Honnan tudhatjuk, hogy egy weboldal nem biztonságos?

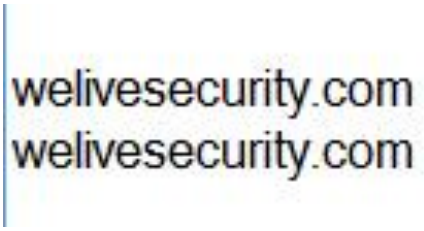
Sajtóközlemény – 2021. augusztus 3. – PResston PR

Naponta valószínűleg több tíz, de akár több száz webhelyet is felkeresünk. Biztosan elolvasunk egy-egy cikket, ellenőrizzük a közösségi média profiljainkat, online nézzük a kedvenc műsorunkat, vagy éppen rákattintunk egy barátunktól kapott linkre. Honnan vehetjük észre, hogy az általunk látogatott oldalak biztonságosak-e, nem pedig az adatainkra vadászó webhelyek?

Az ESET szakértői összegyűjtötték, mire érdemes figyelni, hogy könnyen felismerjük a különbséget a biztonságos és a csaló weboldalak között.

Homoglifa, avagy elgépelt URL-ek és kétértelmű karakterek

A homográf típusú támadások a kiberbűnözők leggyakoribb megtévesztő taktikái közé tartoznak. Ennek lényege, hogy a hamis weboldalakat olyan domain neveken regisztrálják, amelyek nagyon hasonlítanak ismert, megbízható oldalakéhoz, ezek pedig kinézetre **összetéveszthető karaktereket tartalmaznak**. Ilyen például az, ha a „microsoft.com” helyett „rnicrosoft.com”-ot használnak, ahol az „m” betűt „rn” karakterekkel helyettesítik. Előfordulhat az is, hogy az „o” betű helyett a görög eredetű omicront, azaz „o”-t használják a domain névben: itt például a „facebook.com” címben a második „o” helyére az omicron lépett, ám kinézetre szinte nincs is különbség.



Az első verzió „o” betűje helyett a második már omicront használ.

Ide kapcsolódik az úgynevezett **„typosquatting”**, vagyis a szándékos elírással történő megtévesztés is, ahol a támadók népszerű weboldalak neveihez nagyon hasonló domain neveket regisztrálnak, például „google.com” helyett "gogle.com" vagy "gooogle.com" címeket. Érdemes megemlíteni, hogy a példában szereplő, tévesen írt változatokat a Google biztonsági okokból megvásárolta, így ezek szerencsére automatikusan átirányítanak az eredeti oldalra, azonban még így is sokféle hamis változat bukkanhat fel. A hamis oldalak általában megtévesztésig hasonlítanak az eredetire, ezért legyünk nagyon óvatosak, és mindig ellenőrizzük, hogy tényleg a helyes oldalon járunk-e. Szerencsére több olyan biztonsági programot is találunk, amelyek felismerik a homográf támadásokat, és figyelmeztetnek, ha egy gyanús weboldalt próbálunk meg elérni.

Rosszindulatú webhelyek ellenőrzése

Ma már számos megoldást találunk arra, hogy egy weboldal hitelességét ellenőrizni tudjuk. A Google Biztonságos Böngészés felületén lehetőségünk van az adott weboldal URL címének beillesztésével ellenőrizni, hogy a keresett webhely biztonságos-e.
Egy másik hasonló felület a VirusTotal URL ellenőrzője, amely elemzi a webhely címét, és összeveti több tucat felsőkategóriás víruskeresővel, illetve webhely-szkennelő eszközzel, így igen pontos adatokat tud adni nekünk arról, ha esetleg mégis rosszindulatú felülettel van dolgunk.

Hiányzó adatvédelmi szabályzat – árulkodó jel lehet

Ha bizonytalanok vagyunk egy oldal hitelességét illetően, mindig ellenőrizzük, hogy a felületen található-e adatvédelmi szabályzat. Az adatvédelmi törvények értelmében ugyanis minden weboldalnak rendelkeznie kell olyan szabályzattal, amelyben elmagyarázzák, hogyan védik és kezelik a felhasználók személyes adatait. Ha egyáltalán nem találunk erre vonatkozó információkat a honlapon, úgy joggal kérdőjelezhetjük meg az adott weboldal megbízhatóságát.

Elérhetőségek – erre is szükség lehet

Minden törvényes vállalatnak, amely kapcsolatot szeretne fenntartani az ügyfelekkel, el kell helyeznie az elérhetőségeit a weboldalán. Ez lehet egy kapcsolatfelvételi űrlap, telefonszám vagy közvetlen e-mail cím. Ha viszont nem találunk semmit, az már önmagában is gyanús, ahogyan az is, ha a megadott telefonszám huzamosabb ideig nem kapcsolható, vagy olyan személy veszi azt fel, aki egyáltalán nem tűnik illetékesnek. Ilyen esetekben érdemes elgondolkodnunk azon, hogy itt esetleg csalással van dolgunk.

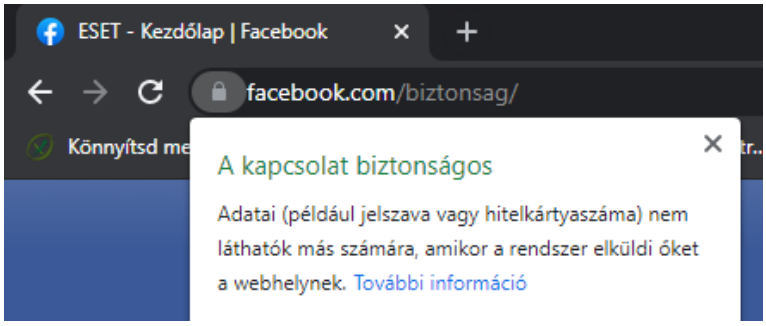
„S" betű a HTTPS-ben

Egy széles körben elterjedt módszer a weblapok biztonságának ellenőrzésére a HTTPS protokoll vizsgálata. A HTTPS-t gyakran a biztonság kulcselemeként tartják számon, a valóság azonban ennél árnyaltabb. Valójában ez a protokoll csak azt biztosítja, hogy a webszerver és a felhasználó böngészője közötti kapcsolat titkosított, azaz védettséget nyújt a lehallgatástól. Nem ad választ azonban arra a kérdésre, hogy bár a webhelyhez titkosított kapcsolaton keresztül csatlakozunk, valóban egy hivatalos weboldalon vagyunk-e, vagy csak egy hamis, adathalász verzióba botlottunk.

Manapság a számítógépes bűnözők ugyanolyan könnyen szerezhetnek érvényes SSL / TLS tanúsítványt a hamis webhelyeikhez, mint egy törvényes vállalkozás. Ezért ezt a módszert érdemes úgy kezelni, mint egy kirakós darabkáját, amely csupán egy nagyobb puzzle része.

Ami a tanúsítványokat illeti, érdemes egy pillantást vetni arra is, hogy milyen szolgáltatásokat kínál a weboldal, és melyik szervezet adta ki az SSL vagy TLS

tanúsítványát. Ha a webhely által kezelt adatok érzékenyek, de a kiadott tanúsítvány olcsó vagy ingyenes, akkor érdemes behúzni a vészféket.
A tanúsítvány érvényességéről, és a kiállító szervezetről bővebb információt a böngésző címsorában található lakat ikonra kattintva kaphatunk.



Megbízható biztonsági szoftverek

Egy naprakész, megbízható biztonsági program használatával további nagy lépést tehetünk a kiberfenyegetésekkel szemben A biztonsági szoftverek általában beépített szkennelési technikával elemzik a weboldalakat, és rosszindulatú tartalmakat keresnek. Ha ilyet észlelnek, nyomban jelzik a veszélyt, majd letiltják a webhelyhez való hozzáférést és a rosszindulatú tartalmak letöltését megóvva ezzel a felhasználót.
Az élvonalbeli biztonsági megoldások emellett általában adathalászat elleni védelemmel is rendelkeznek, megakadályozva a jelszavak, banki adatok és más érzékeny információk megszerzésére irányuló kísérleteket. Amikor megpróbálunk hozzáférni egy adott URL-címhez, a biztonsági szoftver összehasonlítja azt az adathalász webhelyek adatbázisával, egyezés esetén pedig azonnal megszünteti a hozzáférést, és figyelmezteti a felhasználót a veszélyre. A most felsorolt biztonsági tippek betartása mellett érdemes óvakodni még a gyanús hirdetésektől, valamint a helyesírási hibáktól hemzsegő weboldalaktól is.

Összegezve tehát az online biztonságunk megőrzése érdekében legyünk mindig nagyon körültekintőek, hiszen a kiberbűnözők egyre fejlettebb technikákat vetnek be a megtévesztésünk érdekében.

A Sicontact Kft.-ről röviden:

A Sicontact Kft. hazánkban az egyik legjelentősebb **IT biztonsággal foglalkozó** cég, az ESET termékek kizárólagos magyarországi forgalmazója. Mottója és küldetése, ami köré termékportfolióját kialakította: „**biztonság a digitális világban**”.

A Sicontact Kft. Magyarországon az **ESET NOD32** technológiára épülő termékeivel mind a lakossági, mind a vállalati szegmensben meghatározó piaci szereplő.
A cég 2007-ben megszerezte az ESET ausztriai képviseletét, így azóta regionális piaci szereplőként tevékenykedik. A Sicontact Kft. több ízben elny erte a kitüntető **Business**

Superbrands díjat. Az ESET Smart Security programcsomagot többször is **az év antivírus megoldásának** választották.

A független tesztelő szervezet több díjjal is elismerte az otthoni ESET termékeket a 2019-es eredményeket összefoglaló riportjában:
- Arany díjat nyert a fejlett, célzott és fájlnélküli kártevő támadások kivédésében, amely új kategóriaként jelent meg 2019-ben. Az ESET volt azon két gyártó egyike, akik mind a 15 célzott támadást sikeresen blokkolták a tesztelés során.
- 2018-ban ezüst, majd 2019-ben arany díjat szerzett a rendszer gyorsaságára és teljesítményére gyakorolt hatást vizsgáló kategóriában, az ESET szoftverek alacsony erőforrásigényének köszönhetően.
- Bronz díjat nyertek el a téves riasztások kategóriájában, amelyek ugyanúgy gondot okozhatnak, mint egy valós fertőzés, ezért az elkerülésük kulcsfontosságú a biztonsági szoftvereknél.

A Sicontact Kft. az ESET szoftvereit a lehető legrugalmasabb konstrukciókban, magyar nyelvű terméktámogatással kínálja. Az ESET már több mint 25 éve biztosít védelmet a digitális világ fenyegetéseivel szemben. Egy kicsi és dinamikus vállalatból mára egy több mint 100 millió felhasználót számláló és 202 országot és területet lefedő globális márkává nőtte ki magát.
Rengeteg minden változott, de az alapvető törekvéseik és a hozzáállásuk változatlan maradt, továbbra is céljuk egy biztonságosabb digitális világ felépítése, amelyben mindenki élvezheti a biztonságos technológia előnyeit.

További információ és interjúegyeztetés:

Terdik Adrienne | **Ügyvezető igazgató | PResston PR | Rózsadomb Center | 1025 Budapest | Törökvész u. 87-91. | T + 36 1 325 94 88 | F +36 1 325 94 89 | M +36 30 257 60 08 | adrienne.terdik@presstonpr.hu | www.presstonpr.hu**

Szekeres Nikoletta | PR vezető | PResston PR | Rózsadomb Center | 1025 Budapest | Törökvész u. 87-91. | T + 36 1 325 94 88 | F +36 1 325 94 89 | M +36 30 831 64 56 | nikoletta.szekeres@presstonpr.hu | www.presstonpr.hu

Károly Róbert | PR referens | PResston PR | Rózsadomb Center | 1025 Budapest | Törökvész u. 87-91. | T + 36 1 325 94 88 | F +36 1 325 94 89 | M +36 30 769 8697 | robert.karoly@presstonpr.hu | www.presstonpr.hu