

Windows XP Quellcode wurde angeblich ge-leaked – Ein potentielles Risiko für viele Millionen Nutzer und KRITIS-Unternehmen

Bochum (Deutschland), 25. September 2019

Einigen Medienberichten zufolge zirkuliert derzeit der Quellcode von Microsofts Windows XP frei zugänglich im Internet. Den Quellen zufolge erschien das knapp 43 Gigabyte große Datenpaket zunächst auf 4chan und wird derzeit über Torrents im Internet ausgetauscht. Der Torrent enthält neben dem Quellcode von Windows XP unter anderem auch die Quellcodes von Windows 2000/NT/CE/Embedded sowie MS DOS, jeweils in verschiedenen Versionen. Die Daten sind angeblich bereits seit Jahren in Kreisen von Cyberkriminellen geteilt worden, gelangten mit dem aktuellen Leak jedoch das erste Mal in greifbare Nähe für die Öffentlichkeit.



„Sollte sich die Echtheit des Leaks bestätigen wäre das eine sehr schlechte Nachricht für viele Unternehmen. Denn Windows XP-Rechner sind in der Anlagensteuerung noch häufiger in Benutzung, als vielen bewusst ist. Auch Betreiber kritischer Infrastrukturen (KRITIS) könnten getroffen werden, wenn in der Folge des Leaks weitere Schwachstellen in dem Betriebssystem gefunden werden. Diese sollten jetzt dringend Konzepte erstellen, um möglicherweise vorhandene XP-Systeme in ihrem Netzwerk wirkungsvoll zu isolieren“, Hauke Gierow, Sicherheitsexperte bei G DATA CyberDefense.

Sollten diese Quellcodes legitim sein – eine endgültige Prüfung steht noch aus und wird wohl noch Tage auf sich warten lassen – bedeutet das zum einen höchste Gefahr für alle verbliebenen Nutzer der entsprechenden Betriebssysteme. Windows XP läuft auf immerhin 0,82 Prozent aller Windows-Rechner sowie auf vielen Bankautomaten und in älteren Produktionsanlagen. Das letzte Sicherheitsupdate für Windows XP kam 2014 heraus; seitdem hat Microsoft seinen Support eingestellt.

Cyberkriminelle könnten innerhalb kurzer Zeit einen sehr detaillierten Einblick über die verbliebenen Schwachstellen von Windows XP erhalten und kurze Zeit später die erste Welle speziell angefertigter Schadprogramme ausrollen. Allen Nutzern von Windows XP ist nun dringlich angeraten, ihr Betriebssystem auf die aktuelle Windowsversion (Windows 10) zu aktualisieren.

Es bleibt zu hoffen, dass Microsoft schnell auf diesen Vorfall reagiert und alle Gemeinsamkeiten mit ihren aktuellen Betriebssystemen – vor allem Windows 10 – auslötet, um potenzielle Sicherheitslücken zu stopfen. Betreiber von alten Industrieanlagen und von Bankautomaten sollten sich umgehend um

G DATA CyberDefense AG Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299

Pressemitteilung

Klarheit kümmern, ob sie noch das alte Windows XP im Einsatz haben und in diesem Fall einen schnellen Austausch des Betriebssystems anstreben.

Im Zweifelsfall ist es auch denkbar, die Systeme vorerst vom Netz zu nehmen, um kein unnötiges Risiko einzugehen, bis die Sachlage geklärt ist.

Die besten Maßnahmen müssen im Einzelfall bewertet werden; ist ein Wechsel des Betriebssystems aus irgendeinem Grund nicht umsetzbar, sollten die betroffenen Komponenten segmentiert und vom restlichen Netzwerk isoliert werden, um ein Übergreifen auf die gesamte IT-Infrastruktur von vornherein auszuschließen.

Besonders Betriebe der KRITIS dürfen hier keine unnötigen Risiken eingehen.

Es kann auch nie schaden, seine Anti-Malware Lösung ständig auf dem neuesten Stand zu halten, um einen Angriff frühzeitig zu erkennen und abzuwehren. Zwar kann dadurch keine absolute Sicherheit garantiert werden, doch es ist eine erste Abwehr gegen die kommenden Aktivitäten der Cyberkriminellen.



G DATA CyberDefense AG **Unternehmenskommunikation**

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299