RSA

Whitepaper

Starke Authentifizierung für CJIS-Compliance

RSA-Lösungen für den öffentlichen Sektor

Die Abteilung für Strafjustiz-Informationsdienste (Criminal Justice Information Services, CJIS) ist die größte Abteilung des US-amerikanischen FBI. Die CJIS-Abteilung unterhält eine zentrale, nationale Strafverfolgungsdatenbank, in der hochsensible Kraftfahrzeuge, Strafregister, Waffenregister, Fingerabdrücke und vieles mehr gespeichert werden. Das CJIS-System stattet die Strafverfolgungsbehörden, die nationale Sicherheit und Intelligence-Community-Partner mit den Informationen aus, die diese zum Schutz der USA und ihrer Bürger benötigen. Die CJIS-Richtlinie erfordert eine erweiterte Authentifizierung für alle Benutzer, die von unsicheren Standorten aus auf das CJIS-System zugreifen.

Wer ist davon betroffen?

Jedes Unternehmen, das:

- Zugriff auf das CJIS-Informationssystem hat, einschließlich Bundes-, Landes- und Kommunalbehörden sowie zugelassene private Auftragnehmer

Wie hoch ist Ihr Risiko?

- Sind Sie zur Einhaltung der CJIS-Compliance-Standards verpflichtet?
- Haben Sie Mitarbeiter, die von einem mobilen Datenterminal oder Handheld-Gerät aus auf das CJIS-System zugreifen?
- Wie schützen Sie den Remote-Nutzerzugriff von Notebooks und Mobilgeräten auf CJIS?
- Nutzt Ihr Unternehmen eine starke Authentifizierung, Multifaktor-Authentifizierung (MFA) für den Remote-Nutzerzugriff?
- Können Sie für Ihre Nutzer den Zugriff mit geringsten Rechten sicherstellen, prüfen und steuern?

Erfüllen der CJIS-Zugriffsanforderungen

- FBI: Criminal Justice Information Service (CJIS) Security Policy Version 5.8 (2019)[1] in Abschnitt 5.6.2.2.1
- Durch Compliance mit dieser Richtlinie wird sichergestellt, dass Nutzer ein konsistentes Maß an Datensicherheit und Verschlüsselung aufrechterhalten, um die Strafverfolgungsdatenbank mit sensiblen Informationen im System zu schützen.

RSA SecurID® Suite

Komplettlösung für den Zugriff auf Vor-Ort-, Cloud- und mobile Lösungen

Sichert Identität
Risikobasierte und kontextsensitive Authentifizierung sorgt für Sicherheit und Benutzerfreundlichkeit.

Bietet Optionen
Eine breite Palette von Methoden zur Multifaktor-Authentifizierung (MFA) unterstützt eine immer vielfältigere Gruppe von Nutzern und Anwendungsfällen.

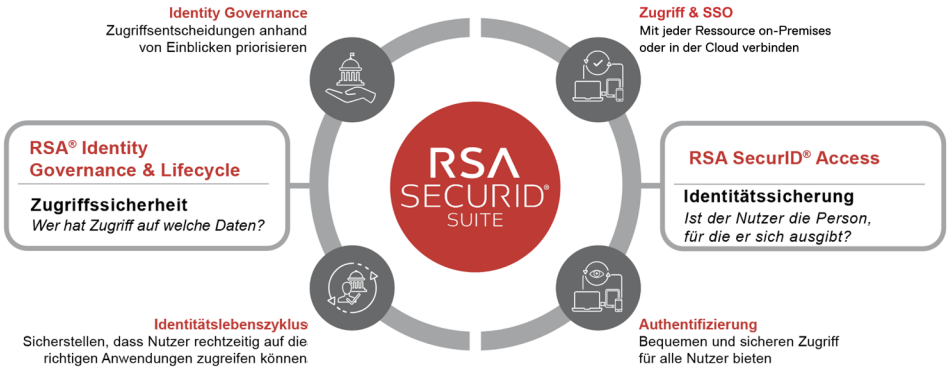
Überbrückt Identitätsinseln
Bietet konsistente Sichtbarkeit und Durchsetzung von Zugriffs- und Authentifizierungsrichtlinien für Cloud-, Vor-Ort- und mobile Anwendungen.

Zugriffssicherheit
Wissen, wer Zugriff hat, ob der Zugriff angemessen ist und ob die Compliance mit Richtlinien und Bestimmungen eingehalten wird.

Zugriffskontrolle mit geringsten Rechten
Management des Zugriffs mit geringsten Rechten und Ansprüchen, sodass Nutzer nur auf das zugreifen können, was sie benötigen.

Besuchen Sie rsa.com/de-de/trysecurid und melden Sie sich für eine kostenlose Testversion an.

- Die CJIS-Sicherheitsrichtlinie erfordert außerdem laut Abschnitt 5.5.2.1, dass Zugriffsberechtigungen kontrolliert und überprüft werden müssen, um sicherzustellen, dass die Zugriffskontrolle mit geringsten Rechten erfolgt.
- Identitäts-Governance und Lebenszyklusmanagement sind nötig, um kontinuierlich zu überwachen, welche Nutzer CJIS-Zugriff haben, um Auditpfade für Änderungen bereitzustellen und um Nutzer zu entfernen, die das Unternehmen verlassen oder keinen Zugriff mehr benötigen.
- Eine fehlende Compliance kann zum Verlust der Zugriffsrechte auf die CJIS-Datenbank, zum Verlust von Arbeitsplätzen und zu einer möglichen strafrechtlichen Verfolgung führen.



Die RSA SecurID Suite bietet Zugriff- und Identitätssicherung für Unternehmen im öffentlichen wie im privaten Sektor. Damit wissen diese genau, wer auf was zugreifen kann und ob der Zugriff angemessen und Compliance-konform ist. Des Weiteren können die Unternehmen darauf vertrauen, dass Nutzer bei einem Zugriffsversuch die sind, für die sie sich ausgeben.

Die RSA SecurID Suite ist eine Lösung, die die wichtigsten CJIS-Anforderungen an die Zugriffssicherheit unterstützt.

RSA-Lösung für sicheren Zugriff

RSA SecurID Access:

- Bietet die von CJIS geforderte 2FA oder MFA
- Umfasst von CJIS genannte Methoden für „erweiterte Authentifizierung“
- Richtliniengesteuerte und risikobasierte MFA kann für mehrere Anwendungsfälle durchgesetzt werden:
  - Mobile-Push- und Biometrie-Authentifizierungsfunktionen
  - Für Hardware, Software und Mobilgeräte optimierte Authentifikatoren und risikobasierte Authentifizierung
- Gewährleistet sichere Zugangsdaten und Zugriff nur von autorisierten Nutzern

Identitäts- und Zugriffssicherheit für öffentlichen Sektor und Contractors

Bietet
Branchenführende Multifaktor-Authentifizierung

Schützt

- Mehr als 25.000 Unternehmen
- 55 Millionen Nutzer

Erweitert Sicherheit auf alle wichtigen Anwendungsfälle

- Cloud
- Mobil
- BYOD
- Webportale
- Herkömmliche VPNs
- Und vieles mehr ...

Steuert Zugriff

- Basierend auf dem Kontext oder Risiko der Situation
- Automatisierte Zugriffsprüfungen und Anspruchsprüfungen zur Reduzierung von Komplexität und manuellem Aufwand

Weitere Informationen
rsa.com/de-de/accessthesolution

RSA Identity Governance and Lifecycle:

- Management des Zugriffs mit geringsten Rechten auf das CJIS-System
- Bereitstellung und Entfernung des Zugriffs auf Basis von Rollen und Richtlinien sowie Aufrechterhaltung des Auditpfads
- Erzwingung einer angemessenen Trennung von Aufgabenkontrollen

Interoperabilität mit den umfangreichsten Ressourcen zur Unterstützung der Zielsetzung

RSA SecurID Access bietet:

- Marktführende Multifaktor-Authentifizierung mit Authentifikatoren für jeden Anwendungsfall
- Mit getesteter, dokumentierter, zertifizierter und vollständig unterstützter Interoperabilität bei mehr als 500 Technologiepartnern und standardbasierter Interoperabilität mit Tausenden mehr
  – Umfasst die Interoperabilität für NetMotion (eine der gängigsten CJIS-Integrationen)
- Eine vollständige Liste der Integrationen finden Sie unter rsa.com/de-de/partner/rsa-ready-program.

Informationen zur RSA SecurID Suite

Die RSA SecurID® Suite bietet modernen Mitarbeitern einen bequemen und reibungslosen Zugriff auf Ressourcen in digitalen Umgebungen und verhindert gleichzeitig unbefugten Zugriff. Die Suite gehört zum RSA-Portfolio unternehmensgesteuerter Sicherheitslösungen, die einen einheitlichen Ansatz für das Management digitaler Risiken bieten, der auf integrierter Sichtbarkeit, automatisierten Einblicken und koordinierten Maßnahmen basiert. RSA schützt Millionen Nutzer auf der ganzen Welt und trägt dazu bei, dass mehr als 90 % der Fortune 500-Unternehmen Erfolg haben und sich kontinuierlich an Transformationsänderungen anpassen. Weitere Informationen finden Sie unter rsa.com/de-de.

1. https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center