RISIKOBASIERTE AUTHENTIFIZIERUNG

RSA Authentication Manager 8.0

AUF EINEN BLICK

- Optionale Lizenzierungsfunktion von RSA Authentication Manager 8.0
- Bewährte Mehrfaktor-Authentifizierungstechnologie für zahlreiche webbasierte Applikationen
- Authentifizierung auf der Basis einer transparenten Analyse von Client-Geräten und Endanwenderverhalten
- Kostengünstige und benutzerfreundliche Authentifizierung für Endanwender und IT-Administratoren
- Risikobasierte Authentifizierung und On-Demand-Authentifizierung in nur einer Lizenz

Moderne Unternehmen stehen zahlreichen Herausforderungen einer zunehmend komplexen IT-Umgebung gegenüber: Anwender sind äußerst verschieden und arbeiten oft mobil, IT-Budgets werden immer kleiner, und die Zahl der Bedrohungen nimmt zu. Unternehmen verwalten immer mehr Informationen online und gewähren den Zugriff auf Ressourcen per Remoteverbindung. Für den entsprechenden Schutz dieser Daten ist eine Authentifizierungslösung gefragt, die Sicherheit, Anwenderfreundlichkeit und den Return on Investment ausgewogen handhabt.

INTELLIGENTE MEHRFAKTOR-AUTHENTIFIZIERUNG

RSA® Authentication Manager 8.0 ermöglicht die risikobasierte Authentifizierung (RBA). Sie ist optional lizenzierbar und erhöht die Sicherheit auf transparente Weise. Die Lösung für die Mehrfaktor-Authentifizierung erhöht die Sicherheit herkömmlicher passwortbasierter Systeme durch die Zuweisung einer Risikostufe zu jeder Anmeldeanfrage. Die ausgereifte Risk Engine bewertet jeden Anmeldeversuch und die Anwenderaktivität in Echtzeit, indem Hunderte Risikoindikatoren verfolgt werden. Auf dieser Basis wird das Risiko jeder Zugriffsanfrage bewertet, darunter:

- Etwas, das der Anwender weiß, z. B. einen bestehenden Benutzernamen oder ein Passwort
- Etwas, das der Anwender besitzt, z. B. ein Notebook, einen Desktop-PC oder ein mobiles Gerät
- Etwas, das der Anwender tut, z. B. aktuelle Kontoaktivitäten

Die Risk Engine bewertet jede Authentifizierungsanfrage in Echtzeit und greift dabei auf das Wissen über das Client-Gerät und die Analyse des Anwenderverhaltens zurück.

RISK ENGINE

RSA zählt zu den führenden Anbietern von Lösungen für die risikobasierte Authentifizierung. Die Risk Engine von RSA Adaptive Authentication schützt bereits heute mehrere Millionen Online-Identitäten. Die Risk Engine von RSA Authentication Manager ist keinesfalls ein statisches regelbasiertes System. Sie passt das Risikomodell dynamisch mit neuen Informationen an. Das geschieht mittels einer Echtzeitanalyse von Geräten und Anwenderverhalten. Die risikobasierte Authentifizierung ist äußerst benutzerfreundlich, da die Anmeldung nach wie vor über das vertraute Verfahren mit Benutzername und Passwort erfolgt.

GERÄTE-PROFILING

Die Risk Engine stellt zahlreiche einzigartige Geräteeigenschaften zusammen und bewertet diese. So wird der PC, das Notebook oder das mobile Gerät des Anwenders im Hintergrund untersucht – und zwar dynamisch bei jedem einzelnen Authentifizierungsversuch. Basierend auf dieser Analyse bestimmt die RSA Risk Engine, ob es sich um ein vertrauenswürdiges Gerät handelt, das bereits zuvor vom Kontoinhaber verwendet wurde. Ist das der Fall, wird der Anwender mit einem gültigen Benutzernamen und einem Passwort authentifiziert. Wird das Gerät jedoch nicht erkannt, wird ein zusätzlicher Identitätsnachweis vom Anwender gefordert. Durch die Geräteanalyse wird das Gerät des Endanwenders zu einem zusätzlichen vertrauenswürdigen Authentifizierungsfaktor. Dabei müssen keine statischen Zugangsdaten bereitgestellt und keine weitere Software installiert werden.

VERHALTENSPROFILE

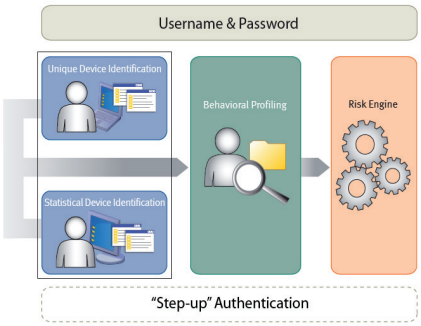
Bei der Verhaltensanalyse werden Verhaltensmuster, Authentifizierungs- und Kontoaktivitäten von Benutzern und andere Faktoren zur Bewertung des Gesamtrisikos jedes Authentifizierungsversuchs herangezogen. Das Verhaltensrisiko wird bewertet, indem die aktuelle Authentifizierungsanfrage mit der Authentifizierungshistorie des Anwenders, dem bekannten Verhalten anderer Anwender und typischen Anzeichen von Authentifizierungsversuchen durch nicht authentifizierte Anwender verglichen wird. Wird das Risiko als gering eingestuft, wird das Anwenderverhalten zu einem zusätzlichen Authentifizierungsfaktor, der die Identität des Kontoinhabers im Hintergrund bestimmt.

BESTÄTIGUNG VON IDENTITÄTEN

Anwender mit geringem Risiko werden auf transparente Weise authentifiziert. Anwender mit hohem Risiko hingegen werden u. U. dazu aufgefordert, einen zusätzlichen Identitätsnachweis zu erbringen.

- On-Demand-Authentifizierung: Der Anwender muss einen einmalig gültigen Passcode richtig eingeben, der über eine Out-of-Band-Authentifizierung per SMS oder E-Mail an eine zuvor festgelegte Nummer eines mobilen Geräts übermittelt wird.
- Persönliche Fragen: Der Anwender muss eine oder mehrere zuvor festgelegte Sicherheitsfragen richtig beantworten.

STARKE, KOSTENGÜNSTIGE AUTHENTIFIZIERUNG



Die risikobasierte Authentifizierung von RSA bietet eine leistungsstarke Mehrfaktor-Authentifizierung. Die Abbildung links zeigt die Bestandteile der risikobasierten Authentifizierung: etwas, das der Anwender kennt (Benutzername und Passwort), etwas, das der Anwender besitzt (Geräteidentifizierung) und etwas, das der Anwender tut (Geräte-Profiling). Durch die risikobasierte Authentifizierung können Unternehmen den zeit- und standortunabhängigen Zugriff zuverlässig auf Mitarbeiter mit Remotezugriff, Partner, Subunternehmer und Kunden ausweiten. Die Lösung ist äußerst flexibel. So lässt sich die starke Authentifizierung an die Ressourcen, Risikotoleranz und Anwenderprofile eines Unternehmens anpassen. Die risikobasierte Authentifizierung kann sowohl als Mehrfaktor-Authentifizierungslösung im Standalone-Betrieb als auch mit RSA SecurID® eingesetzt werden. Ist Letzteres der Fall, nutzt die Risk Engine den RSA SecurID-Token-Code als zusätzliche Sicherheitsebene. RSA SecurID kann jedoch nicht dazu verwendet werden, nach der Risikoanalyse einen zusätzlichen Identitätsnachweis zu erbringen.

TECHNISCHE DATEN

- Unbefristete Lizenz mit jährlicher Wartungspflicht (unabhängig von der RSA SecurCare-Wartung)
- Gemeinsame Lizenz für risikobasierte Authentifizierung und On-Demand-Authentifizierung
- Unterstützung für eine beliebige Anzahl von Anwendern zwischen 5 und 20.000
- Kann mit der Base Edition und der Enterprise Edition von RSA Authentication Manager 8.0 eingesetzt werden
- Kompatibel zu RSA SecurID und RADIUS

KONTAKT

Weitere Informationen darüber, wie Sie mithilfe von Produkten, Services und Lösungen von EMC Ihre Unternehmens- und IT-Herausforderungen angehen können, erhalten Sie bei Ihrem zuständigen Kundenbetreuer oder autorisierten Vertragshändler. Alternativ besuchen Sie uns im Internet unter www.emc.com/rsa.

www.emc.com/rsa

RSA EMC²