OUCH! 2025. január

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Az okosotthon eszközei: biztosítsa őket még a kiberbűnözők előtt

Egy digitális rémálom: Kiberbűnözök az otthonában

Sarah és családja teljesen el voltak ragadtatva az új okosotthoni eszközeiktől: élvezték, hogy egyszerűen, mindössze néhány kattintással, illetve hangjukkal irányíthatták a lámpákat és zárakat. Izgatottságuk azonban hamarosan rémületbe fordult, amikor egy este Sarah észrevette, hogy az okostermosztátja kéretlenül átállítgatja magát. Eleinte ezt csak egy apró hibának vélte, de aggódni kezdett, amikor a lámpák villogni kezdtek, a bejárati ajtó pedig magától kinyílt. A helyzet akkor vált igazán ijesztővé, amikor egy idegen hang szólalt meg a bébiőrön keresztül, részletesen leírva a baba szobáját. Abban a pillanatban Sarah rájött, hogy valaki betört a kis szentélyükbe. A támadók átvették az irányítást okoseszközeik felett, veszélyeztetve a magánszférájukat és biztonságukat. Sarah nagyon sebezhetőnek és kiszolgáltatottnak érezte magát a gondolattól, hogy idegenek figyelik kisbabáját alvás közben. Ez a nyugtalanító élmény világossá tette Sarah számára, hogy az otthoni okoseszközök biztonságos beállítása nem csupán a technológia védelméről szól, hanem a családja biztonságáról és lelki nyugalmáról is.

Mik azok az intelligens otthoni eszközök?

Az intelligens otthoni eszközök olyan internethez csatlakoztatott eszközök és készülékek, mint a termosztátok, biztonsági kamerák, intelligens zárak, lámpák és talán még a mosógép is, amelyek hatékonyabbá, kényelmesebbé és bizonyos esetekben még biztonságosabbá is teszik otthonunkat. Ezeket az eszközöket alkalmazások, hangutasítások vagy automatizált rendszerek vezérlik, ami példátlan kényelmet kínál.

Az általuk nyújtott kényelem azonban kockázatokkal is jár. Mivel ezek az eszközök az internetre csatlakoznak, sebezhetőek, amennyiben nincsenek megfelelően biztosítva. Feltörésük esetén a támadók hozzáférhetnek személyes adataihoz, kémkedhetnek a mindennapi tevékenységei után, sőt, akár át is vehetik az irányítást a konkrét eszközök felett.

Miért olyan fontos az otthoni okoseszközök biztonságossá tétele?

Az okos otthoni eszközök védelme nem csak maguknak a tárgyaknak a védelméről szól: sokkal inkább az egész háztartásáról. A kibertámadást elkövetők gyakran megkeresik a leggyengébb eszközt, és ott kezdenek. Sikeres feltörés után a támadó felhasználhatja a meghackelt eszközt arra, hogy hozzáférjen az otthoni hálózat többi végpontjához, ezzel személyes adatokat lophat vagy akár kinyithatja az ajtókat is. Egy ilyen összekapcsolt világban az okoseszközeink védelme létfontosságú a személyes biztonságunk, magánszféránk és nyugalmunk megtartásának érdekében.

Öt dolog, amit megtehetünk az okoseszközök biztonsága érdekében

1. **Azonnal cseréljük le az alapértelmezett jelszavakat**: Sok otthoni eszköz érkezik alapértelmezett, gyári beállítású jelszavakkal, amelyeket a támadók már jól ismernek, vagy könnyen kitalálnak. Ezeket amint lehet cseréljük erős, egyedi jelszavakra, és használjunk jelszószéfet a nyomon követésük érdekében!

2. **Kapcsoljuk be a többfaktoros azonosítást (MFA-t) – Mert egy már nem elég**: Néhány okoseszköznél szükséges egy online profil létrehozása, hogy hozzáférjünk és kezelhessük az eszközeinket. Ezeket a fiókokat MFA-val védhetjük, ami további biztonsági réteget nyújt azáltal, hogy jelszót és egyedi, egyszer használatos kódot is kér a telefonunkra. A kiberbűnözők utálják a többfaktoros authentikációt, mivel nagyon megnehezíti a munkájukat.

3. **Biztosítsunk az okoseszközeinek dedikált Wi-Fi hálózatot**: Hozzunk létre egy okos eszközeinek szánt külön hálózatot, így különítsük el őket személyes illetve munkahelyi gépeinktől! Ezt számos Wi-Fi hozzáférési ponton és routeren vendéghálózatnak nevezik. Segít elkülöníteni az eszközöket, és korlátozza a károkat, ha egy eszköz biztonsága sérülne.

4. **Frissítsünk, frissítsünk, frissítsünk**: A gyártók rendszeresen adnak ki frissítéseket a sebezhetőségek javítására. Győződjünk meg arról, hogy eszközeink a legújabb firmware- illetve szoftverfrissítésekkel rendelkeznek, hogy védve maradjanak az újonnan megjelenő fenyegetésekkel szemben. Ennek legegyszerűbb módja, ha engedélyezzük az automatikus frissítéseket az eszközeinken. Erősen fontoljuk meg a már nem támogatott, illetve újabb frissítésekkel nem rendelkező eszközök cseréjét.

5. **Nem használt funkciók letiltása**: Az okoseszközök gyakran különböző funkciókkal rendelkeznek, amelyek nagy részét talán soha nem is használjuk. Minél több funkciót hagyunk bekapcsolva, annál több ajtó marad nyitva a kiberbűnözők számára is. Tiltsunk le minden szükségtelen szolgáltatást, például a távoli hozzáférést vagy a hangutasításokat, hogy minimalizáljuk a támadók által kihasználható belépési pontokat!

Az okosotthonunk nem válhat kiberbűnözők játszóterévé! Mindössze néhány egyszerű lépés megtételével kiélvezhetjük mindazt, amit a technológia lehetővé tesz, miközben békésen aludhatunk: hiszen tudjuk, hogy az irányítás nálunk van.

Vendégszerkesztő

Sai Sujitha Venkatesan a Dell termékbiztonsági incidenskezelő csapatának vezető biztonsági mérnöke és a WiCyS (Women in CyberSecurity) szilícium-völgyi igazgatótanácsának tagja. Szenvedélye minden, ami a kiberbiztonsággal kapcsolatos, beleértve a munkaerő sokszínűségét is. LinkedIn: https://www.linkedin.com/in/saisujitha/

Források

A frissítések ereje: https://www.sans.org/newsletters/ouch/power-updating/
A jelmondatok ereje: https://www.sans.org/newsletters/ouch/power-passphrase/
A jelszókezelők ereje: https://www.sans.org/newsletters/ouch/power-password-managers/

A Közösség számára fordította: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)