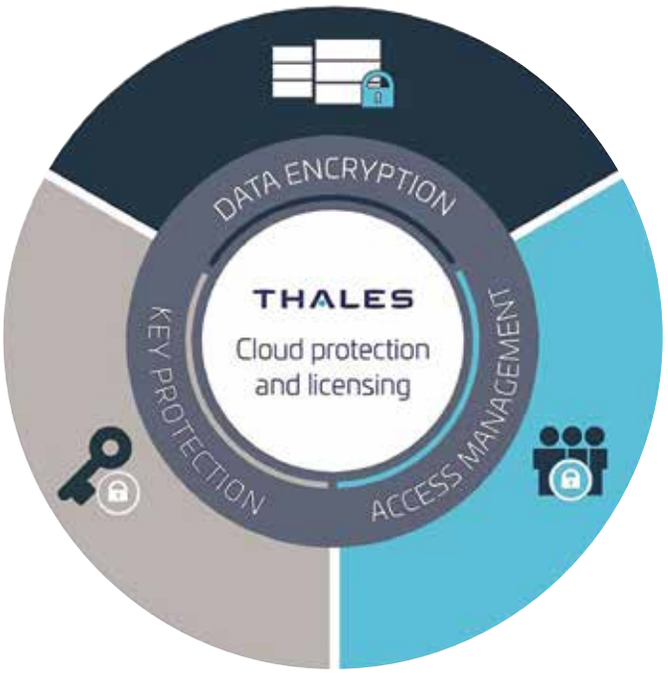
Biztonságos és erős felhasználó-hitelesítés vállalati környezetben: Thales

Az év elején elszaporodott kibertámadások célpontjában a kórházak, tech cégek és olyan szervezetek álltak, ahol a gyenge identitásvédelem vagy annak hiánya volt jellemző. A vállalati IT-biztonság leggyengébb láncszeme maga a felhasználó, aki gyakran ugyanazokat a jelszavakat használja a vállalati alkalmazásoknál, amit a magánfiókjaiban. A felmérések adatai – például a State of Password and Authentication Security Behaviors 2019 – azt mutatják, hogy az informatikai biztonsági szakemberek 50 százaléka átlagosan öt azonos jelszót használ munkahelyi és személyes fiókjaihoz, sőt, közel 70 százalékuk meg is osztja jelszavát kollégáival. Ezenkívül a felmérések azt is jelzik, hogy **a vállalatok 95 százaléka nem titkosítja az adatokat.**



FORRÁS: THALES

A legtöbb vállalatnál még nem történt meg a felhős rendszerre való teljes átállás, így a szervezeteknél gyakoriak a hibrid (belső és a felhőalapú) szolgáltatások. Ennél a modellnél a biztonsági határ már nem a belső hálózat, hanem a felhasználó.

Sok vállalat különböző VPN technológiák irányába mozdult el, viszont ezek önmagukban nem biztosítanak magasabb és kellő szintű védelmet az azonosítási fázisban. Ilyen esetekben tehát elengedhetetlen a **többfaktoros autentikáció (MFA),** amely lehetővé teszi az alkalmazottaknak, hogy VPN-en keresztül biztonságos, külső hozzáférést kapjanak a felhő alapú és a belső szolgáltatásokhoz egyaránt. Mindkét alternatívánál fontos, hogy az ott tárolt adatok ne legyenek kompromittálhatók, ezért elengedhetetlen az **adatok átlátható titkosítása,** amihez szükséges egy eszköz, amely a titkosított kulcsot és az adatot külön kezeli. Ideális megoldás a kulcsok biztonságos tárolására és menedzselésére fejlesztett HSM (Hardware Security Module). Így az MFA-szolgáltatás és HSM társításával kizárólag csak a jogosult és hitelesített felhasználó férhet hozzá a titkosított adatokhoz.

A hazai piacon – a biztributor forgalmazásában – a Thales ad átfogó technológiai választ az adatok és alkalmazások többfaktoros hitelesítéssel történő hozzáféréshez és titkosításához, legyen az alkalmazás, adatbázis, fájl megosztás, virtuális gép, lemezkép, hálózati forgalom, stb.

A **Thales Safenet Trusted Access (STA)** vállalati multi-faktoros autentikáció- és hozzáférésmenedzsment integrálható a legtöbb céges alkalmazáshoz, legyen az helyi vagy felhő alapú (Office365, VPN, AWS, Jira, stb.) Az STA különböző, biztonságos hitelesítési eljárásaival (OTP, Push-OTP, mobil token, fizikai token, stb.) erősíti a felhasználói bejelentkezések folyamatát, illetve a Smart SSO (Single Sign-on) funkciójával szabályozhatók és ellenőrizhetők az alkalmazásokhoz való hozzáférések.

A Thales az adattitkosítás terén teljes körű termékportfólióval rendelkezik. A **Hardware Security Modul (HSM)** Luna 7 FIPS 140-2 L3 tanúsítással egyfajta trezorként funkcionál, védve a titkosítási folyamat legfontosabb elemét, magát a titkosító kulcsot. A HSM jelentősen felgyorsítja a kriptográfiai műveleteket, többek között a titkosítást, aláírást, véletlenszám-generálást.

Ha az ügyfél a titkosító kulcsokat nem csak a PKCS#11 interfészen szeretné használni, a Thales kulcskezelő rendszerét (KMS-ét), a **CipherTrust Managert** javasoljuk, amely a külső, titkosított kulcsok forrásának biztonságos felhasználását kiterjeszti más alkalmazásokra. A rendszer olyan átlátható adattitkosítást kínál agentek segítségével, amik különféle operációs rendszerekre és platformokra telepíthetők, mint például Linux, Windows, Container-ek, SAP HANA, Teradata, stb. A jogosult felhasználók olvasható formában látják a védett és titkosított adatokat, míg a jogosulatlan felhasználók nem férhetnek hozzá az adatokhoz, vagy csak titkosított formában láthatják azokat.

Még több infó a vállalati szintű adattitkosításról, felhasználói hitelesítésről a Thales oldalán https://cpl.thalesgroup.com, vagy kérdezz a forgalmazótól, a biztributortól: thales@biztributor.hu *(X)*