



RSA AUTHENTICATION MANAGER EXPRESS

Megoldás-
összefoglaló



EMC²
where information lives®

A csak jelszavakon alapuló autentikációval kapcsolatos kockázatok jól ismertek. Mégis, a vállalatok 44 százaléka jelszavakra támaszkodik, amikor alkalmazottainak és alvállalkozóinak távoli hozzáférést biztosít¹. Az adatokra irányuló, egyre gyakoribb és egyre kifinomultabb támadásokkal szemben a statikus jelszavakon alapuló biztonsági rendszerek védtelenek, és fenyegeti őket az illetéktelen hozzáférés veszélye.

Az erős autentikáció a széles körben elfogadott megoldás a kritikus adatokhoz és alkalmazásokhoz történő hozzáférés védelmére. A biztonsági megoldások bevezetése azonban gyakran kihívást jelent a kis- és középvállalatok számára, mert nem rendelkeznek a megfelelő erőforrásokkal hálózatuk teljes védelmére, és előfordul, hogy azt hiszik, nem válhatnak támadások célpontjává. A közelmúltban a National Cyber Security Alliance (Nemzeti Cyberbiztonsági Szövetség) által végzett felmérés szerint a kis- és középvállalatok 85 százaléka meg van győződve arról, hogy ők kevésbé válhatnak a cyberbűnözők áldozataivá, mint a nagyvállalatok². Sajnos a cyberbűnözők tisztában vannak azzal, hogy sok kis- és középvállalat nem rendelkezik megfelelő biztonsági felügyelettel, ezért egyre gyakrabban veszik őket célba bizalmas adatok megszerzése céljából.

Az erős autentikáció akadályainak legyőzése

A kis- és középvállalatok esetén a kétfaktoros autentikáció melletti döntést több tényező is akadályozhatja. A három legnagyobb probléma, amely sok kis- és középvállalatot visszatart az erős autentikáció bevezetésétől:

- a magas költségek;
- a felhasználóknak okozott kényelmetlenség;
- a bevezetés és az üzemeltetés bonyolultsága.

Költségek

A kis- és középvállalatok gyakran a meglévő megoldások költségét emelik ki, mint az erős autentikáció bevezetésének legnagyobb akadályát. Például az egyszerű használatos jelszavakon alapuló megoldás bevezetése végfelhasználói eszközökbe, autentikációs szerverbe és hasonló hardvereszközökbe történő befektetést igényel. Ezen túlmenően az ügyfelek támogatásával és szoftverfrissítésekkel kapcsolatos üzemeltetési költségek is jelentkeznek. Ezért a korlátozott IT-költségvetéssel rendelkező kis- és középvállalatok zöme az egyszerű felhasználónéven és jelszón alapuló bejelentkezéssel teszi védetté a hozzáférést.

A felhasználóknak okozott kényelmetlenség

Az erős autentikáció bevezetésekor a felhasználók kényelme fontos szempont. A vállalatoknak át kell gondolni, hogy a fokozott biztonság vajon hátráltatja-e majd alkalmazottaik termelékenységét, és várhatóan ellenállásba ütközik-e az új technológia elfogadtatása. Ez szintén befolyásolhatja a megoldás teljes költségét, ha a fokozott segítséget igénylő felhasználók miatt megnő a helpdeskhívások száma.

Bevezetés és üzemeltetés

Az erős autentikáció kezdeti bevezetése jelentős erőforrás-befektetést igényelhet az IT-osztálytól. A felhasználók be- és kiiktatását, a hardver és szoftver kiosztását és a megoldás folyamatos üzemeltetésével kapcsolatos további hasonló feladatokat is figyelembe kell venni. A kis- és középvállalatok IT-erőforrásai már így is korlátozottak, ezért az erős autentikáció megfelelő üzemeltetéséhez szükséges többletidő és -létszám gondolata elrettentő lehet az amúgy is túlterhelt személyzet számára.

1 Forrester Research: „Best Practices: Implementing Strong Authentication in Your Enterprise”, 2009. július

2 2010 NCSA/Visa Inc. Small Business Study

Erős autentikáció a kis- és középvállalatok számára

Az RSA Authentication Manager Express választ ad a kis- és középvállalatok költségekkel, felhasználói kényelemmel és IT-üzemeltetési korlátokkal kapcsolatos problémáira, emellett költséghatékony, kényelmes megoldást nyújt biztonsági engedmények nélkül. A megoldás egy erős, többfaktoros autentikációs platform, amely biztonságos távoli autentikációt kínál akár 2500 felhasználónak is. Az RSA Authentication Manager Express a vezető SSL VPN-ekkel és webalapú alkalmazásokkal együttműködve lehetővé teszi a kis- és középvállalatok számára, hogy erős autentikációt és a biztonságos hozzáférést nyújtsanak a védett alkalmazásokhoz és adatokhoz.

Az RSA Authentication Manager Express az RSA kockázatalapú autentikációs technológiáján alapul. A középpontban az RSA Risk Engine áll, egy kifinomult rendszer, amely minden egyes bejelentkezési kísérletet és tevékenységet a kockázatjelzők tucatjait követve, valós időben elemez, és minden egyes felhasználói kéréshez egy kockázati szintet rendel. Az RSA Authentication Manager Express az egyes hozzáférési kérelmekhez kapcsolódó kockázatot több faktor figyelembevételével határozza meg:

- valami, amit a felhasználó tud, például egy felhasználónév és jelszó;
- valami, amit a felhasználó birtokol, például egy laptop vagy asztali számítógép;
- valami, amit a felhasználó tesz, például a közelmúltban végzett autentikáció vagy fiókművelet.

Az RSA Risk Engine lehetővé teszi, hogy a vállalatok saját kockázattűrési korlátjainak megfelelő előírásokat határozzanak meg, és a magastól az alacsonyig több kockázati szintet jelöljenek ki.

Az RSA Authentication Manager Express lehetővé teszi a kockázati szintek felhasználói csoportok szerinti beállítását is. A vállalatok úgy is dönthetnek, hogy a vállalatukhoz való viszonyuk alapján a különböző felhasználói profilokhoz különböző autentikációs előírásokat rendelnek. Például a vállalatok magasabb hozzáférési kockázati tűréshatárt állíthatnak be az alkalmazottak számára, mint az ügyfelek vagy partnerek bejelentkezésére. Ha az RSA Risk Engine szerint a hozzáférési kérés kockázati szintje a megengedett korlát alatt van, akkor a felhasználó autentikációja zökkenőmentesen megtörténik. Ha azonban az RSA Risk Engine úgy találja, hogy a hozzáférési kérés kockázata a megengedett korlát felett van, akkor a felhasználótól további bizonyítékot kérhet azonosságának igazolására.

Eszközjellemzők: valami, amit a felhasználó birtokol

Az RSA Risk Engine által az egyes felhasználói hozzáférési kérésekkel kapcsolatosan megvizsgált információk két kategóriába sorolhatók: eszközjellemzők és viselkedési jellemzők. Az első összetevő, az eszközjellemzők vizsgálata a felhasználók túlnyomó többsége számára lehetővé teszi az autentikációt a hozzáféréshez általában használt laptop vagy asztali számítógép jellemzői alapján, az eszköz és a felhasználó korábbi ismert kapcsolata szerint. Az eszközjellemzők vizsgálatának két fő része az egyedi eszközazonosítás és a statisztikai eszközazonosítás.

Az egyedi eszközazonosítás a felhasználó azonosításához két fő elemet helyez el a felhasználó eszközén: (a) biztonságos saját cookie-kat és (b) flash osztott objektumokat (más néven flash cookie-kat). A biztonságos saját cookie-k fontos szerepet játszanak a laptop és asztali gépek azonosításában. Egy egyedi kriptográfiai azonosítót helyeznek el a felhasználó eszközén, és ezek jelentik a felhasználó azonosítására tipikusan használt kezdeti mechanizmust. A flash cookie-k a saját cookie-kal együtt használatosak a megbízhatóság megduplázására. Az RSA Authentication Manager Express flash cookie-kat használ a felhasználó gépének megjelölésére ugyanúgy, ahogy a saját cookie-k tárolják a később előhívható

információkat. A flash cookie-k alkalmazásának előnye az, hogy ezeket nem törlik olyan gyakran, mint a saját cookie-kat, mert a legtöbb felhasználó nem tud a létezésükről. Még azok a felhasználók, akik tudnak róluk, sem mindig ismerik az eltávolítás módszerét.

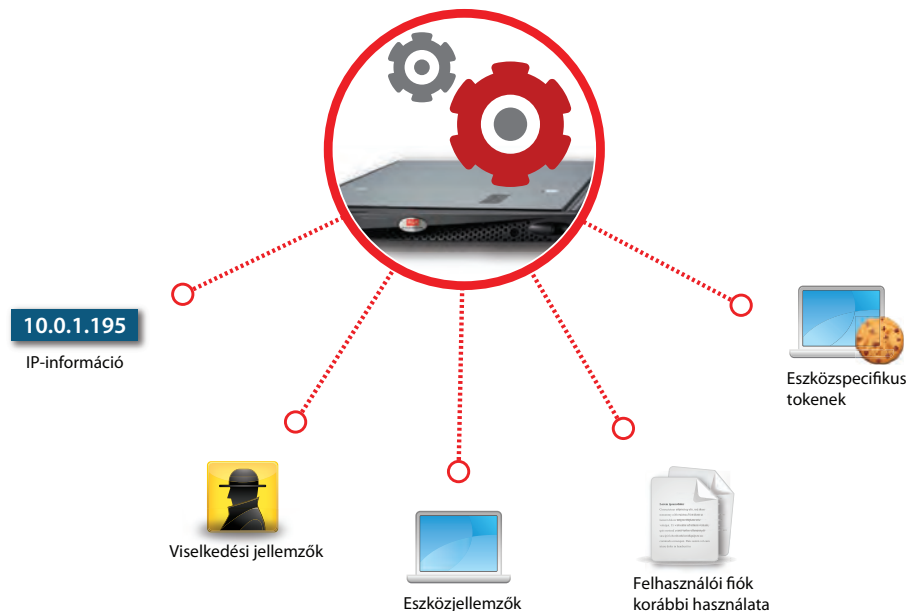
A statisztikai eszközazonosítás egy olyan technológia, amely az eszköz tulajdonságait felhasználva statisztikai módon azonosítja és hozzákapcsolja a felhasználót egy bizonyos eszközhöz. Az eszköznyomozásnak, nyomelemzésnek vagy eszközujjlenyomat-vizsgálatnak is nevezett statisztikai eszközazonosítás általában tartalékmegoldásként használatos, ha az (eszköztől törölhető) egyedi kriptográfiai azonosító hiányzik.

A statisztikai eszközazonosítás során vizsgált tényezők közé tartoznak a HTTP-fejlécekből származó és a Java™-parancsfájlok által gyűjtött adatok, például az operációs rendszer verziószáma, a javítófájlok száma, a képernyőfelbontás, a böngésző verziószáma, a felhasználói agent adatai, a szoftververziók, a képernyő tulajdonságai (méret és színmélység), a nyelvek, az időzóna-beállítások, a telepített böngészőobjektumok, a telepített szoftverek, a területi és nyelvi beállítások és az IP-cím.

Viselkedési jellemzők: valami, amit a felhasználó tesz

Az eszközjellemezőkön túl az RSA Authentication Manager Express megvizsgálja a felhasználó viselkedését, mielőtt a hozzáférési kérelmekhez kockázati szintet rendelne. A viselkedési jellemzők vizsgálatának célja a magas kockázatú bejelentkezések felismerése olyan elemek révén, mint a gyakoriság, az IP-cím, és az autentikációs és felhasználási tevékenységek (pl. változások a felhasználói profilban vagy több sikertelen autentikációs kísérlet). Például, ha a felhasználó általában New Yorkból jelentkezik be, ám egyszer csak Moszkvából kísérel meg bejelentkezni, akkor ezt a rendszer szokatlan viselkedésnek tekintheti. Ha azonban a felhasználó gyakran utazik, és rendszeresen különböző helyekről jelentkezik be, akkor ez nem feltétlenül minősül szokatlannak.

1. ábra: Az RSA Risk Engine tényezők tucatjait vizsgálja meg a felhasználói kérések kockázati szintjének megállapításához



A magas kockázati szintű hozzáférési kérések szigorúbb autentikációja

Az RSA Authentication Manager Express további autentikációs módszereket is elindíthat, ha a hozzáférési kérelem kockázata meghaladja a vállalat által meghatározott szintet. Ez különösen olyan helyzetekben fordul elő, amikor a távoli felhasználó egy ismeretlen eszközről jelentkezik be, amelyet korábban még nem használt a hálózathoz való hozzáférésre. Az RSA Authentication Manager Express további autentikációs lépésként két választási lehetőséget kínál a vállalatoknak: sávon kívüli SMS vagy igazoló kérdések használata.

Sávon kívüli SMS

A sávon kívüli SMS üzenetes autentikációra akkor kerül sor, ha a hozzáférési kéréshez tartozó kockázati szint magas. Ilyenkor az RSA Authentication Manager Express a felhasználót arra kéri, hogy egy könnyen érthető eljárás révén szolgáltasson további bizonyítékot azonosságára.

Először a rendszer kéri a felhasználót annak a titkos PIN kódnak a megadására, amelyet a rendszerbe iktatáskor választott. Ezután a rendszer automatikusan küld egy SMS-t a felhasználó üzenetfogadási célra regisztrált mobiltelefonjára. Az SMS szövege egy egyedi, nyolcjegyű kódot tartalmaz, amelyet a felhasználó begépel a webböngészőjébe. Miután a rendszer ellenőrizte a kód helyességét, a felhasználó megkapja a hozzáférést. Az RSA Authentication Manager Express támogatja az egyszer használatos jelszavak e-mailes küldését is.

A sávon kívüli SMS-autentikáció fő előnye, hogy bármilyen mobiltelefonnal használható, és nem szükséges, hogy a felhasználó új hardvert vásároljon, vagy új szoftvert telepítsen.

Ellenőrző kérdések

Az ellenőrző kérdések olyan kérdések, amelyeket a felhasználó választ egy listáról, és megadja rájuk a helyes választ a kezdeti regisztrációs eljárás során, vagy az erősségi autentikáció vállalati bevezetésekor. A felhasználótól csak a kérdések egy részét kérdezi meg a rendszer az autentikációs ellenőrzés során, így minimalizálja annak esélyét, hogy a felhasználó titkos kérdései és válaszai illetéktelen kezekbe kerülnek. A vállalatok saját kérdéslistát is létrehozhatnak az RSA Authentication Manager Express beépített kérdései helyett.

Bevezetés és üzemeltetés

Az RSA Authentication Manager Express egy kulcsrakész eszköz, amely módosítás nélkül, azonnal támogatja a vezető SSL VPN-eket és webszervereket. Az RSA Quick Setup segítségével a szerver néhány egyszerű lépéssel üzembe helyezhető.

A végfelhasználók felé történő bevezetés is ugyanilyen egyszerű. Az RSA Authentication Manager Express közvetlenül csatlakoztatható egy meglévő címtárszerverhez, és a felhasználók a következő autentikáció alkalmával végzik el az önregisztrációs eljárás automatikusan irányított lépéseit. Mivel a beiktatási eljárás teljesen automatikus, az adminisztrátorok megtakaríthatják az egyéb autentikációs módszereknél ehhez szükséges időt.

Fő előnyök

Az RSA Authentication Manager Express a kis- és középvállalatok erős autentikációval kapcsolatos igényeinek kielégítésére tervezett megoldás.

Költséghatékonyság – Az RSA Authentication Manager Express mind tartalmában, mind árfekvésében ideális a legfejlebb 2500 felhasználóval rendelkező vállalatok számára.

Felhasználói kényelem – Az RSA Authentication Manager Express a legtöbb felhasználó esetén a felhasználónév és a jelszó alapján elvégzi az autentikációt. Ezekben az esetekben a többfaktoros autentikáció láthatatlan a felhasználó számára, mert az RSA Risk Engine a színtalok mögött dolgozik. A felhasználó csak akkor kerül szigorúbb vizsgálat alá, ha az RSA Risk Engine a hozzáférési kérelmet magas kockázati szintűnek minősíti.

Egyszerű bevezetés és üzemeltetés – Az RSA Authentication Manager Express egy kulcsrakész eszköz, amely módosítás nélkül, azonnal támogatja a vezető SSL VPN-eket és webszervereket. Továbbá a beiktatási eljárás teljesen automatikus, így az adminisztrátorok megtakaríthatják azt az időt, amelyet a felhasználók be- és kiiktatásával töltenének.

Bevált technológia – Az RSA Authentication Manager Express azt a kockázatalapú autentikációs technológiát alkalmazza, amelyet több mint 8000 vállalat használ a különböző iparágakban, többek között a pénzügyi szolgáltatási, egészségügyi, biztosítási, kiskereskedelmi és kormányzati szektorban. Jelenleg az RSA kockázatalapú autentikációs technológiája több mint 250 millió felhasználó azonosságát védi, és biztosít hozzáférést számos alkalmazáshoz és rendszerhez, többek között webhelyekhez, portálokhoz és SSL VPN-alkalmazásokhoz.

Következtetés

Az RSA Authentication Manager Express lehetővé teszi a kis- és középvállalatok számára, hogy áttérjenek egy olyan erős autentikációra, amely költséghatékony és kényelmes mind a felhasználók, mind az IT-adminisztrátorok számára. Az RSA Authentication Manager Express révén a kis- és középvállalatok megakadályozhatják az illetéktelen hozzáférést, csökkenthetik az adatsérelem kockázatát, és megoldhatják megfelelőségi problémáikat költségvetési korlátjaikon belül, továbbá kényelmes módon nyújthatnak távoli hozzáférést új felhasználóiknak.

Az erős autentikációval kapcsolatos téveszmék

Téveszme	Valóság
A vállalatom erős jelszavakat használ, és alkalmazottjainknak rendszeresen módosítaniuk kell azokat, ami csökkenti a kockázatot.	Az erős jelszavak, amelyek számokat, nagybetűket vagy egyéb karaktereket tartalmaznak, valóban nehezen kitalálhatók, de ugyanakkor az alkalmazottaknak is nehéz emlékezni rájuk. Ez ahhoz vezethet, hogy az alkalmazottak leírják a jelszavakat, vagy hasonló módszereket alkalmaznak, ami igazából növeli a kockázatot. A valódi erős autentikációhoz több mint egy faktor szükséges – az egyszerű jelszón túl még valami.
A vállalatom számára az erős autentikáció túl költséges.	Az erős autentikáció nagyon költséghatékony is lehet – és nemcsak nagyvállalatok számára. Például az RSA Authentication Manager Express kifejezetten a kisebb felhasználói bázissal és korlátozott IT-költségvetéssel rendelkező vállalatoknak készült, mind tartalmában, mind árfekvésében.
Az erős autentikáció költsége meghaladja az előnyeit.	Az erős autentikáció költsége sokkal alacsonyabb, mint az adatsérelem esetén felmerülő költségek vagy a megfelelési hiányok miatt fizetendő büntetések. Ezen túlmenően az erős autentikáció segít a vállalatoknak új bevételi forrást jelentő üzleti lehetőségek létrehozásában, és hatékonyabbá teszi az üzleti folyamatokat, ami az erősebb biztonság költségeit jelentéktelenné teszi.
A cyberveszélyek csak a nagyvállalatokat és a kormányzati szervezeteket fenyegetik.	Éppen ellenkezőleg. A cyberbűnözők egyre gyakrabban veszik célba a kis- és középvállalatokat, mert ezek a korlátozott biztonsági felügyelet miatt a támadásokkal szemben védtelenebbek.

Az RSA bemutatása

Az RSA, az EMC biztonságtechnikai részlege, a biztonsági, kockázatkezelési és megfelelőségi megoldások elsődleges szolgáltatója, amely a világ vezető vállalatait segíti a legbonyolultabb és legérzékenyebb biztonsági kihívások legyőzésében. Ezek a kihívások kiterjednek a vállalati kockázat menedzselésére, a mobil hozzáférés és együttműködés biztonságossá tételére és a virtuális, illetve felhőkörnyezetek védelmére.

Az azonosságigazolás, adatvesztés elleni védelem, titkosítás és tokenizáció, csalásérzékelés és a biztonsági események kezelésének (SIEM) üzleti szempontból kritikus megoldásait az iparág vezető eGRC-képességével és konzultációs szolgáltatásaival kombinálva az RSA bizalmat és láthatóságot biztosít felhasználói azonosságok milliói, valamint az általuk végrehajtott tranzakciók és generált adatok számára.

Az RSA, az RSA logó, az EMC2, az EMC és a „where information lives” szlogen az EMC Corporation bejegyzett védjegyei vagy védjegyei az Amerikai Egyesült Államokban és más országokban. Minden más hivatkozott védjegy a megfelelő tulajdonos tulajdona. ©2011 EMC Corporation. Minden jog fenntartva. Kiadva az Amerikai Egyesült Államokban.

www.rsa.com

AMX SB 0111

