TREND MICRO™

Verwalten von Legacy-Betriebssystemen

Ein Leben nach Windows XP

HAFTUNGSAUSSCHLUSS

Die in diesem Dokument bereitgestellten Informationen sind lediglich allgemeiner Natur und für Aufklärungszwecke gedacht. Sie stellen keine Rechtsberatung dar und sind nicht als solche auszulegen. Die in diesem Dokument bereitgestellten Informationen finden womöglich nicht auf alle Sachverhalte Anwendung und spiegeln womöglich nicht die jüngsten Sachverhalte wider. Die Inhalte in diesem Dokument sind ohne eine Rechtsberatung auf der Grundlage der vorgestellten besonderen Fakten und Umstände nicht als verlässlich oder als Handlungsanweisungen zu verstehen und nicht in anderer Weise auszulegen. Trend Micro behält sich das Recht vor, die Inhalte dieses Dokuments zu jeder Zeit und ohne Vorankündigung zu ändern.

Übersetzungen in andere Sprachen sind ausschließlich als Unterstützung gedacht. Die Genauigkeit der Übersetzung wird weder garantiert noch stillschweigend zugesichert. Bei Fragen zur Genauigkeit einer Übersetzung lesen Sie bitte in der offiziellen Fassung des Dokuments in der Ursprungssprache nach. Diskrepanzen oder Abweichungen in der übersetzten Fassung sind nicht bindend und haben im Hinblick auf Compliance oder Durchsetzung keine Rechtswirkung.

Trend Micro bemüht sich in diesem Dokument im angemessenen Umfang um die Bereitstellung genauer und aktueller Informationen, übernimmt jedoch hinsichtlich Genauigkeit, Aktualität und Vollständigkeit keine Haftung und macht diesbezüglich keine Zusicherungen. Sie erklären Ihr Einverständnis, dass Sie dieses Dokument und seine Inhalte auf eigene Gefahr nutzen und sich darauf berufen. Trend Micro übernimmt keine Gewährleistung, weder ausdrücklich noch stillschweigend. Weder Trend Micro noch Dritte, die an der Konzeption, Erstellung oder Bereitstellung dieses Dokuments beteiligt waren, haften für Folgeschäden oder Verluste, insbesondere direkte, indirekte, besondere oder Nebenschäden, entgangenen Gewinn oder besondere Schäden, die sich aus dem Zugriff auf, der Verwendung oder Unmöglichkeit der Verwendung oder in Zusammenhang mit der Verwendung dieses Dokuments oder aus Fehlern und Auslassungen im Inhalt ergeben. Die Verwendung dieser Informationen stellt die Zustimmung zur Nutzung in der vorliegenden Form dar.

Nach mehr als zehn Jahren stellt Microsoft am 8. April 2014 die Unterstützung von Windows® XP ein. Anwender erhalten danach keine Sicherheits-Updates mehr, und auch keine sicherheitsunabhängigen Hotfixes oder kostenlose beziehungsweise kostenpflichtige Support-Optionen. Auch die technischen Online-Inhalte werden nicht mehr aktualisiert.

All das kann für Unternehmenssysteme mit Windows XP ernste Konsequenzen haben. Diese Studie zeigt die technischen Gefahren auf, mögliche Haftungs- sowie Compliance-Probleme, aber auch die Mehrkosten für User Computing, wenn Unternehmen das Betriebssystem weiterhin nutzen.

Windows XP im heutigen Betriebssystemmarkt

Bild 1 zeigt die in den vergangenen Jahren weltweit rückläufige Nutzung von Windows XP. Dennoch wird das Betriebssystem noch häufig eingesetzt, schließlich beherrscht Microsoft den Client-Betriebssystemmarkt seit 20 Jahren. Einer IDC-Studie zufolge laufen neun von zehn PCs immer noch mit einem Windows-Betriebssystem.[1] Eine Umfrage von Spiceworks hat außerdem gezeigt, dass im Dezember 2013 immer noch 76% der professionellen IT-Anwender Windows XP nutzten. 97% davon setzen das Betriebssystem auf dem Desktop ein und 68% auf Laptops.[2]

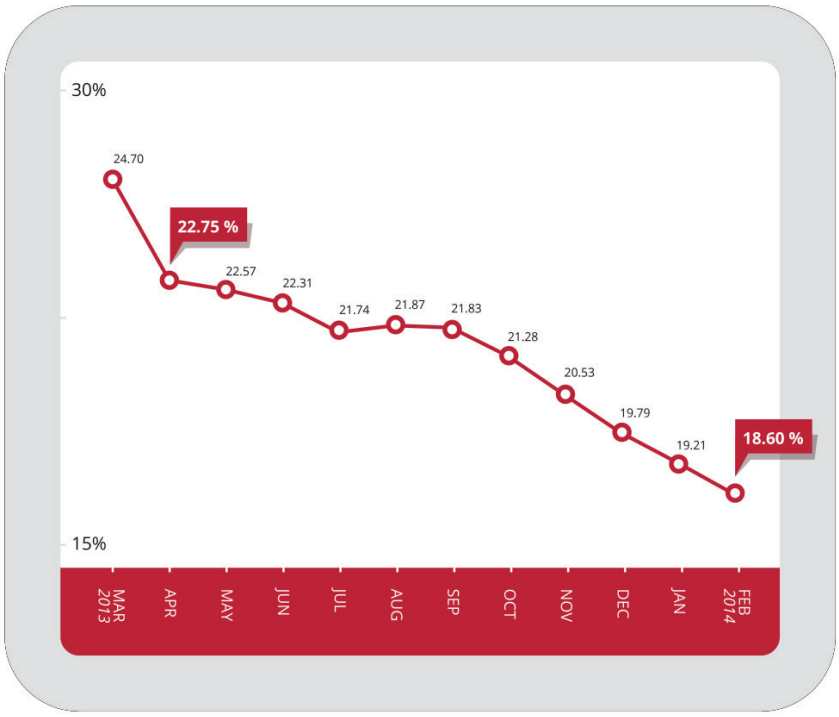

Bild 1: Marktanteile von Windows XP zwischen März 2013 und Februar 2014, *Quelle: StatCounter.com*

1 Al Gillen, Randy Perry, and Nancy Selig. (May 2012). "Mitigating Risk: Why Sticking with Windows XP Is a Bad Idea." Last accessed March 21, 2014, http://www.microsoft.com/de-de/download/details.aspx?id=29883.
2 Spiceworks. (December 2013). "Getting Over Your XP: Windows XP End-of-Life and Why Breaking Up Is Hard to Do." Last accessed March 21, 2014, http://www.spiceworks.com/voit/reports/windows-xp-end-of-life/.

Dies ist nicht das erste Mal, dass Microsoft die Unterstützung für eine Windows-Version einstellt, doch noch nie geschah dies, solange die Version noch genutzt wurde. Möglicherweise ist die Wirtschaftskrise 2008 einer der Faktoren, der zur anhaltenden Dominanz des Betriebssystems beigetragen hat. Denn infolge der Krise litten Unternehmen unter Umsatzeinbußen, Entlassungen und Kostenreduzierungen.[3] Auch mag der fünfjährige Abstand zwischen Windows XP und Windows Vista Unternehmen nicht zu einem Update genötigt haben.

Die Daten in Bild 1 sind beunruhigend, denn sie zeigen, dass ein großer Teil des Desktop-Markts steigenden Bedrohungen ausgeliefert sein wird. Als Windows XP 2001 eingeführt wurde, war Mobilität noch selten, und Netzwerke wurden festverdrahtet betrieben. Der Netzwerkzugriff ging über vom Unternehmen kontrollierte Netzwerke und der Remote-Zugriff über Telefon. Auch waren die PC-Bedrohungen darauf ausgerichtet, Nutzer zu ärgern und ihre Zeit zu verschwenden und nicht ihre kritischen Daten zu entwenden. Kurz gesagt, die Notwendigkeit der Migration von Windows XP ergibt sich aus der Tatsache, dass die Ära, für die das Betriebssystem entworfen wurde, schon lange vorbei ist.

3 Barbara Kiviat. (September 16, 2013). Time. “Explaining the Financial Crisis: Why Do We Still Not Know What Happened?” Last accessed March 21, 2014, http://business.time.com/2013/09/16/explaining-the-financial-crisis-why-do-we-still-not-know- what-happened/.

Schwierigkeiten einer Migration

Trotz der Dringlichkeit ist die Migration auf ein anderes Betriebssystem nicht so einfach. IT-Fachleute fürchten die Herausforderungen, die mit einem Upgrade des Betriebssystems verbunden sind. Das geht aus einer Dell-Studie hervor.[4] Hier werden als Herausforderung die Anwendungskompatibilität (41%) sowie Nutzerschulung und -unterstützung (33%) genannt. Ein Upgrade bringt zudem auch die Notwendigkeit mit sich, neue Hardware zu kaufen – ebenfalls ein mögliches Problem bei der Migration.

Analogie Windows XP und Java 6

Als Oracle im Februar 2013 Java™ 6 abkündigte und keine Sicherheits-Updates für die Schwachstellen mehr lieferte, stürzten sich die Angreifer sofort auf die ungepatchten Versionen der Software. Einige Monate später gab es Versuche, CVE-2013-2463 auszunutzen. Die Lücke betraf einige Java-Versionen, unter anderen auch Java 6.[5] Nicht genug damit, dass Oracle keine Sicherheits-Updates liefert, wurde der verwendete Exploit auch ins Neutrino Exploit Kit integriert, und das kann zu weiteren erfolgreichen Angriffen führen.

Java 6 kann als Beispiel dafür dienen, was Windows XP-Nutzern nach dem 8. April blühen könnte. Windows XP-Bedrohungen werden immer gefährlicher. Doch gemeinsamer Code von Windows XP und neueren Windows-Versionen könnte “Hinweise” auf erkannte Schwachstellen liefern, die gepatcht sein wollen.

Heutige Bedrohungen haben sich bedeutend verändert und eine Wirklichkeit geschaffen, in der Windows XP-Lücken ein ganzes Unternehmen und dessen Daten aufs Spiel setzen können. Daher ist es empfehlenswert, eine Lösung wie Trend Micro™ OfficeScan™ Intrusion Defense Firewall einzusetzen, um die Lücken abzusichern, für die es keine Software-Patches mehr gibt. Der Schutz funktioniert auf Basis der Annahme, dass Exploits einen bestimmten oder definierten Netzwerkpfad zu oder von einer Anwendung weg wählen, um eine Lücke auszunutzen. Daher ist es möglich, die Kommunikation mit der anvisierten Software über Regeln für die Netzwerkschicht zu kontrollieren.

4 Dell Inc. (September 2013) “Migrating Away from Windows XP: A Survey of IT Professionals.” Last accessed March 21, 2014, https://www.kace.com/de/resource-center/resources/analyst-reports/migrating_away_from_windows_xp_a_survey_of_it_professionals.

5 Gelo Abendan. (August 27, 2013). TrendLabs Security Intelligence Blog. “Java 6 Zero-Day Exploit Pushes Users to Shift to Latest Java Version.” Last accessed March 21, 2014, http://blog.trendmicro.de/zero-day-exploit-fuer-java-6-oracle-patcht-diese-version-nicht-mehr/.

Mögliche technische Risiken für Unternehmen

Eine Ankündigung von Microsoft aus dem Oktober 2013 besagt, dass die Zahl der Windows XP-Infektionen nach der Abkündigung der Unterstützung um 66% steigen könnte.[6] Angreifer werden versuchen, Sicherheitslücken in Windows XP zu finden, indem sie Reverse-Engineering-Techniken auf Sicherheits-Updates für neuere Windows-Versionen anwenden. Cyberkriminelle könnten Microsoft zufolge sogar Exploits „horten“, um sie nach dem Support-Ende für Windows XP anzuwenden.[7]

Internet Explorer® (IE) birgt weitere Risiken, die sich dann zeigen werden, denn keine der Browser-Versionen ab IE 8 ist mit der Plattform kompatibel. Natürlich können Nutzer einen anderen Browser einsetzen, doch auch das bedeutet keinen 100-prozentigen Schutz vor Browser-Exploits.

Ein weiteres potenzielles Risiko ergibt sich daraus, dass angreifbare Endpunkte als “Startrampe” für Schadsoftware der nächsten Generation genutzt werden könnten, ein Szenario, mit dem abgekündigte Systeme nur schwer umgehen können. Zielgerichtete Angriffskampagnen nutzen häufig Software Exploits, um in Systeme einzudringen, um Daten zu entwenden oder um zu spionieren. Und jeder PC mit Windows XP ist aus Sicht der Angreifer ein offensichtlicher Schwachpunkt.

Kosten bei nicht vollzogener Migration

Wenn Legacy-Systeme und Software nicht entsorgt oder ersetzt werden, so bedeutet dies ein signifikantes Risiko für Unternehmen, einschließlich möglicherweise nicht kalkulierbarer Kosten und Konsequenzen. Auf der anderen Seite gibt es auch Argumente, die in gewissem Maße für die Beibehaltung des Betriebssystems sprechen: Nutzer müssen dann nicht den Umgang mit einem neuen Betriebssystem erlernen und Entwickler kennen die Plattform in- und auswändig.

Warum also wechseln? In erster Linie sollten IT-Administratoren die Kosten für die Wartung von Windows XP nach der Beendigung der Unterstützung überdenken. Unternehmen, die an Systemen mit dem Betriebssystem festhalten müssen, werden sehr wahrscheinlich Kunden-Support zur Verfügung stellen müssen, und das bedeutet Microsoft Premier Online-Kunde zu werden.

Doch damit nicht genug. Die bereits zitierte IDC-Studie besagt, dass die Administration, der Support und das Management von Windows XP-Systemen bedeutend teurer sind als für Windows 7-Systeme. Tabelle 1 zeigt, dass der Zeitaufwand für den Betrieb von Windows XP auch höher ist als der für Windows 7.

6 Gregg Keizer. (October 30, 2013) Computerworld. “Windows XP Infection Rate May Jump 66% After Patches End in April.” Last accessed March 21, 2014, http://www.computerworld.com/s/article/9243660/Windows_XP_infection_rate_may_jump_66_aft er_patches_end_in_April.

7 Dan Worth. (March 10, 2014). V3.co.uk. “Hackers Hoarding Windows XP Exploits for Cut-Off Bonanza.” Last accessed March 21, 2014, http://www.v3.co.uk/v3-uk/analysis/2333009/hackers-hoarding-windows-xp-exploits-for-cut-off-bonanza.

Durchschnittliche Zeitaufwendungen für betriebliche Aktivitäten	
Windows XP	**Windows 7**
Betriebsaktivitäten	
3 Stunden	0,9 Stunden
Downtime	
2,9 Stunden	0,6 Stunden
Verlorene Zeit der Nutzer pro Jahr	
9 Stunden	1,2 Stunden

Quelle: IDC und Microsoft

Folgen einer nicht vollzogenen Migration

Für den Fall, dass Unternehmen ihre Windows XP-Systeme weiter betreiben müssen, empfiehlt sich der Einsatz von Whitelisting für eine höhere Sicherheit der Unternehmensumgebung. Trend Micro™ Endpoint Application Control™ kontrolliert Anwendungen, die auf Endpunkten laufen. Diese zusätzliche Schutzschicht verhindert die Installation und Ausführung jeglicher unerwünschter, unsicherer oder bösartiger Applikationen auf den Endpunkten. Mit einer Sicherheitssoftware für Endpunkte wie Trend Micro OfficeScan lässt sich die Lösung einfach einsetzen und verwalten.

Bild 2: Es ist einfach, Endpoint Application Control mit Trend Micro Complete User Protection-Lösungen zu integrieren, um mehrere, miteinander verbundene Schichten für den Informationsschutz vor Bedrohungen zu gewährleisten.

Das Upgrade von Betriebssystemen sollte von Unternehmen mit Vorrang angegangen werden. Diejenigen Organisationen aber, die auch künftig bei Windows XP bleiben müssen, sollten die folgenden Best Practices beherzigen. Zwar werden die Empfehlungen vorhandene Probleme nicht lösen, doch können sie dabei helfen, künftige Probleme zu vermeiden:

- **Virtualisieren der Windows XP-Umgebung:** Dadurch entsteht eine zusätzliche Sicherheitsschicht, und ein effizienteres Managment wird möglich.
- **Einsetzen eines Read-Only Domain Controllers (RODC) wie Windows 2008, 2008 R2, 2012 oder 2012 R2 im Windows XP LAN**: Für ein effektives Management empfiehlt sich der Einsatz eines Domain Controllers auf dem LAN-Switch, an den alle Windows XP-Systeme angebunden sind. Wird der Domain Controller im Read-Only-Modus vorgehalten, so können Systemadministratoren Windows-Maschinen aus der Ferne effizient verwalten, ohne die Sicherheit des gesamten Netzwerks zu gefährden.
- **Implementieren der strengsten Settings für die Sicherheits-Gruppenrichtlinie für Windows XP-Maschinen:** Die Sicherheit sollte den Anforderungen eines Unternehmens entsprechen. Dennoch ist es sehr zu empfehlen, die Settings der Specialized Security-Limited Functionality (SSLF)-Gruppenpolicy anzuwenden. Weitere Informationen zu Best Practices für die Gruppenpolicy-Settings gibt es im “Windows XP Security Guide” und im “Threats and Countermeasures Guide”.[8]
- **Wenn möglich, sollte allen Windows XP-Maschinen die Kommunikation mit externen Netzwerken verboten werden:** Unternehmen sollten Updates zu Software von Drittanbietern bei Bedarf manuell liefern. Ist die Kommunikation mit externen Netzwerken unvemeidlich, so empfiehlt sich der Einsatz eines Web Proxys oder einer Application-Layer Firewall.
- **Den Einsatz anderer Browser überlegen:** Wenn die Nutzung von IE unvermeidbar ist, sollte der Browser nur dann verwendet werden, wenn eine Site mit keinem anderen Browser zusammenarbeitet.
- **Einsatz eines Intrusion Prevention System (IPS)-Geräts im LAN:** Dies kann entweder auf dem Switched Port Analyzer (SPAN)-Port geschehen oder zwischen dem LAN-Switch und dem restlichen Netzwerk.

8 Microsoft. (2014). Microsoft Download Center. “Windows XP Security Guide.” Last accessed March 21, 2014, http://www.microsoft.com/en-us/download/details.aspx?id=962;
Microsoft. (2014). Microsoft Download Center. “The Threats and Countermeasures Guide.” Last accessed March 21, 2014, http://www.microsoft.com/en-us/download/details.aspx?id=24696.

Trend Micro wird den Schutz der Endpunkte auch auf Windows XP-Nutzer erweitern, um den Übergang zu neueren Windows-Betriebssystemen zu vereinfachen. Diese Unterstützung der Sicherheit der Endpunkte mit Windows XP in OfficeScan und Trend Micro™ Worry-Free Business Security™ läuft bis zum 30. Januar 2017.[9] Auch wird ein OfficeScan Plug-in, Intrusion Defense Firewall, einen hohen Schutz für die Endpunkte bieten, denn die Firewall ergänzt die hochwirksame Client-Sicherheit mit dem Schutz durch Host Intrusion Prevention System (HIPS) auf Netzwerkebene.

Trend Micro™ Deep Discovery wiederum bietet fortschrittlichen Schutz vor zielgerichteten Angriffen und identifiziert verschleierte Bedrohungen in Echtzeit. Des weiteren bietet Deep Discovery tiefgehende Analysen und Handlungsempfehlungen für die Überprüfung, Wiederherstellung und Verteidigung gegen zielgerichtete Angriffe.

„Das Vorhandensein von Windows XP-Systemen im Unternehmen, auch wenn es nur wenige sind, wird nach der Abkündigung des Support bedeutende Schwachstellen und Sicherheitsrisiken mit sich bringen. Es wird schwierig, ihre Weiterführung zu rechtfertigen. Aufgrund der wachsenden Zahl der Bedrohungen, gegen die das Betriebssystem nicht geschützt werden kann, ist es sehr empfehlenswert, Windows XP aus den Organisationen zu entfernen."

– Edward Ray,
Senior Cyberthreat Researcher

9 Trend Micro Incorporated. (2014). "Trend Micro's Official Statement for Windows XP End of Support." Last accessed March 21, 2014, http://esupport.trendmicro.com/solution/en-us/1101907.aspx.

Entwickelt von:

TrendLabs

Global Technical Support & R&D Center of **TREND MICRO**

Über TREND MICRO

Trend Micro, der international führende Anbieter für Cloud-Security, ermöglicht Unternehmen und Endanwendern den sicheren Austausch digitaler Informationen. Als Vorreiter bei Server-Security mit mehr als zwanzigjähriger Erfahrung bietet Trend Micro client-, server- und cloud-basierte Sicherheitslösungen an. Diese Lösungen für Internet-Content-Security und Threat-Management erkennen neue Bedrohungen schneller und sichern Daten in physischen, virtualisierten und Cloud-Umgebungen umfassend ab. Die auf der Cloud-Computing-Infrastruktur des Trend Micro Smart Protection Network basierenden Technologien, Lösungen und Dienstleistungen wehren Bedrohungen dort ab, wo sie entstehen: im Internet. Unterstützt werden sie dabei von mehr als 1.000 weltweit tätigen Sicherheits-Experten. Trend Micro ist ein transnationales Unternehmen mit Hauptsitz in Tokio und bietet seine Sicherheitslösungen über Vertriebspartner weltweit an.

http://www.trendmicro.de/
http://blog.trendmicro.de/
http://www.twitter.com/TrendMicroDE

TREND MICRO™

Securing Your Journey to the Cloud

TREND MICRO DEUTSCHLAND GMBH

Central & Eastern Europe
Zeppelinstraße 1
85399 Hallbergmoos
Tel: +49 811 88990-700
Fax: +49 811 88990-799
www.trendmicro.com