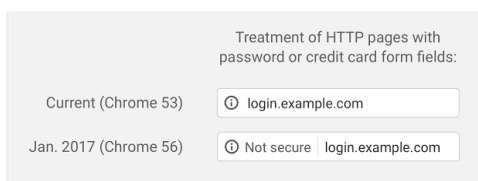


Karanténba zárja jövőre a nem biztonságos oldalakat a Google

- Üzent a Google a nem biztonságos oldalaknak: jövőre a Chrome feltűnően jelzi majd, ha SSL nélküli lapra navigálunk.
- A biztonsággal eddig kevesebbet törődő magyar vállalkozásokat is büntetni fogja a legnépszerűbb webes böngésző új intézkedése, ha nem hitelesítik weboldalukat SSL-tanúsítvánnyal.

A webes biztonság ma már nem luxus, hanem kötelező. Legalábbis úgy tűnik, a Google-nél így gondolkoznak. A keresőóriás blogján jelentette be: 2017 januárjától már nemcsak a keresési eredményekben sorolja hátrébb a nem biztonságos – SSL-protokoll nélkül – működő weboldalakat, de a böngészője szöveges üzenetben is jelzi mindezt.



A Chrome böngésző címsorának jelenlegi és jövőbeni megjelenése nem védett weboldalak esetén.

(Forrás: <https://security.googleblog.com/2016/09/moving-towards-more-secure-web.html>)

„Eddig is tudtuk, hogy a Google-keresésekben hátrányban vannak a hitelesítés nélküli weboldalak, hiszen a keresőmotor automatikusan hátrébb sorolja őket a találati listán. Azonban úgy tűnik, itt nem állnak meg. Az Internetes óriás legutóbbi lépése újabb komoly figyelmeztetés azon vállalatoknak, amelyek eddig nem törődtek a biztonsággal. A tervek szerint a jövőben a böngésző még hangsúlyosabban hívja majd föl a figyelmet a hitelesítés nélküli weboldalakra, sőt az is elképzelhető, hogy belátható időn belül meg sem jeleníti őket.” – mondta el Almási János az internetbiztonsággal foglalkozó NetLock termékfejlesztési vezetője. A szakértő hozzátette, hogy bár hazánkban is egyre több weboldalon védenek SSL-tanúsítvánnyal, még mindig csak a vállalatok töredéke éri át a biztonság üzleti jelentőségét. „A Google bejelentése egyértelművé teszi az SSL/TSL-protokoll alkalmazása a webes kommunikációban nem csupán egy biztonsági tényező, de forintosítható versenyhátrányba is kerülnek azon cégek, akik nem hitelesítik a weboldalukat. Mindez ma már nem luxus: évi néhány ezer forintért, pár kattintással megrendelhető az SSL-tanúsítvány és biztosítható egy weboldal alapszintű védelme. Érdeemes minden vállalatnak lépnie a digitális evolúcióban.” – összegezte.

Miben segít az SSL-tanúsítvány?

Az SSL-tanúsítvány a weboldal gazdáját és látogatóit egyaránt védi. A látogatókat egyrészt biztosítja arról, hogy a megjelenő információk valóban az adott weboldalhoz tartoznak (és azokat senki nem változtatta meg a kommunikáció folyamán), másrészt a webszerver és az ügyfél között zajló kommunikáció titkosításával garantálja, hogy az ügyfél által megadott adatokat kizárólag a weboldal üzemeltetője ismerheti meg. A nagyobb értékű SSL-tanúsítványok a weboldalon túl az azt üzemeltető cégeket, szervezeteket is hitelesen azonosítják, ez különösen a pénzügyi, kereskedelmi területen elengedhetetlen, és komoly bizalmi faktor, de minden cég számára alapvető, hogy az ügyféladatokat ne kerülhessenek illetéktelen kezekbe. Az SSL-tanúsítványok alkalmazásával ezek megszerzésének egyik módját tudják kizárni.

Hogyan győződhetünk meg látogatóként egy weblap biztonságáról?

1. A Chrome címmezőjében (de sok más böngészőben is) egy zártlakat-ikon jelzi, ha egy weboldal hitelesített, biztonságos és az odalátogató ügyféllel zajló kommunikáció titkosított van.
2. Ilyenkor a címmezőben a domainnév <http://> helyett <https://> előtaggal kezdődik.
3. Ha nincs ilyen ikon a weboldal címe előtt, akkor az oldal nincs védelem alatt. Az oldal nem hiteles és a kommunikáció nem titkosított, így az ott megadott adatokat illetéktelenek is könnyedén megszerezhetik.
4. Jövőre a Chrome böngésző üzenettel is jelzi, ha egy oldal nem rendelkezik SSL-tanúsítvánnyal.

Mit kell tenni, ha vállalati weboldalunkat védeni szeretnénk?

1. Az SSL-tanúsítvány kiváltáshoz keressünk fel egy bizalmiszolgáltatót, hitelesítéssel foglalkozó céget vagy azt a dominregisztrátort, ahol a domaincímünket regisztráltuk.
2. Az SSL-tanúsítvány automata (DV SSL) verziója – mint a legegyszerűbb, belépőszintű védelem – egyszerűen és már évi néhány ezer forintért megrendelhető.
3. A fejlettebb OV- és EV-szintű SSL-tanúsítványok megrendeléséhez már szükséges a céges dokumentumok egyeztetése is, de cserébe magasabb szintű hitelesítést kapunk, amivel szolgáltatásunk komolyságát is hatékonyan hangsúlyozhatjuk és még inkább védjük ügyfeleinket.

Milyen szintű SSL-tanúsítványt válasszunk?

Az SSL-tanúsítványoknak különböző minőségei léteznek:

1. Az alap **DV** (domain validation) SSL annyit igazol, hogy a böngésző címsorában megjelenő domainnév mögött valóban a hozzá tartozó weboldal található és már ez a tanúsítvány is biztosítja a titkosított kommunikációt.
2. Az **OV** (organization validation) SSL-tanúsítvány egy bejegyzett szervezethez is köti az adott domainnel azonosított szolgáltatást. A tanúsítványt kiállító bizalmi szolgáltató (pl. Netlock) ilyenkor ellenőrzi a cég, egyesület vagy más jogi személy létezését és a domain feletti használati jogosultságát, s a tanúsítványban feltünteti a szervezet nevét.
3. Az **EV** (extended validation) SSL-tanúsítványok kiállításához magasabb szintű ellenőrzések kapcsolódnak, ezért az ilyen oldalak címsorát a böngészők zöld színben tüntetik fel.
4. Az új egységes európai szabályozás által bevezetett, jogilag is elismert **minősített weboldal-hitelesítő tanúsítvány** képviseli a legmagasabb szintet. A jövő évi piaci megjelenését követően ezt lesz érdemes választani minden olyan európai cégnek, amely komoly internetes jelenléttel bír.

A NETLOCK-ról

A Docler cégcsoport tulajdonában álló NETLOCK az elektronikus hitelesített üzleti megoldások vezető fejlesztője, szolgáltatója és integrátora Magyarországon. Minősített hitelesítés-, időbélyegzés- és archiválásszolgáltató, PKI-tanácsadó és PKI-rendszerintegrátor-vállalként az elektronikus üzleti megoldások technológiai és jogi szakértője, szállítója.

A NETLOCK az első, a közigazgatásban is elfogadott hitelesítésszolgáltató Magyarországon. Olyan innovatív megoldásokat kínál hazai és nemzetközi partnerei részére, mint például az elektronikus számlázás, az e-Archiválás, az elektronikus másodbizonylat-megőrzés, az üzleti kommunikáció titkosítása SSL-tanúsítványokkal vagy a 2013-ban Magyar Termék Nagydíjjal elismert CityPass intelligens közlekedési és városkártyarendszer. Miközben lehetővé teszi, hogy ügyfelei e-tudatosabbá és ezáltal versenyképesebbé váljanak, maga is tudatosan keresi az elektronikus üzleti folyamatok minél szélesebb körű felhasználási lehetőségeit. A NETLOCK világszerte megbízható legfelső szintű hitelesítésszolgáltatóként szerepel a jelentősebb operációs rendszerekben – Windows, Mac OS X, iOS (iPhone, iPad),

Sajtóközlemény

Budapest – 2016. 10. 04.



Android OS –, a legfontosabb böngészőkben – Mozilla Firefox, Internet Explorer, Google Chrome, Safari – és levelezőalkalmazásokban – MS Outlook, MS Outlook Express, Mozilla Thunderbird, Mac OS Mail.

Sajtókapcsolat:

Drágus Richárd
vezető tanácsadó
NETLOCK
mobil: 06 30 626 7668
dragus.richard@netlock.hu
www.netlock.hu

Nemes Tamás
Kommunikációs és CSR-vezető
DoclerHolding Kft.
tel.: 06 1 432-3000
mobil: 06 30 573 96 42
nemes.tamas@doclerholding.hu