Windows XP-Support ist am Ende ? was nun?

Windows XP-Support ist am Ende - was nun?

Kommentar von Marcus Henschel, Geschäftsführer secion GmbH
Zum April 2014 stellte Microsoft den Support für sein Betriebssystem Windows XP ein. Für manche ist die sinnvollste Konsequenz ein Update auf die aktuelle Version des neuen Betriebssystems Windows 8. Auch aus sicherheitstechnischer Sicht ist ein Wechsel die beste Alternative. Denn für Windows 8 ist die Auswahl an Antivirus-, Firewall- und Verschlüsselungs¬lösungen vergleichsweise groß; außerdem versorgt Microsoft das System mit aktuellen Patches.
Doch dieser Schritt kommt nicht für alle Unternehmen in Frage. Aus verschiedenen Gründen ist Windows XP noch allgegenwärtig, z.B. bei Banken und Versicherungen in Kassen, Serviceterminals, Cash- und Non Cash-Systemen, in der Industrie bei Steuerungssystemen (Automationsanlagen), in der Energiewirtschaft und der chemischen Industrie. Umfragen von secion zufolge sprechen sich Unternehmen aus mehreren Gründen gegen eine Ablösung von XP aus, z.B. weil auf den Windows XP-Clients Anwendungen laufen, die unter den aktuellen Windows 7-/8-Versionen nicht betrieben werden können. Auch Mangel an Budget, Zeit und internen Ressourcen erschweren den Wechsel. Wie sollen sich Betroffene verhalten, die aus verschiedenen Gründen ihre Windows XP-Systeme nicht so einfach austauschen können und vor der Frage stehen, wie aus Security-Sicht der fortlaufende Einsatz von Windows XP verantwortet und sicher geregelt werden kann?
Eine der größten Gefahren liegt darin, dass Microsoft keine Security Patches mehr bereitstellen wird und damit Schwachstellen ab sofort nicht mehr behoben werden. Somit könnte Windows XP zu einem der gefährdetsten Betriebssysteme überhaupt werden. Denn die Gefahr für sogenannte "Zero Day Exploits" steigt täglich. Dennoch gibt es Möglichkeiten, diese Systeme abzusichern - unabhängig von der Branche. Die Mechanismen lassen sich allein oder in Kombination anwenden.
Als erste Aktion empfiehlt sich das Härten des Betriebssystems, also eine strikte Konfiguration von Windows XP. Können beispielsweise bestimmte Dienste und Benutzerkonten, die für den spezifischen Einsatz des Systems überflüssig sind, komplett abgeschaltet werden? Ziel ist, möglichst viele Angriffsvektoren auszuschalten. Dies kann durch Software Whitelisting unterstützt werden: Damit werden nur Programme ausgeführt, die auf der Positivliste (Whitelist) stehen. Zudem sollte die Windows Firewall aktiviert sein, um ein- und ausgehenden Netzwerkverkehr ausschließlich zu definierten IP-Adressen und/oder Netzen zu erlauben.
Als zweite Aktion ist eine Netzwerksegmentierung hilfreich, bei welcher das Netzwerk, bestehend aus Windows XP-Systemen, von anderen vorhandenen getrennt wird. So können sich im Angriffsfall Bedrohungen nicht in die komplette Infrastruktur ausbreiten. Eine Segmentierung kann grundlegend am Switch (VLAN) durchgeführt werden; es empfiehlt sich zudem, eine Firewall anzubinden. Sie ist in der Lage, Netzsegmente, in denen sich die Windows XP-Systeme befinden, noch feinmaschiger aufzuteilen und zugleich den Datenverkehr auf Anomalien zu untersuchen oder den gesamten Datenverkehr der XP-Systeme in Richtung Internet zu blockieren. Aktuelle Firewall-Systeme stellen dazu Virenscanner, Intrusion Detection-
 Prevention-Funktionen zur Verfügung, die für eine möglichst sichere Datenkommunikation sorgen.
Als dritte Aktion sollte die Windows XP-Systemintegrität überwacht werden. Dazu ist Sicherheitssoftware erhältlich, die wie eine Art Firewall für die Festplatte agiert und anders als Antivirussoftware gänzlich ohne Signaturen auskommt. Die Technologie kontrolliert die Schreibzugriffe auf die Festplatte und macht Windows-Systeme immun gegen Angriffe und die Ausnutzung von Zero Day Exploits, indem sie die Ausführung von Schadcodes schon im Ansatz unterbindet.
Diese Maßnahmen können bei der Absicherung vorhandener Windows XP-Systeme helfen; sind aber letztendlich eher Workaround-Methoden. Unabhängig davon entsteht jedoch eine solide Sicherheitsarchitektur, die sich auch auf die kommenden (Windows-)Betriebssysteme anwenden lässt.
User, die sich genauer mit den einzelnen Möglichkeiten im Umgang mit Windows XP beschäftigen möchten, finden weitere Informationen unter https://www. secion.de/windows-xp-support-ist-am-ende.html?pk_campaign=PR .
Über secion GmbH
"Service nach Maß - der Sicherheit halber" - Nach diesem Motto lösen wir, die secion GmbH mit Sitz in Hamburg, seit unserer Gründung im Jahr 2004 verlässlich die Herausforderungen unserer Kunden. Begonnen als Dienstleister für IT-Sicherheitsüberprüfungen haben wir uns rasch zu einem in Norddeutschland führenden Systemhaus für IT Security entwickelt. Mit unserem Leistungsspektrum und technischem Know-how decken wir alle relevanten Themen im Bereich IT-Sicherheit ab und sind branchenübergreifend erfolgreich. Zusätzlich hat sich die secion GmbH als Spezialist für Output Management insbesondere in Deutschland, Österreich und der Schweiz etabliert. Maßgeblich hierfür ist unsere Erfahrung in Projektmanagement, individueller Entwicklung und Implementierung. Unsere Philosophie ist, unseren Serviceanspruch in Punkto Zuverlässigkeit, Schnelligkeit und Kompetenz im internen Umgang und im Umgang mit allen Geschäftspartnern permanent zu leben - und stets zu reflektieren.
Neben unserer objektiven Lösungsfindung schätzen unsere Kunden besonders die initiative Beratung über neuste IT-Sicherheitsthemen und Trends am Markt. Kontinuität in der Zusammenarbeit mit fest definierten Ansprechpartnern, kombiniert mit unserem Expertenwissen, sind für Unternehmen weitere wesentliche Kriterien, sich für secion und eine langfristige Zusammenarbeit zu entscheiden.

secion GmbH
Paul-Dessau-Str. 8
D-22761 Hamburg
Tel+49-40-389071-0
Fax +49-40-389071-299
info@secion.de
 https://www.secion.de
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=563010" width="1" height="1">

Pressekontakt

secion GmbH

22761 Hamburg

Firmenkontakt

secion GmbH

22761 Hamburg

Weitere Informationen finden sich auf unserer Homepage