DE IBK

Tanácsok, tippek, ha baj van

Bármilyen weboldal megnyitása során az első dolog, amivel a felhasználók szinte biztosan találkoznak, egy felugró ablak, ahol kiválaszthatják, hogy mely sütik (cookies) használatát engedélyezik a weboldalnak. Bár a felhasználói élményben sokszor nincs érezhető különbség a teljes és a minimális sütihasználat között, érdemes megérteni, mi történik a háttérben – és miért lehetnek a sütik komoly biztonsági kockázatot jelentő célpontok a kiberbűnözők számára.

Mik azok a sütik?

Amikor meglátogatunk egy weboldalt, az küld egy sütit a böngészőnknek. Ez egy **kis szöveges fájl**, amely adatokat tárol a rendszerünkről és az oldalon végrehajtott műveleteinkről. Böngészőnk ezeket eltárolja, és minden alkalommal, amikor visszatérünk az oldalra, visszaküldi a szervernek. Ez leegyszerűsíti a webes élményt: nem kell újra bejelentkeznünk, megmaradnak a megjelenítési beállításaink, a webshopok kosárban tartják a tételeinket, a streaming szolgáltatások pedig megjegyzik, hol tartottunk a sorozatban.

A sütik azonban nemcsak kényelmi funkciókat biztosítanak: **tárolhatják a bejelentkezési adatainkat, biztonsági tokenjeinket, telefonszámunkat, lakcímünket, banki adatainkat és a munkamenet-azonosítónkat (session ID)** is. A session ID egyedi kód, amellyel a weboldal azonosítja a felhasználót. Ha egy támadó megszerzi ezt, akár **bejelentkezhet a nevünkben** anélkül, hogy tudná a jelszavunkat.

Milyen típusú sütik léteznek?

A sütik több szempont szerint is csoportosíthatók, és egyazon süti egyszerre több kategóriába is tartozhat.

Tárolási idő szerint:

- **Munkamenet-sütik (session cookies):** csak a látogatás ideje alatt élnek, majd automatikusan törlődnek. Ezek biztosítják például, hogy több oldal között navigálva is bejelentkezve maradjunk.

- **Állandó sütik (persistent cookies):** hosszabb ideig (jellemzően hónapokig vagy akár egy évig) tárolódnak, így nem kell minden alkalommal elfogadni a sütiszabályzatot vagy újra bejelentkezni.

Forrás szerint:

- **Elsődleges sütik (first-party):** közvetlenül a meglátogatott weboldal hozza létre. A működéshez és a felhasználói élményhez nélkülözhetetlenek.
- **Harmadik féltől származó sütik (third-party):** külső szolgáltatók (pl. hirdetési hálózatok, analitikai platformok, közösségi média) hoznak létre, hogy követni tudják a felhasználói viselkedést több webhelyen.

Fontosság szerint:

- **Szükséges (esszenciális) sütik:** alapfunkciókhoz kellenek (bejelentkezés, kosár tartalma, munkamenet azonosítása).
- **Opcionális sütik:** marketing és analitikai célra szolgálnak. Ezek nélkül is működik a weboldal, de személyre szabott hirdetéseket és ajánlásokat biztosítanak.

Tárolás módja szerint:

- **Hagyományos sütik:** a böngészőben tárolt, könnyen törölhető szöveges fájlok.
- **Szupersütik (supercookies):** olyan sütik, amelyeket nehezebb törölni, mert a böngésző mélyebb rétegeiben tárolódnak.
- **„Öröksüti" (evercookies):** különböző tárhelyek kombinációjában (pl. cache, Flash LSO, HTML5 storage) rejti el magát, és törlés után is képes visszaállítani magát a megmaradt adatokból. Ezáltal szinte lehetetlen végleg eltávolítani, és tartós azonosítót biztosít a felhasználó hosszú távú követéséhez.

Hogyan lopnak sütiket a hackerek?

- **Munkamenet-eltérítés (Session Hijacking):** A támadó lehallgatja a felhasználó és a szerver közötti forgalmat, és megszerzi a session ID-t, amellyel átveheti a felhasználó munkamenetét. Ez főleg HTTP-t használó, titkosítatlan oldalaknál fordul elő, különösen nyilvános Wi-Fi hálózatokon. Megelőzés: mindig használjunk HTTPS-t, és kerüljük a védtelen hálózatokat.
- **Cross-site scripting (XSS):** Egy weboldal sebezhetőségét kihasználva a támadó rosszindulatú JavaScript kódot juttat be, ami kiolvassa és továbbítja a sütiket. A fejlesztők HttpOnly attribútum használatával és bemeneti adatok szűrésével csökkenthetik a kockázatot.
- **Cross-site request forgery (CSRF/XSRF):** A felhasználó böngészője – tudta nélkül – egy támadó által előkészített kérést küld el a weboldalnak a meglévő sütikkel együtt. Így akár jelszót is módosíthat a támadó nevében. A védekezéshez a weboldalak egyedi CSRF tokeneket alkalmaznak.
- **Kiszámítható session ID-k:** Ha az oldal egyszerű, előrejelezhető algoritmust használ az azonosítók generálására, a támadók mintagyűjtéssel kitalálhatják a következő session ID-t, és beléphetnek a felhasználó helyett. Megoldás: kriptográfiailag biztonságos, véletlenszerű ID-k.

- **Közbeékelődéses támadás (Man-in-the-Middle – MitM):** A támadó a felhasználó és a webhely közé ékelődik, figyeli vagy módosítja a kommunikációt, és így hozzáfér a sütikhez is. Megelőzés: HTTPS, tanúsítvány-ellenőrzés és – lehetőség szerint – VPN használata.

Így védekezhetünk a sütitolvajok ellen

Bár a sütik védelme elsősorban a weboldalak felelőssége, a felhasználók is tehetnek sokat az adataik biztonságáért:

- **Csak HTTPS-es oldalakon adjunk meg személyes adatokat!** Ha a címsorban „http” szerepel és nincs biztonsági tanúsítvány, ne fogadjunk el sütiket és ne adjunk meg érzékeny adatokat!
- **Figyeljünk a böngésző figyelmeztetéseire!** Érvénytelen tanúsítvány esetén hagyjuk el az oldalt!
- **Frissítsük a böngészőt!** Kapcsoljuk be az automatikus frissítést a sebezhetőségek gyors befoltozása érdekében!
- **Töröljük rendszeresen a sütiket és a cache-t!** Beállíthatjuk, hogy a böngésző bezárásakor automatikusan törlődjenek.
- **Tiltjuk vagy korlátozzuk a harmadik féltől származó sütiket!** Ez minimalizálja a követést.
- **Használjunk privát/inkognitó módot**, ha nem szeretnénk, hogy a sütik hosszabb ideig megmaradjanak!
- **Ne kattintsunk gyanús linkekre, ismeretlen e-mailekre!**
- **Engedélyezzük a kétfaktoros hitelesítést (2FA)**, hogy egy ellopott session ID önmagában ne legyen elég a belépéshez!
- **Ne fogadjuk el az összes süti használatát a weboldalakon!** Igaz egyes weboldalaknál ez több kattintással jár, de jelentősen kevesebb adat kerül rólunk rögzítésre a „Kötelező/csak nélkülözhetetlen sütik” elfogadásával.
- **Kerüljük a nyilvános Wi-Fi használatát**, vagy ha muszáj, használjunk VPN-t a forgalom titkosításához!