



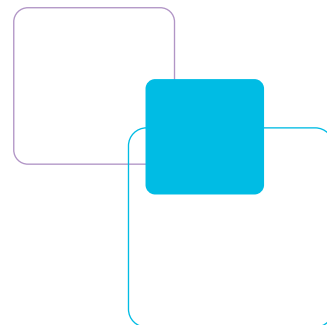
Ein Leitfaden zum Thema:
**Sicherheit für
kritische Ressourcen**

Sichere Daten

Sicherer Zugriff

Sichere Kundenidentitäten und Kundendaten

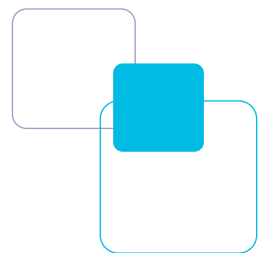
Management von Compliance- und Sicherheitsinformationen





Inhalt

Absichern kritischer Ressourcen mit EMC	3
Management der Beziehung zwischen Personen und Daten	3
Die ersten Schritte	4
Sichere Daten	5
Sicherer Zugriff	6
Sichere Kundenidentitäten und Kundendaten	8
Management von Compliance- und Sicherheitsinformationen	10



Absichern kritischer Ressourcen mit EMC

Ihre Informationen gehören zu Ihren wichtigsten Ressourcen. Natürlich möchten Sie sicherstellen, dass diese Informationen niemals zum Problem werden - durch Verlust, Manipulation oder Diebstahl. RSA, The Security Division of EMC, ist der Experte für informationszentrierte Sicherheit. Wir unterstützen weltweit führende Unternehmen bei der Erfüllung der komplexesten und sensibelsten Sicherheitsanforderungen. Mit unserem informationszentrierten Sicherheitsansatz können Sie Ihre kritischen Ressourcen wie folgt absichern:

- Direkter Schutz der Informationen selbst
- Sicherer Zugriff auf Informationen von allen Standorten aus
- Management von Sicherheitsinformationen zur Erzielung von Compliance

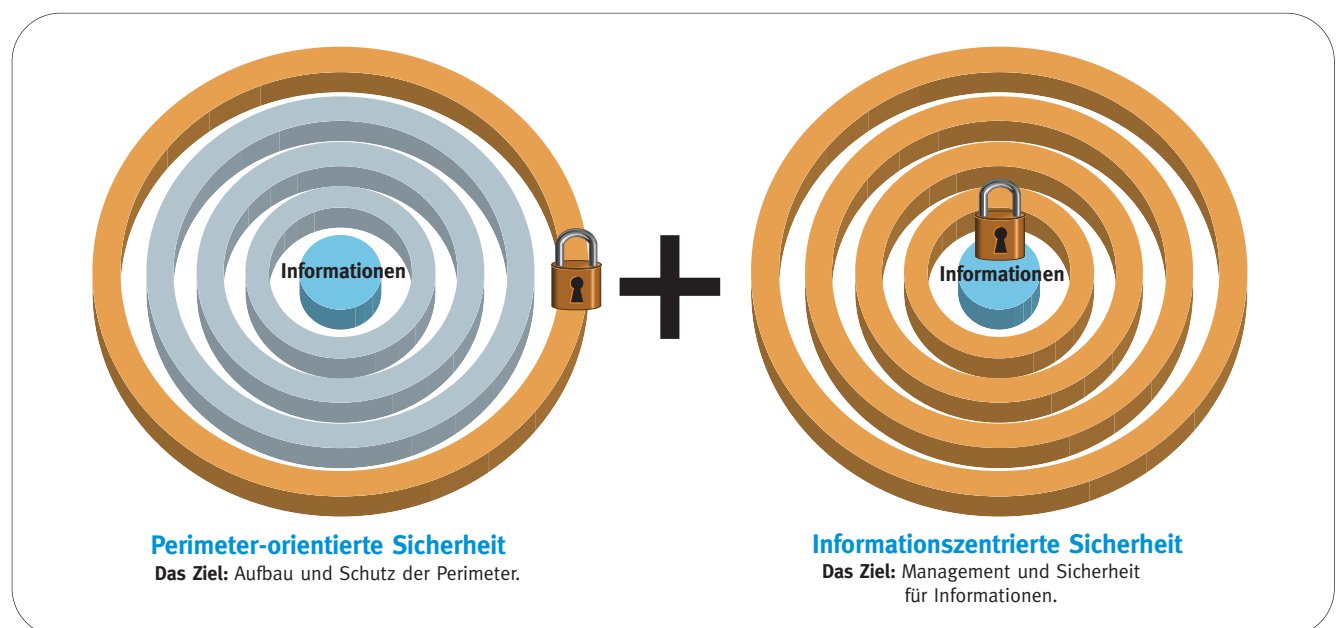
Wir haben diesen Leitfaden erstellt, um Ihnen unser Konzept und die entsprechenden Lösungen zu erläutern. Mit EMC können Sie Ihr Unternehmen und die Geschäftsabläufe absichern und darauf vertrauen, dass Ihre Informationen nicht zum Problem werden.

Management der Beziehung zwischen Personen und Daten

Die meisten Unternehmen werden zustimmen: Informationen sind ihr wichtigstes Kapital. Zum Erhalt der Vertraulichkeit, der Integrität und des Nutzens müssen Informationen vor zahlreichen Bedrohungen geschützt werden. Hierzu zählen unbefugter Zugriff, unbefugte Nutzung, Weitergabe, Unterbrechung, Veränderung und Löschung.

Trotz erheblicher Investitionen in Personal, Prozesse und Technologien im Bereich Sicherheit sind nur wenige Unternehmen der Meinung, dass ihre Daten sicher sind. Der Grund hierfür ist einfach: Die Mehrzahl der aktuellen Sicherheitslösungen schützen nicht die Informationen. Tools wie Firewalls und Virenschutz-Software schützen Informations-Proxies, wie z. B. Netzwerke und Laptops. Diese Perimeter-orientierten Sicherheitsansätze ignorieren die Tatsache, dass Informationen und deren Anwender konstant in Bewegung sind. Wenn Daten oder Personen den sicheren Bereich verlassen, sind sie ungeschützt.

Abbildung 1. Der Nutzen eines informationszentrierten Sicherheitsansatzes



Unternehmen können nach einer Sicherheitsverletzung mit erheblichen Kosten konfrontiert. Außerdem zieht die Verletzung einer Sicherheitsvorschrift erhebliche Strafen nach sich. Obwohl er notwendig ist, reicht ein am Perimeter ausgerichteter Ansatz allein angesichts dieser möglichen Folgen nicht aus. Darüber hinaus hindert die Angst vor Sicherheitsproblemen Unternehmen an der umfassenden Nutzung von Informationen zur Erzielung von Wettbewerbsvorteilen. Unternehmen müssen die Konvergenz von Sicherheits- und Informationsmanagement erkennen und verstehen, dass sich die Sicherheit im Grunde bedeutet, die Beziehungen zwischen Personen und Daten zu managen. Dieser Ansatz wird als informationszentrierte Sicherheit bezeichnet.

Durch die Ergänzung von am Perimeter orientierten Lösungen um einen informationszentrierten Ansatz (siehe Abbildung 1) können Sie sicherstellen, dass Ihr wichtigstes Kapital - Ihre Informationen - nicht zum Problem werden.

Die ersten Schritte

Wenn Sie angemessene Prioritäten für die Implementierung und Durchsetzung von Sicherheitsmaßnahmen festlegen möchten, müssen Sie zunächst den Sicherheitsstatus Ihrer Umgebung kennen. Für Ihr Unternehmen sind dabei die folgenden Schritte hilfreich:

Definieren Sie Ihre Sicherheits-Policy

Ermitteln Sie, ob Sie über eine Policy verfügen, die genau festlegt, welche Informationen sensibel sind. Stellen Sie die derzeit vorhandenen Sicherheitsvorkehrungen zusammen. Eine umfassende Policy bietet die Grundlage und ist der beste Weg zur Gliederung, Implementierung und Überwachung von Sicherheitsmaßnahmen.

Klassifizieren und Ermitteln

Definieren Sie, welche Daten sensibel sind. Im Hinblick auf die Kosten müssen Sicherheitsmaßnahmen selektiv angewendet werden. Lokalisieren Sie sensible Daten. Informationen können nur dann abgesichert werden, wenn sie auch gefunden werden können. Finden Sie heraus, ob verschiedene Kategorien der Informationssicherheit entstehen.

Identifizieren Sie die Informationsinfrastruktur, die sensible Daten unterstützt. Informationen können nur so sicher sein wie der Ort, an dem sie sich befinden. Identifizieren Sie alle Anwendungen, die auf sensible Daten zugreifen müssen. Möglicherweise müssen Sie für bestimmte Anwendungen weitere Sicherheitsmaßnahmen definieren.

Sichern Sie Ihre sensiblen Daten ab

Ermitteln Sie, ob sensible Daten strukturiert oder unstrukturiert sind. Verschiedene Datentypen erfordern unterschiedliche Sicherheitsmaßnahmen. Ermitteln Sie, ob sensible Daten von angepassten Anwendungen, Datenbanken oder Dateisystemen erzeugt werden. Je nachdem, wo die Daten erzeugt werden, werden unterschiedliche Technologien zu deren Absicherung eingesetzt.

Ermitteln Sie, ob Verschlüsselung und das Verschlüsselungsmanagement durch eine Policy geregelt werden. Ohne eine angemessene Policy kann die Verschlüsselung mehr Probleme hervorrufen als beheben. Ermitteln Sie das Verfahren, das für das

Verschlüsselungsmanagement eingesetzt wird. Steht kein Verschlüsselungsalgorithmus zur Verfügung, können die verschlüsselten Daten nicht verwendet werden.

Stellen Sie fest, wer Ihre Daten nutzt

Stellen Sie fest, wer auf sensible Daten zugreifen kann. Die Nutzung sensibler Daten müssen auf jene Personen beschränkt bleiben, die diese Daten für ihre täglichen Aufgaben benötigen. Ermitteln Sie, wie der Mitarbeiterzugriff innerhalb der Firewall kontrolliert wird. Der Zugriff muss sicher sein - wenn aber die entsprechenden Sicherheitsmaßnahmen die Anwender übermäßig belasten oder sehr zeitraubend sind, werden Sicherheitsmaßnahmen auch umgangen oder die Nutzung geschützter Ressourcen wird vermieden.

Stellen Sie fest, wie der Mitarbeiterzugriff kontrolliert wird. Die Bereitstellung eines Remote-Zugriffs bringt Produktivitätsverbesserungen mit sich, aber auch zusätzliche Sicherheitsrisiken für das Unternehmen.

Stellen Sie fest, ob Partner Zugriff erhalten. Die Zusammenarbeit mit Partnern erweitert die geschäftlichen Möglichkeiten, kann jedoch sensible Informationen einem Risiko aussetzen.

Stellen Sie fest, ob Kunden Zugriff erhalten. Online-Transaktionen für Kunden senken die Kosten, setzen die Kunden jedoch einem Missbrauchsrisiko aus.

Demonstrieren der Compliance

Ermitteln Sie, ob von allen Devices Audit-/Protokolldaten zusammengestellt werden. Audit-Daten sind insgesamt sehr wertvoll, da diese Informationen zu allen Aktivitäten in Ihrer Umgebung enthalten. Ermitteln Sie, wie Bedrohungen und Policy-Verletzungen in Echtzeit erkannt werden. Die Erkennung und Analyse in Echtzeit ermöglicht eine schnelle Reaktion auf Sicherheitsbedrohungen.

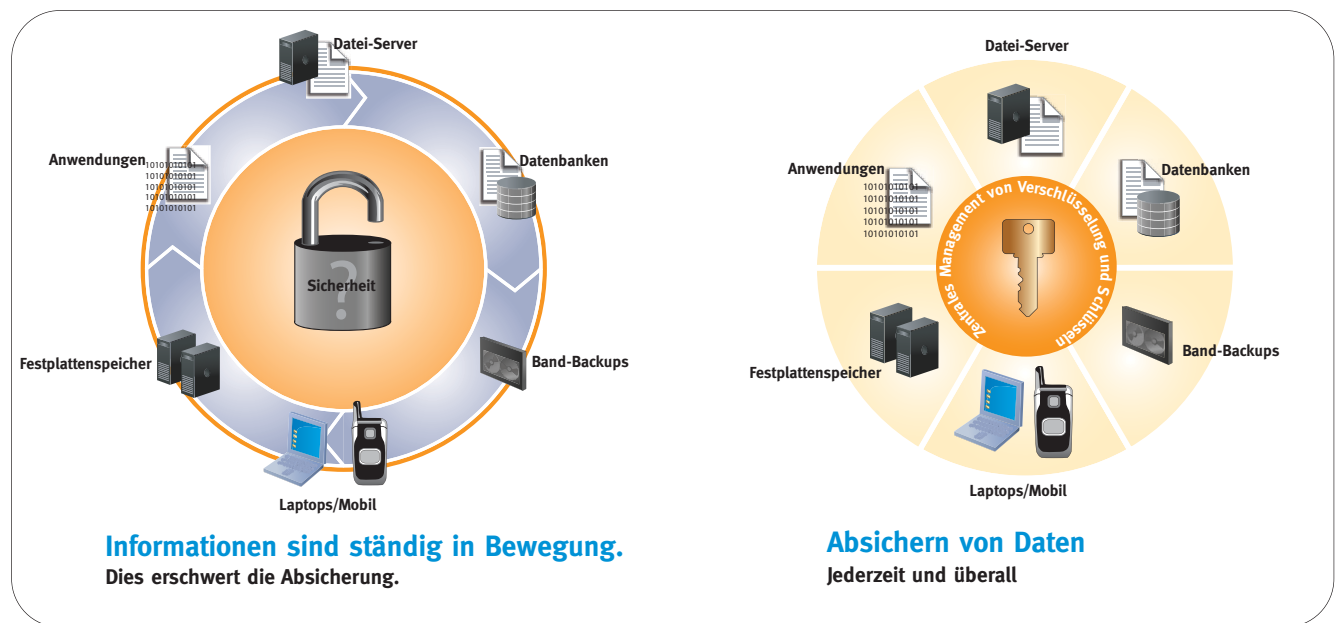
Identifizieren Sie die Prozesse, die zum Nachweis der Compliance mit Policy und Auflagen für interne Prüfer und externe Behörden verwendet werden. Die Durchsetzung von Sicherheits-Policies muss grundsätzlich nachgewiesen werden, um Ausgaben zu validieren und die Einhaltung von Vorschriften Regelungen zu belegen.

Absichern der Daten

Trotz erheblicher Investitionen in diesem Bereich glauben nur wenige Unternehmen, dass ihre Daten wirklich sicher sind. Die meisten herkömmlichen Sicherheitslösungen errichten und schützen den Randbereich, tun jedoch nur wenig für die Absicherung der Informationen selbst.

Die Kosten einer Sicherheitsverletzung können in die Millionen gehen – und es gibt weitere negative Konsequenzen.

Abbildung 2. Absichern von Daten – jederzeit und an jedem Ort



Der Wert der Marke kann beeinträchtigt werden, die Aktienkurse können fallen und das Vertrauen von Kunden, Investoren und Partnern kann beschädigt werden. Neben diesen drohenden Konsequenzen sind außerdem informationsspezifische Compliance-Anforderungen durch Branchen- und Behördenrichtlinien zu beachten.

Wenn Sie eine Compliance-Überprüfung nicht bestehen, können erhebliche zivil- und strafrechtliche Konsequenzen daraus resultieren. Durch die Erzwingung von Schutzmaßnahmen am jeweiligen Ort der Nutzung – unabhängig vom Standort – können Sie die Vertraulichkeit und Integrität sensibler Informationen wirksam schützen.

Sichern Sie Daten an jedem Punkt des Lebenszyklus.

Sensible Informationen sind in Bewegung und befinden sich an vielen Orten. Dies erschwert die Absicherung. Verschiedene Systeme weisen häufig unterschiedliche Policies für die Absicherung von Informationen auf. Versuche, die Daten zu schützen, sind häufig nicht kompatibel. Mit dem Ansatz von EMC (siehe Abbildung 2) ist der Schutz nicht an ein bestimmtes System gebunden, sondern an die Daten selbst. Der Schutz folgt den Daten und setzt die Policies Ihres Unternehmens durch, ganz unabhängig davon, wo die Daten sich befinden.

EMC bietet eine umfassende Palette von Lösungen für die Datensicherheit, mit deren Hilfe digitale Informationen an jedem Ort und an jedem Punkt des Lebenszyklus sicher sind und bleiben.

RSA Classification for Information Security Service ermittelt und klassifiziert Daten auf der Basis der Sensibilität und entwickelt entsprechende Strategien, um sicherzustellen, dass die Sicherheit den geschäftlichen Nutzen widerspiegelt.

RSA Key Manager vereinfacht die Implementierung und Verwaltbarkeit der Verschlüsselungsfunktionen in Unternehmensanwendungen und trägt so zur Absicherung von Daten ab dem Zeitpunkt ihrer Erstellung bei.

RSA Database Security Manager unterstützt die (für Anwender und Anwendungen transparente) Policy-basierte, granulare Verschlüsselung von Datenbankobjekten.

RSA File Security Manager unterstützt (transparent für geschäftliche Anwendungen) die selektive Verschlüsselung von Datei- oder Ordnerobjekten in Dateisystemen.

EMC Documentum Information Rights Management-Software ist eine Lösung für das Digital Rights Management, mit der Sie dynamisch den Zugriff und die Nutzung von Dokumenten und E-Mails innerhalb und außerhalb des Unternehmens kontrollieren können.

RSA Design and Implementation for Storage Encryption Service analysiert die Band- oder IP-Replikationsumgebung vor der Installation branchenführender Verschlüsselungs-Appliances von Partnern.

EMC Certified Data Erasure ermöglicht die sichere und effektive Löschung von Daten von allen Netzwerkspeicher-Systemen oder Medien gemäß den Standards des U.S. Government Department of Defense.

EMC Disk Retention ermöglicht die Vernichtung bzw. Erhaltung von Medien zum Zeitpunkt des Austauschs.

Sicherer Zugriff

Zur Maximierung der Produktivität sollten Ihre Mitarbeiter einen einfachen, sicheren Zugang zu Unternehmensressourcen haben – von praktisch jedem Ort aus.

Für den Remote-Zugriff stellen viele Unternehmen Virtual Private Network (VPN) Technologie bereit. VPNs schützen die Remote-Kommunikation mit Verschlüsselungstechnologien. Ein VPN kann Dritte daran hindern, geschützte Kommunikation abzufangen und zu entschlüsseln. Die Identität der Person, die das Remote-Gerät nutzt, wird jedoch nicht bestätigt.

Die meisten Unternehmen verwenden eine einfache Kombination aus Passwort und Anwendername, um den Zugriff auf Remote-Geräte abzusichern. Leider werden einfache Passworte nur allzu leicht bekannt und gelten daher nicht als sicher. Zur Nutzung des vollen Potenzials von VPNs benötigen Sie einen rigoroseren Ansatz, um unbefugtes Eindringen zu verhindern. Hier ergänzen die Vorteile einer starken Authentifizierung die Merkmale für den Remote-Zugriff.

Das Verhindern eines unbefugtem Zugriffs erfordert die Authentifizierung oder die Sicherstellung der Identität einer Person. Auf Basis dieser Identität wird der Zugriff auf die relevanten Ressourcen, Anwendungen und Daten gewährt, so dass autorisierte Anwender ihre beruflichen Aufgaben wahrnehmen können.

Die Identität wird anhand von persönlichen Merkmalen, Kenntnissen oder Attributen zugewiesen. Dies kann einen Anwendernamen, eine PIN oder eine Secure ID FOB umfassen („zweistufige Authentifizierung“).

Der Authentifizierungsprozess klingt einfach, ist jedoch in der Praxis eher komplex. Authentifizierung, die auf statischen, wiederverwendbaren Passworten basiert, ist für Hacker leicht zu durchbrechen, so dass Identitäten nicht mit Gewissheit bestätigt werden können. Policies, die das häufige Ändern komplexer Passworte erfordern, sind für Anwender sehr schwierig und führen zu zahlreichen Help Desk-Anrufen oder – was noch schlimmer ist - zur Umgehung der Policy.

Das Ziel ist daher, die Risiken zu verringern und hohen Aufwand beim Anwender zu vermeiden. Hierzu ist die Ausdehnung einer breiten Palette starker Authentifizierungsoptionen für Anwender auf Geräten erforderlich, die von Smartcards, Hardware Tokens und Laptops bis hin zu PDAs und Mobiltelefonen reichen.

Zur Maximierung der Produktivität benötigen Ihre Mitarbeiter einen einfachen, sicheren Zugriff auf Unternehmensressourcen von praktisch jedem Ort aus.

Sicheres Arbeiten – überall und jederzeit

RSA, The Security Division of EMC, bietet Authentifizierungslösungen mit bewährter und flexibler Technologie, verfügt über Beziehungen und Partnerschaften in der Branche sowie umfassende Erfahrungen in der Bereitstellung dieser wichtigen Sicherheitstechnologie.

Die Authentifizierungslösungen von RSA bieten folgende Merkmale:

- Steigerung der Produktivität, da Anwender überall und jederzeit mit Unternehmensressourcen arbeiten können
- Verbesserung der Sicherheit durch starke Authentifizierung, die bisher niemals durchbrochen wurde
- Verringerung der Help Desk-Anrufe zu Passwörtern durch automatisches Ändern der Zugangscodes alle 60 Sekunden
- Direkte, nahtlose Integration

RSA SecurID ist eine zweistufige Authentifizierungslösung mit einer breiten Palette von Optionen zur Anwenderauthentifizierung. Diese Lösung bietet Interoperabilität mit mehr als 300 Produkten von über 200 Anbietern.

RSA Authentication Manager ist eine Management-Software der Enterprise-Klasse mit starker Authentifizierung für die RSA SecurID-Lösung, bei der nur korrekt authentifizierte Anwender auf sensible Ressourcen zugreifen können. RSA SecurID Appliance stellt Authentication Manager-Software über eine integrierte, Rack-fähige, vorkonfigurierte Hardware-Appliance bereit.

Sichere Kundenidentitäten und Kundendaten

Verbrauchern ist der einfache Self-Service im Internet sympathisch. Wenn Sie diesen bieten, erfüllen Sie Kundenanforderungen und verringern den Overhead, den Transaktionen auf herkömmlichen Wegen mit sich bringen. Leider nehmen die Häufigkeit und die Komplexität von Bedrohungen der Online-Sicherheit ständig zu, so dass die Risiken bei der Durchführung solcher Transaktionen steigen und das Kundenvertrauen geschädigt wird.

Wenn Sie die Vorteile der Online-Transaktionen nutzen möchten, müssen Sie sicherstellen, dass Ihr Online-Angebot sowie der entsprechende Channel vertrauenswürdig und sicher ist. Unterschiedliche Kundentypen haben unterschiedliche Sicherheitsbedürfnisse. Bestimmte Transaktionsarten sind stärker mit Risiken behaftet als andere. Verschiedene Kunden bevorzugen verschiedene Schutzmaßnahmen. Risiken und Sicherheit müssen in ein vernünftiges Verhältnis gebracht werden, ohne das Kundenerlebnis oder den Gewinn zu beeinträchtigen.

Angesichts der Zunahme der Gefahren im Internet werden Unternehmen mit der Herausforderung konfrontiert, Anwendern flexible, kostengünstige Lösungen bereitzustellen, die die Compliance berücksichtigen und eine optimale Auswahl und einfache Bereitstellung ermöglichen. Dabei muss das höchste Maß an Schutz erhalten bleiben.

Abbildung 3. RSA SecurID Authenticators



SecurID Authenticators (siehe Abbildung 3) erzeugen einen einfachen, einmaligen Code, der alle 60 Sekunden geändert wird. Dieser Code wird zusammen mit einer PIN zur Authentifizierung von Anwendern im Netzwerk sowie für den Zugriff auf geschützte Ressourcen verwendet. Wenn ein Anwender versucht, auf eine geschützt Ressource zuzugreifen, muss er seine PIN und den Kenncode eingeben, der zu diesem Zeitpunkt im Authenticator angezeigt wird. RSA Authentication Manager-Software ist der Authentifizierungs-Engine des Systems und prüft die Kombination aus PIN und Kenncode. Sie stellt außerdem sicher, dass diese Angaben korrekt sind, bevor der Zugriff gewährt wird.

Sicherheit = Kundenzufriedenheit

Die RSA Consumer Protection Suite umfasst starke Authentifizierung und Anti-Missbrauchslösungen zum Schutz Ihrer Umgebung und Ihrer Kunden vor den neuesten Online-Bedrohungen. Die RSA Consumer Protection Suite:

- Erfüllt Kundenanforderungen und senkt Kosten, denn sichere Online-Transaktionen und Geschäftsprozesse werden ermöglicht
- Verringert den Missbrauch um 80 Prozent
- Steigert das Kundenvertrauen, die Anzahl der Online-Transaktionen und die Bestandskonsolidierung
- Schützt mehr als 100 Millionen Kundenidentitäten Online
- Hat bereits mehr als zwei Milliarden Transaktionen verarbeitet und geschützt
- Hat mehr als 30.000 Phishing Sites geschlossen und die durchschnittliche Dauer eines Phishing-Angriffs von rund 115 Stunden auf nur 5 Stunden verkürzt

Das RSA Produkt- und Service-Portfolio bietet abgestuften End-to-End-Schutz, einschließlich:

- Risikobasierter Authentifizierung für Online- und Telefon-Channels
- Site-to-User Online-Authentifizierung
- Transaktionsüberwachung und Signatur
- Anti-Phishing-/Pharming- und Trojaner-Services

Die RSA Consumer Protection Suite (Abbildung 4) ermöglicht Unternehmen die sichere Erweiterung von Online-Geschäftsprozessen und Transaktionen auf Kunden.

RSA Adaptive Authentication for Web ermöglicht Finanzinstituten die dynamische Anpassung der Online-Authentifizierung von Kunden auf der Basis von Kundenpräferenzen, Policy-Anforderungen und behördlichen Vorschriften sowie Risikostufen.

RSA FraudAction ist ein Anti-Phishing/Anti-Missbrauchs-Service, der Echtzeit-Schutz vor vorhandenen und neuen Online-Bedrohungen für Unternehmen und deren Online-Nutzer bietet.

RSA Identity Verification from Verid ist eine anwenderfreundliche Plattform mit Knowledge-Based Authentication (KBA) zur Bestätigung von Kundenidentitäten in Echtzeit. Durch das Anfordern von Antworten auf reale Fragen zu Einzelpersonen durch Scannen von Milliarden öffentlicher Datensätze bestätigt RSA Identity Verification Identitäten innerhalb weniger Sekunden, ohne dass eine vorherige Kundenbeziehung erforderlich ist.

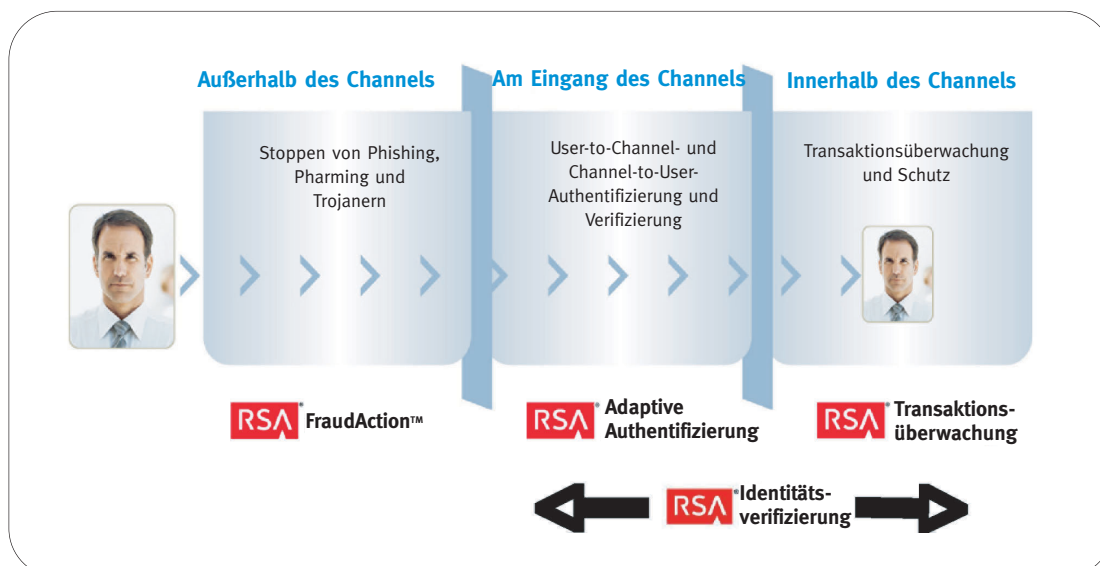
RSA Transaction Monitoring ist eine vollständige Online-Missbrauchserkennungs- und Managementlösung, die nachgewiesen hat, dass der Missbrauch mit dieser Lösung um bis zu 80 Prozent verringert werden kann.

RSA Go ID Authentication Service ist eine netzwerk-basierte Authentifizierungslösung, die zeitsynchrone Einmal-Passworttechnologie mit leistungsstarken Back Office Tools und -Services kombiniert.

RSA eFraudNetwork ist ein institutionsübergreifendes Online-Netzwerk zum Schutz vor Online-Betrug, das proaktiv Betrugs- und Betrügerprofile, Muster und Verhalten auf der ganzen Welt verfolgt und identifiziert.

Die RSA Consumer Protection Suite ermöglicht Unternehmen die sichere Erweiterung von Online Business-Prozessen und -Transaktionen auf Ihre Kunden.

Abbildung 4. Die RSA Consumer Protection Suite: End-to-End-Datensicherheit mit mehreren Stufen



Management von Compliance- und Sicherheitsinformationen

Ihr Unternehmen steht unter erheblichem Druck, die Compliance mit internen Audit-Richtlinien und externen Auflagen nachweisen zu müssen. Das gilt in besonderem Maße für stark reglementierte Branchen. Da die Häufigkeit und Komplexität von Sicherheitsbedrohungen ständig zunehmen, sind Sicherheitsrisiken außerdem in Echtzeit zu ermitteln und zu stoppen.

Die Belastungen durch den Nachweis der Compliance und der Aufrechterhaltung effektiver Sicherheitsmaßnahmen sind für das Compliance- und Sicherheitspersonal zu einer enormen Herausforderung geworden. Audit-Daten enthalten insgesamt umfassende Informationen zu allen Zugriffen auf Devices, zu den ausgeführten Aktionen und zu Konfigurationsänderungen in der IT-Umgebung eines Unternehmens. Allein der enorme Umfang der zu sammelnden Informationen ist für diese Gruppen kaum zu bewältigen. Die Koordination und Korrelation dieser Informationen über zahlreiche Systeme und Infrastrukturkomponenten hinweg ist sehr schwierig.

Sie benötigen eine flexible Plattform, die von allen Gruppen im Unternehmen (Betrieb, Sicherheit, Compliance) verwendet werden kann, um relevante Audit-Daten zu sammeln, Sicherheitsbedrohungen zu identifizieren und Compliance-Berichte zu vereinfachen. Außerdem setzen die behördlichen Anforderungen im Bereich Aufbewahrung voraus, dass Unternehmen die große und schnell wachsende Menge an Audit-Daten drei bis sieben Jahre bzw. länger speichern. Unternehmen benötigen eine kostengünstige, effiziente und manipulationssichere Lösung für die langfristige Archivierung von Audit-Daten.

Einfache Compliance und erweiterte Sicherheit

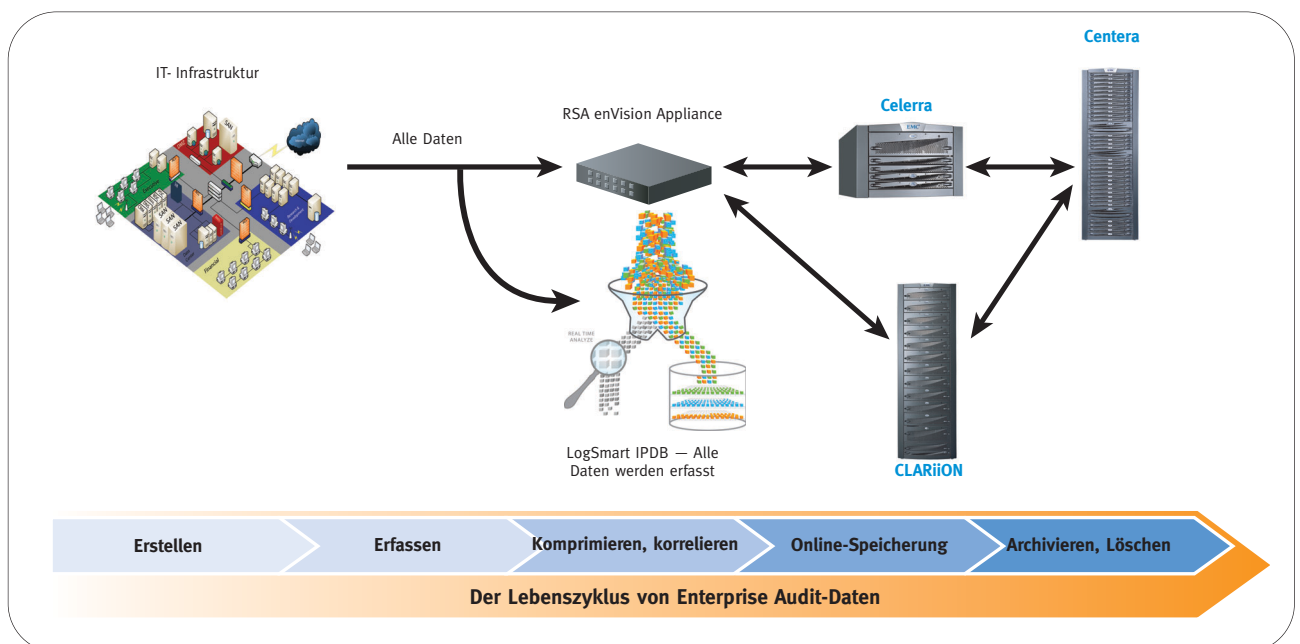
RSA und EMC bieten Ihnen die umfassende Unternehmensplattform, die Sie für das Management von Compliance- und Sicherheitsinformationen benötigen.

RSA enVision ist ein Produkt für das Management von Sicherheitsinformationen und Ereignissen, das eine einzigartige Internet Protocol Data Base (IPDB) nutzt. Die verteilte, Appliance-basierte Architektur ermöglicht das Sammeln „aller Daten“ ohne Filtern oder Löschen von Informationen. Außerdem sind keine speziellen Ressourcen wie DBAs für die Ausführung und den Erhalt erforderlich. Darüber hinaus ist enVision eine echte Unternehmensplattform für das Sammeln, Analysieren und Reporting von Sicherheitsdaten. Diese Lösung erfüllt die vielfältigen Anforderungen des Sicherheits-, Betriebs- und Compliance-Personal mit einem einzigen Produkt.

Das Expertenwissen von EMC in den Bereichen Speicher und Informationsmanagement trägt zum Nutzen der Gesamtlösung bei - mit optimiertem Unternehmensspeicher für die Speicherung und Aufbewahrung großer Mengen an Audit-Daten, die die Plattform sammelt. Schließlich kann Sie das EMC Service Team bei der Entwicklung und Implementierung einer hochgradig optimierten Lösung unterstützen, die die Anforderungen der verschiedensten Unternehmen oder Service-Anbieter unterstützt.

RSA enVision verwendet eine erweiterte Architektur zur Erfassung aller Protokolldateien aus den Netzwerk-, Sicherheits-, Server-, Anwendungs- und Speicherebenen

Abbildung 5. RSA enVision und EMC Speicher



des Unternehmens. Nach der Zusammenstellung der Informationen wandelt die enVision-Software diese in nützliche Daten um.

RSA enVision bildet die Grundlage einer Unternehmensplattform für Compliance- und Sicherheitsoperationen. Diese umfasst **EMC CLARiiON**- und **EMC Celerra**-Speichersysteme sowie die Möglichkeit zur Integration weiterer EMC Speichersysteme bei Bedarf (siehe Abbildung 5). Auf diese Weise können Sie die Anforderungen der Aufbewahrungsregeln und behördlichen Vorschriften mit dem passenden Speicher in Einklang bringen, die Sicherheit verbessern und die Compliance vereinfachen.

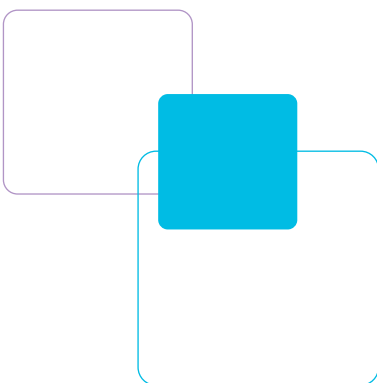
RSA enVision NAS3500 bietet hochgradig verfügbaren Network-Attached-Speicher auf der Basis von EMC Celerra-Systemen, die auf die Bereitstellung von RSA enVision auf mehreren Servern ausgelegt sind.

RSA enVision DAS2000 bietet Direct-Attached Storage auf Basis von EMC CLARiiON für die Bereitstellung von RSA enVision auf einem Server.

Übersteigt der Speicherbedarf die Kapazität des integrierten Speichers, können weitere Speichersysteme hinzugefügt werden, um spezifische Anforderungen zu erfüllen. Hierzu zählen z. B. die EMC Symmetrix, die Celerra und die CLARiiON für Online-Speicherung sowie die EMC Centera für Nearline-Archivierung.

Design and Implementation Service for Security Information Management ermöglicht den Beratungsexperten von RSA die Berücksichtigung geschäftlicher und technischer Anforderungen vor der Entwicklung einer individuellen Lösung für das Compliance- und Sicherheitsmanagement.

RSA enVision bildet die Grundlage einer Unternehmensplattform für Compliance- sowie Sicherheitsoperationen.



Weitere Leitfäden von EMC

- Intelligenter speichern
- Backup, Recovery und Archivierung der nächsten Generation
- Mehr geschäftlicher Nutzen aus Microsoft-Umgebungen
- Effektiverer und kostengünstigerer Schutz
- Automatisierung des Rechenzentrumsbetriebs
- Schneller profitieren vom geschäftlichen Nutzen aus SAP-Anwendungen
- Virtualisierung der Informationsinfrastruktur
- Die Nutzung von Content zur Erzielung von Wettbewerbsvorteilen
- Absicherung kritischer Ressourcen
- Mehr geschäftlicher Nutzen aus Oracle-Umgebungen

Machen Sie den nächsten Schritt.

Weitere Informationen, wie EMC den Betrieb Ihrer Informationsinfrastruktur verbessern kann, erhalten Sie von Ihrem EMC Vertriebsbeauftragten, telefonisch unter 0800 10 16 944 (gebührenfrei in Deutschland), oder besuchen Sie unsere Website www.emc2.de.

EMC², EMC, EMC ControlCenter, AlphaStor, ApplicationXtender, Avamar, Captiva, Catalog Solution, Celerra, Centera, ContraStar, CLARAlert, CLARiiON, ClientPak, CodeLink, Connectix, Co-StandbyServer, Dantz, Direct Matrix Architecture, DiskXtender, DiskXtender 2000, Documentum, EmailXaminer, EmailXtender, EmailXtract, eRoom, FLARE, HighRoad, InputAccel, Invista, Max Retriever, Navisphere, NetWorker, nLayers, OpenScale, Powerlink, PowerPath, Rainfinity, RepliStor, ResourcePak, Retrospect, Smarts, SnapShotServer, SnapView/IP, SRDF, Symmetrix, TimeFinder, VisualSAN, VSAM-Assist, WebXtender, where information lives, Xtender und Xtender Solutions sind eingetragene Marken, und EMC Developers Program, EMC OnCourse, EMC Proven, EMC Snap, EMC Storage Administrator, Acartus, Access Logix, ArchiveXtender, Authentic Problems, Automated Resource Manager, AutoStart, AutoSwap, AVALONidm, C-Clip, Celerra Replicator, CLARevent, Codebook Correlation Technology, Common Information Model, CopyCross, CopyPoint, DatabaseXtender, Direct Matrix, EDM, E-Lab, Enginuity, enVision, FarPoint, Global File Virtualization, Graphic Visualization, InfoMover, Infoscape, MediaStor, MirrorView, NetWin, OnAlert, PowerSnap, RepliCare, SafeLine, SAN Advisor, SAN Copy, SAN Manager, SDMS, SnapImage, SnapSure, SnapView, StorageScope, SupportMate, SymmAPI, SymmEnabler, Symmetrix DMX, UltraPoint, UltraScale, Viewlets und VisualSRM sind Marken der EMC Corporation. RSA und enVision sind eingetragene Marken von RSA Security Inc. VMware ist eine eingetragene Marke von VMware, Inc. Alle anderen hier verwendeten Marken sind Eigentum der jeweiligen Inhaber.

© Copyright 2007 EMC Corporation. Alle Rechte vorbehalten.
Herausgegeben in den USA. 10/07

H2958

