Windows-7-Ende

Am 14. Januar 2020 endet der Support für Windows 7. Doch was bedeutet das eigentlich genau und welche Auswirkungen hat es? c't beantwortet die wichtigsten Fragen.

Von Axel Vahldiek

Bedeutung

Welche Auswirkungen hat das Support-Ende genau?

Im Grunde nur eine: Microsoft wird nach diesem Zeitpunkt keine kostenlosen Sicherheitsupdates mehr zur Verfügung stellen. Kostenpflichtig sind solche Updates für Firmen weiterhin verfügbar, für Privatkunden hingegen nicht.

Sonst ändert sich nichts. Andere Updates für Windows 7 stellt Microsoft ohnehin schon seit 2015 nicht mehr zur Verfügung. Was hingegen bleiben wird, sind die Angebote, die Microsoft als „Hilfe zur Selbsthilfe" bezeichnet. Gemeint sind etwa die Artikel der Knowledge-Base (https://support.microsoft.com) und die Hilfeforen unter https://answers.microsoft.com. Sicherer wird eine Windows-7-Installation dadurch aber nicht.

Windows 7 bleibt weiterhin voll funktionstüchtig, läuft also auch nach dem Support-Ende weiter (sofern es nicht durch Viren oder Ähnliches lahmgelegt wird). Es lässt sich neu installieren, sofern das nicht etwa am fehlenden DVD-Laufwerk, an zu moderner Hardware (USB 3.x, UEFI, Secure Boot ...) oder fehlenden Treibern scheitert. Das Aktivieren bleibt möglich und notwendig, die Aktivierungsserver werden nicht abgeschaltet. Windows 7 wird auch nicht zur Freeware, die nun jeder kostenlos nutzen dürfte.

Windows 7 ausgereift

Da Windows 7 nun schon über zehn Jahre alt ist: Stecken da überhaupt noch Sicherheitsprobleme drin? Die sollten doch so langsam mal alle gefunden worden sein, oder?

Leider ist das Gegenteil der Fall, und das ist kein Zufall, denn während Windows 7 technisch immer noch auf dem Stand von 2009 steht, haben Angreifer heutzutage breiteres Wissen und besseres Werkzeug zur Verfügung. Das führt dazu, dass die Anzahl der in Windows 7 neu entdeckten Sicherheitslücken sogar steigt.

Das lässt sich mit Zahlen belegen: Die Datenbank „CVE Details" verzeichnete von 2009 (Veröffentlichung von Windows 7) bis 2019 insgesamt 1283 Probleme, doch 641 davon wurden erst in den letzten drei Jahren gefunden – 2019 wurde mit 250 neu entdeckten Lücken sogar der bisherige Höchststand von 2017 übertroffen, obwohl das Jahr noch nicht zu Ende ist. Von diesen Lücken sind zwar zugegebenermaßen nicht alle gleichermaßen dramatisch. Doch wenn man sich nur die besonders gefährlichen Lücken ansieht, die das Einschleusen und Ausführen beliebigen Codes erlauben (code execution), sind die Zahlen sogar noch deutlicher: Von insgesamt 372 Code-Execution-Lücken wurden 100 erst 2019 entdeckt.

Auswirkungen

Ist mein PC ohne Updates konkreten Gefahren ausgesetzt?

Ob wirklich etwas passieren wird, lässt sich seriös nicht vorhersagen, doch ein Blick in die Vergangenheit ist lehrreich: 2017 beispielsweise kompromittierten die Krypto-Trojaner WannaCry und Petya durch den EternalBlue-Exploit ungepatchte PCs, und zwar übers Netz und ganz ohne Nutzeraktion. Für XP gab es seinerzeit keine Updates, sodass XP-Installationen besonders betroffen waren. Solche Gefahren drohen nun auch Windows 7.

Virenscanner als Ersatz?

Reicht es nicht aus, einfach einen aktuellen Virenscanner zu installieren?

Nein. Ein Virenscanner kann immer nur ein Teil einer Sicherheitsstrategie sein, ebenso wie Backup, Firewall, Verschlüsselung, Software Restriction Policies, Skriptblocker im Browser und so weiter. Und auch Sicherheitsupdates sind ein solcher Baustein. Das Titelthema in c't 10/2017 hat das in mehreren Artikeln detailliert erklärt und Tipps zu den einzelnen Bausteinen gegeben.

Die Rolle der Updates besteht darin, Einfallstore zu schließen, denn jedes geschlossene ist eines, das Angreifern nicht mehr offen steht. Das gilt übrigens keineswegs nur für Windows, sondern auch für alle Anwendungen. Um es aber auch ganz deutlich zu sagen: Kein einzelner Baustein kann echte Sicherheit garantieren, das können nicht mal alle zusammen. Anders formuliert: Nur ein ausgeschalteter PC ist vor Schädlingen wirklich geschützt. Aber jeder einzelne Baustein trägt dazu bei, das Risiko zu minimieren, und es gibt keinen vernünftigen Grund, auch nur auf einen davon zu verzichten.

Recht auf Updates

Kann man Microsoft juristisch zwingen, weiterhin Updates für Windows 7 zur Verfügung zu stellen?

Vergessen Sie das: Alle Garantie- und Gewährleistungspflichten sind zehn Jahre nach der Veröffentlichung von Windows 7 längst abgelaufen, und Verbraucherfreundlichkeit ist nicht einklagbar. Hinzu kommt, dass Microsoft in vielen Fällen ohnehin zu keinerlei Unterstützung verpflichtet ist. Denn das ist stets nur der Vertragspartner, und das ist gerade bei Privatkunden üblicherweise nicht Microsoft selbst, sondern der Händler, bei dem man Windows solo oder als Vorinstallation auf einem PC erworben hat.

Alte Updates

Bedeutet das Support-Ende, dass sich die bereits erschienenen Updates für Windows 7 auch nicht mehr herunterladen lassen?

Nein, es gibt nur keine neuen mehr. Die bereits erschienenen bleiben verfügbar. Wie lange, weiß zwar nur Microsoft, doch wenn man im Update-Katalog nach Updates für Windows XP sucht, findet man immer noch alle bis Support-Ende veröffentlichten Sicherheitsupdates (https://www.catalog.update.microsoft.com).

Updates auf anderen Wegen?

Kann man sich Sicherheitsupdates nicht auch irgendwie anders besorgen?

Falls jemand verspricht, an Microsofts Stelle Updates liefern zu wollen, dann dürften das zumeist nur Workarounds sein, also der Versuch, das System irgendwie so zu schützen, dass Sicherheitslücken nicht ausnutzbar sind. Schadsoftware könnte solche Workarounds aber umgehen.

Denkbar ist allerdings, dass es nach dem Support-Ende irgendwie gelingt, von Microsoft selbst bereitgestellte Updates in Systeme zu fummeln, für die sie eigentlich nicht gedacht sind. Bei Windows XP etwa gab es einen Hack, mit dem man Updates für eine Version namens „Windows Embedded POSReady 2009“ installieren konnte. Diese Version basierte auf XP, war aber eben nicht XP. Als Folge waren die Updates nicht auf herkömmlichen XP-Installationen getestet. Was noch gravierender war: Die Updates sollten nur Sicherheitslücken in der POSReady-Version schließen. Die war im Vergleich zu herkömmlichem XP aber stark eingeschränkt (weil nur für Kassensysteme gedacht). In XP steckten also naturgemäß mehr Lücken als in POSReady, und diese zusätzlichen Lücken blieben offen. Kurzum: Mit so einem Hack holt man sich Updates ins System, die nicht alle Lücken schließen und ungetestet sind, also Nebenwirkungen haben können. Falls Sie trotzdem vor solchen Hacks nicht zurückscheuen: Viel Glück, aber Sie machen das auf eigenes Risiko. Wir empfehlen, es lieber zu lassen.

Sicherheitslücken in Windows 7

Die Anzahl der pro Jahr gefundenen Sicherheitslücken in Windows 7 sinkt nicht etwa, sondern steigt stetig. 2019 erreichte sie einen neuen Höchststand.

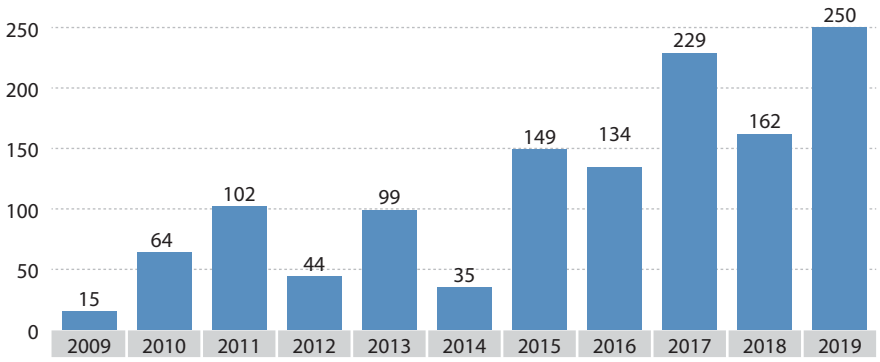


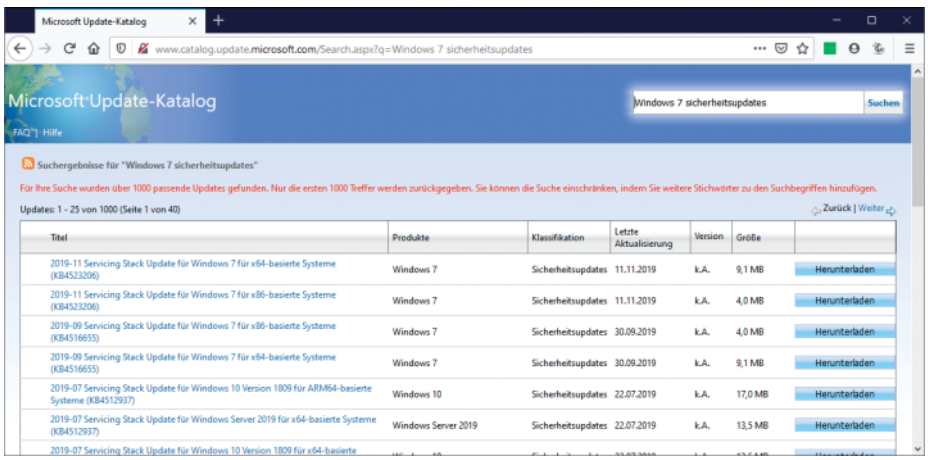
Bild: CVE Details

Endlich kein Stress mehr

Also ich freu mich darauf, wenn der monatliche Update-Stress endlich vorbei ist.

Freuen Sie sich nicht zu früh: Wenn durch eine offen gebliebene Sicherheitslücke erst mal ein Schädling eingedrungen ist, haben Sie mit der Beseitigung des Schadens mutmaßlich weit mehr Arbeit als nur einmal pro Monat einen Neustart durchzustehen. Und während Updates üblicherweise nur am Patchday einmal pro Monat erscheinen, greifen die Schädlinge das ganze Jahr rund um die Uhr an. So gesehen: Ja, das Einspielen von Updates mag nervig sein, doch das Beseitigen von durch fehlende Updates verursachten Schäden ist noch weit nerviger.

(axv@ct.de)



Es wird zwar keine neuen Sicherheits-Updates für Windows 7 geben, die bereits veröffentlichten dürften aber bis auf Weiteres verfügbar bleiben.

CVE Details: ***ct.de/y51q***