Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- ● Überblick
- ● Lebenszyklus eines Betriebssystems
- ● Schützen Sie sich

Das Ende von Windows XP

Überblick

Windows XP hat sich als eines der beliebtesten Betriebssysteme in der Geschichte der Personal Computer erwiesen, es war zeitweilig sogar auf der Mehrzahl aller PCs weltweit im Einsatz. Windows XP ist jedoch alt, und Microsoft wird jegliche Unterstützung dafür in Kürze einstellen. Es wurde vor mehr als 12 Jahren veröffentlicht und erreicht das Lebensende (EOL) am 8. April 2014. Microsoft wird von diesem Zeitpunkt ab keine weiteren Endbenutzer-Aktualisierungen oder Sicherheitspatches bereitstellen. Da ca. 25% aller Desktop-PCs weltweit noch Windows XP nutzen (nur Windows 7 ist weiter verbreitet), sehen sich Millionen Anwender mit großen Risiken konfrontiert wenn dies geschieht. Heimanwender sind jedoch nicht allein betroffen, Windows XP ist noch immer auch in Büros, Industriesteuerungen, Geldautomaten, Medizin- und Kassensystemen und vielen weiteren Geräten weit verbreitet. Wir beschreiben im folgenden Text die durch ein nicht länger unterstütztes Windows XP entstehenden Risiken, und wie Sie sich davor schützen können.

Gastautor

Jason Fossen ist Spezialist für Microsoft Windows Sicherheit bei Enclave Consulting LLC, der Autor des sechstägigen Kurses Securing Windows with the Critical Security Controls (SEC505) bei SANS, und stellt PowerShell Sicherheitsskripte unter http://cyber-defense.sans.org/blog/ bereit.

Lebenszyklus eines Betriebssystems

Es ist Ihnen vielleicht nicht bewusst, doch jedes Betriebssystem hat eine gewisse, begrenzte Lebenszeit. Der Hersteller, der das Betriebssystem geschaffen hat, stellt Aktualisierungen und Sicherheitspatches bereit die neue Funktionen hinzufügen, die Stabilität und Performance verbessern und das System sicher halten. Das Problem entsteht wenn der Hersteller ein Betriebssystem nicht mehr länger unterstützt, weil er seine Kapazitäten auf das neueste, beste Betriebssystem aus seinem Hause konzentriert. Das bedeutet dass der Hersteller keinerlei Aktualisierungen mehr bereitstellen wird, auch wenn sich herausstellt dass das alte Betriebssystem verwundbar ist und Cyberkriminelle die Kontrolle darüber übernehmen können. Exakt dies wird mit Windows XP ab April geschehen. Selbst wenn Microsoft davon erfährt, dass unzählige PCs weltweit von einer neuentdeckten Schwachstelle in Windows XP betroffen sind, wird es diese nicht mehr schließen.

Schützen Sie sich

Um sich gegen Angriffe von Cyberkriminellen zu wappnen, müssen Sie ein Betriebssystem einsetzen dass noch aktiv vom Hersteller unterstützt wird. Wenn Sie es sich leisten können empfehlen wir sogar die Anschaffung eines komplett neuen Computers, denn viele PCs die bisher mit Windows XP betrieben wurden werden von heutigen Betriebssystemen gar nicht mehr oder nur teilweise unterstützt. Falls Sie sich keinen neuen PC leisten können, investieren Sie aber unbedingt

© The SANS Institute 2014

Das Ende von Windows XP

in ein neues Betriebssystem. Für Unternehmen ist der Umstieg wahrscheinlich einfacher, wenn sie auf Windows 7 statt Windows 8 migrieren, da dessen Benutzeroberfläche Windows XP noch mehr ähnelt. Windows 8 ist jedoch nochmals sicherer als vorherige Versionen von Windows. Sie können natürlich auch Betriebssysteme anderer Hersteller in Betracht ziehen oder sogar auf ein kostenloses Betriebssystem wie Linux wechseln. Welchen Weg Sie auch einschlagen, es gibt keine Zeit mehr zu verlieren. Falls gewichtige Gründe einen Umstieg vor April unmöglich machen, berücksichtigen Sie die folgenden Vorsichtsmaßnahmen:

Wenn Windows XP nicht länger unterstützt wird sollten Sie schnellstmöglich zu einem modernen Betriebssystem wechseln das aktiv von seinem Hersteller weiterentwickelt wird, und darauf achten es stets aktuell zu halten.

- Benutzen Sie Ihren Windows XP Computer nur für das absolut Notwendigste. Wenn Ihr Unternehmen z.B. ein altes Programm nutzt dass nur unter Windows XP lauffähig ist, nutzen Sie diesen PC nicht für andere Aktivitäten wie den Zugriff auf E-Mails oder das Internet.

- Falls Sie Ihren Windows XP Computer weiterhin für das Surfen im Internet nutzen müssen, wechseln Sie vom Internet Explorer zu einem alternativen Browser wie Mozilla Firefox, Google Chrome, oder Opera. Achten Sie darauf diesen Browser stets aktuell zu halten, und dass der Hersteller diesen Browser auch zukünftig unter Windows XP unterstützt.

- Nutzen Sie keine in Windows XP eingebauten Anwendungen, die Dateien aus dem Internet abrufen, wie z.B. Windows Media Player. Greifen Sie stattdessen auf separate Anwendungen anderer Hersteller zurück, die noch aktiv entwickelt werden, und halten Sie diese aktuell.

- Ziehen Sie in Betracht, netzwerkseitige Absicherungen z.B. durch Dienste wie das kostenlose OpenDNS einzusetzen. Diese Dienste schützen Sie vor Zugriffen auf bekannt bösartige Webseiten. Einige Dienste können zudem erkennen ob Ihr Computer versucht, sich zu einem bekannten Botnetz zu verbinden – ein klares Anzeichen, dass er mit Schadsoftware infiziert ist.

- Stellen Sie sicher dass jegliche Sicherheitssoftware wie z.B. Antiviren-Programme, die Sie einsetzen, noch immer aktiv entwickelt und weiterhin für Windows XP unterstützt werden.

- Wenn Ihr Computer keine Internetverbindung benötigt, z.B. weil Sie ihn nur zum Briefeschreiben einsetzen, entfernen Sie die Verbindung zum Netzwerk. Wenn er mit dem Netzwerk verbunden sein muss, stellen Sie sicher dass er

Das Ende von Windows XP

sich hinter einer Firewall befindet, und dass die bordeigene Firewall jegliche eingehende Verbindung unterbindet. Unternehmen sollten alle Windows XP Computers in ein separates Netzwerk umheben, um sicherzustellen dass eine Infektion der alten Systeme keine Auswirkungen auf die restliche Organisation hat.

- Sichern Sie regelmäßig die Daten von Windows XP Systemen als Vorbereitung auf eine mögliche Kompromittierung. Bewahren Sie mindestens ein Backup getrennt vom Computer auf. Wenn Sie Daten wiederherstellen müssen, sollte das wenn irgend möglich auf einem separaten, neuen System erfolgen. Wenn Sie auf Windows XP wiederherstellen, wird wahrscheinlich in Kürze eine erneute Infektion stattfinden.

Wenn Sie Windows XP in Ihrem Unternehmen verwenden, hat Ihr Arbeitgeber vielleicht noch weitere Schritte vorbereitet, die Sie befolgen müssen. Bedenken Sie immer, dass all diese Maßnahmen nur kurzfristig helfen, sie sind kein Ersatz für den Einsatz eines aktuellen, ordentlich abgesicherten Betriebssystems auf dem Stand der Technik. Früher oder später werden Sie auf ein solches umstellen müssen – warum also nicht früher?

Weiterführende Informationen

Microsoft Abkündigung von WindowsXP:
http://www.microsoft.com/de-de/windows/xp/
OpenDNS:
www.opendns.org
Hilfe bei der Migration:
http://www.zdnet.de/41555638/migration-leicht-gemacht-xp-software-unter-win-7-nutzen/
OUCH: Backup & Recover:
http://www.securingthehuman.org/ouch/2013#september2013

Informieren Sie Sich

Abonnieren Sie den monatlichen OUCH! Security Awareness Newsletter, greifen Sie auf die OUCH! Archive zu und lernen Sie mehr über SANS Security Awareness Angebote unter http://www.securingthehuman.org.

Deutsche Ausgabe

OUCH! wurde aus dem Englischen übersetzt von Marek Kreul und René Wiedewilt. Beide arbeiten für das CERT eines deutschen IT-Dienstleisters und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

OUCH! wird durch das SANS Securing The Human Programm herausgegeben und unter der Creative Commons BY-NC-ND 3.0 Lizenz vertrieben. Die Erlaubnis zur Weitergabe dieses Newsletters oder Verwendung in einem Weiterbildungsprogramm wird gewährt, solange der Newsletter unverändert bleibt. Für Übersetzungen und weitere Informationen kontaktieren Sie bitte ouch@securingthehuman.org.

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis