In Windows 10 klafft eine gefährliche Lücke

11.03.2020 10:33:24 | AH-WEB, Adrian Hetzke | 0 Kommentare
Offenbar macht Microsoft aus Versehen bekannt, dass in Windows 10 eine Sicherheitslücke klafft, die noch durch kein Update geschlossen werden kann. Eine spezielle Eigenschaft macht die Schwachstelle besonders gefährlich.
Aktuell verteilt Microsoft Updates für Windows 10, die insgesamt 117 Schwachstellen beseitigt. Unter ihnen befindet sich allerdings keine Aktualisierung, die eine besonders gefährliche Lücke schließen könnte, die in einem Protokoll (SMBv3) des Betriebssystems klafft, das den Zugriff auf Netzwerkdateien regelt. Das bedeutet, dass sie ein offenes Tor für Angriffe aus der Ferne darstellt. Betroffen sind neben Windows-10-Rechnern auch Windows Server.

So gefährlich wie WannaCry?

Besonders gefährlich macht die Schwachstelle, dass sie den Weg für Malware freimacht, die sich wurmartig weiterverbreiten kann. Dazu genügt es offenbar, dass ein Rechner mit einem infizierten SMBv3-Server verbunden ist, der schadhaften Code verschickt, der auf dem angegriffenen System dann ausgeführt werden kann. Auf ähnliche Weise verbreitete sich 2017 der Erpresser-Trojaner WannaCry, der weltweit enorm großen Schaden anrichtete.

Eigentlich hätte das Problem noch nicht bekannt gemacht werden sollen, da Microsoft noch keinen Patch hat. Doch laut "Winfuture" war ein Update offenbar geplant, weswegen das Unternehmen vorab bereits Sicherheitsanbieter informierte, die wiederum die Schwachstelle publik machten.

Einfache Notfallmassnahmen

Microsoft hat reagiert und Massnahmen veröffentlicht, mit denen betroffene Systeme notdürftig geschützt werden können, bis ein Patch zur Verfügung steht. Unter anderem empfiehlt das Unternehmen die Kompression des betroffenen Protokolls zu deaktivieren. Dazu genügt die Eingabe eines Befehls in die Windows PowerShell. Man findet sie am einfachsten, indem man "PowerShell" ins Suchfenster links unten in der Taskleiste eingibt. Den Befehl kopiert man sich einfach von der Microsoft-Seite, er steht unter "Problemumgehungen" im ersten grauen Feld. Um diese Maßnahme durchzuführen sind Administrator-Rechte nötig.

Außerdem rät Microsoft in der Firewall den TCP-Port 445 zu schließen, beziehungsweise zu überprüfen, dass er blockiert ist. Die Windows-Firewall findet man, wenn man im Suchfenster "Firewall" eingibt und dann in den Suchergebnissen unter Apps *Windows Defender Firewall mit erweiterter Sicherheit* auswählt.

Dort klickt man im Menü links oben auf *Eingehende Regeln* und dann rechts im Menü unter Aktionen auf *Neue Regel*. Im sich öffnenden Fenster wählt man *Port* aus und klickt auf *Weiter*. Im nächsten Fenster tippt man dann ins Eingabefenster "445" und klickt dann wieder auf *Weiter*. Dann wählt man *Verbindung blockieren* aus und klickt im danach zweimal auf *Weiter*. Zum Schluss gibt man für die Regel noch einen Namen ein. So kann man sie leicht wiederfinden und löschen beziehungsweise den Port freigeben. Ist das erledigt, klickt man auf *Fertigstellen*.

Quelle: ntv.de, kwe

- Version zum Drucken
- Newsletter abonnieren

Keine Kommentare vorhanden.

Datenschutz-Einstellungen

Diese Website verwendet Cookies und Targeting Technologien, um Ihnen ein besseres Internet-Erlebnis zu ermöglichen. Diese Technologien nutzen wir außerdem, um Ergebnisse zu messen, um zu verstehen, woher unsere Besucher kommen oder um unsere Website weiter zu entwickeln. Weitere Informationen zu Cookies erhalten Sie in unserer Datenschutzerklärung und im Impressum.

Details Nur essentielle Alle akzeptieren
Notwendig Notwendige Cookies helfen dabei, eine Webseite nutzbar zu machen, indem sie Grundfunktionen wie Seitennavigation und Zugriff auf sichere Bereiche der Webseite ermöglichen. Die Webseite kann ohne diese Cookies nicht richtig funktionieren. ☐ Details anzeigen
NameBesuchersitzung ZweckLogin, Warenkorb. Wird nur gesetzt, wenn ein entsprechendes Feature verwendet wird. Cookie NamenPHPSESSID, clxsid
NameFrontend Sprache ZweckDie gewählte Sprache im Frontend. Cookie NamenlangId
NameDatenschutzhinweis ZweckEinstellungen des Datenschutzhinweises merken. Cookie NamenClxCookieNote
Schliessen