

Sicherheit über Jahre

WINDOWS-SUPPORT. Extended Support und Security Updates für Windows 2000 durch Microsoft enden heuer im Juli. Industrieanwender sollten sich darüber Gedanken machen, wie sie in Zukunft die Sicherheit ihres Systems erhalten können. Clevere Schutzmaßnahmen müssen aber nicht teuer sein.

Never touch a running system.“ Wer kennt den Spruch nicht, der in vielen IT-Abteilungen zu den Standardfloskeln gehört. Nicht nur bei den Usern am Heim-PC, auch in vielen Unternehmen ist der Spruch gleichbedeutend mit dem krampfhaften Halten eines fragwürdigen Status quo. Nichts anzurühren heißt nämlich oft, auf die so notwendigen Updates des Systems zu verzichten.

Wie Torsten Rössel, Director Business Development der Innominate Security Technologies AG, berichtet, sind damit auch vernetzte industrielle Automatisierungskomponenten mit Microsoft-Windows-Betriebssystemen gefährdet. Dabei hat Microsoft in seinen Support-Lifecycle-Richtlinien für Business- und Entwicklerprodukte aus dem Jahr 2002 einen Mindestzeitraum von 10 Jahren Support garantiert. Über fünf Jahre läuft der so genannte „Mainstream Support“, über weitere fünf der „Extended Support“.

Längerer Bedarf. Einmal abgesehen davon, dass viele Unternehmen nicht mal die angebotenen Sicherheitsupdates nützen, ist es auch eine Tatsache, dass die Lebensdauer von industriellen Maschinen und Anlagen den Zeitrahmen von zehn Jahren weit übersteigt. Viele bleiben



Diesen Anblick werden Sie nur noch einen Sommer sehen: Im Juli 2010 endet der Extended Support für Windows 2000.



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

15, 20 und noch mehr Jahre in Betrieb. Wenn der Support für Windows 2000 im Juli nun ausläuft, ist das, so Torsten Rössel, ein durchaus bekanntes 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“, sagt Rössel und setzt nach: „Wenn die IT-Sicherheitsrichtlinien Ihres Unternehmens es vorschreiben oder Sie schlicht Vernunft und Sorgfalt walten und nur nach Stand der Technik sichere Systeme an Ihr Produktionsnetz lassen, bringen diese Ereignisse Sie in Zugzwang.“

Wer nach dem Motto agiert „Was soll nach 10 Jahren noch groß passieren“, der begeht möglicherweise einen fatalen Fehler. Alleine im Jahr 2008 gab Microsoft 36 relevante Sicherheitsupdates für Windows 2000 heraus. Immerhin 19 davon wurden mit der höchsten Wichtigkeitsstufe „Critical“ versehen, der Rest lief immerhin noch unter „Important“.

Auch 2009 gab es weitere Updates – und beinahe im Monatstakt wurden dazu noch

Tools zur Entfernung von Schadsoftware wie Win32/Conficker oder dem Trojaner Win32/Srizbi herausgegeben.

Teuer investiert ... Selbstverständlich gibt es mehrere Problemlösungsansätze. Einer davon ist der – teure – Umstieg auf ein neueres Betriebssystem. Ein Vorhaben, das aber leicht einen Rattenschwanz an Konsequenzen und Kosten nach sich ziehen kann. „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“, berichtet der Innominate-Experte. „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.“ Die richtige Kostenlawine wird aber damit losgetreten, wenn nach Branchenvorschriften zertifizierte Systeme neue Approbationsverfahren durchlaufen müssen.

... oder günstig nachgerüstet. Torsten Rössel hat für die User aber auch eine gute Nachricht: Eine Nachrüstung durch Security Appliances muss nicht viel Geld kosten. Denn fast allen Software-Sicherheitsrisiken ist gemeinsam, dass ihre Schwachstelle oftmals Protokolle oder Dienste sind, die durch Angreifer von infizierten Systemen über ein IP-basiertes Netzwerk ausgenutzt werden. Diesen so genannten „Exploits“ lässt sich aber ganz praktisch ein Riegel verschieben. „Wenn man also mangels weiterer Sicherheitsupdates 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“, sagt Rössel. „Insbesondere nicht vom System selbst initiierte, sondern von au-

mit Stromversorgung über USB extern an PCs oder als PCI-Karte gleich im PC-Gehäuse verbauen. Durch ihren patentierten Single Stealth Mode lassen sich die Geräte völlig transparent in ein bestehendes Netzwerk nachrüsten. Mac- und IP-Adressen werden auto-

matisch übernommen, Änderungen an der Netzwerkkonfiguration sind nicht notwendig. Dank individueller Konfigurationsmöglichkeiten kann die Sicherheit mit weiteren auf den Geräten vorhandenen Mechanismen noch erhöht werden. ■



ßen dort eingehende Verbindungen können dabei weitgehend und oft sogar völlig unterbunden werden.“

Heißer Tipp: Firewall. Filterung und Kontrolle der Kommunikation von Internet- und IP-basierten Systemen ist die Aufgabe von Firewalls. Torsten Rössel: „Eben solche lassen sich in Form industrieller Network Security Appliances für je nach Bauform zirka 300 bis 800 Euro pro Gerät kostengünstig und punktgenau dezentral dort nachrüsten, wo sie aus den hier diskutierten Gründen benötigt werden.“

Innominate bietet dazu die mGuard-Technologie, die in Form einer kompletten Familie zur Verfügung steht. Sie lässt sich im Schaltschrank auf Hutschiene, in 19-Zoll-Schränken,

Infos im Web

www.innominate.de
[http://support.microsoft.com/
lifecycle/](http://support.microsoft.com/lifecycle/)