OUCH! I 2020. május

SANS SECURITY AWARENESS

OUCH!

A Havi Tudatosságról szóló hírlevele

A frissítés ereje

Áttekintés

Lehet, hogy nem veszi észre, de a számítógépes támadók folyamatosan keresnek és találnak új sebezhetőségeket és sérülékenységeket az emberek által naponta használt szoftverekben. Ezek lehetnek a laptopján futó programok, az okostelefonján található alkalmazások, vagy akár a babamonitoron és más otthoni eszközökön található szoftverek. A rosszfiúk kihasználják ezeket a szoftveres gyengeségeket, ezzel lehetővé válik számukra, hogy behatolhassanak a világ bármely részén található eszközökbe. Ezzel egy időben a szoftver- és eszközgyártók folyamatosan foltozzák be ezeket a hiányosságokat, és szoftverfrissítések útján juttatják célba a javításokat. Az egyik legjobb módja annak, hogy megvédje magát, ha mindig telepíti az Ön által használt technológiák legfrissebb változatait, így a számítógépes támadók számára sokkal nehezebbé válik azok feltörése.

Hogyan működnek a frissítések

A szoftver sebezhetőségének felfedezését követően a fejlesztők szoftverfrissítést (más néven javítást) készítenek és bocsátanak ki. Manapság a legtöbb szoftver és eszköz rendelkezik olyan mechanizmussal, amely az Interneten keresztül kapcsolódik a gyártó szerveréhez és onnan tölti le a szoftverfrissítést. Maga a frissítés nem más, mint egy kis program, amely jellemzően telepíti önmagát és kijavítja a biztonsági hibát. A folyamatosan frissítésre szoruló szoftverekre jó példa a laptopokon futó operációs rendszerek, mint például a Microsoft Windows, az OSX, vagy okostelefonok esetében az Android és az iOS. Továbbá — bár erre gyakorta nem fordítunk kellő figyelmet — frissíteni kell az eszközökön futó programokat is, például a webböngészőt, a szövegszerkesztőt, az üzenetküldő szoftvereket vagy a telefon mobilalkalmazásait — különösen a közösségi média alkalmazásokat.

Mindezek miatt, amikor új számítógépes programot vagy mobilalkalmazást vásárol, először ellenőrizze, hogy a szoftvergyártó aktívan frissíti-e a programot vagy eszközt. Minél hosszabb ideig működik egy szoftver biztonsági frissítés nélkül, annál valószínűbb, hogy olyan sebezhetőségeket tartalmaz, amelyeket a számítógépes bűnözők kihasználhatnak. Ez az oka annak, hogy sok gyártó, mint például a Microsoft, legalább havonta automatikusan ad ki új javításokat.

Végül, ha már nem használ egy bizonyos számítógépes programot, szoftvert vagy mobilalkalmazást, távolítsa el azt a rendszeréből. Minél kevesebb szoftvert kell frissítenie, annál nagyobb biztonságban van.

Frissítés

Egy rendszer két lehetséges módon frissíthető:

Automatikus - Amikor egy eszköz, operációs rendszer, program vagy mobilalkalmazás észleli, hogy a gyártó kiadott egy új frissítést, és automatikusan letölti, valamint telepíti azt. Az automatikus frissítés előnye, hogy Önnek semmit sem kell tennie. A szoftver biztosítja, hogy az Ön által használt technológiák naprakészek legyenek. Az automatikus frissítés hátránya, hogy egy frissített program okozhat olyan problémát, amely adott esetben funkciók vagy adatok elvesztéséhez vezethet. Ez ritka a személyes használatú eszközök esetében, azonban bonyolultabb — például nagyvállalati — környezetekben megtörténhet.

Manuális - Amikor egy eszköz, operációs rendszer, program vagy mobilalkalmazás frissítése elérhetővé válik, és a frissítést Önnek manuálisan kell letöltenie és telepítenie. Ez nagyobb kontrollt biztosít Önnek afelett, hogy mikor és milyen frissítések kerüljenek telepítésre. A nagyobb szervezetek — például kórházak vagy közművek — általában kedvelik a manuális frissítéseket, mivel azok lehetővé teszik számukra, hogy először teszteljék a módosításokat, amelynek során fel tudják fedezni és kezelni tudják a frissítés által okozott problémákat. A manuális frissítés hátránya, hogy sokkal hosszabb időt vehet igénybe a rendszer frissítése, vagy az is előfordulhat, hogy megfeledkezik azok telepítéséről.

Következtetés

Magánszemélyek, családok és kisvállalkozások számára erősen javasoljuk, hogy minden eszközükön engedélyezzék az automatikus frissítést. Ez biztosítja, hogy az összes használt technológia, az okostelefontól és a laptoptól kezdve a babafigyelőig és az ajtózárakig, rendelkezzen a legújabb szoftverekkel. A naprakész eszközök és szoftverek megnehezítik a rosszfiúk számára azok megtámadását. Az automatikus frissítések engedélyezése az egyik legegyszerűbb és leghatékonyabb módja annak, hogy megvédje magát és biztonságosan használhassa a mai technológiákat.

A szerzőről

Don C. Weber információbiztonsági vezető, 2002 óta széles körű tapasztalattal rendelkezik a DFIR, a pentesztelés, a kutatás és irányítás terén. Don részt vett a SANS tanácsadó testületében, az etikai bizottságban, az Arany Programban, és jelenleg az ICS410 egyik oktatója. Don elérhetősége: @cutaway és https://www.cutawaysecurity.com.

Források:

Rendelkezik biztonsági mentéssel? https://www.sans.org/security-awareness-training/resources/got-backups

Négy egyszerű lépés, hogy biztonságban maradjon
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Szerkesztette: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley I Fordította: Nemzeti Kibervédelmi Intézet