RSA SECURID® ACCESS

SICHERHEIT UND GELASSENHEIT BEI EINER BETRIEBSUNTERBRECHUNG

AUF EINEN BLICK

- Flexible Erweiterung Ihrer Bereitstellung von RSA SecurID Access, um Nutzer bei einer Betriebsunterbrechung zu unterstützen
- Unterstützt Nutzer mit „Zero Footprint"-On-Demand-Authentifikatoren
- Jederzeit selbst aktivierbar
- Ideales Tool für Business Continuity und Planungsprozesse bei Pandemien

RSA SecurID Access bietet eine Lösung für die Aufrechterhaltung einer konsistenten Multi-Faktor-Authentifizierungs-Policy während eines geschäftlichen Notfalls, wenn eine große Anzahl von Nutzern für einen bestimmten Zeitraum aus der Ferne arbeiten muss. RSA SecurID Access erhöht die Sicherheit Ihres Unternehmens, indem es sicherstellt, dass unabhängig vom Zustand Ihres Unternehmens die Nutzeridentitäten sicher überprüft werden und der Zugriff auf kritische Anwendungen und Daten intakt bleibt. Die Lösung ist ein wichtiger Bestandteil eines Business Continuity- oder Pandemieplans.

In vielen Unternehmen verwenden häufig nur solche Nutzer Multi-Faktor-Authentifizierung, die ständig außerhalb der Firewall arbeiten. Benutzer innerhalb der Firewall haben möglicherweise keine Token. Für den Fall, dass ein Nutzer Remotezugriff benötigt, gibt die IT einfach einen Authentifikator an die Person aus. Das Problem besteht darin, dass dieser Prozess im Fall einer Betriebsunterbrechung nicht skalierbar ist. In einem solchen Szenario kann es sein, dass viele Benutzer, oft unerwartet, remote arbeiten müssen. Dies führt zu einer „Krise in der Krise", da IT-Mitarbeiter, die es möglicherweise selbst nicht ins Büro schaffen, sich nun darum kümmern müssen, diese Nutzer zu unterstützen. Bei einer beträchtlichen Anzahl von Nutzern in der Organisation, die keine Authentifikatoren haben, deaktiviert die IT-Abteilung oft vorübergehend die Zwei-Faktor-Authentifizierung, um diesen Nutzern den Zugriff zu ermöglichen. Auf diese Weise geht das Unternehmen jedoch unannehmbare Risiken ein.

SCHUTZ DER DATEN UND SICHERE ÜBERPRÜFUNG DER NUTZERIDENTITÄTEN WÄHREND EINER UNTERBRECHUNG

Es gibt zwei Möglichkeiten, dieses Problem zu lösen. Die erste Möglichkeit besteht darin, jeden Nutzer zu verpflichten, die Multi-Faktor-Authentifizierung zu verwenden. Dies ist eine sinnvolle Lösung für Unternehmen, die über mobile Mitarbeiter verfügen. Die andere Möglichkeit, die Business-Continuity-Option, bietet eine flexible Methode, um die Anzahl der Nutzer in einem Unternehmen zu erweitern, ohne das Budget für die Multi-Faktor-Authentifizierung zu erhöhen.

TECHNISCHE DATEN

- Verfügbar für eine feste 3-jährige Laufzeit
- Bis zu sechs Aktivierungen während der Laufzeit des Vertrags
- Jede Aktivierung ist 60 Tage gültig
- Unterstützung für eine beliebige Anzahl von Benutzern von 5 bis über 25.000
- Funktioniert mit allen drei Editionen von RSA SecurID Access – Base, Enterprise und Premium

SO FUNKTIONIERT DIE LÖSUNG

Bei der Business-Continuity-Option handelt es sich um eine Lizenzierungsfunktion, die optional mit RSA SecurID Access verfügbar ist. Sobald sie zu der Lizenzierungsseite hinzugefügt wurde, kann ein Administrator mit den erforderlichen Rechten die Funktion bei Bedarf einfach anzeigen, auswählen und aktivieren. Die Aktivierung „entsperrt" die entsprechende Anzahl von Serverplätzen und On-Demand-Authentifikatoren, die dann für alle Remotenutzer bereitgestellt werden können, die Zugriff benötigen. On-Demand-Authentifikatoren stellen einmalige Passwörter per SMS (Short Message Service) oder E-Mail bereit. Es ist kein Hardware-Authentifikator erforderlich und es muss keine Software auf dem Mobiltelefon oder PC des Nutzers installiert werden.

Nutzer fordern On-Demand-Authentifikatoren über das Self-Service-Webportal an, das in RSA SecurID Access integriert ist. Das Portal bietet einen bequemen Rund-um-die-Uhr-Service, mit dem Nutzer alle Aspekte ihrer Tokenlebenszyklen verwalten und Zugriff anfordern können. Damit ein Nutzer einen On-Demand-Authentifikator erhält, muss er sich beim Self-Service-Portal anmelden, das dann ein einmaliges Passwort an das vorher festgelegte Ziel des Nutzers sendet, z. B. die Mobiltelefonnummer in der Datenbank. Die Regeln der Multi-Faktor-Authentifizierung werden durchgesetzt: etwas, das Sie kennen (Login/Passwort), und etwas, das Sie haben (Einmalpasswort, das per SMS oder E-Mail an das mobile Gerät geliefert wird).

INFORMATIONEN ÜBER RSA

RSA bietet unternehmensgesteuerte Sicherheitslösungen, mit denen Unternehmen einen einheitlichen Ansatz für das Management digitaler Risiken nutzen können, der auf integrierter Sichtbarkeit, automatisierten Einblicken und koordinierten Aktionen basiert. RSA-Lösungen sollen Unternehmen die effektive Erkennung und Abwehr komplexer Angriffe, die Verwaltung der Benutzerzugriffskontrolle sowie die Verringerung von Geschäftsrisiken, Betrug und Cyberkriminalität ermöglichen. RSA schützt Millionen von Benutzern auf der ganzen Welt und trägt dazu bei, dass mehr als 90 Prozent der Fortune 500-Unternehmen Erfolg haben und sich kontinuierlich an Transformationsänderungen anpassen. Weitere Informationen finden Sie unter rsa.com.

RSA

3/20 Whitepaper, H18197 W342473.