OUCH! | 2014. Március

Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadványban...

- Áttekintés
- Egy operációs rendszer életciklusa
- Így védekezzünk!

A Windows XP korszak vége

Áttekintés

A Windows XP az egyik legnépszerűbb operációs rendszerré vált a számítástechnika történetében, amely egy időben az egész világon a legelterjedtebb rendszer volt. Azonban a Windows XP kiöregedett, és a Microsoft hamarosan meg fogja szüntetni termékkel kapcsolatos támogatást. Több, mint 12 évvel az első kiadás után, a szoftveróriás 2014. április 8-ára tűzte ki az operációs rendszer életciklusának végét (End of Life - EOL). Ez azt jelenti, hogy a Microsoft ezután már nem ad ki semmilyen frissítést vagy biztonsági javítást. Megközelítőleg az asztali számítógépek 25%-a még mindig Windows XP operációs rendszert futtat (ennél csak a Windows 7 elterjedtebb) és ez a sokmilliónyi felhasználó hatalmas kockázatnak lesz kitéve. Nem árt tudni, hogy ez nem csak az otthoni felhasználókat érinti, hanem egyéb területet is, hiszen számos területen terjedt el széles körben ez az operációs rendszer. Ilyenek például az irodák, ipari irányító rendszerek, bankjegykiadó automaták (ATM), orvosi eszközök, bankkártya terminálok (POS) és egyéb más eszközök. Az alábbiakban bemutatjuk, hogy milyen veszélyek fognak leselkedni ránk, miután lejár az operációs rendszer életciklusa, illetve hogy milyen lépéseket tehetünk a saját védelmünk érdekében.

A szerzőről

Jason Fossen a Enclave Consulting LLC Microsoft Windows biztonságra specializálódott szakértője, a SANS hat napos Securing Windows with the Critical Security Controls (SEC505) kurzusának szerzője, illetve a http://cyber-defense.sans.org/blog/ weboldalon található, biztonsággal kapcsolatos PowerShell script-ek írója.

Egy operációs rendszer életciklusa

Talán nem is vagyunk tisztában vele, de a számítógépen lévő operációs rendszernek van egy életciklusa. A gyártó frissítéseket és javításokat biztosít hozzá, amelyek új funkciókat tartalmaznak, növelik a stabilitást és a teljesítményt, valamint biztonságosabbá teszik a rendszert. A problémát az jelenti, hogy a gyártó egy idő után már nem nyújt támogatást a termékre, mivel az erőforrásait az újabb és jobb technológiák fejlesztésére fogja összpontosítani. Ez azt jelenti, hogy az életciklus lejárta után a gyártó nem ad ki újabb frissítéseket vagy javításokat még akkor sem, ha tudomására jutottak olyan biztonsági rések, amelyeken keresztül a bűnözők fel tudják törni az operációs rendszert. A Windows XP ezt az állapotot fogja elérni most áprilisban, és a Microsoft akkor sem ad ki több biztonsági frissítést, ha a bűnözők egy sérülékenységet aktívan kihasználnak.

Így védekezzünk!

A védekezéshez fontos, hogy az operációs rendszert aktívan támogassa a gyártó. Amennyiben van rá lehetőség, cseréljük le az operációs rendszert, például új számítógép vásárlásával, mivel a ma Windows XP-t futtató gépek hardverei közül számos nem teljesíti az újabb operációs rendszerek minimális hardver követelményeit. Mivel a Windows 7 kezelőfelülete nagyon hasonlít a Windows XP-hez, a cégek számára jobb választás lehet a Windows

A Windows XP korszak vége

8 helyett. Azonban tisztában kell lenni azzal is, hogy a Windows 8 sokkal biztonságosabb, mint az elődei, köszönhetően számos fejlesztésnek. Ezeken kívül vannak még más operációs rendszerek is, amiket választhatunk (például az Apple MaOS X). Bárhogy is nézzük, itt az ideje a váltásnak. Ha még ezek után sem tudunk váltani Windows XP-ről április előtt, legalább az alábbi lépéseket tegyük meg!

Miután lejár a Windows XP életciklusa, a védekezés legjobb módja az lesz, ha átállunk egy, a gyártója által aktívan támogatott új operációs rendszerre.

- Csak azt a Windows XP-s funkciót vagy alkalmazást használjuk, amire feltétlenül szükség van! Előfordulhat például, hogy egyetlen program vagy alkalmazás miatt, amely csak Windows XP alatt fut nem lehet váltani újabb operációs rendszerre. Ebben az esetben ne használjuk másra a számítógépet (például levelezni vagy böngészni)!

- Amennyiben Windows XP-t kell használnunk internetezésre, akkor ne az Internet Explorer-t használjuk, hanem váltsunk egy másik böngészőre (például Mozilla Firefox, Opera, Google Chrome)! Győződjünk meg arról, hogy mindig a legfrissebb böngésző verzió van telepítve, és hogy a gyártó még mindig támogatja a Windows XP-t!

- Ne használjunk olyan Windows XP-be épített alkalmazást, amellyel az Internetről letöltött fájlokat meg lehet nyitni (például Windows Media Player)! Telepítsünk olyan programot ezekre a célokra, amelyek gyártója még mindig ad ki frissítéseket az adott verzióhoz!

- Használjunk valamilyen hálózatbiztonsági szolgáltatást, mint például OpenDNS! Az ehhez hasonló szolgáltatások segítenek abban, hogy elkerüljük az ismert, káros szoftverekkel fertőzött weboldalakat, valamint vannak olyan megoldások is, amelyek észlelik, ha egy botnet hálózathoz akar csatlakozni a számítógép.

- Telepítsünk valamilyen biztonsági szoftvert, mint például anti-vírus program, és győződjünk meg arról, hogy a gyártója még támogatja a Windows XP-t azért, hogy folyamatosan naprakész legyen.

- Amennyiben csak olyan célra használjuk a számítógépet, amihez nem szükséges Internet kapcsolat (például szövegszerkesztés), válasszuk le a hálózatról! Amennyiben muszáj hálózatra csatalakoznia, akkor legyen tűzfal mögött, amely blokkolja az összes befelé irányuló forgalmat! A vállalatok például az összes Windows XP-s számítógépüket egy különálló hálózatra tehetik, amely a fertőzést nem engedi továbbterjedni a szervezet többi része felé.

A Windows XP korszak vége

- Rendszeresen készítsünk biztonsági másolatot a Windows XP-s számítógépen lévő adatokról, felkészülve arra az esetre, ha az mégis megfertőződik! A biztonsági mentések közül legalább egyet valamilyen offline eszközön tároljunk, mint például leválasztott USB meghajtó. Egy esetleges fertőzés miatt, ha vissza kell állítani az adatokat, akkor azt már egy új rendszerre célszerű megtenni, mert egy Windows XP-s számítógép könnyen újra megfertőződhet.

Amennyiben a munkahelyen használunk Windows XP-s rendszert, a munkáltatónak további lépéseket javasolt tennie. Ne felejtsük el, hogy a fentiek csak rövid távú, „tűzoltásra" alkalmas tanácsok, amelyek nem helyettesítik a naprakészen tartott, megfelelően beállított rendszert! Előbb vagy utóbb mindenképpen át kell állni egy újabb operációs rendszerre!

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a http://www.securingthehuman.org weboldalon keresztül.

Magyar Kiadás

Kormányzati, távközlési és informatikai szolgáltatóként, Magyarország egyik stratégiai fontosságú gazdasági társasága a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Társaságunk kiemelt feladata a kormányzati infrastruktúra működtetése, az e-közigazgatási megoldások támogatása, valamint kormányzati szintű informatikai szolgáltatások nyújtása. További információ a http://www.nisz.hu oldalon olvasható.

Hivatkozások

Microsoft EOL közlemény:
http://www.microsoft.com/en-us/windows/enterprise/endofsupport.aspx
OpenDNS:
www.opendns.org
Migrálási kézikönyv:
http://www.zdnet.com/windows-xp-end-of-life-migration-guide-7000023800/
OUCH: Biztonsági mentés és visszaállítás:
http://www.securingthehuman.org/ouch/2013#september2013

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Fordította: Birkás Bence, Benyó Pál, Árvai Gábor