



Halloween und Windows XP-Systeme: Zombies töten ist nicht leicht - Für den Mittelstand sind veraltete Systeme ein unkalkulierbares Risiko

Windows XP-Systeme sind wie Zombies: Sie sind nur schwer tot zu kriegen. In vielen mittelständischen Unternehmen sind immer noch Computer mit dem veralteten Betriebssystem im Einsatz. Gerade im produzierenden Gewerbe laufen viele Steuercomputer nur unter Windows XP oder anderen veralteten Betriebssystemen. Hierdurch haben Cyberkriminelle leichtes Spiel bei Angriffen. Die Rechner sollten schnellstmöglich aus dem Netzwerk entfernt oder zumindest wirkungsvoll separiert werden. Ansonsten drohen Schäden durch Angriffe, die schnell existenzbedrohend sind.

"Hexen und Zombies sind zu Halloween allgegenwärtig, aber nach dem Fest wieder verschwunden. In vielen Unternehmen sind Untote das ganze Jahr über aktiv. Kritische Systeme laufen noch mit Windows XP, Serversysteme sind total veraltet und der Herstellersupport seit Jahren abgelaufen. Das ist unverantwortlich, denn es gefährdet die Sicherheit und damit auch den wirtschaftlichen Erfolg der Firmen", sagt Tim Berghoff, Security Evangelist bei G DATA CyberDefense. "Die Aktualisierung der betroffenen Systeme ist schwierig, in einigen Fällen ist nur eine Neuanschaffung oder die Separierung des Netzwerkes erfolgversprechend. Fakt ist aber, dass hier ein dringender Handlungsbedarf bei den Unternehmen besteht, ansonsten drohen hohe Image- und wirtschaftliche Verluste."

Windows XP: Ein Untoter lebt weiter

Jedes Jahr werden weltweit Millionen neuer Computer verkauft. Trotzdem liegt der Anteil der Rechner mit einem Windows XP-Betriebssystem insgesamt bei 0,8 Prozent. Immer noch setzen viele Unternehmen teils notgedrungen auf ein System, das schon lange nicht mehr mit Updates versorgt wird und dessen Quellcode teilweise geleakt wurde.

Nach den Erfahrungen der Security-Experten von G DATA CyberDefense zeigt sich das Problem immer wieder. Ein Beispiel: Ein Unternehmen kauft einen neuen Industriedrucker, der Lackproben für Autos drucken kann. Kunden können so nachvollziehen, wie sich der Lack eines Autos anfühlt. Dieser Drucker kostet mehrere Millionen Euro und wird durch ein XP-System gesteuert. Dieses Beispiel zeigt: Veraltete Betriebssysteme lassen sich auf vielen Computern zur Steuerung von Industriemaschinen oder ganzen Produktionsanlagen finden. Oft ist die Steuerungssoftware für die Maschine, die das System kontrolliert, nicht mit aktuellen Windows-Versionen kompatibel.

Alte Server sind immer noch im Einsatz

Jeder Zombie-Experte weiß: Einen Zombie muss man enthaupten, um ihn unschädlich zu machen. Bei Windows XP ist das schwer, da das Unternehmen streng genommen ohne den Zombie-PC aufgeschmissen ist. Zudem sind Firmen oft an vertragliche Laufzeiten oder Abschreibungsfristen gebunden oder haben es bei Aktualisierungen mit hohen Neu-Lizenzierungskosten zu tun.

Ein weiteres Problem: Manchmal existiert die Herstellerfirma nicht mehr und ein Update ist ausgeschlossen oder eine neue Version ist mit einem aktuellen Betriebssystem inkompatibel. Dann hilft nur noch eine Neuanschaffung.

Generell ist die Durchführung eines Updates mit einem hohen Aufwand verbunden. Die Produktion, die oft ohne Unterbrechung läuft, muss dafür angehalten werden. Eine Aktualisierung ist daher schwierig und teuer. Zudem behindern Zertifizierungen und Regulierungen einen Updateprozess: Wenn die Umgebung in einem bestimmten Zustand abgenommen wurde, kann nicht einfach eine neue Software aufgespielt werden. Daher ist die Investition in eine kostspielige Neuanschaffung eine Alternative.

Netzwerk separieren

Eine andere Möglichkeit ist die konsequente Separierung des Netzwerkes, in dem die betroffenen Computer laufen. Hierdurch kann ein Angreifer nicht vom Verwaltungsnetzwerk aus auch auf die Steuerung der Produktions-IT zugreifen. Dieses System sollte gehärtet sein, also nach Möglichkeit über keine Internetverbindung verfügen und nur mit den allernotwendigsten Diensten ausgestattet sein. Zusätzlich sollte ein hartes Regelwerk etabliert werden, was sicherstellt, dass nur ein Minimum an notwendigem Datenverkehr möglich ist.

"Welchen Weg ein Unternehmen auch immer geht, es muss etwas passieren. Ansonsten droht auch ein gravierender Imageverlust, wenn bekannt wird, dass ein Angriff aufgrund veralteter Betriebssysteme erfolgreich war. Es lohnt sich also, das Problem anzupacken und für mehr Sicherheit zu sorgen", so Tim Berghoff.