SAJTÓKÖZLEMÉNY
AZONNAL KÖZÖLHETŐ
2012. január 17.

Egységes, visszafejthetetlen biztonság a NetLock minden ügyfelénél

- *A NetLock Kft. 2011. december 31-i hatállyal minden érintett ügyfelénél lecserélte az SHA-1 algoritmusú tanúsítványokat a biztonságosabb SHA-256 algoritmusúra.*
- *Az új SHA-256 típusú kriptográfiai lenyomatképző algoritmusok a korábbiaknál is erősebb hitelesítést tesznek lehetővé, visszafejtésük gyakorlatilag lehetetlen.*

Budapest, 2012. január 17. – A NetLock Kft., az elektronikusan hitelesített üzleti megoldások vezető fejlesztője, szolgáltatója és integrátora már 2009 óta ajánlja ügyfeleinek a korábbi megoldásoknál jóval hatékonyabb SHA-256 típusú kriptográfiai lenyomatképző algoritmusra épülő tanúsítványok használatát. Bár még a megoldás előző generációja, az SHA-1 visszafejtésére sem volt példa, a NetLock minden érintett ügyfelénél lecserélte a régi technológiát használó tanúsítványokat.

A mostantól egységesen használt SHA-256 algoritmus esetén a képzett lenyomat hossza 256 bit (79 karakter), amelyet csak $1{,}16*10^{77}$ számú próbálkozással lehet visszafejteni. Talán az mutatja legjobban az algoritmus visszafejtésének lehetetlenségét, hogy ez közel akkora számot takar, mint amennyi atom található a látható világegyetemben. Az SHA-256 típusú kriptográfiai lenyomatképző algoritmust használó tanúsítványkiadók a legfrissebb kriptográfiai ajánlásoknak és szabványoknak (ETSI TS 102 176-1 v 2.1.1) is megfelelnek.

„A változás azokat az SHA-1 algoritmussal, például időbélyegzővel korábban hitelesített elektronikus dokumentumokat is érinti, amelyek megőrzését és hitelességének fenntartását törvény írja elő. Emiatt az eArchiválás szolgáltatásunk keretében nálunk tárolt iratokat is felülhitelesítettük új tanúsítvánnyal rendelkező időbélyeggel” – mondta el Rózsahegyi Zsolt, a NetLock Kft. ügyvezetője. „Fontos azonban megjegyezni, hogy a felülbélyegzésről azoknak is gondoskodnia kell, akik maguk tárolják a hiteles dokumentumokat. Ezeket az iratokat felülhitelesíthetik saját maguk is, de igénybe vehetik minősített archiválás-szolgáltatónk segítségét is.”

A NetLock Kft. a Nemzeti Média- és Hírközlési Hatóság határozatának kézhezvételét követően, azonnal értesítette minden érintett ügyfelét a technológiai váltás tényéről, valamint honlapján pontos tájékoztatót

és útmutatót helyezett el. Végül a határidőt betartva, 2011. december 31-i hatállyal, minden érintett partnerének díjmentesen lecserélte a korábbi minősített aláíró tanúsítványokat SHA-256 típusú algoritmusokat használókra.

A törvényi kötelezettségnek eleget téve ma a NetLock teljes ügyfélbázisa egységesen naprakész, erős és megbízható biztonsági háttérrel felvértezett tanúsítványokat használ.

A NetLock Kft.-ről

A NetLock az elektronikusan hitelesített üzleti megoldások vezető fejlesztője, szolgáltatója és integrátora Magyarországon. Termékei és szolgáltatásai lehetővé teszik, hogy elektronikusan is hitelesek és biztonságosak legyenek a vállalatok és intézmények mindennapi üzleti folyamatai. Minősített hitelesítés-, időbélyegzés- és archiválás-szolgáltató, PKI tanácsadó és PKI rendszerintegrátor vállalatként a hazai elektronikus üzleti megoldások meghatározó technológiai és jogi szakértője, szállítója. A NetLock az első, a közigazgatásban is elfogadott hitelesítés-szolgáltató Magyarországon. Szakértő tanácsadóként segítséget nyújt a vállalatok hosszú távú versenyképességéhez, illetve hatékonyságuk növeléséhez nélkülözhetetlen üzleti folyamatok elektronizálásában, valamint rendelkezik nagyvállalati, intézményi hitelesítési infrastruktúrák kialakításához szükséges speciális jogi és informatikai know-how-val. A NetLock olyan innovatív elektronikus megoldásokat kínál, melyek lehetővé teszik, hogy ügyfelei e-tudatossá váljanak. Mindeközben maga is tudatosan keresi az elektronikus üzleti folyamatok minél szélesebb körű felhasználási lehetőségeit, ennek köszönhetően folyamatosan képes csökkenteni környezeti terhelését. 1999 óta világszerte szerepel valamennyi Microsoft termékben (Internet Explorer, Outlook, Outlook Express), valamint 2005 óta a Mozilla Suite, Firefox, Safari, Thunderbird böngészőkben és levelező szoftverekben, a PGP alkalmazáscsomagban is jelen van, mint megbízható legfelső szintű hitelesítés-szolgáltató.

Sajtókapcsolat:

Haász Nóra
team leader
Morpho Communications
tel.: 488 0255
mobil: 30 390 1394
haasz.nora@morpho.hu
www.morpho.hu