



RSA AUTHENTICATION MANAGER EXPRESS

Solution Brief



EMC²
where information lives®

De risico's van authenticatie met alleen een wachtwoord zijn bekend. En toch maakt 44 procent van alle bedrijven tegenwoordig nog steeds alleen gebruik van wachtwoorden om de externe toegang voor werknemers en onderaannemers te beveiligen¹. Doordat de bedreigingen steeds geavanceerder worden en het aantal gevallen van gegevensdiefstal blijft toenemen, zijn systemen die vertrouwen op statische wachtwoorden zeer kwetsbaar en bestaat het risico van ongeautoriseerde toegang.

De alom erkende oplossing voor het beschermen van bedrijfskritische gegevens en applicaties is sterke authenticatie. Voor kleine en middelgrote bedrijven is het implementeren van beveiligingsoplossingen een flinke uitdaging, omdat ze de middelen missen om hun netwerk volledig te beschermen en daarnaast mogelijk denken dat ze geen interessant doelwit zijn. Uit een onderzoek van de National Cyber Security Alliance blijkt dat 85 procent van bedrijven in het mkb denkt dat ze minder kans lopen om slachtoffer te worden van cybercriminaliteit dan grote ondernemingen². Helaas zijn ook cybercriminelen op de hoogte van het feit dat het midden- en kleinbedrijf niet over geavanceerde beveiliging beschikt, en gebruiken hun systemen steeds vaker om juist daar gevoelige gegevens te stelen.

De hindernissen voor sterke authenticatie uit de weg ruimen

Kleine en middelgrote bedrijven moeten meerdere hindernissen nemen op hun weg naar authenticatie op basis van twee factoren. De drie belangrijkste redenen waarom ze niet overstappen op sterke authenticatie zijn:

- hoge kosten
- ongemak voor gebruikers
- uitrol en beheer zijn complex

Kosten

Bedrijven in het mkb noemen vaak de kosten van de bestaande oplossingen als de grootste hindernis voor het overstappen op sterke authenticatie. Voor het uitrollen van een oplossing voor eenmalige wachtwoorden zijn investeringen in hardware zoals apparatuur voor eindgebruikers en een verificatieserver vereist. En daar komen nog de kosten voor het onderhoud bij, zoals ondersteuning en software-updates. Omdat ze maar over een beperkt IT-budget beschikken, houden deze bedrijven het bij een eenvoudige login met gebruikersnaam en wachtwoord.

Ongemak voor gebruikers

Bij het uitrollen van sterke authenticatie is het gebruiksgemak een belangrijke overweging. Organisaties moeten overwegen of aanvullende beveiliging de productiviteit van hun werknemers vermindert en of ze weerstand zullen ondervinden van gebruikers die niet willen overgaan op een nieuwe technologie. Dit kan ook de totale kosten van de oplossing hoger maken, doordat de helpdesk vaker wordt gebeld door gebruikers die ondersteuning nodig hebben.

Uitrol en beheer

De initiële uitrol van een oplossing voor sterke authenticatie kan een behoorlijke investering in middelen vereisen van de IT-afdeling. Daarnaast moet het doorlopende beheer van de oplossing worden overwogen. Dit kan taken omvatten zoals het toevoegen en verwijderen van gebruikers en het distribueren van hardware en software. De IT-middelen van het mkb zijn beperkt. De tijd en het aantal mensen dat nodig is voor een goed beheer van de sterke verificatiestrategie kan het de toch al drukbezette medewerkers nog moeilijker maken.

1 Forrester Research, "Best Practices: Implementing Strong Authentication in Your Enterprise," juli 2009

2 2010 NCSA/Visa Inc. Small Business Study

Sterke authenticatie voor kleine en middelgrote bedrijven

RSA Authentication Manager Express houdt rekening met de kosten, gebruiksvriendelijkheid en beperkingen van het IT-beheer in het mkb, en biedt een oplossing die kosteneffectief en gemakkelijk is zonder compromissen op het gebied van beveiliging. De oplossing is een sterk platform voor authenticatie op basis van meerdere factoren, dat veilige externe authenticatie biedt voor maximaal 2500 gebruikers. RSA Authentication Manager Express werkt met bekende SSL VPN's en webapplicaties waarmee bedrijven in het mkb sterke authenticatie en veilige toegang tot beschermde applicaties en gegevens kunnen uitrollen.

RSA Authentication Manager Express is gebaseerd op RSA's technologie voor op risico gebaseerde authenticatie (Risk-Based Authentication). De kern van de oplossing is de RSA Risk Engine, een geavanceerd systeem dat elke toegangspoging en alle activiteit in real time analyseert, door op tientallen risico-indicatoren te controleren en aan ieder gebruikersverzoek een risiconiveau toe te kennen. RSA Authentication Manager Express houdt rekening met meerdere factoren bij het bepalen van het risiconiveau van ieder toegangsverzoek, zoals:

- informatie die de gebruiker kent, zoals een gebruikersnaam en wachtwoord;
- iets dat de gebruiker heeft, zoals een laptop of een desktop;
- iets dat de gebruiker doet, zoals recente authenticatie en accountactiviteit.

Met de RSA Risk Engine kunnen bedrijven hun eigen, aangepaste beleid instellen aan de hand van een risicodrempel die ze zelf kunnen bepalen, van hoog tot laag.

RSA Authentication Manager Express maakt het ook mogelijk om een risiconiveau in te stellen per gebruikersgroep. Een organisatie kan per gebruikersprofiel een apart verificatiebeleid instellen, afhankelijk van de relatie van de gebruikers binnen dat profiel met de organisatie. Zo kan de risicodrempel van toegang door werknemers hoger worden ingesteld dan de risicodrempel van de toegang door een klant of partner. Wanneer de RSA Risk Engine vaststelt dat het risiconiveau van een toegangsverzoek lager is dan de toegestane drempel, wordt de gebruiker zonder omwegen toegelaten. Als de RSA Risk Engine echter bepaalt dat een toegangsverzoek boven de drempel ligt, kan de gebruiker om meer bewijs van identiteit worden gevraagd.

Apparaat profiel: iets dat de gebruiker heeft

De RSA Risk Engine onderzoekt informatie over elk toegangsverzoek van een gebruiker in twee hoofdcategorieën: apparaatprofiel en gedragsprofiel. Het eerste klas, apparaatprofiel, maakt de authenticatie van de meerderheid van de gebruikers mogelijk door een analyse van het apparaatprofiel van de fysieke laptop of desktop waarmee ze meestal om toegang verzoeken, en door na te gaan of het apparaat eerder aan de gebruiker is gekoppeld. De twee belangrijkste factoren van het apparaatprofiel zijn unieke apparaatidentificatie en statistische apparaatidentificatie.

Unieke apparaatidentificatie helpt bij het identificeren van een gebruiker door twee zaken op het apparaat van de gebruiker te plaatsen, (a) beveiligde *first-party* cookies en (b) gedeelde flash-objecten (ook wel "flash cookies" genoemd). Beveiligde first-party cookies spelen een belangrijke rol bij het identificeren van laptops en pc's. Hierbij wordt een unieke cryptografische identifier op het apparaat van de gebruiker geplaatst, die meestal als eerste identificatiemiddel wordt gebruikt. Flash-cookies worden tegelijk met first-party cookies gebruikt voor extra betrouwbaarheid. RSA Authentication Manager Express gebruikt Flash-cookies om de machine van een gebruiker te 'taggen' op dezelfde manier als first-party cookies informatie opslaan voor later gebruik. Het voordeel van Flash-cookies is dat ze niet zo vaak worden verwijderd als first-party cookies, omdat de meeste gebruikers niet eens weten dat ze bestaan. En zelfs al weten ze dat wel, dan weten ze vaak niet zeker hoe ze de cookies moeten verwijderen.

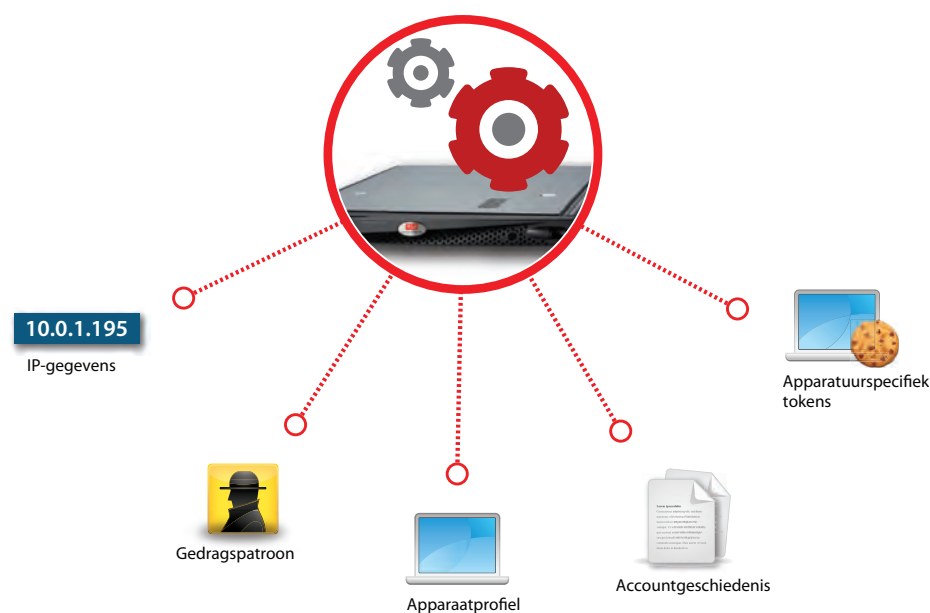
Statistische apparaatidentificatie is een technologie die gebruikmaakt van de kenmerken van een apparaat om een gebruiker statistisch te identificeren en koppelen aan een specifiek apparaat. Statistische apparaatidentificatie wordt ook wel 'forensische analyse' of 'device fingerprinting' genoemd en wordt meestal gebruikt als uitwijkmechanisme wanneer een unieke cryptografische identifier ontbreekt – deze kan tenslotte worden verwijderd van het apparaat.

Elementen die kunnen meetellen in het proces van statistische apparaatidentificatie zijn bijvoorbeeld gegevens uit HTTP-headers en Java™-scripts, versie en patchniveau van het besturingssysteem, schermresolutie, browserversie, gegevens van de gebruikersagent, softwareversies, weergave-eigenschappen (grootte en kleurdiepte), taal, tijdzone, geïnstalleerde browserobjecten, geïnstalleerde software, regio- en taalinstellingen en het IP-adres.

Gedragsprofiel: iets dat de gebruiker doet

Naast apparaatprofiel bekijkt RSA Authentication Manager Express ook het gedrag van een gebruiker voordat zijn of haar toegangsverzoek een risiconiveau krijgt toegewezen. Het gedragsprofiel wordt gebruikt om te bepalen welke aanmeldingen risicovol zijn, door te letten op snelheid, IP-adresgegevens en authenticatie- en accountactiviteit (zoals recente wijzigingen in het gebruikersprofiel of meerdere mislukte verificatiepogingen). Als een gebruiker zich bijvoorbeeld normaal gesproken aanmeldt vanuit een kantoor in New York, en deze keer probeert binnen te komen vanuit een locatie in Moskou, zal het systeem dit beschouwen als ongebruikelijk. Als de gebruiker echter veel onderweg is en zich regelmatig vanaf allerlei locaties ter wereld aanmeldt, wordt een dergelijke situatie niet als ongebruikelijk beoordeeld.

Afbeelding 1: de RSA Risk Engine evalueert tientallen elementen bij het toewijzen van een risiconiveau aan elk gebruikersverzoek



Aanvullende authenticatie voor risicovolle toegangsverzoeken

RSA Authentication Manager Express kan aanvullende verificatiemethoden activeren wanneer een toegangsverzoek de toegestane drempel overschrijdt die door een organisatie is vastgesteld. Dit komt met name voor wanneer een externe gebruiker zich aanmeldt met een apparaat dat niet wordt herkend en nog niet eerder toegang tot het netwerk heeft gehad. RSA Authentication Manager Express biedt organisaties vervolgens twee methoden voor aanvullende authenticatie: out-of-band sms en beveiligingsvragen.

Out-of-band sms

De out-of-band sms-methode wordt gebruikt wanneer het risiconiveau van het toegangsverzoek hoog is. In dat geval vereist RSA Authentication Manager Express van de gebruiker dat deze een aanvullend bewijs van diens identiteit levert door middel van een eenvoudig proces.

Ten eerste wordt de gebruiker gevraagd de geheime pincode in te voeren die hij bij zijn registratie heeft opgegeven. Vervolgens stuurt het systeem een geautomatiseerd sms-bericht naar de mobiele telefoon die de gebruiker heeft geregistreerd. De sms bevat een unieke code van 8 cijfers die de gebruiker in de webbrowser moet invoeren. Zodra het systeem de code heeft geverifieerd krijgt de gebruiker toegang. RSA Authentication Manager Express ondersteunt ook het per e-mail versturen van een eenmalig wachtwoord.

De belangrijkste voordelen van de out-of-band sms-authenticatie zijn dat die met elke mobiele telefoon werkt en de gebruiker geen hardware hoeft aan te schaffen of software hoeft te installeren.

Beveiligingsvragen

Beveiligingsvragen zijn vragen die een gebruiker in een lijst selecteert en beantwoordt tijdens het eerste registratieproces, dus wanneer een organisatie sterke authenticatie uitrolt voor haar gebruikers. De gebruiker hoeft tijdens het verificatieproces maar een deel van zijn vragen te beantwoorden, om het risico te verminderen dat een onbevoegde over

alle geheime vragen en antwoorden van een gebruiker kan beschikken. Organisaties kunnen een eigen reeks vragen gebruiken of de ingebouwde standaardvragen van RSA Authentication Manager Express.

Uitrol en beheer

RSA Authentication Manager Express is een plug-and-play apparaat en ondersteunt standaard alle bekende SSL VPN's en webservers. Dankzij RSA Quick Setup is de server met een paar eenvoudige stappen ingesteld en actief.

De uitrol voor eindgebruikers is al net zo eenvoudig. RSA Authentication Manager Express kan direct worden aangesloten op een bestaande directoryserver en gebruikers worden automatisch door het registratieproces geleid wanneer ze zich de volgende keer aanmelden. Doordat dit een volledig geautomatiseerd proces is, kunnen beheerders zich in de tussentijd wijden aan het instellen van andere verificatiemethoden.

Belangrijkste voordelen

RSA Authentication Manager Express is bedoeld voor kleine en middelgrote bedrijven die behoefte hebben aan sterke authenticatie.

Kosteneffectief. RSA Authentication Manager Express is ontworpen – en geprijsd – voor organisaties met maximaal 25000 gebruikers.

Gebruiksvriendelijkheid. Met RSA Authentication Manager Express kunnen de meeste gebruikers zich aanmelden met hun normale gebruikersnaam en wachtwoord. In deze gevallen is de multifactor-authenticatie transparant voor de gebruiker, omdat de RSA Risk Engine op de achtergrond actief is. De gebruiker krijgt alleen te maken met uitgebreidere authenticatie wanneer zijn toegangsverzoek wordt gezien als risicovol door de RSA Risk Engine.

Gemakkelijk uit te rollen en beheren. RSA Authentication Manager Express wordt geleverd op een plug-and-play apparaat en ondersteunt standaard alle bekende SSL VPN's en webservers. Bovendien is het registratieproces volledig geautomatiseerd, waardoor beheerders minder tijd kwijt zijn aan het toevoegen en verwijderen van gebruikers.

Bewezen technologie. RSA Authentication Manager Express past dezelfde op risico gebaseerde verificatietechnologie toe die al in gebruik is bij ruim 8000 organisaties in vele sectoren, zoals financiële dienstverlening, gezondheidszorg, verzekeringen, de retailbranche en de overheid. Op dit moment wordt deze technologie gebruikt om de identiteit van meer dan 250 miljoen gebruikers te beschermen en ze toegang te bieden tot verschillende applicaties en systemen, zoals websites, portals en SSL VPN-applicaties.

Conclusie

Dankzij RSA Authentication Manager Express kunnen kleine en middelgrote bedrijven overstappen op sterke authenticatie, die kosteneffectief is en gebruiksvriendelijk voor zowel eindgebruikers als IT-beheerders. Met RSA Authentication Manager Express kunnen bedrijven in het mkb ongeautoriseerde toegang voorkomen, het risico van gegevensdiefstal verminderen, voldoen aan compliancevereisten op een manier die binnen hun budget past, en met vertrouwen toegang bieden aan nieuwe externe gebruikers.

De mythes over sterke authenticatie ontkracht

Mythe	Realiteit
In mijn bedrijf worden sterke wachtwoorden gebruikt en de werknemers moeten die regelmatig wijzigen. Daardoor loop ik minder risico.	Sterke wachtwoorden met cijfers, hoofdletters of speciale tekens zijn misschien moeilijker te raden voor een hacker, maar ook lastiger te onthouden voor de werknemers. Dat betekent dat ze hun wachtwoorden gaan opschrijven, of iets anders doen waardoor het risico juist groter wordt. Echte sterke authenticatie vereist meer dan een factor en meer dan alleen een wachtwoord.
Mijn bedrijf kan de kosten voor sterke authenticatie niet opbrengen.	Sterke authenticatie kan zeer kosteneffectief zijn – en niet alleen voor grote ondernemingen. RSA Authentication Manager Express is bijvoorbeeld speciaal gebouwd – en geprijsd – voor bedrijven met weinig gebruikers en een beperkt IT-budget.
De kosten van sterke authenticatie zijn hoger dan de baten.	De kosten van sterke authenticatie zijn veel lager dan de kosten die uw organisatie moet betalen wanneer er gegevens worden gestolen of wanneer u een boete krijgt voor non-compliance. Daarnaast kan sterke authenticatie helpen bij het creëren van zakelijke kansen die nieuwe inkomsten genereren en bedrijfsprocessen stroomlijnen. Daarbij vergeleken stellen de kosten van beveiliging niet zoveel voor.
Alleen grote ondernemingen en overheidsinstellingen hebben te maken met cybercriminaliteit.	Integendeel. Cybercriminelen richten zich juist op het mkb, omdat die bedrijven vaak over slechts beperkte veiligheidsmaatregelen beschikken, waardoor ze veel kwetsbaarder zijn.

Over RSA

RSA, de beveiligingsdivisie van EMC, is de belangrijkste aanbieder van beveiligings-, risico- en compliance-oplossingen, waarmee toonaangevende organisaties over de hele wereld de meest ingewikkelde en gevoelige beveiligingskwesaties kunnen oplossen. Daarbij gaat het om het beheren van bedrijfsrisico's, het bewaken en beveiligen van mobiele toegang en samenwerking, het aantonen van compliance en het beveiligen van virtuele en cloudomgevingen.

RSA combineert bedrijfskritieke controles, zoals identiteitsverificatie, beveiliging tegen gegevensverlies, versleuteling, tokenisatie, fraudebeveiliging en SIEM, met toonaangevende eCRG-oplossingen en consultancy om voor vertrouwen en zichtbaarheid te zorgen in verband met de identiteit van miljoenen gebruikers, de transacties die ze uitvoeren en de gegevens die gegenereerd worden.

RSA, het RSA-logo, EMC², EMC en Where Information Lives zijn geregistreerde handelsmerken of handelsmerken van EMC Corporation in de Verenigde Staten en andere landen. Alle andere genoemde handelsmerken zijn eigendom van de respectieve houders. ©2011 EMC Corporation. Alle rechten voorbehouden. Gepubliceerd in de Verenigde Staten van Amerika.

AMX SB 0111

www.rsa.com

