

Zeit zum Handeln

Windows 2000 in der Automation – Extended Support und Security Updates enden Juli 2010

Torsten Rössel

Alles hat ein Ende – darüber sollte sich Gedanken machen, wer industrielle Applikationen auf Basis von Windows 2000 über den Sommer 2010 hinaus sicher in Betrieb halten will. Dann enden der Extended Support und die Verfügbarkeit von Sicherheitsupdates für dieses System. Gibt es lebensverlängernde Alternativen zum Wechsel auf ein neueres Betriebssystem?



Torsten Rössel ist Director Business Development bei der Innominate Security Technologies AG in Berlin

Vernetzte industrielle Automatisierungskomponenten mit Microsoft Windows Betriebssystemen sind heute weit verbreitet und wie ihre Pendanten in Büronetzen leider durch regelmäßig neu entdeckte Sicherheitslücken und Verwundbarkeiten gefährdet. Immerhin bietet Microsoft nach seinen seit Oktober 2002 und aktuell gültigen Support Lifecycle-Richtlinien für Business- und Ent-

wicklerprodukte einen Mindestzeitraum von zehn Jahren an Support (fünf Jahre Mainstream Support und fünf Jahre Extended Support) und stellt für diese Produkte bis einschließlich der Extended Support-Phase auch Sicherheitsupdates 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 selbst diese Support-Dauer allerdings immer noch nicht mithalten.

Im Juli 2010 ist es für eine Generation der Microsoft Betriebssysteme mal wieder soweit: auch der Extended Support für Windows 2000, dessen Mainstream Support im

„Die richtige Zeit zum Handeln beginnt jetzt“

Torsten Rössel

Juni 2005 endete, wird dann ablaufen. Kein grundsätzlich neues Ereignis, die Geschichte wiederholt sich 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 eben mit Windows 2000.

Was soll schon passieren?

Allerhand! Nichts tun, Augen zu, und einfach „weiter so“ ist keine gute Alternative wie ein wenig Statistik zeigt. In 2008 gab Microsoft immer noch 36 für Windows 2000 relevante Sicherheitsupdates heraus. Allein im ersten Quartal des Jahres 2009 erschienen weitere fünf Sicherheitsupdates für das System. Auch fand von Januar bis März 2009 jeden Monat eine weitere Schadsoftware Berücksichtigung im Windows-Tool zum Entfernen besonders schädlicher Software. Was also tun?

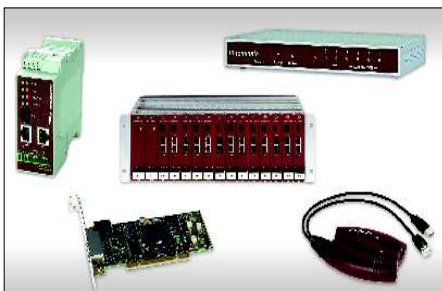
Teure Upgrades und eine folgende Kostenlawine

Ein nahe liegender Lösungsansatz ist natürlich das Upgrade auf ein neueres Betriebssystem, für das wieder einige weitere Jahre Support zur Verfügung steht. Doch ein solches Vorhaben zieht schnell einen ganzen Rattenschwanz an Konsequenzen und Kosten nach sich. So müssen nicht nur neue Lizenzen beschafft und neue Systeme installiert, sondern meist auch noch deren gewachsener Hunger nach Hardware-Ressourcen gestillt werden, was Aufrüstungen oder komplette Neubeschaffung von Hardware zur Folge haben kann. Dann geht die Arbeit aber erst richtig los, denn die eigentlichen Nutzapplikationen müssen für die neue Plattform, auf der sie nur in glücklichen Fällen „einfach so“ klaglos weiterlaufen werden, neu beschafft oder auf diese portiert werden. Das muss doch auch anders und günstiger gehen. – Geht es auch.

Schutz durch Nachrüstung von Security Appliances

Praktisch allen hier betrachteten Software-Sicherheitsrisiken ist gemeinsam, dass sie auf Schwachstellen und Verwundbarkeiten von Protokollen oder Diensten basieren, die durch Angreifer, insbesondere so genannte „Exploits“ in Schadsoftware von bereits infizierten Systemen aus über ein IP-basiertes Netzwerk ausgenutzt werden können, um Schäden anzurichten und sich weiter zu verbreiten. Wenn man also mangels weiterer Sicherheits-Updates schon nichts mehr gegen neu entdeckte Krankheiten tun kann, bleibt einem daher immer noch die Alternative, die Ansteckungsgefahr für das alte System drastisch zu reduzieren, indem man seine Kommunikation auf die Partner, Protokolle, Ports und Verbindungsrichtungen beschränkt, die für das Funktionieren der Gesamtanlage erforderlich sind. Insbesondere nicht vom System selbst initiierte, sondern von außen dort eingehende Verbindungen können dabei weitgehend und oft sogar völlig unterbunden werden. Aber auch von innen nach außen muss längst nicht alles erlaubt bleiben, z. B. der Zugriff auf beliebige File Shares und andere Server im Firmennetz, geschweige denn ins Internet.

Die Kontrolle und gezielte Filterung der in Ethernet- und IP-basierten Netzwerken zunächst einmal offenen und unbeschränkten Kommunikation ist die Aufgabe von Firewalls. Eben solche lassen sich in Form industrieller Network Security Appliances für je nach Bauform ca. 300 bis 800 Euro pro Gerät kostengünstig und punktgenau dezentral dort nachrüsten, wo sie aus den hier diskutierten Gründen benötigt werden. So steht etwa mit der mGuard Technologie von Innominate eine ganze Familie solcher Geräte in verschiedenen Bauformen zur Verfügung, die sich im Schaltschrank auf Hutschiene, in 19-Zoll-Schränken, mit Stromversorgung über USB extern an PCs oder als PCI-Karte gleich im PC-Gehäuse verbauen lassen. Der besondere Clou: durch ihren patentierten Single Stealth Mode lassen sich die Geräte völlig transparent in ein bestehendes Netzwerk nachrüsten. Sie übernehmen dabei automatisch die MAC- und IP-Adressen ihres jeweiligen Schützlings, so dass weder zusätz-



Netzwerksicherheit für nicht (mehr) patchbare industriell eingesetzte Windows Systeme lässt sich mit den mGuard Security Appliances nachrüsten

liche Adressen für das Management der Geräte selbst vergeben noch sonst irgendwelche Änderungen an der Netzwerkkonfiguration der beteiligten Systeme vorgenommen werden müssen. Trotz dieses bzgl. der Netzwerktopologie transparenten Betriebs überwachen und filtern sie natürlich fortan als Stateful Packet Inspection Firewall anhand eines konfigurierbaren Regelwerks den Netzwerkverkehr von und zu den so geschützten Systemen. Dies geschieht dank bidirektionalem „Wire Speed“, ohne zum Flaschenhals für ein 100 MBit/s Ethernet Netzwerk zu werden. Die mGuard Security Appliances können durch eine flexible, skriptbare Flash- und Rollout-Prozedur sehr effizient ausgerollt und sowohl einzeln über ein integriertes Web Interface als auch gemeinsam zentral über den Innominate Device Manager verwaltet werden.

Bei Bedarf kann die Sicherheit mit weiteren auf den Geräten vorhandenen Mechanismen noch weiter erhöht werden: etwa durch eine User Firewall zur gezielten Berechtigung individuell angemeldeter Benutzer, durch VPN-Technologie (Virtual Private Networking) zur sicheren Authentisierung von Gegenstellen und Verschlüsselung von Datenverkehr.

Nicht patchbare Systeme

Wohl den bis hierher betrachteten industriell eingesetzten Windows Systemen, die überhaupt in den Genuss eines regelmäßigen Patch Managements kommen. Die Regel ist das nicht. Zu groß ist die berechtigte Sorge, dass ein unbedachtes, pauschales Einspielen von Sicherheitsupdates ohne ausgiebige und damit (zu) teure vorherige Tests die Funktion, Stabilität und Qualität sorgfältig abgestimmter Prozesse in Mitleidenschaft ziehen könnte. So gilt denn auch eher „Never change a running system“ und nicht ein obligatorischer monatlicher Patch-Day als vorherrschende Maxime in der Produktion. Die mögliche Gefährdung von Zertifizierungen und Garantieansprüchen gegenüber Maschinen- und Anlagenlieferanten gibt dem Thema dann häufig den Rest, so dass gerade viele Embedded PC-Systeme von vornherein als nicht patchbar eingestuft werden müssen – nicht erst nach Ende ihres Extended Supports. Auch all diesen Systemen kann nach dem beschriebenen Prinzip zu mehr Sicherheit verholfen werden.

Die Zeit läuft, und dutzende oder gar hunderte von Windows-2000-Systemen sicher in Betrieb zu halten, bleibt unabhängig von der Methode ein Projektvorhaben mit angemessenem Zeitbedarf für Analyse und Bewertung von Alternativen, Entscheidung, Planung, Vorbereitung und Durchführung. Die richtige Zeit zum Handeln ist jetzt.