

## NETLOCK TIPPEK

2013. január 15.

### SSL: pajzs az online térben

Valószínűleg sokan találkoztak már olyan weboldallal, amely felugró ablakban figyelmeztet arra, hogy a kapcsolat nem titkosított, és ezért csak saját felelősségünkre lépünk tovább. Vajon ez csak jóindulatú tanács, vagy valós veszélyt jelez? Hogyan lehetünk biztosak abban, hogy egy internetes szolgáltatás tényleg biztonságos, és nem a titkainkra utazik?

#### *Mennyire elterjedt az SSL tanúsítványok használata?*

*Az SSL Labs 2012-ben végzett „SSL Pulse” felmérése szerint a weboldalak üzemeltetői közül nemzetközi szinten egyre többen ismerik fel a hitelesítés előnyeit. Az SSL-lel védett oldalak aránya tavaly április és október között 3,8 százalékkal nőtt, így a vizsgált 180 000 weboldal 13,6 százaléka már rendelkezik tanúsítvánnyal. Ugyancsak erősödött ezek között a minimum 128 bites titkosítási algoritmust használók száma. A titkosítási protokollok közül pedig a legfrissebbnek számító TLS 1.2 használata növekszik a leggyorsabban.*

Egy magára valamit is adó webes szolgáltatás esetében manapság már alapfelszereltségnek számít a digitálisan aláírt SSL tanúsítvány, amely biztonságossá teszi a kommunikációt a kliens – tehát a felhasználó számítógépe – és a szolgáltatás webszervere között. Ez azt jelenti, hogy ha egy SSL technológiával hitelesített webes szolgáltatással kommunikálunk, akkor onnantól kezdve, hogy leütünk egy billentyűt saját gépünk billentyűzetén, majd ezt az adatot az interneten továbbítjuk, azt már senki más nem láthatja, csak a hitelesített weboldal maga – és ugyanígy a válasz is csak a mi gépünkön lesz értelmezhető.

Azonban nem csak a szolgáltatókon és a weboldalak üzemeltetőjén múlik, hogy az interneten biztonságosan utazzanak az ügyfeladatok, hanem az felhasználókon is. Tudatosan oda kell figyelni a ránk leselkedő veszélyek elkerülésére, vagyis arra, hogy azok az oldalak, ahol nap mint nap bankolunk, fizetünk, személyes adatainkkal regisztrálunk vagy csak épp az emailjeinket olvassuk, megfelelő titkosítással rendelkezzenek. Fehér Krisztián, a NetLock Kft. termékmenedzsere öt tippel segít abban, mit tehetünk annak érdekében, hogy adataink az interneten is biztonságban legyenek.

#### 1. Navigáljunk mi a keresett oldalra!

Ha ismerjük a meglátogatni kívánt oldal webcímét, akkor ne más oldalról kattintva érkezzünk oda, hanem lehetőleg mi magunk írjuk be azt a böngésző címsorába. Így biztosan a keresett honlapot böngésszük.

## 2. Ellenőrizzük a weblap tartalmát!

Figyeljünk arra, hogy a címsorban szereplő domain valóban összhangban van-e a megjelenő tartalommal. Ezzel elkerülhetjük azokat a hamis, klónozott a weboldalakot, amelyek az eredetihez kísértetiesen hasonló webcímmel vagy tartalommal mutatkozva szereznek személyes adatokat a gyanútlan ügyfelektől.

## 3. Keressük az SSL biztonságot jelképező jeleket!

Az SSL tanúsítvánnyal rendelkező oldalak felismerésében segítenek a biztonságos böngészést mutató hivatalos jelzések, vagyis a böngésző címsorában megjelenő, SSL kapcsolat felépülését jelző **https://** tag, illetve a biztonságot jelképező **lakat szimbólum**.

## 4. Frissítsünk!

Tartsuk naprakészen számítógépünket és mobiltelefonunkat! Nem elég, ha csak az online szolgáltatást nyújtó fél kezdeményezi adataink SSL védelmét, de mi is legyünk felkészülve a technológia fogadására. Ennek érdekében mindig alkalmazzuk operációs rendszerünk és böngészőnk legújabb frissítéseit!

## 5. Ellenőrizzük az SSL tanúsítványt!

Érdemes ellenőrizni azt is, hogy honnan származik egy weboldal SSL tanúsítványa, amit a böngésző címsorában levő lakat szimbólumra kattintva tehetünk meg. Fontos, hogy csak minősített hitelesítés-szolgáltatók (CA) által kiállított tanúsítványokban bízunk meg! Ha egy SSL-lel védett oldalra lépve a böngésző nem kéri idegen tanúsítvány elfogadását és nem figyelmeztet biztonsági veszélyekre, akkor hitelesített helyen járunk.