Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

A frissítés ereje

Áttekintés

A kibertámadók folyamatosan új sérülékenységek után kutatnak a mindennapok során használt szoftvereinkben. A sérülékenység egy szoftver fejlesztése során elkövetett hiba vagy hiányosság. Sérülékenység érinthet bármilyen szoftvert, például a laptopunkon, az okostelefonunkon futó alkalmazásokat vagy akár az otthoni termosztát vezérlését is. A kibertámadók a szoftveres sebezhetőségek kihasználásával képesek bejutni különböző digitális rendszerekbe, ezáltal akár az általunk használtakba is. Ugyanakkor az eszközöket és szoftvereket gyártó cégek folyamatosan készítik a javításokat, amiket biztonsági frissítés formájában adnak ki. Az egyik legjobb módja a védekezésnek, ha gondoskodunk az általunk használt eszközökön a legújabb biztonsági frissítések telepítéséről. Ezek a frissítések nem csak az ismert sérülékenységeket javítják ki, hanem gyakran új biztonsági funkciókat is tartalmaznak, így a támadók sokkal nehezebben tudnak bejutni az eszközeinkbe.

Hogyan működik a frissítés?

Amint egy szoftver sérülékenysége ismertté válik, a fejlesztő vagy a szállító szoftverfrissítést készít a biztonsági réshez (ez az úgynevezett patch vagy biztonsági javítás), amelyet később publikálnak. A rendszerünk ezután letölti és telepíti ezt a frissítést, javítva ezzel a biztonsági réseket. Példák a frissítendő szoftverekre:

- A laptopunkon (például Microsoft Windows vagy Apple OSX) vagy az okostelefonunkon futó operációs rendszerek (például Android vagy iOS).
- Az otthoni hálózati berendezések, például a router, vagy a Wi-Fi hozzáférési pont, otthoni okoseszközök (például: termosztát, csengő, háztartási készülékek vagy biztonsági kamerák).
- Az eszközeinken futó programok (például a laptop webböngészője vagy a telefon mobilalkalmazásai).

Éppen ezért, amikor új eszközt vagy új számítógépes programot szeretnénk vásárolni, illetve mobilalkalmazást telepítünk, először ellenőrizzük, hogy az eladó aktívan frissíti-e a programot vagy az eszközt! Minél hosszabb idő telik el a szoftver frissítése nélkül, annál valószínűbb, hogy vannak olyan sebezhetőségei, amelyeket a támadók képesek kihasználni. Ez az oka annak, hogy sok gyártó, például a Microsoft, minden hónapban automatikusan új javításokat ad ki. Ezért felül, ha már nem használunk egy bizonyos számítógépes programot, szoftvert vagy mobilalkalmazást, távolítsuk el azt a rendszerből*! Minél kevesebb szoftvert telepítünk, annál kisebb a potenciális sebezhetőségek száma, ezáltal nagyobb biztonságban vagyunk.

Végül, ha bármelyik eszközünk vagy alkalmazásunk elavult és a gyártója már nem készít hozzá frissítéseket, akkor javasolt, hogy cseréljük le azokat újabb verziókra, amelyek aktívan támogatást élveznek.

Hogyan frissítsünk?

A rendszerek frissítésének alapvetően két módja van.

1. **Manuális frissítés (a nehezebbik út)**: Amennyiben elérhető egy frissítés, akkor azt manuálisan töltsük le és telepítsük a rendszereinken. Így jobban szabályozhatjuk, hogy milyen frissítések és mikor kerüljenek telepítésre. A kézi frissítések hátránya, hogy sokkal több munkával jár, hiszen nem csak azt kell követnünk, hogy mikor kell frissíteni az egyes készülékeinket, programjainkat, hanem manuálisan kell azt megtennünk, így arról könnyen megfeledkezhetünk.

2. **Automatikus (egyszerűbb módszer)**: Engedélyezzük eszközeinken az automatikus frissítést, ami azt jelenti, hogy valahányszor új javítást válik elérhetővé, eszközeink maguktól letöltik és telepítik azokat! Az automatikus frissítés előnye, hogy a munka nagy részét elvégzi helyettünk. Az automatikus frissítések hátránya, hogy a frissített program váratlanul problémát okozhat, ami a funkcionalitásbeli hibát vagy az adatok elvesztését eredményezheti. Ez személyes eszközeink esetében ritkán, azonban nagyvállalati környezetben nagyobb eséllyel fordulhat elő. Amennyiben az automatikus frissítések engedélyezését választjuk, elengedhetetlen, hogy folyamatosan ellenőrizzük rendszereinket, megbizonyosodva arról, hogy a legújabb frissítések valóban települtek-e.

Javasoljuk, hogy minden személyes eszközünkön legyen engedélyezve az automatikus frissítés. Ez biztosítja, hogy az általunk használt összes technológia, az okostelefontól a laptopon át a babaőrzőig és az ajtózárakig a legújabb szoftverrel rendelkezzen. A naprakész eszközök és szoftverek sokkal nehezebbé teszik a támadók számára, hogy feltörjék eszközeinket.

A szerzőről

Dr. Janell Straach a Rice Egyetem oktatója, aki kiberbiztonságot és mesterséges intelligenciát oktat. Janell emellett a Women In CyberSecurity (WiCyS) igazgatótanácsának elnöke is. Dr. Straachl a janell@wicys.org címen érhető el.

Források

Digitális „tavaszi nagytakarítás”: https://www.sans.org/newsletters/ouch/digital-spring-cleaning-7-simple-steps/
Szükségem van biztonsági szoftverre?: https://www.sans.org/newsletters/ouch/security-software/
Érzelmi triggerek – Így csapnak be minket a kibertámadók: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)