WELCHE AUTHENTIFIZIERUNGSLÖSUNG EIGNET SICH AM BESTEN FÜR MEIN UNTERNEHMEN?

Diese Frage stellen sich regelmäßig viele Unternehmen in aller Welt. Da ständig neue Sicherheitsprodukte angeboten und von den Analysten als „Wunderwaffe“ angepriesen werden, sind auf dem Markt mittlerweile eine Vielzahl von Authentifizierungslösungen verfügbar. Bevor ein Unternehmen endgültig entscheiden kann, welche Authentifizierungslösung am besten geeignet ist, müssen die Authentifizierungsanforderungen der Anwender, die potenziellen Bedrohungen, die Geschäftsziele und die gesetzlichen Vorgaben der jeweiligen Branche bestimmt werden.

RSA hat einen Entscheidungsbaum für die Authentifizierung entwickelt. Dabei handelt es sich um ein umfassendes Tool, mit dem Unternehmen die optimale Authentifizierungslösung für die Anforderungen ihrer Anwender und Geschäftsabläufe verstehen, bewerten und auswählen können. Der Entscheidungsbaum für die Authentifizierung von RSA dient als Grundlage, um die Auswahl möglicher Authentifizierungslösungen anhand von fünf kritischen Faktoren einzugrenzen. In diesem Whitepaper erhalten Sie zunächst einen Überblick über den Entscheidungsbaum für die Authentifizierung. Anschließend werden die fünf kritischen Faktoren bei der Auswahl einer Authentifizierungslösung dargestellt, und Sie erfahren, wie Sie eine geeignete Lösung auswählen, die ein Gleichgewicht zwischen Risiko, Kosten und Anwenderkomfort herstellt.

DIE NOTWENDIGKEIT STARKER AUTHENTIFIZIERUNG

Der Schutz des Datenzugriffs und die Überprüfung der Anwenderidentitäten, die diesen Zugriff anfordern, spielen bei jeder Sicherheitsinitiative eine zentrale Rolle. Ursprünglich diente die Anwenderauthentifizierung hauptsächlich dazu, den Remote-Zugriff auf Unternehmensdaten zu schützen, doch mittlerweile gibt es noch weitere Gründe für den steigenden Bedarf an starker Authentifizierung im gesamten Unternehmen.

Online- und Mobile-Kanäle. Der Zugriff auf Informationen in Echtzeit bietet Vorteile hinsichtlich neuer Geschäftsmöglichkeiten, Kosteneffizienz und Kundenservice. Mehr und mehr Unternehmen erkennen dies und bieten daher in immer größerer Zahl webbasierte Kundenportale und Geschäftsanwendungen, um Ihren Kunden die Möglichkeit zu geben, ihre Accounts rund um die Uhr zu verwalten. Mobile Zugänge – insbesondere über Smartphones – ermöglichen Kunden gleichwertigen Zugang und bieten oft sogar bessere Funktionalitäten durch ihre kundenspezifischen Anwendungen.

Steigender Bedarf an Remote-Zugriff. Durch die globalen Geschäftsabläufe und die Mobilität der Mitarbeiter sind viele Unternehmen gezwungen, jederzeit und überall einen Zugriff einzurichten, um die Produktivität der Mitarbeiter zu gewährleisten.

Zugriffsrechte für neue Anwendergruppen. Subunternehmer, Partner und Lieferanten benötigen einen On-Demand-Zugriff auf unternehmensinterne Informationen wie z.B. Vertriebsplanungen, Wettbewerbsvergleiche, Preislisten, Lagerbestand und Kundendaten.

DER STATUS QUO DER AUTHENTIFIZIERUNG

Trotz der Tatsache, dass eine rein passwortbasierte Authentifizierung nur unzureichende Sicherheit bietet, bleibt die Verwendung eines einzelnen Passworts das häufigste Verfahren zur Überprüfung der Anwenderidentität. Doch diese Methode, die einst als „kostenfrei" betrachtet wurde, verursacht im Laufe der Zeit hohe Verwaltungs- und Supportkosten. Nach Angaben des Help Desk Institute beziehen sich etwa 30 % aller Helpdesk-Anrufe auf das Zurücksetzen eines Passworts und verursachen Kosten in Höhe von $25 bis $50 pro Anruf.

Da laufend neue Authentifizierungslösungen auf dem Markt angeboten werden, stehen Unternehmen vor einer echten Herausforderung, wenn sie eine geeignete Strategie für eine starke Authentifizierung wählen müssen. Der Zugriff auf unternehmensinterne Ressourcen wird immer noch in erster Linie durch Hardware-Authentifizierungskomponenten geschützt. Doch die Mobilität der Mitarbeiter und die Nutzung von Smartphones und Tablet-PCs führen zu einem steigenden Bedarf an Software-Authentifizierungskomponenten. Bei Portalen mit Kundenzugriff werden als Sicherheitsmechanismen meist die risiko-basierte oder wissensbasierte Authentifizierung verwendet, da diese benutzerfreundlich und leicht für eine große Anwenderzahl skalierbar sind.

Angesichts der unzähligen Authentifizierungsprodukte auf dem Markt fällt es den Unternehmen schwer, sich für eine Authentifizierungsstrategie zu entscheiden. Bei vielen Unternehmen kommen mehrere Authentifizierungsoptionen infrage; dabei spielen Auswahlkriterien wie Anwendergruppe, Wert der zu schützenden Informationen, Portabilität und Benutzerfreundlichkeit eine Rolle. RSA hat einen Entscheidungsbaum für die Authentifizierung entwickelt, mit dem Unternehmen auf objektive Weise die verschiedenen Optionen gewichten und mit den Anforderungen ihrer Anwender und Geschäftsabläufe abgleichen können, um die optimale Entscheidung zu treffen.

KRITISCHE FAKTOREN BEI DER ENTWICKLUNG EINER AUTHENTIFIZIERUNGSSTRATEGIE

Bei der Entwicklung einer geeigneten Authentifizierungsstrategie müssen fünf kritische Faktoren beachtet werden:

– Der Wert der zu schützenden Informationen

– Die erforderliche Stärke der Anwenderauthentifizierung

– Die geplante Verwendung

– Die Anforderungen der Endanwender

– Die technische Umgebung

Der Wert der zu schützenden Informationen

Als Erstes müssen der Wert der zu schützenden Informationen und die Kosten von unberechtigten Zugriffen auf diese Informationen berücksichtigt werden. Vertrauliche Geschäftsinformationen, Bankkonto- und Kreditkartendaten, Krankenakten oder personenbezogene Daten (PII) sind Daten mit hohem Wert.

Der unberechtigte Zugriff auf diese Informationen kann kostspielig werden und der Marke und dem Ruf eines Unternehmens schaden. Je höher der Wert der Informationen und je höher das Unternehmensrisiko im Falle unberechtigter Datenzugriffe, desto stärker muss die Authentifizierungslösung zum Schutz dieser Daten sein.

Die erforderliche Stärke der Anwenderauthentifizierung

Anhand der Anwendergruppen und der abgerufenen Informationen können Unternehmen die erforderliche Stufe der Anwenderauthentifizierung bestimmen. Beispiel: Seinen Kunden kann ein Unternehmen nicht einfach eine Authentifizierungslösung aufzwingen, sondern muss bei dieser Anwendergruppe die Benutzerfreundlichkeit und Akzeptanz berücksichtigen. Bei Mitarbeitern und Partnern hingegen hat das Unternehmen eine freiere Auswahl und betrachtet vor allem Aspekte wie Portabilität, Total-Cost-of-Ownership und allgemeine Verwaltung.

Die geplante Verwendung

Bei der Implementierung einer Authentifizierungslösung verfolgen Unternehmen in der Regel mehr als ein Geschäftsziel. Oder anders gesagt: Je nach Art der Anwender und Aktivitäten kann ein Unternehmen entscheiden, dass über die Überprüfung der Anwenderidentität hinaus weitere Authentifizierungsstufen benötigt werden. So könnte z.B. ein Finanzdienstleister, der Betrugsverluste vermeiden möchte, eine Überwachungslösung für Transaktionen einrichten, um Geldtransfers mit hohem Risiko abzusichern. Ein weiteres Beispiel sind die Anwender in einem Unternehmen. Einige arbeiten mit streng vertraulichen Informationen und tauschen diese aus (z.B. Personalabteilung, Lohnbuchhaltung, Finanzabteilung), sodass eine Authentifizierungslösung nötig ist, die Datei- und E-Mail-Verschlüsselung ermöglicht.

Die Anforderungen der Endanwender

Bei der Bereitstellung von Authentifizierungslösungen für Endanwender müssen viele Faktoren berücksichtigt werden, abhängig von der jeweiligen Anwendergruppe. Aus Anwendersicht müssen Unternehmen z.B. die Benutzerfreundlichkeit, die Anwenderakzeptanz und die Art der angeforderten Informationen beachten. Aus Unternehmenssicht spielen Faktoren wie Total-Cost-of-Ownership, Schulungsaufwand, Skalierbarkeit für Endanwender und Mobilität der Lösung eine Rolle.

Die technische Umgebung

Abschließend muss die technische Umgebung, in der die Lösung implementiert wird, berücksichtigt werden, um z.B. die erforderliche Stärke der Authentifizierung zu bestimmen. Beispiel: In einer Umgebung mit stärkerer Desktop-Steuerung und stets aktueller Antiviren-Software sind die Sicherheitsanforderungen nicht so hoch wie in einer weniger zu kontrollierenden Umgebung, in der viele Anwender an Remote-Standorten weltweit auf das Netzwerk zugreifen. Eine weitere technische Einflussgröße bilden die Endanwendergeräte, über die der Zugriff erfolgt. Bei allen Anwendungen mit Mitarbeiter- oder Kundenzugriff gilt, dass die Endanwender die Informationen auf verschiedensten Geräten abrufen, von Laptops und Desktops über Smartphones und Tabelt-PCs bis hin zu Infoterminals. Die Art der Zugriffsgeräte muss beachtet werden, um den Endanwendern die richtigen Formfaktoren für die Authentifizierung bereitzustellen.

Heutzutage geben viele Unternehmen Smartphones aus, um den Zugriff auf Unternehmensmails zu ermöglichen. Dieser verhältnismäßig neue Aspekt der Mobility steigert die Produktivität und Flexibilität der Mitarbeiter. Diese Vorteile, zusammen mit neuen Geräten mit immer mehr Funktionen, verstärken den Trend, Geräte, die für den Endverbraucher entwickelt wurden, auch zu Geschäftszwecken einzusetzen („Consumerization“ der IT). Diese Entwicklung jedoch hält für Unternehmen neue Fragen und Aufgaben bereit.

Wie kann man die Kosten des IT-Supports für die schier explodierende Vielfalt der Geräte kontrollieren, wo zieht man die Grenze für diesen Support und wie kann man den durch Mobility wachsenden Sicherheitsbedrohungen begegnen?

DER ENTSCHEIDUNGSBAUM FÜR DIE AUTHENTIFIZIERUNG

Aufgrund der zahlreichen neuen Authentifizierungsmethoden und -technologien, des steigenden Informationswerts, der neuen Anwendergruppen mit Zugriff auf Netzwerke und Anwendungen, der steigenden Anzahl neuartiger Bedrohungen und der komplexen gesetzlichen Vorschriften sehen sich Unternehmen gezwungen, ihre derzeitige Authentifizierungsstrategie zu überdenken.

Dabei müssen zahlreiche Authentifizierungslösungen bewertet werden, doch diese Aufgabe wird vielen Unternehmen erschwert, da bestimmte Authentifizierungstechnologien auf dem Markt für besonderes Aufsehen sorgen. So erhalten z.B. Biometrielösungen in den Medien eine hohe Aufmerksamkeit, die in keinem Verhältnis zu ihrer tatsächlichen Nutzungsrate auf dem Markt steht. Diese Lösungen erfordern teure und umständliche Lesegeräte, sodass sie für den mobilen oder Remote-Zugriff oder für eine hohe Anwenderzahl ungeeignet sind.

Der Entscheidungsbaum von RSA für die Authentifizierung wurde für Unternehmen entwickelt, die ihre Anwender- und Geschäftsanforderungen auf objektive Weise mit den verfügbaren Authentifizierungstechnologien auf dem Markt abgleichen möchten, um die Entscheidungsfindung zu erleichtern. Da der Markt noch keine Universallösung bietet, die alle Geschäftsanforderungen und den Sicherheitsbedarf aller Anwender und Szenarien abdeckt, können Unternehmen mit dem Entscheidungsbaum von RSA die geeignetste Authentifizierungslösung oder eine Kombination von Lösungen wählen und dabei ein Gleichgewicht zwischen Risiko, Kosten und Anwenderkomfort herstellen.

Nutzen Sie unser interactives Online Tool „RSA Authentication Decision Tree“ unter

http://www.rsa.com/go/authtree/auth/index.html

VERWENDUNG DES ENTSCHEIDUNGSBAUMS FÜR DIE AUTHENTIFIZIERUNG

Mit dem Entscheidungsbaum von RSA für die Authentifizierung werden die folgenden Kriterien untersucht, um die optimale(n) Lösung(en) für ein Unternehmen zu ermitteln:

– Steuerung der Endanwenderumgebung

– Verwendete Zugriffsmethoden

– Bedarf an jederzeitigem, standortunabhängigem Zugriff

– Notwendigkeit von Datenträger-, Datei- oder E-Mail- Verschlüsselung

– Betrugsprävention

Steuerung der Endanwenderumgebung

Die Steuerung der Endanwenderumgebung spielt bei der Bestimmung der geeigneten Authentifizierungsmethode eine zentrale Rolle. Zu den wichtigen Aspekten zählt z.B., ob das Unternehmen selbst Software auf dem Endanwendersystem installieren oder die Betriebssystemplattform für die Aufgaben des Endanwenders vorgeben darf.

Warum ist dies so wichtig? Einfache Aspekte wie z.B. die Auswahlmöglichkeit beim Betriebssystem sind deshalb von Bedeutung, weil nicht alle Authentifizierungslösungen uneingeschränkt mit allen Betriebssystemen kompatibel sind. In der eigenen Umgebung kann ein Unternehmen die Betriebssysteme auf den Anwendergeräten selbst bestimmen. Die Betriebssysteme von externen Anwendern wie Kunden und Partnern können jedoch nicht beeinflusst werden, sodass diese Gruppen möglicherweise andere Authentifizierungsmethoden erfordern.

Verwendete Zugriffsmethoden

Die Zugriffsmethoden müssen bei der Bestimmung der Authentifizierungsstrategie unbedingt berücksichtigt werden. Manche Authentifizierungsmethoden eignen sich nur für den Zugriff auf webbasierte Anwendungen, während andere auch für die Authentifizierung an mehreren, nicht webbasierten Anwendungen genutzt werden können. Daher wirken sich die Anwendergruppen, deren Zugriffsrechte und die geplante Verwendung direkt auf die Auswahl der Authentifizierungsmethode aus.

Bedarf an Zugriff unabhängig von Standort und Gerät

Die globalen Geschäftsabläufe und die zunehmende Mobilität der Mitarbeiter erfordern Zugriff rund um die Uhr, unabhängigt von Standort und Geräten - inklusive Mobile Devices. Für Mitarbeiter und Partner ist diese Möglichkeit Grundvorassetzung für die Produktivität; für Kunden wichtig für deren Zufriedenheit.

Vor allem ist die Möglichkeit zu jeder Zeit von überall sicher auf Informationen zugreifen zu können unabdingbar für den Unternehmensbetrieb.

Dabei müssen folgende Faktoren beachtet werden:

– Müssen Sie einen Anwenderzugriff von wechselnden Remote-Standorten einrichten?

– Müssen Sie einen Anwenderzugriff von unbekannten Systemen wie z.B. Terminals, Hotelsystemen oder gemeinsam genutzten Workstations einrichten?

– Müssen Sie einen Anwenderzugriff von wechselnden Geräten wie z.B. Smartphones oder Tablet-PCs einrichten?

Datenträger-, Datei- oder E-Mail-Verschlüsselung

Bei der Festlegung einer Authentifizierungsstrategie müssen Unternehmen auch weitere Geschäftszwecke berücksichtigen berücksichtigen, die die Authentifizierungsmethode unterstützen soll. Organisationen im Gesundheitswesen müssen z.B. geschützte Patientendaten oder personenbezogene Informationen bei der Übermittlung zwischen Abteilungen und Einrichtungen verschlüsseln, um die HIPAA-Vorschriften zu erfüllen. In diesem Fall müssen möglicherweise einzelne Anwender mit Zugriffsrechten auf diese speziellen Datentypen eingerichtet werden, damit die Daten nur auf vertrauenswürdigen Systemen aufgerufen werden können.

Betrugsprävention

Manche Authentifizierungsmethoden sind erforderlich, um die Transaktionen und Aktivitäten eines Anwenders nach der anfänglichen Authentifizierung bei der Anmeldung zu überwachen und dadurch Betrug zu vermeiden. Obwohl dies in der Regel die Anwendungen von Finanzdienstleistern betrifft, werden auch in anderen Branchen immer häufiger gezielte Angriffe gestartet (z.B. durch Phishing und Malware), durch die Betrüger nur ein Ziel verfolgen, nämlich persönliche und unternehmensrelevante Daten zu sammeln, um diese am Schwarzmarkt zu verkaufen.

Anzahl der Nutzer

Die Anzahl der zu schützenden Nutzer ist wichtig, da der Kostenfaktor, insbesondere für kleine und mittlere Unternehmen, von großer Bedeutung ist. Etliche Authentifizierungslösungen wurden speziel für entweder sehr kleine oder sehr große Anwenderzahlen entwickelt und bepreist.

VIELFÄLTIGE AUTHENTIFIZIERUNGSMÖGLICHKEITEN

Passwörter

Passwörter ermöglichen die Überprüfung von Anwenderidentitäten anhand eines einzigen Faktors. Diese Methode scheint zunächst kostenfrei, kann aber im Laufe der Zeit hohe Verwaltungs- und Supportkosten verursachen (z.B. für das Zurücksetzen von Passwörtern). Passwörter bieten nur geringe Sicherheit, sind anfällig gegen Hackerangriffe, und es besteht die Gefahr der gemeinsamen Nutzung durch mehrere Personen.

Wissensbasierte Authentifizierung

Wissensbasierte Authentifizierung ist eine Methode, bei der eine Person auf Basis von persönlichen Informationen authentifiziert wird. Dazu wird ein Echtzeit-Prozess mit interaktiven Fragen und Antworten verwendet. Die Fragen an einen Anwender werden nach dem Zufallsprinzip aus öffentlichen Datenbanksätzen zusammengestellt, sodass sie dem Anwender nicht vorab bekannt sind oder schon einmal gestellt wurden.

Risikobasierte Authentifizierung

Bei der risikobasierten Authentifizierung handelt es sich um ein System, mit dem eine Reihe von Risikoindikatoren im Hintergrund gemessen werden, um Anwenderidentitäten zu überprüfen bzw. Online-Identitäten zu authentifizieren. Zu diesen Indikatoren können z.B. bestimmte Gerätemerkmale, Profile des Anwenderverhaltens und die IP-Geoposition zählen. Je höher die Risikostufe, desto höher die Wahrscheinlichkeit, dass eine Identität oder Aktion zu betrügerischen Absichten dient. Sobald die Risk-Engine die Authentifizierungsanfrage als außerhalb der festgelegten Policies bewertet, erfolgt ein weiterer Authentifizierungsschritt. In dieser nächsten Stufe kann der Anwender seine Identität belegen, indem er z.B. persönliche Fragen beantwortet oder sich mit einem Code authentifiziert, den er via SMS oder E-Mail erhalten hat.

Authentifizierung mit einmalig gültigem Passwort

Die Authentifizierung mit einmalig gültigem Passwort (OTP) stellt eine führende Zwei-Faktor-Authentifizierungslösung dar und basiert auf etwas, das der Anwender weiß (eine PIN oder ein Passwort), und auf etwas, das der Anwender besitzt (eine Authentifizierungskomponente). Die Authentifizierungskomponente generiert alle 60 Sekunden einen neuen, einmalig gültigen Code, sodass nur der echte Anwender den richtigen Code zu einem bestimmten Zeitpunkt eingeben kann. Für den Zugriff auf Informationen oder Ressourcen, die durch einmalig gültige Passwörter geschützt sind, kombiniert der Anwender einfach seine geheime PIN mit dem Token-Code, den die Authentifizierungskomponente zu genau diesem Zeitpunkt anzeigt. Diese Methode liefert ein eindeutiges, einmalig gültiges Passwort für die zuverlässige Überprüfung der Anwenderidentität. Einmalig gültige Passwörter sind mit verschiedenen Formfaktoren erhältlich, darunter:

- Hardware-Token: Traditionelle Hardware-Token (auch als „Key Fobs“ bezeichnet) sind tragbare Geräte, die sich am Schlüsselbund befestigen lassen, und eignen sich für Anwender, die eine greifbare Lösung bevorzugen oder von mehreren Standorten aus auf das Internet zugreifen.
- Software-Token (für PCs, USB-Laufwerke oder mobile Geräte): Software-Token werden in der Regel als Anwendung oder Symbolleiste bereitgestellt, die auf sichere Weise auf dem Desktop, Laptop, Tablet-PC oder Smartphone des Anwenders angezeigt wird.
- On-Demand: On-Demand-Authentifizierung bedeutet die Bereitstellung eines eindeutigen Codes „auf Anfrage“ per SMS (Textnachricht) auf das Mobilgerät oder an die registrierte E-Mail-Adresse eines Anwenders. Diesen eindeutigen Code gibt der Anwender zusammen mit seiner PIN ein, um auf das Unternehmensnetzwerk oder eine Online-Anwendung zuzugreifen.

Digitale Zertifikate

Ein digitales Zertifikat ist ein einzigartiges Dokument, dessen Informationen die an das Zertifikat gebundene Person oder Gerät indentifiziert. Das digitale Zertifikat kann auf einem Desktop, einer Smart Card oder einem USB aufbewahrt werden. Für eine stärkere Zwei-Faktor-Authentifizierung, kann das digitale Zertifikat auf einer Smart Card oder einem USB anfangs gesperrt sein und erst nach Eingabe einer PIN genutzt werden. Digitale Zertifikate können zur Authentifizierung an Netzwerken oder Anwendungen verwendet werden. Über die Verwendung als Authentifizierungslösung hinaus, können digitale Zertifikate für digitale Signaturen und E-Mail-Verschlüsselung verwendet werden.

Durch die Benutzung eines Hybrid-Token können digitale Zertifikate auch mit OTP-Lösungen kombiniert werden. In diesem Fall speichert der Hybrid-Token mehrere Credentials und erhöht so die Benutzerfreundlichkeit. Ein häufiger Anwendungsfall für eine Kombination aus Zertifikat und OTP ist das Entsperren einer Festplatten-Verschlüsselung durch das Zertifikat, gefolgt von der Authentifizierung an einem VPN mit einem Einmal-Passwort.

ANALYSE DER AUTHENTIFIZIERUNGSMERKMALE

Nachdem ein Unternehmen die Anforderungen seiner Geschäftsabläufe und Anwender bestimmt hat, muss bei der Auswahl der geeigneten Authentifizierungsstrategie aus den verfügbaren Optionen vor allem ein Kompromiss zwischen verschiedenen Variablen gefunden werden:

– Grad der Sicherheit

– Typische Verwendung

– Anforderungen auf Client-Seite

– Portabilität

– Mehrere Einsatzzwecke

– Benutzerfreundlichkeit

– Bereitstellungsanforderungen

– Systemvoraussetzungen

– Kosten

Mithilfe des Entscheidungsbaums für die Authentifizierung von RSA können Unternehmen vergleichen, welche Authentifizierungsmethoden für ihre Anforderungen geeignet sind. Durch dieses einfache Tool sind Unternehmen in der Lage, die führenden Authentifizierungslösungen objektiv zu bewerten.

Obwohl die Kosten eine maßgebliche Rolle spielen, müssen Unternehmen bei der Bestimmung einer geeigneten Lösung für ihre Anforderungen noch eine Reihe weiterer Faktoren berücksichtigen. Viel zu oft werden nur die Anschaffungskosten betrachtet, doch allein das Beispiel der rein passwortbasierten Authentifizierung zeigt, dass nicht nur diesem Aspekt hohe Priorität beigemessen werden darf. Passwörter sind zwar bei der Anschaffung „kostenfrei“, erweisen sich jedoch später bei Verwaltung und Support als überraschend kostspielig.

RSA-LÖSUNGEN

RSA bietet seit über 20 Jahren starke Zwei-Faktor- Authentifizierungslösungen für Unternehmen jeder Größe an. Durch die breite Palette an RSA-Lösungen können Unternehmen eine starke Authentifizierung gewährleisten und dabei ein Gleichgewicht zwischen Risiko, Kosten und Anwenderkomfort herstellen.

RSA SecurID® Authentifizierung

Die RSA SecurID®-Technologie mit einmalig gültigen Passwörtern stellt eine führende Zwei-Faktor- Authentifizierungslösung dar und basiert auf etwas, das der Anwender weiß (eine PIN oder ein Passwort), und auf etwas, das der Anwender besitzt (eine Authentifizierungskomponente). Die Authentifizierungskomponente generiert alle 60 Sekunden einen neuen, einmalig gültigen Passwortcode, sodass nur der echte Anwender den richtigen Token-Code zu einem bestimmten Zeitpunkt eingeben kann. Für den Zugriff auf Ressourcen, die durch das RSA SecurID-System geschützt sind, kombiniert der Anwender einfach seine geheime PIN mit dem Token-Code, den die Authentifizierungskomponente zu genau diesem Zeitpunkt anzeigt. Diese Methode liefert ein eindeutiges, einmalig gültiges Passwort für die zuverlässige Überprüfung der Anwenderidentität.

RSA SecurID ist in den folgenden Formfaktoren verfügbar, um den Anforderungen aller Unternehmen und Anwender gerecht zu werden:

Hardware-Token

Traditionelle Hardware-Token (auch als „Key Fob“ bezeichnet) sind so klein, dass sie sich am Schlüsselbund befestigen lassen, und eignen sich daher für Anwender, die eine greifbare Lösung bevorzugen oder von mehreren Standorten aus auf das Internet zugreifen.

Hybrid-Token mit digitalen Zertifikaten

Der RSA SecurID 800 ist ein Hybrid-Token, der in einem handlichen USB-Formfaktor die einfache Anwendung und Portabilität der RSA SecurID Authentifizierung mit der Flexibilität und Leistung einer Smart Card vereint. Der 800er unterstützt standardkonform digitale Zertifikate zur Festplatten- und Dateiverschlüsselung, zur Authentifizierung und für Signatur- und andere Anwendungen. Darüber hinaus stärkt er die einfache Authentifizierung durch Passwörter indem die Domänen-Zugangsdaten des Anwenders auf einem geärteten Sicherheitsgerät abgespeichert sind. Indem mehrere Credentials und Anwendungen auf einem einzigen Gerät kombiniert werden, wird der 800er zu einem Generalschlüssel, der in einer heterogene IT-Umgebung dem Anwender auf einfache Weise die nahtlose starke Authentifizierung ermöglicht.

ENTSCHEIDUNGS-SZENARIO

Unternehmensprofil	Eine große Gesundheitsorganisation, die mehrere regionale Krankenhäuser und spezielle Gesundheitszentren mit mehr als 1,5 Millionen Patienten betreut.
Benutzergruppen	Ärzte, Beitragszahler und Versicherer, Patienten, Administratoren im Gesundheitswesen
Geschäftsbereich und Benutzeranforderungen	Ärzte sind ständig unterwegs und greifen dabei mithilfe eines Blackberrys oder eines anderen mobilen Geräts auf Gesundheitsdaten und Patientenakten zu. Dieser sofortige und sichere Zugriff auf wichtige Krankendaten gewährleistet eine bestmögliche Patientenbetreuung. Beitragszahler und Versicherer benötigen Zugriff auf Patientenakten sowie Anamnesen und erbrachte Gesundheitsdienste, um die Anspruchsregulierung durchführen zu können. Administratoren im Gesundheitswesen benötigen stets Zugang zu vertraulichen Krankendaten und persönlich identifizierenden Informationen (PII) von Patienten. Sowohl für Sachbearbeiter als auch für Buchhalter ist der Zugang zu Patienteninformationen unabdingbar. Patienten können ihre persönlichen Daten und Anamnese über ein Web-Portal abrufen. Dort können sie nicht nur ihre persönlichen Daten aktualisieren, sondern auch zahlreiche komfortable Online-Dienste nutzen, z.B. Termine vereinbaren, Rezepte erneut anfordern oder Behandlungskosten begleichen.
Authentifizierungsmöglichkeiten	Durch die unterschiedlichen Arten von Benutzern, die alle Zugriff auf verschiedene Systeme benötigen und deren Anforderungen sich unterscheiden, müsste diese Gesundheitsorganisation unzählige Authentifizierungslösungen in Betracht ziehen: – Ärzte: softwarebasierte, einmalig gültige Passwörter (OTP) für mobile Geräte – Beitragszahler und Versicherer: Hardware-Token – Administratoren im Gesundheitswesen: Hardware-Token – Patienten: risikobasierte Authentifizierung (RBA)

Software-Token

RSA SecurID-Software-Token verwenden dieselben Algorithmen wie die RSA SecurID Hardware-Token und eignen sich für Anwender, die kein spezielles Hardwaregerät mitführen möchten. Der symmetrische Schlüssel befindet sich nicht auf der RSA SecurID Hardware, sondern ist sicher auf dem PC, Smartphone oder USB-Gerät des Anwenders gespeichert.

Mobile Geräte

RSA SecurID-Software-Token sind für verschiedene Smartphone- Plattformen erhältlich, darunter BlackBerry®, iPhone®, Android®, Nokia®, Windows®Mobile und Symbian OS.

Microsoft Windows® Desktops

Der RSA SecurID-Token für Windows-Desktops ist ein praktischer Formfaktor, der sich auf einem PC befindet und die automatische Integration mit führenden Fernzugriff-Clients ermöglicht.

Token-Symbolleiste für einmalig gültige Passwörter

Der RSA SecurID-Toolbar-Token vereint den Bedienkomfort von automatischen Eintragsfunktionen für Webanwendungen mit der Sicherheit von Anti-Phishing-Technologien.

On-Demand (Bereitstellung per SMS oder E-Mail)

RSA On-Demand-Authentifizierung bedeutet die Bereitstellung eines eindeutigen, einmalig gültigen Passworts „auf Anfrage“ per SMS (Textnachricht) auf das Mobilgerät oder an die registrierte E-Mail-Adresse eines Anwenders. Diesen eindeutigen Code gibt der Anwender zusammen mit seiner PIN im Web-Browser ein, um auf das Unternehmensnetzwerk oder eine Online-Anwendung zuzugreifen.

RSA® AUTHENTICATION MANAGER EXPRESS

Der RSA® Authentication Manager Express ist eine Plattform zur starken Multi-Faktor-Authentifizierung, die kleinen und mittleren Unternehmen kosteneffektiven Schutz bietet. Der Authentication Manager Express unterstützt führende SSL VPNs und Web-Anwendungen bei der Bereitstellung von starker Authentifizierung und dem sicheren Zugriff auf geschützte Daten und Anwendungen.

Der Authentication Manager Express nutzt dieselbe risiokobasierte Authentifizierungs-Technologie von RSA, die bereits weltweit die Identitäten von über 250 Millionen Nutzern schützt. Diese hochentwickelte Lösung wertet hinter den Kulissen eine Reihe von Risikoindikatoren aus, um die Identität des Anwenders sicher zu stellen.

Die Risk Engineverfolgt jeden Anmeldeversuch in Echtzeit, wertet Dutzende Risikoindikatoren aus und weist jeder Anfrage eine bestimmte Risikostufe zu. Zur Ermittlung der Risikostufe werden Faktoren aus verschiedenen Kategorien berücksichtigt:

– „Wissen“: Benutzername und Passwort eines Benutzers

– „Besitz“: Laptop oder Desktop eines Benutzers

– „Benutzerverhalten“

Falls der Anmeldeversuch nicht den erforderlichen Sicherheitsanforderungen entspricht, kann der RSA Authentication Manager Express weitere Identitätsbelege anfordern. Das ist beispielsweise der Fall, wenn ein Anwedner von einem bisher unbekannten Gerät aus zugreift. RSA Authentication Manager Express bietet 2 Methoden zur zusätzlichen Authentifizierung an: Out-of-Band SMS und persönliche Sicherheitsfragen.

Der RSA Authentication Manager Express ist auf einer sicheren und benutzerfreundlichen Appliance direkt einsatzbereit und unterstützt bis zu 2.500 Nutzer.

RSA® ADAPTIVE AUTHENTICATION

RSA® Adaptive Authentication ist eine Plattform für Multi-Channel-Authentifizierung und Betrugserkennung, die eine kostengünstige Sicherheit für alle Anwender ermöglicht. Die Adaptive Authentication berücksichtigt zusätzliche Identifikatoren durch die Hinzunahme eines Cookies und/oder eines Flash Cookies und ermöglicht so die einzigartige Identifizierung eines Anwendergeräts. Die Lösung bietet starken und komfortablen Schutz

indem sie die Nutzeraktivitäten aufgrund von Risikostufen, institutionellen Maßgaben und Anwendersegmentierung überwacht und authentifiziert. Mithilfe der RSA-Technologie für risikobasierte Authentifizierung verfolgt Adaptive Authentication mehr als hundert Indikatoren, um potenzielle Betrugsfälle zu erkennen, darunter Geräteerkennung, IP-Geoposition und Verhaltensprofile. Jeder Aktivität wird ein eindeutiger Risikowert zugewiesen; je höher dieser Wert, desto höher die Wahrscheinlichkeit für betrügerische Absichten. Adaptive Authentication sorgt für eine Kontrolle im Hintergrund, die für den Anwender unsichtbar bleibt. Nur wenn eine Aktivität als sehr riskant eingestuft wird, muss der Anwender eine zusätzliche Authentifizierung leisten, meist in Form von persönlichen Fragen oder Out-of-Band-Telefonauthentifizierung. Durch die hohe Erfolgsquote dieses Prozesses bietet Adaptive Authentication einen starken Schutz sowie hohe Benutzerfreundlichkeit und eignet sich optimal für eine große Anwenderzahl.

RSA Adaptive Authentication ist sowohl as SaaS (Software as a Service) als auch als für den Einsatz vor Ort verfügbar. Die Lösung ist überaus skalierbar und kann Millionen von Anwendern unterstützen.

RSA® IDENTITY VERIFICATION

RSA Identity Verification nutzt wissensbasierte Authentifizierung für die Echtzeit Überprüfung von Anwenderidentitäten. Mit RSA Identity Verification werden dem Anwender eine Reihe von „aktuellen“ Fragen gestellt. Diese beruhen auf Informationen zu dieser Person, die aus Dutzenden von öffentlichen Datenbankarchiven gewonnen wurden. RSA Identity Verification bestätigt innerhalb weniger Sekunden die Identität, ohne zuvor eine Beziehung zu diesem Anwender hergestellt zu haben.

RSA Identity Verification sorgt außerdem durch das Modul „Identity Event“ für eine höhere Genauigkeit bei der Anwenderauthentifizierung. Mit diesem Modul steigt die Sicherheit, da das mit einer Identität verbundene Risiko ermittelt wird und das System den Schweregrad der Fragen beim Authentifizierungsprozess automatisch so anpassen kann, dass er dem erkannten Risiko entspricht. Zu den ausgewerteten Ereignissen für einzelne Identitäten zählen:

– Suchvorgänge in öffentlichen Archiven. Verdächtige Zugriffe auf öffentliche Datensätze eines Anwenders.

– Geschwindigkeit einer Identität. Ein hohes Aktivitätsvolumen einer Person bei mehreren Unternehmen.

– IP-Geschwindigkeit. Mehrere Authentifizierungsanfragen über dieselbe IP.

RSA® CERTIFICATE MANAGER

RSA® Certificate Manager ist eine Internet-basierte Zertifizierungsstelle (CA), die die Kernfunktionen für die Vergabe, Verwaltung und Validierung digitaler Zertifikate bereitstellt. Die Lösung beinhaltet einen sicheren Web-Server sowie eine leistungsstarke Signatur-Engine für das digitale Signieren von Anwenderzertifikaten. Außerdem ist ein integrierter Datenspeicher für Zertifikate, Systemdaten und Informationen über den Zertifikatsstatus vorhanden. Der RSA Certificate Manager wurde als erste Lösung durch Common Criteria zertifiziert und verfügt darüber hinaus über die IdenTrust-Zertifizierung.

RSA® Certificate Manager wurde auf Basis offener Branchenstandards entwickelt. So wird die integrierte Kompatibilität mit mehreren Hundert auf Standards basierenden Anwendungen sichergestellt. Aus diesem Grund lässt sich die Lösung auch mit anderen Anwendungen wie Web-Browsern, E-Mail-Anwendungen und VPN-Clients nutzen, um einen maximalen ROI zu garantieren. Außerdem besteht die Möglichkeit, Zugangsdaten in Web-Browsern, auf Smart Cards oder USB-Token zu hinterlegen. Digitale RSA-Zertifikate lassen sich beispielsweise mit der SecurID 800-Hybrid-Authentifizierungskomponente kombinieren, um verschiedene Zugangsdaten auf einem Gerät zu konsolidieren und so die Benutzerfreundlichkeit zu verbessern. Weitere RSA-Lösungen für digitale Zertifikate sind z. B. RSA Registration Manager, RSA Validation Manager, RSA Key Recovery und RSA Root Signing-Dienste.

ÜBER RSA

RSA, The Security Division of EMC, ist ein führender Anbieter von Sicherheits-, Risiko- und Compliance-Management-Lösungen. Für die Kunden von RSA ist die Lösung ihrer komplexen sicherheitsspezifischen Herausforderungen ein kritischer Faktor für den Unternehmenserfolg. Zu den Herausforderungen zählen das Management organisatorischer Risiken, die Absicherung des Zugriffs auf unternehmensinterne Ressourcen, der Nachweis der Einhaltung von Sicherheitsanforderungen sowie der Schutz von virtuellen Infrastrukturen und Cloud-Umgebungen.

Mit Identitätsprüfung, Kryptographie, Schlüsselmanagement, Security Information und Event Management (SIEM), Data Loss Prevention und Betrugsbekämpfung bis hin zu Enterprise Governance, Risk & Compliance (eGRC) sowie umfassenden Beratungsleistungen sorgt RSA für Transparenz und Vertrauen in digitale Identitäten, Transaktionen und Daten von Millionen von Anwendern.

www.RSA.com

DECTREE wp DE0711

www.rsa.com

RSA

EMC²