Személyes kulcsok biztonsága Linux Sysadmin munkaállomásán

Írta: Konstantin Ryabitsev - **2017. június 7-én – Linux.com**-on

Linux adminisztrátoroknak szóló sorozatunk ezen cikkében kifejtünk néhány javaslatot arról, hogyan gondoskodjunk a személyes kulcsunk (private key) biztonságáról. Ha más biztonsági javaslatok és további olvasmány-források (a Linux biztonságának rejtelmeiről) is érdekelnek, akkor javaslom, hogy töltsd le a „free security guide for sysadmins" könyvünket.

Személyre szabott titkosítási kulcsok, közötte SSH és PGP személyes kulcsok, a Linux munkaállomásod legértékesebb elemei. A támadók nagyon szeretnék megszerezni, mivel azokon keresztül tovább támadhatják a rendszert, vagy felléphetnek nevedben más adminokkal szemben. A linux-rendszergazdának további lépéseket kell tennie annak érdekében, hogy a személyes kulcsot ellopás ellen megvédje:

* erős jelszavakat használni a személyes kulcsok védelmére (Alapvető);
* PGP mesterkulcsot eltávolítható eszközön tárolni (Jó ha van);
* Auth (azonosító), Sign (aláíró) és Encrypt (titkosító) al-kulcsok tárolása chipkártyás eszközön (Ajánlott)
* SSH beállítása úgy, hogy a PGP Auth kulcsot használja ssh személyes kulcsként (Ajánlott)A személyes kulcs jobb biztonságának eljárásai

A személyes kulcs biztonsága elérésének legjobb eljárásai

A személyes kulcs ellopás elleni védelmének legjobb módja, hogy a személyes titkosító kulcsodat intelligens kártyán tárolod és soha sem másolod ki a munkaállomásra. Sok gyártó kínál OpenPGP-képes eszközöket:

* Kernel Concepts, itt mind OpenPGP-képes intelligens kártyát, mind USB-olvasót kaphatsz, ha szükséged lenne ezekre;
* Yubikey, OpenPGP intelligens kártyát csakúgy kaphatsz itt, mint más kiváló eszközt (U2F, PIV, HOTP stb.).
* NitroKey, nyílt forráskódú szoftveren és hardveren alapul.

Nagyon fontos gondoskodni arról is, hogy a mester PGP-kulcsot semmiképpen se tárold a fő munkaállomáson, és csak al-kulcsokat használj. Mester kulcs csak akkor kell. Amikor valaki más kulcsát kell aláírni, vagy új al-kulcsot kell készíteni – olyan műveletek, amik nem túl gyakran fordulnak elő. A mesterkulcs eltávolítható médiára mozgatásának és al-kulcsok készítésének módjára kövesd a Debian „subkey guide”-ját.

Emellett beállíthatod úgy a gnupgp programot, hogy az ssh kezelőként is működjön és intelligens kártyán elhelyezett PGP Auth kulcsot használjon személyes ssh-kulcsodként. Van egy olyan kiadványunk, ami leírja, hogyan csináljuk kártyaolvasó, vagy Yubikey NEO használatával.

Ha nem mennél el eddig, legalább arról gondoskodj, hogy mind a PGP, mind az SSH személyes kulcsod, egyaránt erős jelszót használjon, amivel megnehezíted a támadók dolgát azok ellopása és használata tekintetében.