BELDEN
SENDING ALL THE RIGHT SIGNALS®

White Paper

WP 1007HG

Support-Ende für Windows XP: Konkrete Möglichkeiten für Industrieanwendungen

Frank Williams
Senior Manager Security Initiative
frank.williams@belden.com

Scott Howard
Technical Sales Manager
scott.howard@belden.com

Inhalt

Überblick

Eine neue Herausforderung kommt auf die Industrie zu. Ein zuverlässiger Bestandteil von Industrieanwendungen wird vom Hersteller nicht mehr unterstützt. Ein zwölf Jahre altes, bewährtes und leistungsstarkes Betriebssystem „Windows XP" wird von Microsoft nicht mehr mit Service- und Securitypatches versorgt. Dieses Betriebssystem das weltweit überall in Fertigungsstätten, Energieanlagen und vielen entscheidenden Infrastrukturen zu finden ist, muss über kurz oder lang abgelöst werden.

War es für Sie auch erschreckend zu erfahren, wie viele Windows XP-basierte Systeme noch in Ihrem Unternehmen vorhanden sind? Das sollte uns zu denken geben. In der Produktionsumgebung und in den Leiständen ist überall noch Windows XP zur finden, auf denen wichtige Fertigungs-, Prozess- oder Produktionsanwendungen laufen. Aber oftmals ist das Betriebssystem nicht so leicht zu erkennen, wie z.B. in Steuerungen, Geräte zur Konfiguration und Überwachung der Prozesse.

Aber das war noch nicht alles: Auch Embedded-Komponenten in Tausenden von Geräten zur Steuerung von Fabrikautomations- und Prozesssteuerungsaufgaben nutzen Windows XP. So wird verständlicher, wie leicht bestimmte Gerätetypen übersehen werden können. Ein großer Pharmahersteller beispielsweise war sehr überrascht, als er bei einer entsprechenden Überprüfung immer neue Gruppen mit Hunderten von Geräten entdeckte, die mit Windows XP laufen.

Es gibt drei Optionen für den Umgang mit dem Risiko für Industrieanwendungen durch die Einstellung des Supports für Windows XP.

Erste Option: Sie unternehmen nichts und erhalten den gegenwärtigen Zustand aufrecht. In diesem Fall müssen Sie sich damit arrangieren, dass Sie bei unerklärlichen Ereignissen nicht mehr bei Microsoft oder anderen Software-Anbietern anrufen und einen Patch oder Treiber bekommen können.

Zweite Option: Sie steigen auf eine neuere Windows-Version um. Das ist kein schnell durchführbares Projekt, auch wenn letztlich kein Weg daran vorbei führt. Es ist vielmehr äußerst komplex, weil eine Betriebssystemaktualisierung einen Dominoeffekt auslöst, der Folgendes umfassen kann:

- Betriebssystem-Upgrade
- Neue PC-Hardware und/oder Automatisierungsgeräte
- Neue Software für die neuen Geräte
- Neue Treiber für die neue Software
- Austausch von Automatisierungsgeräten, die nicht mit der neuen Software und den neuen Treibern laufen
- Systemintegrationsaufwand für unternehmenskritische Anwendungen, die sich in der neuen Umgebung nicht mehr wie gewohnt verhalten
- Implementierung der geänderten Anwendungen
- Umfassende Tests der neuen Systeme
- Niedrigere Produktivität während des Migrationsprojektes
- Benutzerschulungen und -support für die neuen Systeme

Hochgerechnet auf die Zahl aller vorhandenen Windows XP-Installationen erhalten Sie damit eine gewisse Vorstellung davon, wie schnell ein „einfaches" Betriebssystem-Upgrade mehrere Mannjahre erfordern kann.

Die gute Nachricht: Es gibt noch eine dritte, erheblich weniger komplexe Option. Wenn Sie Windows XP behalten möchten oder in nächster Zukunft noch nicht für eine Migration bereit sind, können Sie einfach Industrie-Firewalls implementieren und so Ihre Windows XP-basierten Systeme schützen. Dadurch gewinnen Sie ohne Risiken für Ihre Umgebung die für eine Betriebssystemaktualisierung benötigte Zeit.

Industrie-Firewalls haben den Vorteil, dass sie im laufenden Betrieb in Netzwerke implementiert werden können und außerdem einfach zu installieren und konfigurieren sind. Sie erfordern keine Maßnahmen wegen des für die zweite Option genannten Dominoeffekts. Damit sind Industrie-Firewalls eine kostengünstige, zeitsparende Möglichkeit, Ihre Systeme zu schützen, und Sie können in Ruhe die Migration auf ein anderes Betriebssystem planen und durchführen.

Dieses White Paper untersucht, welche Auswirkungen das Support-Ende für Windows XP für die Verantwortlichen bedeutet, die dafür sorgen müssen, dass der Industriebetrieb störungsfrei weiterläuft. Es gibt wichtige Informationen und nennt Vor- und Nachteile der drei Optionen für das weitere Vorgehen.

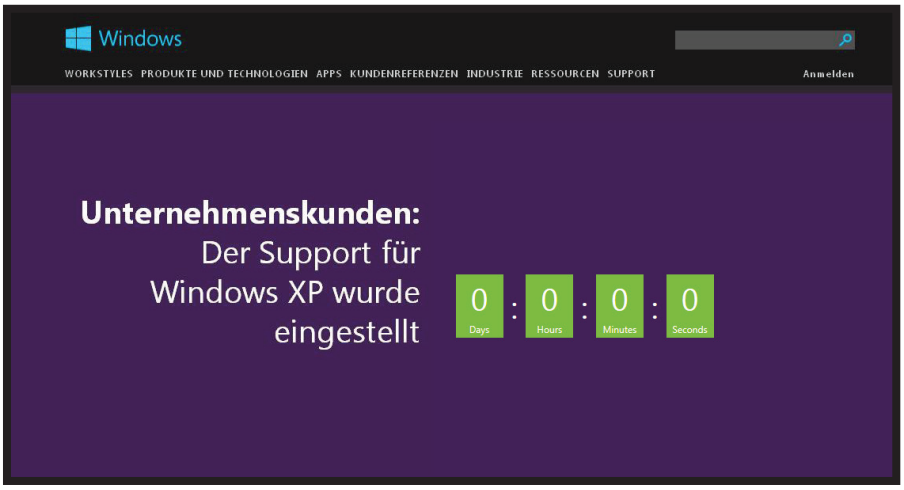

Abbildung 1: Microsoft-Website, die Unternehmenskunden informiert, dass der Support für Windows XP eingestellt wurde. Quelle: Microsoft.com[1]

Ende des Supports für Windows XP

Microsoft stellt den Support für das Betriebssystem Windows XP ein

Am 8. April 2014 beendete Microsoft die Unterstützung für das Betriebssystem Windows XP[2]. Das war keine Überraschung, denn Microsoft hatte diesen Termin schon vor Jahren angekündigt und die Benutzer im letzten Support-Jahr aktiv daran erinnert.

In den Tagen vor und nach dem Stichtag für das Support-Ende fand dieses Ereignis ein großes Medienecho. Vielleicht war es auch für Sie oder Ihr Unternehmen ein Weckruf, um die damit verbundenen Fragen zum Lebenszyklus von Computern und Geräten zu prüfen.

Was bedeutet das Ende des Support für Windows XP?

Das Ende des verlängerten Supports für Windows XP bezieht sich auf den Zeitpunkt, ab dem Microsoft keine automatischen Fehlerkorrekturen (Bugfixes) und Updates mehr durchführt und auch keine technische Online-Unterstützung mehr leistet.

Das heißt nicht, dass Windows XP plötzlich nicht mehr funktioniert, sondern dass Microsoft keine Sicherheits-Updates und Hotfixes mehr bereitstellt, wie es bis zum 8. April 2014 regelmäßig geschah.

Microsoft selbst schrieb dazu: „Wenn Sie Windows XP nach Ende des Supports weiterhin verwenden, ist Ihr Computer anfälliger für Sicherheitsrisiken und Viren".

Wird Windows XP ohne Unterstützung weiterverwendet, steigt das Risiko für die Systeme im selben Maß, wie Anzahl und Schweregrad der Sicherheitslücken zunehmen.

Bedenken Sie:

70 % der 2013 von Microsoft herausgegebenen Sicherheits-Newsletter betrafen Windows XP.

Es gibt keinen Grund anzunehmen, dass sich hier in nächster Zukunft etwas ändert (abgesehen von einer weiteren Zunahme der Risiken).

Microsoft bietet einen eingeschränkten Support für Unternehmen, die für eine verlängerte Unterstützung („Extended Support") zahlen – eine Option, die mindestens 100.000 US-Dollar im Jahr kostet. Trotzdem sollten weitsichtige Unternehmen einen Plan entwickeln, wie sie ihre Systeme sofort absichern, und langfristig auf ein anderes Betriebssystem migrieren.

Wie dringend ist der Handlungsbedarf?

Windows XP war für mehr als zwölf Jahre ein stabiles, leistungsstarkes Betriebssystem. Experten schätzen, dass Windows XP weltweit noch immer auf 28 Prozent der PC-Desktops eingesetzt wird. Andere Marktstudien zeigen, dass Windows XP nur noch einen Marktanteil von 20 Prozent hat. Unabhängig davon, welche Zahl näher am tatsächlichen Wert liegt, kann man davon ausgehen, dass mindestens einer von fünf PCs weltweit noch unter Windows XP läuft.

Es wird jedoch vermutet, dass der Anteil bei Industrieanwendungen erheblich höher liegt. XP war die erste Windows-Version, der Ingenieure bei Industrieanwendungen vertrauten, und sie ist weit verbreitet.

Deshalb wird Windows XP als Betriebssystem seit mehreren Generationen von Automatisierungsgeräten für wichtige Industrieanwendungen eingesetzt – und das mit relativ wenigen Wartungs- oder Interoperabilitätsproblemen. Viele Produktionsstätten verwenden spezielle Anwendungssoftware, die häufig nicht eigenständig lauffähig ist oder nur für Windows XP gründlich getestet wurde, so dass noch keine Erfahrungen für andere Betriebssysteme vorliegen.

Sie werden wahrscheinlich überrascht sein, wie häufig Windows XP noch in Ihrem Unternehmen eingesetzt wird. Überprüfen Sie, welches Betriebssystem in folgenden Bereichen genutzt wird:

- PCs mit wichtigen Fertigungs-, Prozess- oder Produktionsanwendungen in Werkshallen, Leitständen oder Technikzentralen
- Ruggedized PCs, auf Stuerungen, dezentrale Leitsysteme (DCS) und andere Anwendungen zur Gerätekonfiguration/-überwachung

Windows XP Embedded

Windows XP gibt es auch als „Windows XP Embedded", einer abgespeckten Version dieses Betriebssystems. Microsoft hatte es speziell für OEM-Geräte und -Systeme entwickelt, beispielsweise für Werkzeugmaschinen, Leittechnik und Bedienterminals.

Diese Geräte sind keine „Computer" im herkömmlichen Sinne. Oft ist gar nicht allgemein bekannt, dass sie unter Windows XP laufen und demselben Sicherheitsrisiko wie ein Desktop-PC oder Laptop unterliegen.

Sie sollten auch an weiteren Stellen nach Windows XP-basierten Geräten suchen:

- Embedded-Bauteile und Syteme , die verschiedene Fabrikautomations- und Prozesssteuerungsaufgaben oder Stromversorgungs-, Wasserversorgungs- sowie Verkehrssysteme steuern und überwachen.

Selbst wenn Sie wissen, dass Sie in diesen Bereichen noch Geräte mit Windows XP haben, gibt es normalerweise keine praktikable Möglichkeit, diese zu aktualisieren oder zu patchen, so dass nur noch der Austausch bleibt.

Wenn Sie eine Bestandsaufnahme für Windows XP-Geräte machen:

Achten Sie darauf, auch die Systeme am Werks-/Anlagen-/Fertigungsstandort zu prüfen, die nicht in einem als solchen erkennbaren Computergehäuse untergebracht sind.

Prüfen Sie gründlich alle beschriebenen Möglichkeiten, damit Sie alle Geräte mit Windows XP finden.

Upgrade industrieller Systeme auf eine neue Windows-Version ist nicht einfach

Die Einstellung des Supports für Windows XP bringt viele industrielle Nutzer in eine äußerst unangenehme Lage.

Ab sofort steigt das Risiko von Sicherheitsproblemen und daraus resultierenden Ausfällen kontinuierlich. Trotzdem sind die Kosten für eine Betriebssystemaktualisierung oder eine Migration (insbesondere die Kosten der damit verbundenen Betriebsunterbrechung) oft ein Grund, bei Windows XP zu bleiben.

Unternehmenskritische Netzwerke werden mit Fokus auf absoluter Sicherheit, Zuverlässigkeit und Verfügbarkeit entwickelt, implementiert und verwaltet. Selbst eine Unterbrechung von nur wenigen Minuten muss verhindert werden, denn jede Art von Anlagenstillstand hat sofort erhebliche finanzielle Folgen. So können die Kosten eines Ausfalls schnell in die Hundertausende pro Stunde gehen.

In vielen Industrieanlagen laufen außerdem sicherheitsrelevante Prozesse, die entsprechend gesteuert werden müssen, um Leben und Gesundheit von Mitarbeitern oder Anwohnern nicht zu gefährden oder schwere Umweltfolgen zu verhindern. Deshalb legen die Betreiber besonderen Wert auf stabile Systeme.

An einem Industriestandort herrscht meist die Mentalität: „Solange es funktioniert, muss auch nichts verändert werden".

Sobald ein Anlagensteuerungssystem getestet, in Betrieb genommen wurde und störungsfrei läuft, nehmen Techniker nur sehr ungern Änderungen vor – aus gutem Grund!

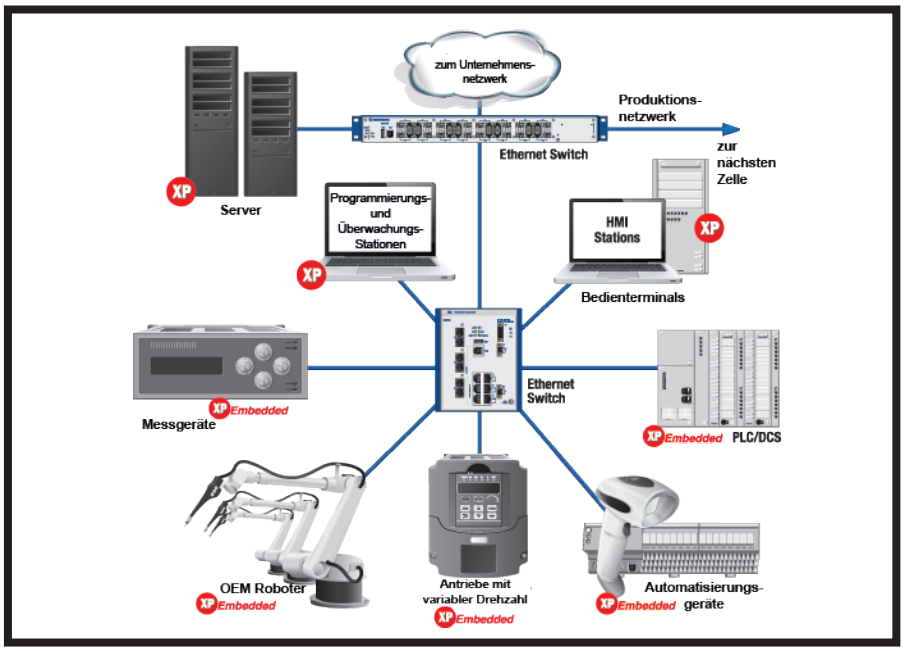

Abbildung 2: Vereinfachte Darstellung eines industriellen Netzwerks mit möglichen Gerätetypen in einer Windows XP- oder Windows XP Embedded-Umgebung

Konkrete Möglichkeiten für Industrieanwendungen

Option 1: Status quo aufrechterhalten und nichts unternehmen

Sie schätzen die Stabilität von Windows XP und wollen kein Upgrade. Möglicherweise haben Sie in den letzten zehn Jahren keine Patches implementiert und erinnern sich nicht, dass es seit der Einführung von Windows XP jemals ernsthafte Probleme mit Computern, Geräten oder Anwendungen gegeben hätte.

Allerdings gab es manchmal Situationen mit einem unerklärlichen Problem. Dann mussten Sie bei Microsoft oder einem Softwareanbieter anrufen und erhielten einen Patch, einen neuen Treiber oder eine aktualisierte Software, die Ihr System zurück in den Normalzustand brachten.

Wahrscheinlich gab es mit Windows XP im Vergleich zu anderen Betriebssystemen relativ wenig Störungen. Bis jetzt mussten Sie sich keine Sorgen machen, weil Sie sich bei Bedarf immer an den Support wenden konnten.

Sie müssen jetzt also entscheiden, ob das Risiko einer Störung ohne Support-Möglichkeit mit den Verfügbarkeitsanforderungen Ihres Unternehmens vereinbar ist.

Dabei ist zu bedenken, dass auch über einen USB-Stick oder Laptop Viren bzw. Schadsoftware in das industrielle Netzwerk eingeschleppt werden können, die ein System mit Windows XP attackieren.

Hinzu kommt, dass sich Cyberangriffe auf Industriesysteme in den letzten fünf Jahren vervielfacht haben. Seit dem Support-Ende für Windows XP ist das Risiko gezielter Angriffe auf dieses Betriebssystem enorm gestiegen.[3, 4]

Option 2: Auf eine neuere Windows-Version migrieren

Sie können Ihre Anwendungen durch ein Upgrade auf eine neuere Windows-Version schützen.

Die meisten Industriebetriebe, die sich für eine Migration auf ein anderes Betriebssystem entscheiden, wissen, dass dafür Planung und Zeit erforderlich sind. Als Zeitrahmen für eine komplette Migration sollten 12 bis 24 Monate veranschlagt werden, um zu gewährleisten, dass alles einwandfrei funktioniert, sobald die Systeme wieder hochgefahren werden.

Als ersten Schritt sollten Sie in Ihrem Anlagennetzwerk eine Bestandsaufnahme von Geräten mit Windows XP und denen mit anderen Betriebssystemen vornehmen. Berücksichtigen Sie dabei auch die bereits beschriebenen, nicht unmittelbar erkennbaren Geräte auf Windows XP-Basis.

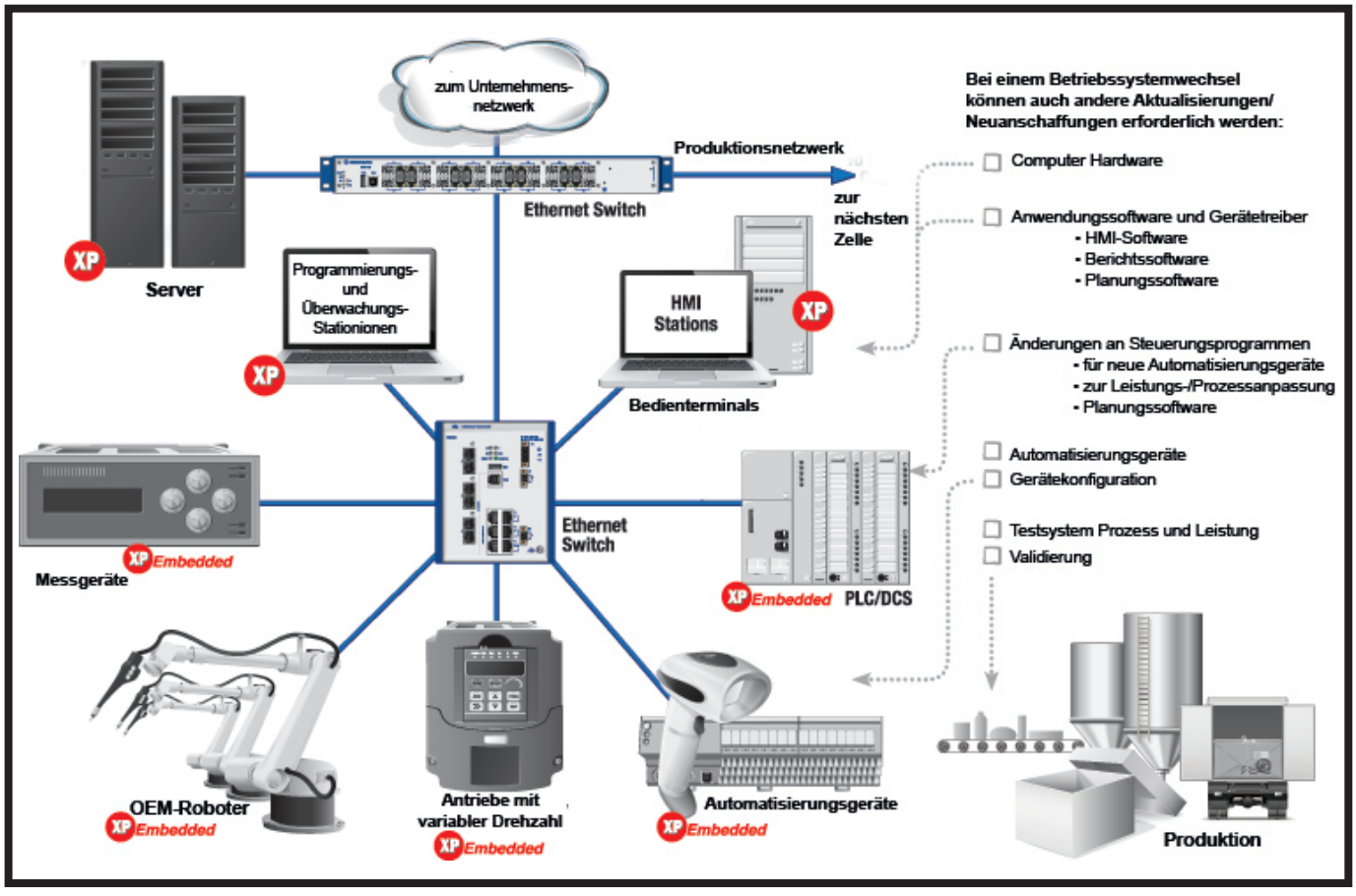

Abbildung 3: Wird nur ein Computer mit Windows XP auf ein neues Betriebssystem umgestellt, sind viele weitere Upgrades nötig, die Tests und Validierungen erfordern, bevor das System wieder in Betrieb genommen werden kann.

Und denken Sie an das Beispiel des großen Pharmaherstellers, der überrascht war, auf wie vielen Geräten Windows XP lief und immer neue Gruppen von Hunderten von Geräten entdeckte.

Beachten Sie den Dominoeffekt, den die Migration auf ein anderes Betriebssystem hat, und stellen Sie fest, welche Bereiche die größte Herausforderung für Ihr Unternehmen darstellen.

Der Dominoeffekt durch die Umstellung von Windows XP auf ein anderes Betriebssystem kann Folgendes umfassen:

- Betriebssystem-Upgrade
- Neue PC-Hardware und/oder Automatisierungsgeräte
- Neue Software für die neuen Geräte
- Neue Treiber für die neue Software
- Austausch von Automatisierungsgeräten, die nicht mit der neuen Software und den neuen Treibern laufen
- Systemintegrationsaufwand für unternehmenskritische Anwendungen, die sich in der neuen Umgebung nicht mehr wie gewohnt verhalten
- Implementierung der geänderten Anwendungen
- Umfassende Tests der neuen Systeme
- Niedrigere Produktivität durch das Migrationsprojekt
- Benutzerschulungen und -Support für die neuen Systeme

Stellen Sie einen Plan auf, der alle Herausforderungen und Maßnahmen gegen den Dominoeffekt sowie Zeitkonflikte mit sonstigen betrieblichen oder IT-Programmen berücksichtigt. Gehen Sie besonders sorgfältig bei der Budgetplanung und der Auswahl geeigneter Mitarbeiter vor. Sehen Sie auf jeden Fall ausreichend Zeit vor, denn bei solchen Projekten ist der Zeitbedarf erfahrungsgemäß oft drei- bis fünfmal größer als ursprünglich angenommen.

Bedenken Sie auch, dass eine Betriebssystemmigration, so notwendig sie auch ist, sich nicht über Nacht bewerkstelligen lässt.

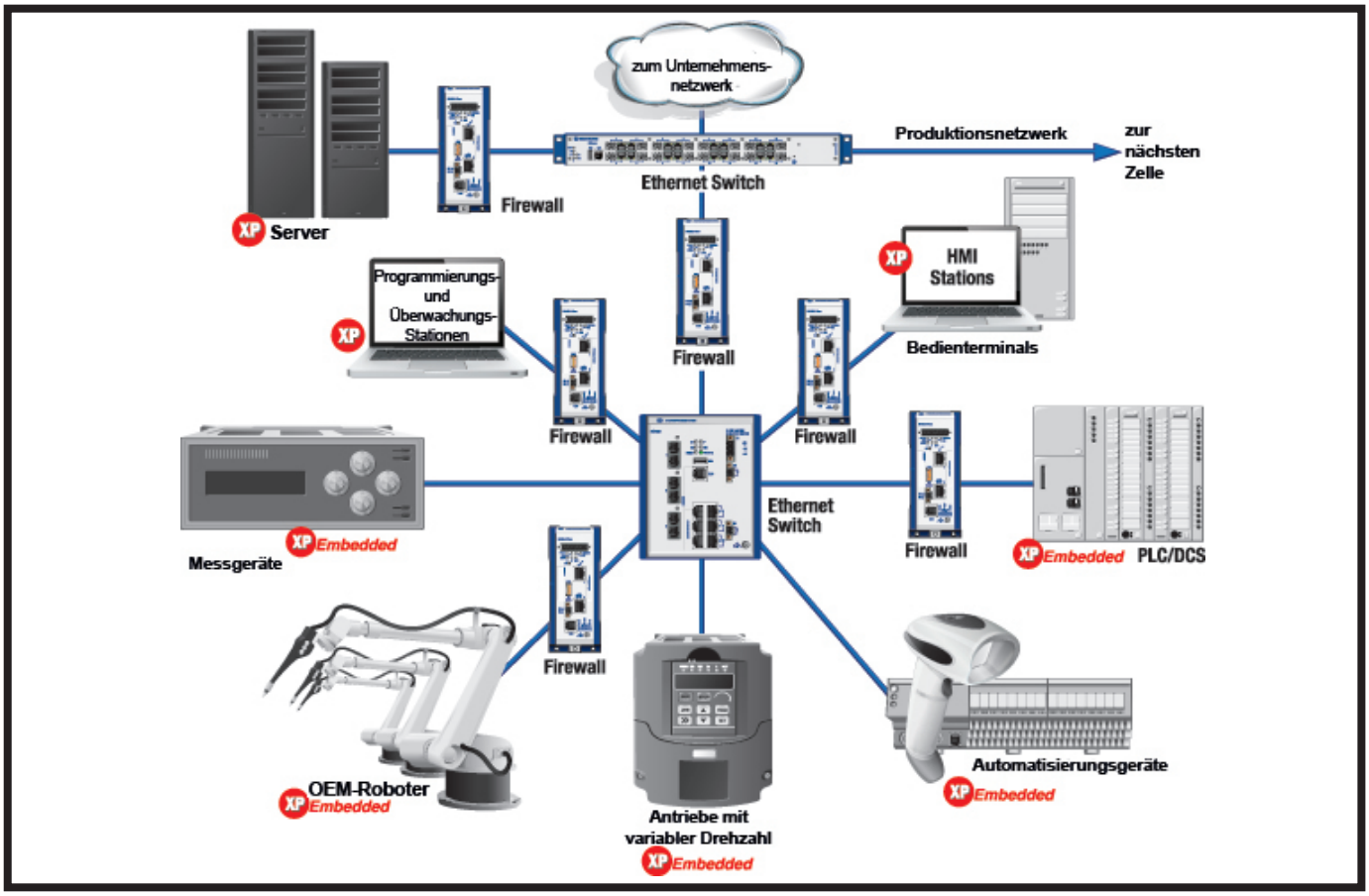

Abbildung 4: Vereinfachte Darstellung eines industriellen Netzwerks mit Belden-Firewalls als Schutz für Computer und Geräte mit Windows XP

Option 3: Risiko von Ausfällen durch Industrie-Firewalls senken

Industrie-Firewalls bieten sofortigen Schutz, und Sie haben Zeit, einen längerfristigen Plan für die Migration auf ein anderes Betriebssystem aufzustellen. In diesen Plan fließt auch die Umstellung der nicht migrationsfähigen Geräte ein.

Industrie-Firewalls können problemlos so konfiguriert werden, dass sie Netzwerkdatenverkehr blockieren, der Schwachstellen in Systemen mit Windows XP ausnutzt, aber trotzdem zulassen, dass die Hauptfunktionen störungsfrei ausgeführt werden. Vorteile dieser Firewalls:

- Netzwerkimplementierung im laufenden Betrieb
- Einfache Installation und Konfiguration
- Speziell für eine Implementierung in Industrieumgebungen ausgelegt, das heißt für raue Bedingungen geeignet und zertifiziert
- Bei Bedarf integrierte Logik für Industrieprotokolle und erstklassiger Schutz durch Deep-Packet-Inspection-Technologie
- Implementierung ohne Maßnahmen gegen einen Dominoeffekt durch die Umstellung auf ein anderes Betriebssystem

Auswirkungen	Option 1: Nichts unternehmen	Option 2: Upgrade auf neue Windows-Version	Option 3: Industrie-Firewalls installieren
Risiko von Ausfällen	Erheblich	Erheblich, bis das Upgrade beendet ist	Minimal
Zeitbedarf	Keiner – bis eine Störung eintritt	Erheblich	Klein
Auswirkungen auf die Produktivität	Keine – bis eine Störung eintritt	Erheblich	Gering
Kosten	Keine – bis eine Störung eintritt	Hoch	Niedrig
Dominoeffekt durch Windows-Upgrade	Keiner – bis eine Störung eintritt	Maßnahmen erforderlich	Nicht vorhanden
Betriebssystem-Upgrade	“	“	“
PC-Hardware-Upgrades	“	“	“
Neue Software für neue Hardware	“	“	“
Neue Treiber für neue Software	“	“	“
Systemintegration von Anwendungen	“	“	“
Austausch von Automatisierungsgeräten	“	“	“
Umfangreiche Tests	“	“	“
Implementierung geänderter Anwendungen	“	“	“
Anwenderschulung und -unterstützung	“	“	“
Niedrigere Produktivität	“	“	“

Tabelle 1: Vergleich der drei Optionen zum Schutz von industriellen Anwendungen nach dem Ende des Supports für Windows XP

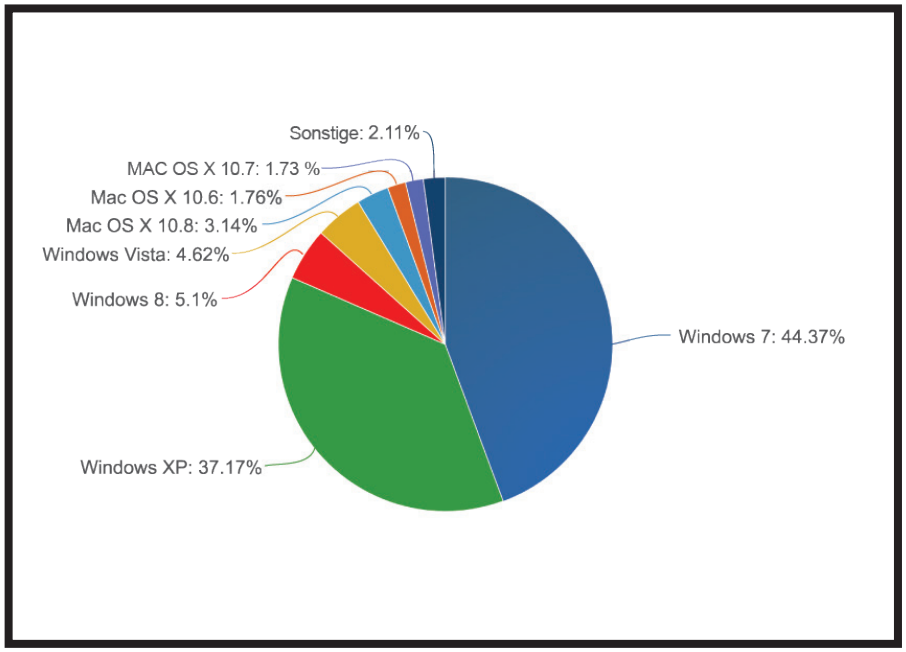

Abbildung 5: : Die Grafik zeigt den globalen Anteil von Windows XP mit Stand vom 8. April 2014. Quelle: Net Market Share[5]

Fazit

Die Einstellung des Supports für Windows XP bedeutet leider den Abschied von einem zuverlässigen Bestandteil von Industrieanwendungen. Dieses Betriebssystem wird weder einfach noch schnell zu ersetzen sein. Bevor Sie das Upgrade auf ein anderes Betriebssystem planen und durchführen, müssen Sie Ihre Systeme so schnell wie möglich schützen.

Belden empfiehlt als Sofortmaßnahme die Installation von Industrie-Firewalls. Das erfordert minimalen Personaleinsatz, ist schnell erledigt, verursacht kaum Schulungs- und Support-Aufwand, macht Migration und Austausch von anderen Systemen überflüssig und ist kostengünstig.

Industrie-Firewalls bieten sofortigen Schutz vor Cyberattacken und ermöglichen eine Migration auf ein anderes Betriebssystem – ganz in Ihrem eigenen Tempo.

Weitere Ressourcen

1. Bei Fragen hilft Ihnen gern ein Belden-Vertriebspartner weiter:
   - Telefon:**+49 (0)7127/14-1809**
   - Verwenden Sie alternativ unser Kontaktformular unter **http://www.beldensolutions.com/de/Kontakt/Standorte/index.phtml**

2. Produktinformationen zu Belden-Industrie-Firewalls und Netzwerkmanagement:
   - **Security-Router EAGLE One**
     http://www.hirschmann.com/de/Hirschmann/Industrial_Ethernet/security-firewall/EAGLE_One/index.phtml
   - **Industrielle Sicherheitslösung Tofino**
     http://www.hirschmann.com/de/Hirschmann/Industrial_Ethernet/security-firewall/Tofino_Xenon/index.phtml
   - **Netzmanagement-Software Industrial HiVision**
     http://www.hirschmann.com/de/Hirschmann/Industrial_Ethernet/Netzmanagement/index.phtml

3. Informationen zum Belden Certified Industrial Network Program, das Services von Netzwerkdesign-Experten, hervorragende Garantieleistungen und Flexibilität für die Zukunft bietet:
   - **http://www.beldensolutions.com/en/Service/CINP/index.phtml**

Lösungen von Belden

Wahrscheinlich denken Sie bei Belden zunächst an Verdrahtungs- und Kabelprodukte. Zu unserem Portfolio gehören aber auch:

- Switches, Router und Industrie-Firewalls von Hirschmann und Garrettcom
- Tofino-Sicherheitsprodukte für die Industrie

Unsere Industrie-Firewalls berücksichtigen insbesondere das Problem, dass der Support für Windows XP ausgelaufen ist. Sie nutzen dieselbe führende Technologie wie IT-Infrastrukturen und Unternehmensnetzwerke, sind jedoch an die speziellen Anforderungen von industriellen Steuerungssystemen und SCADA-Systemen angepasst. Diese Firewalls ermöglichen:

- Eine Netzwerkimplementierung im laufenden Betrieb
- Eine einfache Installation und Konfiguration
- Eine Implementierung in Industrieumgebungen, weil sie speziell dafür ausgelegt und außerdem für raue Bedingungen geeignet und zertifiziert sind
- Bei einigen Modellen integrierte Logik für Industrieprotokolle und erstklassiger Schutz durch Content-Überwachung für geschäftskritische Anwendungen

Mit der Software Industrial HiVision bieten wir Ihnen zudem unentbehrliche Netzwerkmanagement-Tools, mit denen Sie ganz einfach eine Bestandsaufnahme der Geräte in Ihrem Netzwerk machen, Änderungen nachverfolgen und die Leistung des Standortnetzwerks überwachen. Mit diesen Tools können Belden-Lösungen unkompliziert von punktuellen auf standort- oder sogar weltweite Implementierungen skaliert werden.

Belden unterhält Partnerschaften mit Unternehmen, durch deren Kompetenzen und Ressourcen Belden auch Komplettlösungen liefern kann, unter anderem:

- Bewertung von Sicherheitsrisiken
- Design, Implementierung und Zertifizierung von Netzwerken
- Schulungen

Dank dieses gut ausgebauten Partnernetzes können Beldens Industriekunden sich immer auf schnelle, kostengünstige Lösungen verlassen.

Quellenhinweise

1. Microsoft-Website: „Unternehmenskunden: Der Support für Windows XP wurde eingestellt“
   https://www.microsoft.com/en-us/windows/enterprise/end-of-support.aspx
2. Microsoft-Website: „Unternehmenskunden: Der Support für Windows XP wurde eingestellt“
   https://www.microsoft.com/en-us/windows/enterprise/end-of-support.aspx
3. Belden-Präsentation: „ICS Security: What's Happening and What are the Challenges“, Byres, Eric J.
   http://info.belden.com/ics-security-whats-happening-pr-lp-bc
4. Belden Blog: S4 SCADA Security Symposium Takeaway: Time for a Revolution (ICS Security is in Worse Shape than I Thought)
   https://www.tofinosecurity.com/blog/s4-scada-security-symposium-takeaway-time-revolution
5. Website von Netmarketshare: „Market Share Reports“ (Marktanteil von Windows XP anzeigen: Unter „Operating Systems“ oben in der Seitenmitte auswählen)
   http://www.netmarketshare.com/

Referenzen

- Website von Norton by Symantec: „Werden Windows XP-Computer weiterhin geschützt, nachdem Microsoft den Support von Windows XP eingestellt hat?“
  https://support.norton.com/sp/en/us/home/current/solutions/v95977279_EndUserProfile_en_us
- White Paper von Belden: „7 Steps to ICS and SCADA Security“, 16. Februar 2012, Byres, Eric J. und Cusimano, John
  http://web.tofinosecurity.com/download-7-steps/
- Belden-Blog: Industrial Networking: Easy Security Risk Assessment
  http://www.belden.com/blog/industrialsecurity/Industrial-Networking-Easy-Security-Risk-Assessment.cfm
- White Paper von Belden: „Understanding Deep Packet Inspection for SCADA Security“, 20. Dezember 2012, Byres, Eric J.
  http://info.belden.com/dpi-tk-lp
- White Paper von Belden: „Using ANSI/ISA 99 (IEC 62443) to Improve Control System Security“, Januar 2012, Byres, Eric J.
  http://web.tofinosecurity.com/download-the-white-paper-using-ansi-/-isa-99-standards-to-improve-control-system-security
- Belden-Blog: Why Industrial Networks are Different than IT Networks (and What To Do About IT)
  http://www.belden.com/blog/industrialsecurity/Why-Industrial-Networks-are-Different-than-IT-Networks-and-What-to-do-About-It.cfm
- Belden-Blog: Why Patching for SCADA and ICS Security is a Broken Model
  http://www.belden.com/blog/industrialsecurity/Why-Patching-for-SCADA-and-ICS-Security-is-a-Broken-Model.cfm
- Belden-Blog: ICS Security: How Your IT Dept. Can
  http://www.belden.com/blog/industrialsecurity/ICS-Security-How-Your-IT-Dept-Can-Help.cfm

Über Belden

Belden Inc., ein weltweit führender Anbieter von hochwertigen Signalübertragungslösungen, bietet ein umfassendes Produktportfolio, das auf die Anforderungen unternehmenskritischer Netzwerkinfrastrukturen in den Branchen Industrie- und Gebäudeautomation sowie Broadcast zugeschnitten ist.

Mit innovativen Lösungen für die zuverlässige und sichere Übertragung stetig wachsender Datenmengen für Audio- und Videoinformationen, die für moderne Anwendungen benötigt werden, übernimmt Belden eine Schlüsselrolle bei der globalen Veränderung hin zu einer vernetzten Welt.

Das Unternehmen mit Hauptsitz in St. Louis, USA, wurde 1902 gegründet und betreibt Fertigungsstätten in Nord- und Südamerika, Europa und Asien.
Für weitere Informationen besuchen Sie uns unter www.belden.com und folgen Sie uns auf: @BeldenInc.

Phone **+49 (0)7127/14-1809** **www.beldensolutions.com**