Ein Blick auf Windows

Windows XP hat das Ende seiner Lebensdauer erreicht – was sind die Folgen?

VOLKER JUNG, ANTHONY BYATT – Das erfolgreiche und äußerst populäre Betriebssystem Windows XP von Microsoft ist mittlerweile über zehn Jahre alt. Doch auch wenn rund 30 % der Windows-Nutzer weltweit noch immer XP verwenden, kann ein so altes Betriebssystem nicht ewig unterstützt werden. Dementsprechend hat Microsoft den Support für XP am 8. April 2014 eingestellt. Das bedeutet, dass es keine neuen Sicherheitsupdates, keine neuen Patches und keinen aktiven Support mehr gibt. Die Folge ist, dass XP langsam unsicher, unzuverlässig und mit einem Großteil der neuen IT-Hardware wie PCs, PC-Komponenten, Netzwerkgeräten und Druckern inkompatibel wird. Mit anderen Worten, das Ende der XP-Ära hat Auswirkungen auf viele industrielle Anwendungen und erfordert ein proaktives Handeln der Nutzer.

Es gab Zeiten, in denen hätte man nicht daran gedacht, eine industrielle Anwendung auf Microsoft Windows zu betreiben. Als Microsoft vor über zehn Jahren aber das Betriebssystem Windows XP auf den Markt brachte, wurde die Industrie aufmerksam. Windows XP bot die von vielen industriellen Nutzern benötigte Stabilität, Flexibilität und Funktionalität und wurde bald für jede denkbare Art von Anwendung eingesetzt.

Doch alles hat ein Ende: Am 8. April 2014 endete die Ära Windows XP, als Microsoft den Support für das Produkt einstellte. Natürlich hat Microsoft seine Kunden rechtzeitig informiert, und viele Unternehmen haben sich seit Jahren auf die Umstellung vorbereitet. Dennoch blieben eine ganze Reihe von Fragen offen: Könnte ein autonomes XP-System weiterhin unbeeinflusst laufen? Was würde passieren, wenn das XP-System in ein anderes integriert würde? Wäre neue Hardware erforderlich, und was würde dies für das gesamte Unternehmen kosten? Welches Budget wäre für die Umstellung notwendig? Könnte das Problem durch Virtualisierung gelöst werden? Welche Unterstützung steht bei einer Migration auf ein neues System zur Verfügung?

Titelbild
Microsoft hat die Unterstützung für Windows XP am 8. April 2014 eingestellt. Was bedeutet dies für industrielle Nutzer?

Die Antworten auf diese Fragen waren nicht immer einfach und es wurde schnell deutlich, dass durch das Ende des XP-Supports in der Tat erhebliche Probleme aufgeworfen wurden. Diese lassen sich in vier Hauptkategorien einteilen:
– Sicherheit
– Compliance
– Fehlende Unterstützung von unabhängigen Softwareanbietern
– Unterstützung von Hardwareherstellern

Von all diesen Aspekten ist die Sicherheit an kritischsten.

Windows XP-Sicherheitsupdates

Im Jahr 2010 sorgte der Stuxnet-Wurm weltweit für Schlagzeilen, als das nur 500 kB große Schadprogramm mindestens 14 Industrieanlagen im Iran, darunter eine Anlage zur Urananreicherung, infizierte. Der Struxnet-Angriff verlief in drei Phasen: Zuerst infizierte der Wurm Rechner und Netzwerke auf Microsoft-Windows-Basis. Dann spürte er (ebenfalls Windows-basierte) Software auf, die zur Programmierung industrieller Steuerungssysteme verwendet wurde, um schließlich in die zur Steuerung von Maschinen verwendeten speicherprogrammierbaren Steuerungen einzugreifen.

Seit Stuxnet ist die zielreiche industrielle IT-Landschaft einer ständigen, immer raffinierter werdenden Bedrohung ausgesetzt. Ein Beispiel ist die sogenannte Watering-Hole-Strategie zur Einschleusung von Schadsoftware in die Zielsysteme. Dabei infiziert der Angreifer Websites, die vom Zielunternehmen häufig genutzt werden. Danach braucht er nur zu warten, bis sein Opfer die Site besucht und unwissentlich die Malware auf seinen Computer herunterlädt. Diese als SWC (Strategic Web Compromise) bezeichnete Taktik trifft das Opfer unwissentlich, da die infizierten Websites zuvor vertrauenswürdig waren.

Eine weitere Möglichkeit ist die Manipulation vorhandener echter Benutzerprofile auf einem System, um Außenstehenden Zugang zu verschaffen. Auch PC-Konfigurationen können manipuliert werden, um diese für sogenannte RATs (Remote Access Trojans) zu nutzen. Dies sind Schadprogramme, die dem Angreifer administrative Kontrolle über den Zielcomputer geben. RATs können z. B. über einen E-Mail-Anhang auf einen PC geschleust werden.

1 Betroffene Steuerungs-/MMS-Systeme (MMS = Mensch-Maschine-Schnittstelle)

System/HMI	Anmerkung
System 800xA	800xA-Kernsysteme (V5.0 und älter)
Freelance	Freelance-Systeme (V6.2–V9.1)
Power Generation Portal/Tenore	Alle Windows-basierten Versionen
Conductor NT	Alle Windows-basierten Versionen; entscheidend ist die Zahl der Server, nicht die Zahl der Systeme
Process Portal B	Alle Versionen

Ist das Hostsystem infiziert, kann es der Angreifer nutzen, um weitere RATs zu verbreiten und ein sogenanntes Botnet einzurichten – eine Gruppe von infizierten Computern, die zusammen genutzt werden, um weiteren Schaden anzurichten.

Da ein RAT die Kontrolle über einen Computer ermöglicht, kann ein Angreifer das Verhalten des Computernutzers mithilfe von Keyloggern oder anderer Spyware überwachen, eine Webcam aktivieren, auf vertrauliche Daten zugreifen, Laufwerke formatieren, Dateien löschen oder verändern usw.

Im Juni 2014 sorgte die Havex-Trojanerfamilie für Schlagzeilen, als diese Steuerungssysteme in verschiedenen Industriezweigen einschließlich des Energiesektors befiel. Eine Hauptkomponente von Havex ist ein RAT. Der Trojaner infizierte Websites von Herstellern industrieller Leitsysteme (ICS) und SCADA-Systemen (Supervisory Control and Data Acquisition). Insgesamt wurden 146 Server von 88 Varianten des Havex-Trojaners angegriffen, und 1.500 IP-Adressen wurden verfolgt, um mögliche Opfer zu finden. Zweifellos stellte Havex eine ernstzunehmende Bedrohung für die Industrie dar.

Im Juli 2014 infizierte der Virus „Energetic Bear“ über 1.000 Energieunternehmen in Europa und den USA. Dieser Virus bietet Hackern theoretisch die Möglichkeit, die Kontrolle über Kraftwerke zu übernehmen.

Diese Beispiele zeigen, wie angreifbar die industrielle IT-Umgebung offensicht-

2 XP-Upgradestrategien

Windows XP		Controller			Windows 7	Windows 8.1
800xA	3.1 4.0 4.1 5.0	Alle	→	800xA	5.1	6.0
Freelance	6.2 7.1 7.2 8.1 8.2 9.1	Alle	→	Freelance	2013	2015
Conductor NT	Alle	DCI	→	800xA	5.1	6.0
		Freelance	→	Freelance	2013	2015
			→	800xA	5.1	6.0
		Harmony	→	800xA	5.1	6.0
			→	Symphony +	2.0	
PPB	Alle	MOD 300	→	800xA	5.1	6.0
		Freelance	→	Freelance	2013	2015
			→	800xA	5.1	6.0
		Harmony	→	800xA	5.1	6.0
			→	Symphony +	2.0	
PGP/Tenore	Alle	Freelance	→	Freelance	2013	2015
			→	800xA	5.1	6.0
		Harmony	→	800xA	5.1	6.0
			→	Symphony +	2.0	

lich ist. Ohne die wichtigen Windows XP-Sicherheitsupdates sind PCs Angriffen durch Viren, Spyware und andere Schadsoftware ausgeliefert, die Geschäftsdaten oder -informationen stehlen oder beschädigen können. Antiviren-Software bietet keinen vollständigen Schutz für XP-Systeme mehr. Jedes Gerät, das weiterhin mit XP betrieben wird, kann von Angreifern als Zugangspunkt zu IT-Netzwerken genutzt werden. Das bedeutet, dass auch Computer, die unterstützte Betriebssysteme nutzen, geschädigt werden können.

Hardware

Die meisten Hersteller von PC-Hardware, Druckern und Netzwerkgeräten haben ihre Unterstützung von Windows XP bereits eingestellt. Das bedeutet, dass die Softwaretreiber, die erforderlich sind, um neue Hardware unter Windows XP zu betreiben, in den meisten Fällen nicht mehr verfügbar sind. Mit anderen Worten, es gibt keine XP-Treiber für neue Festplatten, Drucker, Grafikkarten, Netzwerkgeräte usw. Der Kauf eines neuen XP-Computers als Ersatz wird nicht leicht bzw. nicht günstig. XP-basierte Hardware wird zunehmend veraltet und immer schwerer zu finden sein. Die Zahl der ungeplanten Abschaltungen aufgrund nicht verfügbarer Handwarekomponenten wird hingegen zunehmen.

Compliance

Unternehmen, die aufsichtsbehördlichen Verpflichtungen wie dem US-amerikanischen Health Insurance Portability and Accountability Act (HIPAA) zum Schutz von Patientendaten unterliegen, sind möglicherweise nicht mehr in der Lage, diese Anforderungen zu erfüllen, wenn sie an Windows XP festhalten. Angesichts der großen Menge an persönlichen und privaten Daten, die mittlerweile auf Servern gespeichert sind, ist die Datensicherheit eine äußerst wichtige Angelegenheit.

Fehlende Unterstützung von unabhängigen Softwareanbietern

Viele Softwarenbieter unterstützen ihre Produkte, die auf Windows XP laufen, nicht mehr, da sie keine Updates für Windows XP mehr bekommen. So nutzt das neue Microsoft Office-Paket z. B. das neueste Windows und läuft nicht unter Windows XP.

Was ist zu tun?

Angesichts so vieler Probleme, die es zu lösen gilt, stellt sich die Frage, wie man vorgehen sollte. Microsoft und alle IT-Sicherheitsunternehmen empfehlen den Upgrade auf Windows 7 oder 8. Dies gilt auch für Anbieter von Leitsystemen mit Steuerungssystemen, die mit Windows XP oder älteren Betriebssystemen laufen → 1–2.

Natürlich kann man die Kosten für einen Upgrade den Kosten gegenüberstellen, die zur Sicherung der XP-Installationen erforderlich wären. Das Festhalten an Windows XP ist mit einem hohen Wartungsaufwand verbunden und erfordert Tools und Unterstützung von erfahrenen IT-Sicherheitsunternehmen. Zu den erforderlichen Maßnahmen gehören unter anderem:

- Reduzierung der Registry auf die absolut notwendigen Dienste
- Nutzung von DNS-Sinkholes (Domain Name Server), um den Zugang zur echten Website zu blockieren
- Ausgabe eines Alarms, wenn eine von einem Endpunkt initiierte Remote-Desktop- oder virtuelle Netzwerkverbindung erkannt wird.
- Verhindern der Ausführung von Binärcode für temporäre Benutzer im Dateisystem oder Ausgabe eines Alarms, wenn dies passiert.
- Whitelisting der Binärdateien von Diensten im Betriebssystem
- Ausgabe eines Alarms für Starts/Stopps/Änderungen von Diensten
- Prüfung von Zugriffskontrolllisten usw.
- Durchführung von regelmäßigen Backups des Steuerungssystems
- Beschaffung eines Vorrats an kompatiblen IT-Teilen

Ein Festhalten an Windows XP ist meist nicht möglich. Evolutionäre Softwareupgrades sind ein unvermeidlicher Teil des industriellen IT-Lebens, und der Upgrade von Windows XP gehört zu den bedeutenderen Schritten. Durch ihn sind Nutzer bestens gerüstet, um die Anforderungen der modernen industriellen IT-Welt in puncto Sicherheit, Hardware, Software und Compliance zu erfüllen.

ABB empfiehlt Kunden mit Betriebssystemen auf der Basis von Windows XP dringend, die Lebenszyklusplänе für ihre Systeme und ihre Strategien zur Risikominderung zu evaluieren. Gleichzeitig bietet ABB Lösungen, die die Risiken beseitigen oder mindern und Kunden dabei helfen, ihre Anlagen und Mitarbeiter besser zu schützen und gleichzeitig einen sicheren Betrieb und eine kontinuierliche Produktion sicherzustellen. Für die Bedürfnisse jedes Kunden stehen entsprechende Services zur Verfügung – auch für Kunden, die nicht in der Lage sind, sofort aufzurüsten, oder sich entschieden haben, bei Windows XP zu bleiben.

Volker Jung
Process Automation Division
Mannheim, Deutschland
volker.jung@de.abb.com

Anthony Byatt
Redaktioneller Berater
Louth Village, Irland