

Extended-Support und Security-Updates für Windows 2000 enden im Juli 2010

Windows 2000: Security-Probleme müssen nicht sein

Wer industrielle Anwendungen auf Basis von Windows 2000 über den Sommer 2010 hinaus sicher in Betrieb halten will, sollte sich unverzüglich Gedanken über das weitere Vorgehen in Sachen Security (Datensicherheit) machen. Im Juli enden nämlich der Extended-Support und die Verfügbarkeit von Sicherheits-Updates für das Betriebssystem. Security-gerechte Alternativen zum Wechsel auf ein neueres Betriebssystem sind aber gegeben.

Vernetzte industrielle Automatisierungskomponenten mit Microsoft-Windows-Betriebssystemen sind heutzutage weit verbreitet und wie ihre Pendants in Büronetzen durch regelmäßig neu entdeckte Sicherheitslücken gefährdet. Immerhin gewährt Microsoft nach seinen seit Oktober 2002 gültigen Support-Life-cycle-Richtlinien für Business- und Entwickler-Produkte mindestens zehn Jahre lang Support (fünf Jahre Mainstream-Support und fünf Jahre Extended-Support) und stellt für die Produkte bis zum Ende der Extended-Support-Phase auch Sicherheits-Updates zur Verfügung. Mit der außerordentlich langen Lebensdauer von Investitionsgütern wie industriellen Maschinen und Anlagen, die nicht selten 15, 20, und noch mehr Jahre in Betrieb bleiben, kann aber selbst diese Support-Dauer nicht mithalten.

Im Juli 2010 ist es für eine Generation der Microsoft-Betriebssysteme wieder soweit: Fünf Jahre nach dem

Mainstream-Support für Windows 2000 endet der Extended-Support. Die Geschichte von Windows wiederholt sich also auch hier: nach Windows 95 im Dezember 2001, Windows NT 4.0 im Juni 2004, Windows 98 im Juli 2006 und der älteren Windows-CE-Version 3.0 im Oktober 2007 jetzt mit Windows 2000. »Wer in seinem Unternehmen entsprechende IT-Sicherheitsrichtlinien umsetzen muss, schlicht Vernunft und Sorgfalt walten lassen will oder ausschließlich nach dem Stand der Technik sichere Systeme an sein Produktionsnetz anschließen möchte, den bringen diese Ereignisse in Zugzwang«, erläutert Torsten Rössel, Director Business Development bei der Innominate Security Technologies AG in Berlin. »Augen zu und durch' ist jedenfalls keine gute Alternative, wie die Statistik zeigt.« Im Jahr 2008 habe Microsoft immer noch 36 für Windows 2000 relevante Sicherheits-Updates herausgegeben, davon 19 mit der höchsten Einstufung »Critic-

cal« und 16 weitere als »Important« deklarierte. Allein im ersten Quartal des Jahres 2009 seien noch fünf weitere Sicherheits-Updates für das System erschienen, zwei »critical« und drei »important«. Zudem sei von Januar bis März 2009 jeden Monat eine weitere Schad-Software in das Windows-Tool zum Entfernen besonders schädlicher Software einbezogen worden, darunter der Wurm »Win32/Conficker« und der Trojaner »Win32/Srizbi«. »Für Anwender von Windows 2000 in industriellen Applikationen besteht also dringender Handlungsbedarf«, resümiert Rössel.

Ein nahe liegender Lösungsansatz ist der Upgrade auf ein neueres Betriebssystem, für das wieder einige weitere Jahre Support garantiert sind. Doch ein solches Vorhaben zieht weit reichende Konsequenzen und hohe Kosten nach sich. »So müssen nicht nur neue Lizenzen beschafft und neue Systeme installiert, sondern dafür meist auch noch größere Hardware-Ressourcen bereitgestellt werden, was Aufrüstung oder komplette Neubeschaffung von Hardware zur Folge haben kann«, verdeutlicht Rössel. »Dann geht die Arbeit aber erst richtig los, denn die eigentlichen Nutzapplikationen müssen für die neue Plattform, auf der sie nur in günstigen Fällen ‚einfach so‘ weiterlaufen können, neu beschafft oder >



Netzwerksicherheit für nicht (mehr) patchbare industriell eingesetzte Windows-Systeme lässt sich mit den »mGuard«-Security-Appliances von Innominate transparent und kostengünstig in verschiedenen Bauformen nachrüsten.



Torsten Rössel, Innominate

» 'Augen zu und durch'
ist keine gute Alternative. «

auf diese portiert werden. Handelt es sich gar um nach Branchenvorschriften zertifizierte Systeme, sind aufwändige Approbationsverfahren erneut zu durchlaufen.« Wegen etwaiger, noch dazu schwer kalkulierbarer Sicherheitsrisiken wolle kaum jemand diese Kostenlawine losstreifen. Es gehe aber auch anders und kostengünstiger.

Security lässt sich nachrüsten

Praktisch alle erwähnten Software-Sicherheitsrisiken beruhen auf Schwachstellen und Sicherheitslücken von Protokollen oder Diensten, die durch Angreifer, besonders sogenannte »Exploits« in Schad-Software, von bereits infizierten Systemen aus über ein IP-gestütztes Netzwerk ausgenutzt werden können, um Schäden anzurichten und sich weiter zu verbreiten. »Wer also mangels weiterer Sicherheits-Updates nichts mehr gegen neu entdeckte Krankheiten tun kann, vermag daher immer noch die Ansteckungsgefahr für das alte System drastisch zu reduzieren, indem er seine Kommunikation auf die Partner, Protokolle, Ports und Verbindungsrichtungen beschränkt, die für das Funktionieren der Gesamtanlage erforderlich sind«, führt Rössel aus. »Besonders nicht vom System selbst initiierte, sondern von außen dort eingehende Verbindungen lassen sich dabei weitgehend und oft sogar völlig unterbinden.«

Aber auch von innen nach außen müsse längst nicht alles erlaubt bleiben, etwa der Zugriff auf beliebige File-Shares und andere Server im Firmennetz oder gar auf das Internet.

Die Kontrolle und gezielte Filterung der in Ethernet- und IP-gestützten Netzwerken zunächst einmal offenen und unbeschränkten Kommunikation ist die Aufgabe von Firewalls. Sie lassen sich in Form industrieller Network-Security-Appliances für je nach Bauform etwa 300 bis 800 Euro pro Gerät kostengünstig und dezentral dort nachrüsten, wo sie aus den erwähnten Gründen nötig sind. »Die ‚mGuard‘-Produktfamilie von Innominate beispielsweise umfasst Geräte in verschiedenen Bauformen, die sich im Schaltschrank auf der Hutschiene, in 19-Zoll-Schränken, mit Stromversorgung über USB extern an PCs oder als PCI-Karte direkt im PC-Gehäuse verbauen lassen«, stellt Rössel fest. »Wegen ihres patentierten Single-Stealth-Mode sind die Geräte völlig transparent in ein bestehendes Netzwerk integrierbar. Sie übernehmen dabei automatisch die MAC- und IP-Adressen ihres jeweiligen Schützlings, so dass der Anwender weder zusätzliche Adressen für das Management der Geräte selbst vergeben noch sonst irgendwelche Änderungen an der Netzwerkkonfiguration der beteiligten Systeme vornehmen muss.« Obwohl die Geräte bezüglich der Netzwerktopologie völlig transparent arbeiten, überwachen und filtern sie als »Stateful-Packet-Inspection-Firewall« anhand eines konfigurierbaren Regelwerks den Netzwerkverkehr von und zu den geschützten Systemen. Dank bidirektionalem »Wire-Speed« geraten sie dabei auch nicht zum Flaschenhals für ein 100-MBit/s-Ethernet-Netzwerk. Aufgrund einer flexiblen, skriptbaren Flash- und Rollout-Prozedur lassen sich die Security-Appliances sowohl einzeln über ein integriertes Web-Interface als auch gemeinsam zentral über den Device-Manager von Innominate verwalten.

Bei Bedarf kann der Anwender die Sicherheit mittels zusätzlicher Funktionen der Geräte noch weiter erhöhen: etwa durch eine User-Firewall zur gezielten Berechtigung

individuell angemeldeter Benutzer, durch VPN-Technik (Virtual Private Networking) zur Authentisierung von Gegenstellen und Verschlüsselung von Datenverkehr oder durch die »mGuard-CIFS-Integrity-Monitoring«-Funktion zur Überwachung auf Basis von CIFS/SMB freigegebener Windows-Dateisysteme auf unerwartete Veränderungen (Common Internet File System / Server Message Blocks). »Kunden etwa aus der Automobilindustrie haben mit diesem auf Security-Appliances gestützten Schutzkonzept gute Erfahrungen gemacht und viele der produktionsnah eingesetzten Windows-95-, Windows-98- und Windows-NT-Systeme geschützt und sicher in Betrieb gehalten«, betont Rössel.

Die meisten Windows-Systeme in der Industrie kommen allerdings nicht in den Genuss eines regelmäßigen Patch-Managements. Zu groß ist die berechtigte Sorge, dass ein unbedachtes, pauschales Einspielen von Sicherheits-Updates ohne ausgiebige und damit teure vorherige Tests die Funktion, Stabilität und Qualität sorgfältig abgestimmter Prozesse in Mitleiden-

schaft ziehen könnte. »So gilt eher 'Never change a running system' und nicht ein obligatorischer monatlicher Patch-Day als Maxime in der Produktion«, legt Rössel dar. »Die mögliche Gefährdung von Zertifizierungen und Garantieansprüchen gegenüber Maschinen- und Anlagenlieferanten gibt dem Thema dann häufig den Rest, so dass viele Embedded-PC-Systeme von vornherein als nicht patchbar eingestuft werden müssen – nicht erst nach dem Ende ihres Extended-Supports.« Auch diesen Systemen lasse sich aber gemäß dem beschriebenen Prinzip zu mehr Sicherheit verhelfen.

Bis zum Ende des Extended-Supports für Windows 2000 bleibt nicht mehr viel Zeit. Dutzende oder gar Hunderte von Windows-2000-Systemen sicher in Betrieb zu halten, ist aber unabhängig von der Methode ein Projektvorhaben mit erheblichem Zeitbedarf für Analyse und Bewertung von Alternativen, Entscheidung, Planung, Vorbereitung und Durchführung. Das Projekt sollte also unverzüglich in Angriff genommen werden. (ak) ■