Technische Universität Berlin

Der Präsident

R U N D S C H R E I B E N

☒ ALLE (Prof., WM, SM, Tut)		Schlagwort : **XP Nutzung an der TU beenden**	Gruppe **G**
Bearbeiter/in: Hiller Hildmann			
Stellenzeichen / Telefon: K3-DS / 314-21784 tubIT / 314-21060	Datum: 15.04.2015	**Dieses Rundschreiben**	
		ersetzt:	

XP Nutzung an der TU beenden

Sehr geehrte Damen und Herren,

seit dem 08.04.2014 wird Windows XP nicht mehr unterstützt, d.h. es gibt seitdem keine Sicherheitsupdates für Windows XP mehr.

Für PCs, die noch nicht auf eine neuere Windows-Version aufgerüstet wurden, kann nicht mehr garantiert werden, dass die ausgeführten Programme stabil laufen und vor Zugriffen Dritter sicher sind.

Der Verlauf der entdecken Sicherheitslücken mit bis zuletzt 7 Stück vom Januar 2014 bis Supportende lässt aber vermuten, dass seitdem mindestens 30-60 weitere Sicherheitslücken entdeckt und nicht mehr geschlossen wurden. Microsoft selbst erklärt, dass ein Betrieb von Windows XP nicht mehr sicher ist.

Die gleiche Warnung gilt für den weiteren Betrieb der ebenfalls eingestellten Büro-Software Office 2003. Hier könnten Anwender über den Internet Explorer 8 eine infizierte Datei öffnen, die dann eine Office-Schwachstelle ausnutzt. Da Office-Programme mit dem Betriebssystem Windows und dem Browser "Internet Explorer" technisch "verzahnt" sind, könnten sich hieraus Angriffsvektoren ergeben. Die Anfälligkeit von PCs, die mit dem Internet Explorer 8 im Netz surfen, für Viren und andere Schadsoftware (Malware) potenziert sich je länger das Supportende zurück liegt.

Die von tubIT angebotene Antiviren- und Anti-Malware-Software kann dieses Risiko nicht abfedern. Ferner wird auch von den Antiviren-Herstellern Windows XP nicht weiter betrachtet. Der Mechanismus, dass jedes Sicherheitsupdate gleichzeitig ein Verzeichnis potentiell anfälliger Stellen preisgibt, die aber von den Entwicklern sofort für das nächste Sicherheitsupdate weiter bearbeitet werden, ist unterbrochen. Die potentiellen Eingriffsstellen, die das letzte Update offenbart hat, liegen unumkämpft frei, Entwickler von Schadsoftware können auf dieser Grundlage jetzt ungehindert nach Einbruchsstellen in das System suchen. Für erfolgreiche Angriffe gibt es weder einen Abwehr-Patch noch einen Support zur Wiederherstellung kompromittierter Systeme und der darauf verarbeiteten Daten.

Es besteht weiter die Befürchtung, dass neue in Windows XP gefundene Schwachstellen von Kriminellen bewusst zurückgehalten wurden und nach Ende des Supports – also jetzt! – aktiv eingesetzt werden, um Gegenmaßnahmen zu erschweren. Darüber hinaus ist anzunehmen, dass mancher zukünftig entdeckte Angriffsweg für moderne Windows-Versionen auch bei Windows XP funktioniert und von Angreifern durch eine Analyse der Patches nutzbar gemacht werden kann. Zusammen führt dies zu einer erhöhten Bedrohungslage für Systeme mit veralteten Betriebssystemen.

Auf Grundlage dieser Kenntnisse wird dringend empfohlen, Windows XP Systeme überhaupt nur noch ohne Netzwerkverbindung oder in einem weder nach außen noch nach innen erreichbaren (isolierten) Netz zu betreiben. Laborsysteme auf Basis von XP sollten nur noch in einem Intranet betrieben werden und so bald wie möglich ausgetauscht werden. Zusätzliche Netze für diesen Zweck können über den Netzwerkverwalter der Einrichtung beantragt werden. tubIT unterstützt gerne bei der Konfiguration dieser Netze und geeigneter Firewall-Regeln.

Bestehende Systeme, auf denen Windows XP oder eine andere veraltete Version eines Betriebssystems läuft, sollten schnellstmöglich auf eine moderne Version migriert werden. Geschieht dies nicht, so ist nicht nur das betroffene, sondern auch jedes damit vernetzte System einer stark erhöhten Gefährdung ausgesetzt. Dies gilt selbst dann, wenn auf den anderen Systemen im Netz moderne Betriebssysteme im Einsatz sind, da das Altsystem als Einfallstor genutzt werden und beispielsweise auch Zugangskennungen enthalten kann, die in anderen Systemen mitunter nutzbar sind.

Eine Verarbeitung von personenbezogenen Daten auf Windows XP Systemen ist nicht datenschutzgerecht und muss unterbleiben.

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit Dr. Alexander Dix fordert, alle PCs in der Berliner Verwaltung mit dem veralteten Betriebssystem Windows XP sofort abzuschalten. Er sagt, die Behörde werde den Online-Betrieb von Rechnern mit Windows XP ab Mittwoch (08.04.) beanstanden. Ohne die Abschaltung seien die persönlichen Daten der Bürger, die in den Berliner Verwaltungen verarbeitet werden, sonst einem unverantwortlichen Risiko durch mögliche Hacker-Angriffe ausgesetzt.

Ein eigenes Bild von der Gefährdungslage kann man sich machen unter folgenden Links (Auswahl):

Windows selbst:

http://windows.microsoft.com/de-de/windows/end-support-help

Microsoft Cyber Trust Blog:

http://blogs.microsoft.com/cybertrust/2013/08/15/the-risk-of-running-windows-xp-after-support-ends-april-2014/

Bundesamt für Sicherheit in der Informationstechnik:

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/anwender/software/BSI-CS_085.pdf?__blob=publicationFile

und

https://www.bsi-fuer-buerger.de/BSIFB/DE/Wissenswertes_Hilfreiches/Service/Aktuell/Meldungen/Support-Ende-WinXP_04022014.html

Der Heise-Verlag hat Informationen zum Supportende von Windows XP zusammengestellt:

http://www.heise.de/thema/Windows-XP

Mit freundlichen Grüßen

Annette Hiller,
Behördliche Datenschutzbeauftragte der TUB

Dr. Thomas Hildmann
IT-Service-Center (tubIT)