen über Ihren Rechner her, sind Sie fein raus: Sie stellen Ihre Fotos, Dokumente und was Ihnen sonst wichtig ist einfach aus einer möglichst aktuellen Sicherung wieder her, statt den Erpressern Geld in den Rachen zu werfen [1].

All diese Maßnahmen ersetzen aber nicht den gesunden Menschenverstand und ein Betriebssystem, das es Malware so schwer wie möglich macht, sich einzunisten. Viren, Trojaner und andere Schädlinge verwenden vor allem zwei Methoden, um in ein System einzudringen: Social Engineering und das Ausnutzen von Schwachstellen im System. Bei der ersten wird dem Anwender vorgegaukelt, dass es sich bei der Datei, die er da jetzt gerade anklickt, um etwas ganz anderes handelt. Dagegen hilft neben einem Virenscanner mit aktuellen Signaturen nur ein gehöriges Maß an Misstrauen gegenüber Software und anderen Dateien aus unbekannten Quellen. Unangekündigte Anhänge in E-Mails, seltsame Fehlermeldungen auf Webseiten mit angeblich kostenlosen und legalen Kinofilmen, der neueste Spiele-Blockbuster auf einem USB-Stick vom Freund eines Freundes – all das sollte die Alarmglocken schrillen lassen, statt einen unüberlegten Klick-Reflex auszulösen.

Wenn diese Vorsichtsmaßnahmen versagen, braucht ein Schädling immer

noch erhöhte Rechte, um beispielsweise Systemdateien zu infizieren. Unbemerkt schafft er das nur, indem er eine bekannte Schwachstelle ausnutzt. Weil Windows das mit Abstand weltweit am meisten genutzte Software-Paket ist, stellt es natürlich auch das lohnendste Ziel für solche Angriffe dar. Sie zu unterbinden gelingt nur, wenn bekannt gewordene Sicherheitslücken möglichst schnell geschlossen werden. Dazu ist das zeitnahe Einspielen von Patches des Softwareherstellers unerlässlich.

225 Lücken in Windows 10

Anlässlich des bei Redaktionsschluss letzten Windows-Patchdays im Dezember 2016 stopften allein sechs der veröffentlichten Updates Lücken, die Microsoft als „kritisch“ einstuft – das ist die höchste Gefahrenstufe. Microsoft nutzt sie für Schwachstellen, durch die ein Angreifer beliebigen Code ohne Zutun des Nutzers einschleusen und ausführen kann.

Schwachstellen-Datenbank „CVE Details“ zählte bisher 225 Sicherheitslücken in Windows 10 – 172 davon im vergangenen Jahr. Rund jede fünfte davon kann ein Angreifer zum Einschleusen von Code missbrauchen, mehr als ein Drittel eignet sich für eine Ausweitung der Nutzerrechte – also etwa, um Befehle mit Systemrechten auszuführen, obwohl das aktive Nutzerkonto lediglich eingeschränkte Rechte hat. Die Dunkelziffer der gefundenen Schwachstellen dürfte noch höher sein, da die Datenbank ausschließlich Lücken berücksichtigt, denen eine sogenannte CVE-Nummer zugeteilt wurde. Dabei handelt es sich um eine international anerkannte Identifikationsnummer, anhand derer man Schwachstellen eindeutig zuordnen kann. Nicht jede Lücke bekommt jedoch eine CVE-Nummer und taucht in der zitierten Statistik auf.

Mit jedem veröffentlichten Patch spitzt sich die Lage für all jene zu, die ihr System nicht auf dem aktuellen Stand halten: Schwachstellen, die zuvor lediglich einem ausgewählten Kreis zugänglich waren und nur für gezielte Attacken ausgenutzt wurden, werden durch die Patches einer breiten Masse bekannt. Mit jedem Patchday nimmt die Zahl der öffentlich bekannten Windows-Lücken zu und damit wächst auch das Waffenarsenal der Online-Schurken. Während die Systeme der einen immer sicherer werden, ähneln die Windows-Installationen der Patch-Verweigerer mehr und mehr einem Schweizer Käse.

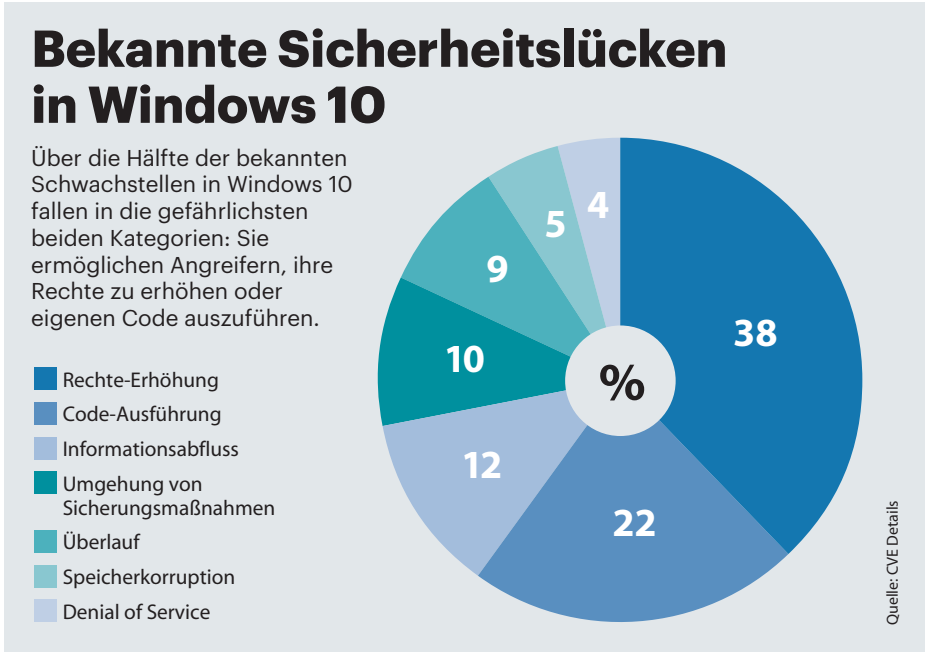
Besonders dramatisch ist die Lage für unverbesserliche XP-Anhänger: Das Steinzeit-Betriebssystem erhält nun schon seit fast drei Jahren keine offiziellen Sicherheits-Updates aus Redmond mehr. Wer das System noch heute ins Internet lässt, handelt grob fahrlässig. Desgleichen kann der Kontakt mit jeglichen anderen Daten, die nicht absolut vertrauenswürdig sind – etwa von USB-Sticks –, gefährlich enden. Auch wenn es in letzter Zeit keine Schlagzeilen über massenhaft gehackte XP-Systeme gab: Die Lücke, die morgen bekannt wird, bleibt ungestopft und setzt die Anwender einem unbekannten Risiko aus.

Das gleiche Schicksal ereilt auch Vista-Nutzer schon sehr bald: Laut derzeitiger Planung wird Microsoft nach dem 11. April dieses Jahres keine Sicherheitslücken in Windows Vista mehr stopfen. Bei Windows 7 ist 2020 Schluss, bei Version 8 zieht Microsoft drei Jahre später den Stecker. Für die aktuelle Version 10 hingegen gibt es bislang gar kein Support-Ende: Dank „Windows as a Service“ verspricht Microsoft, das System dauerhaft mit Security-Updates zu versorgen, sofern man denn brav alle Versions-Upgrades mitmacht.

Neue Schutzfunktionen

Microsoft reagiert nicht nur auf bekannte Sicherheitslücken, sondern versucht auch Angriffe durch bisher unbekannte Schwachstellen im Vorfeld durch neue Schutzfunktionen zu vereiteln. So hat das Unternehmen mit dem im August 2016 veröffentlichten Anniversary Update für Windows 10 am Kernel geschraubt und ihn gegen diverse Exploit-Techniken abgesichert. Für die Nutzer sollte sich das schon kurze Zeit später auszahlen: Googles Sicherheitsteam entdeckte im Oktober eine ausgefeilte Spear-Phishing-Kampagne, in deren Rahmen zwei bisher unbekannte Schwachstellen ausgenutzt wurden – eine in Adobe Flash und eine im Windows-Kernel. Durch die Flash-Lücke sind die Täter in die Systeme eingestiegen, die Windows-Lücke missbrauchten Sie für einen Ausbruch aus der Browser-Sandbox.

Nach Angaben von Microsoft klaffte die Lücke zwar im Kernel aller Windows-Versionen, die neuen Sicherheitsvorkehrungen des Anniversary Update von Windows 10 hätten die Ausführung des Exploits jedoch verhindern können. Die ausgenutzte Schwachstelle schloss Microsoft im Zuge seines regulären November-Patchdays. *(hos@ct.de)* c't



Literatur

[1] Ronald Eikenberg, Erpresser-Schutz, Windows und Daten gegen Erpressungs-Trojaner wappnen, c't 7/16, S. 78

CVE Details, Literatur: ***ct.de/ydzv***