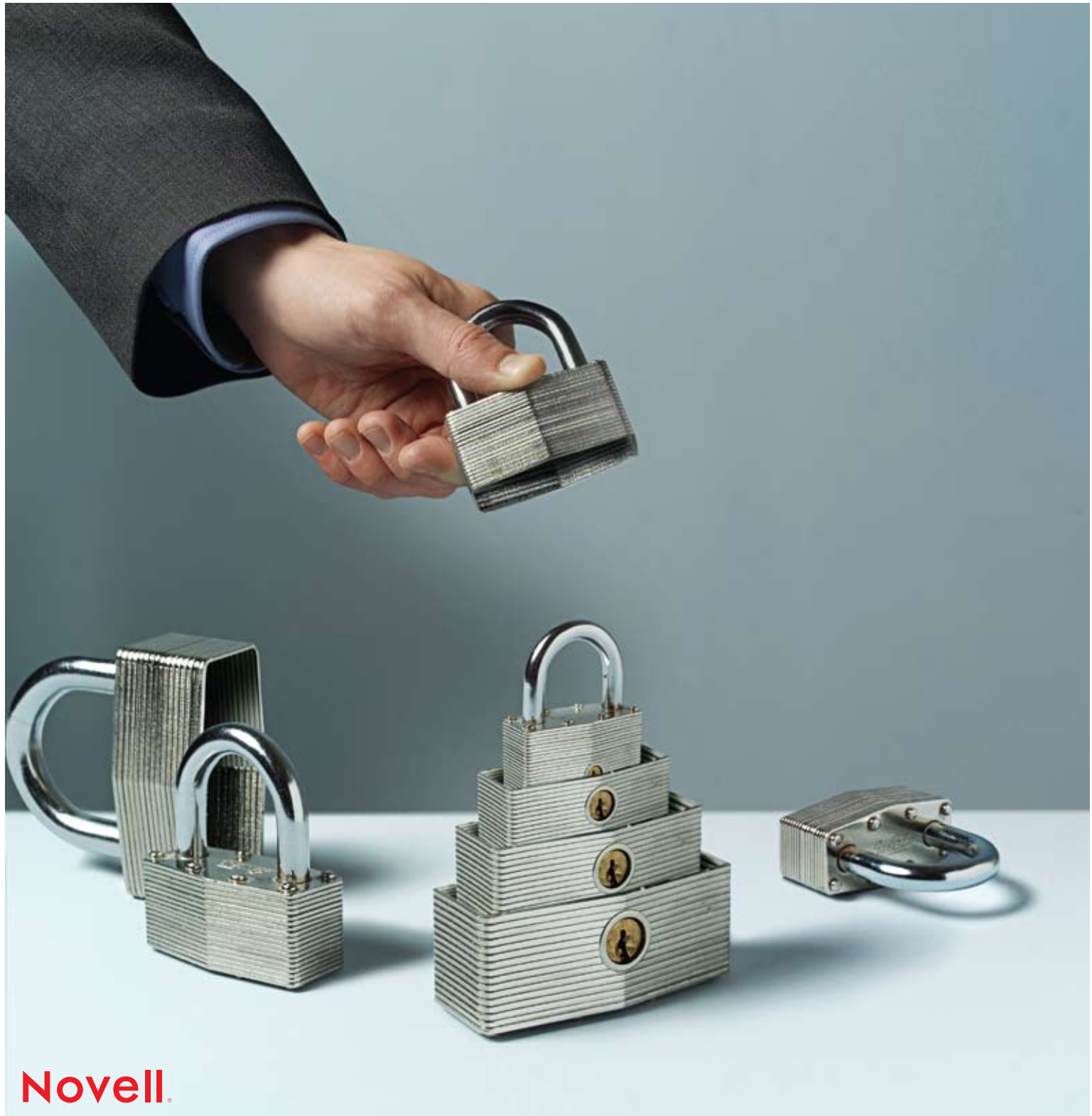


LÖSUNGEN FÜR IDENTITÄT UND SICHERHEIT

Aufbau einer sicheren Umgebung



Novell.

Zuverlässigkeit

Zuverlässigkeit ist das wichtigste Merkmal einer guten Identitäts- und Sicherheitsmanagementlösung. Mit der schriftlichen Niederlegung der Management- und Sicherheitsverfahren allein ist es nicht getan – Sie müssen die Gewissheit haben, dass Sie mit der gewählten Lösung wie gewohnt weiterarbeiten können, dass Richtlinien durchgesetzt und Vorschriften eingehalten werden. Das Ziel heißt „**Making IT Work As One**“ – die Vereinigung aller Komponenten zu einem harmonischen Ganzen.



novell.com/security

Integrierte Sicherheit

Die Novell Lösungen für Compliance-Management sowie Identitäts- und Zugriffsmanagement dienen der Verwaltung von Identitäten, der Automatisierung des Provisioning, der Verwaltung des Zugriffs auf Anwendungen sowie der Durchsetzung von Richtlinien und dem Nachweis ihrer Einhaltung. **Dabei achten wir insbesondere darauf, dass unsere Lösungen mit Ihren bestehenden Anwendungen und Betriebssystemen interoperabel sind und sich in diese integrieren lassen.**

Die Lösung Ihrer Probleme im Bereich Identität und Sicherheit ist unsere vordringlichste Aufgabe. Novell stellt zwei umfassende Lösungen bereit – eine für das Compliance-Management und eine für das Identitäts- und Zugriffsmanagement. Diese Lösungen bieten die folgenden Funktionen:

Compliance-Management

1. Compliance-Automatisierung und -Validierung
2. Zugangsregelung
3. Sicherheits- und Schwachstellenmanagement

Identitäts- und Zugriffsmanagement

1. Identitätslebenszyklus-Management: Benutzer-Provisioning
2. Identitätslebenszyklus-Management: Rollenmanagement
3. Identitätslebenszyklus-Management: Storage-Management
4. Zugriffsmanagement
5. Single Sign-on im Unternehmen
6. Passwortmanagement





COMPLIANCE-MANAGEMENT



Durchgängige Transparenz. Compliance-Management-Lösungen schöpfen das Potenzial der Infrastruktursoftware aus: Sie vereinfachen die Business Governance, verringern das Risiko und sorgen für Compliance im gesamten Unternehmen.

Unsere Technologien sorgen für die Prüfung und Durchsetzung von Aktivitäten zu Unternehmensrichtlinien und -prozessen. Dies senkt die Gefahr von Sicherheitslücken, verkürzt die Reaktionszeiten und erhöht die Transparenz von Compliance-Aufgaben. Mit den Compliance-Management-Lösungen von Novell können Kunden die Einhaltung interner und externer Richtlinien kosten- und ressourcenschonend nachweisen und die dadurch eingesparten Mittel in den Ausbau des Unternehmens investieren.

- 1. Szenario:**
Compliance-Automatisierung und -Validierung
- 2. Szenario:**
Zugangsregelung
- 3. Szenario:**
Sicherheits- und Schwachstellenmanagement

1

1. Szenario: Compliance-Automatisierung und -Validierung

In der komplexen Unternehmenswelt von heute ist die zentrale Überwachung von Zugriffsrechten eine echte Herausforderung. Wem hier der Überblick fehlt, kann nur mangelhaft über die Aktivitäten im Unternehmen berichten. Dies wiederum bedeutet, dass weder die Erfüllung von Compliance-Auflagen noch die Minimierung von Risiken möglich ist. Mit Novell Technologien überwachen Sie den Compliance- und Sicherheitsstatus in Echtzeit, sodass Sie schon bei den ersten Anzeichen von Verstößen Abhilfemaßnahmen ergreifen können – und nicht erst dann, wenn es bereits zu spät ist.

Situation des Kunden

Ein großer Finanzdienstleister in Asien muss den Zugriff auf seine Systeme und Daten rund um die Uhr an 365 Tagen im Jahr gewährleisten, ohne dabei gegen die zunehmende Zahl brancheninterner und behördlicher Auflagen zu verstoßen. In der IT-Umgebung des Unternehmens, die Linux-, UNIX-, Windows- und Mainframe-Betriebssysteme umfasst, gestaltete sich diese Aufgabe allerdings immer schwieriger. Aufgrund des hohen Datenvolumens konnten trotz eines gut besetzten Teams von Analysten nur besonders wichtige Systeme umfassend überwacht werden. Dass die Protokolldateien separat erfasst wurden, erschwerte überdies das Erstellen von Berichten für Auditoren und Prüfer.

Die Schwierigkeiten bei der Erfassung und Analyse der Daten zwangen das IT-Personal außerdem zu rein reaktivem Verhalten, wobei die Mitarbeiter zum Teil erst Monate nach dem Auftreten verdächtiger Ereignisse auf diese reagierten. Hinzu kam, dass die manuellen Prozesse der Erfassung und Analyse von Daten kostspielig und fehleranfällig waren und die schriftlich fixierten Sicherheitsrichtlinien des Unternehmens nicht konsequent eingehalten wurden.

Die Lösung

Das Unternehmen implementierte Funktionen für die Compliance-Automatisierung und -Validierung und erreichte so für Netzwerke jeder Größe eine zentralisierte Echtzeitüberwachung und Ereignisquellenverwaltung. Aufgrund der Komplexität der vorhandenen Systeme beschloss das Unternehmen, bei der Implementierung der neuen Novell Technologie mit einem zuverlässigen Novell Partner zusammenzuarbeiten. Dieser globale Consulting Systems Integrator (CSI) unterstützte das Unternehmen dabei, die Vorteile der Novell Produkte so effizient wie möglich zu nutzen.

Die Unternehmensleitung kann sich nun einen umfassenden Überblick über den Sicherheits- und Compliance-Status verschaffen, selbst in einer heterogenen IT-Umgebung mit weit verstreuten Netzwerkkomponenten. Unsere Software erfasst und korreliert Daten zu Sicherheitsereignissen aus dem gesamten Netzwerk und standardisiert

diese Daten, damit sie verarbeitet werden können. Anstatt sich mit Dutzenden von Protokollen in verschiedenen Formaten befassen zu müssen, arbeiten die Analysten des Unternehmens nun mit benutzerfreundlichen Protokollen in einem einheitlichen Format. Auf diese Weise konnte der Zeit- und Kostenaufwand, der mit dem Nachweis der Richtlinieneinhaltung verbunden ist, deutlich gesenkt werden.

Dank dieser Technologien wurde zudem die Flexibilität des Unternehmens erhöht. Bislang war es dem Unternehmen aufgrund der Komplexität der Systeme und der zu erfüllenden rechtlichen Auflagen nicht möglich, schnell auf Änderungen der Vorschriften oder auf neue Sicherheitsrisiken zu reagieren. Jetzt hingegen können IT-Administratoren über eine zentrale Konsole neue Richtlinien fast augenblicklich implementieren und ihre Durchsetzung automatisieren. Bei Erfassung einer Richtlinienverletzung oder Netzwerkbedrohung wird automatisch eine Benachrichtigung an den Administrator gesendet, und es werden vordefinierte, anpassbare Aktionen ausgeführt. Dabei werden alle Aktivitäten in einer zentralen Protokolldatei gespeichert, um den einfachen Zugriff und die problemlose Berichterstellung zu ermöglichen.

Die Einarbeitung der IT-Administratoren in die Überwachung und Verwaltung der Funktionen stellte das Unternehmen vor eine schwierige Aufgabe, da die Mitarbeiter an verschiedenen, über den Kontinent verstreuten Standorten beschäftigt waren. Hier halfen der Einsatz eines Novell Online-Schulungsleiters und die Technologie des virtuellen Klassenzimmers. Damit gelang es, alle IT-Mitarbeiter in einer einzigen Veranstaltung unabhängig von ihrem Standort effizient zu schulen. So sparte das Unternehmen während der Implementierung sowohl Zeit als auch Geld.

Mit Novell Technologie können IT-Administratoren nun proaktiv Probleme verhindern und bei Verstößen sofort eingreifen, ehe das Unternehmen Gefahren ausgesetzt wird. Wenn trotz allem ein Problem auftritt, ist der Dedicated Support Engineer des Unternehmens vor Ort zur Stelle und sorgt dafür, dass alles schnell wieder in die richtigen Bahnen gelenkt wird.



„Benutzeridentitäten lassen sich nun wesentlich einfacher verwalten, und vor allem können wir zuverlässig sicherstellen, dass ausscheidenden Mitarbeitern umgehend die Zugriffsrechte entzogen werden. Dank der Unterstützung von Novell sind wir jetzt in der Lage, unsere Assets zu schützen und das Identitätsmanagement zu vereinfachen.“

Walter Mondino
IT Security Manager
Grupo Arcor

2

2. Szenario: Zugangsregelung

Für komplexe Unternehmen kann sich die Regelung des Zugangs zu Daten als ziemlich mühselig erweisen. Benutzer müssen ihre Arbeit erledigen können, doch Rollen ändern sich häufig so schnell, dass die Gewährung von Zugriffsrechten mit immer größeren Risiken und Kosten verbunden ist. Wenn zeitaufwändige manuelle Prozesse die Sicherheitsrisiken in Ihrem Unternehmen erhöhen, heißt die Lösung Zugangsregelung. Mit der Novell Access Governance Suite werden fehleranfällige manuelle Verfahren überflüssig. Außerdem erleichtern Sie damit die Richtlinieneinhaltung und bringen die Kosten für das Zugriffsmanagement unter Kontrolle.

Situation des Kunden

Ein führender internationaler Finanzdienstleister hatte Mühe, sämtliche gesetzlichen Auflagen und branchenspezifischen Vorschriften wie SOX, PCI-DSS und Basel II einzuhalten. Gesucht wurde nach einer Methode, die fehleranfälligen manuellen Prozesse durch automatisierte Verfahren für das Zugriffsmanagement und den Nachweis der Richtlinieneinhaltung zu ersetzen. Das Unternehmen benötigte ein neues System für die Zugangszertifizierung und Compliance-Berichterstellung. Darüber hinaus waren bessere Prozesse für die Überprüfung und Bescheinigung von Funktionstrennungen zwischen Abteilungen erforderlich.

Automatisierung und Skalierbarkeit waren ebenfalls wichtige Faktoren, die bei der Entscheidung des Unternehmens für eine bestimmte Lösung eine Rolle spielten. Die Verantwortlichen erkannten, dass eine Automatisierung zur Durchführung verschiedener Aufgaben erforderlich war: erstens zur Beschränkung des Benutzerzugriffs auf die Daten, die jeder einzelne Benutzer tatsächlich im Rahmen seiner Aufgaben benötigt, zweitens, um Zugriffsverletzungen zu erkennen und zu verhindern, und drittens, um das gesamte System der Weiterentwicklung und dem Wachstum des Unternehmens entsprechend skalieren zu können.

Als Finanzdienstleister musste das Unternehmen seinen Kunden gegenüber nachweisen, dass ihre persönlichen Daten sicher aufbewahrt werden. Der Markenwert des Unternehmens war abhängig von seiner Fähigkeit, diese Informationen zu schützen und das Vertrauen der Kunden zu erhalten. Wäre es nicht gelungen, zugriffsbezogene Geschäftsrisiken zu mindern, hätte sich dies negativ auf den Ruf und den geschäftlichen Erfolg des Unternehmens ausgewirkt.

Die Lösung

Das Unternehmen entschied sich für die Implementierung einer Zugangsregelung im Rahmen einer breiter angelegten Compliance-Management-Lösung. Durch den Einsatz der Novell Access Governance Suite war es dem Unternehmen möglich, Zugriffsrichtlinien durchzusetzen, Zertifizierungsverfahren zu optimieren und die Einhaltung von Richtlinien nachzuweisen. Dank dieses umfassenden Produkts lässt sich nun ohne Weiteres feststellen, wer auf welche Informationen zugreifen kann und wer diesen Zugriff genehmigt hat. Die Novell Access Governance Suite umfasst ein automatisiertes Prüf- und Zertifizierungsverfahren für den Zugriff aller Benutzer. Zudem überprüft sie, ob Berechtigungen auch tatsächlich gewährt oder entzogen wurden.

Dank unserer Technologien kann der Finanzdienstleister nun den Benutzerzugriff zuverlässig verwalten, Kosten, Komplexität und Risiken verringern und dabei gleichzeitig die Einhaltung branchenspezifischer Richtlinien nachweisen. Um von Anfang an den optimalen Einsatz der neuen Technologien zu gewährleisten, entschied sich das Unternehmen für die Zusammenarbeit mit Novell Technical Training. Das Team von Novell Technical Training vereinbarte einen Termin mit der IT-Abteilung, verschaffte sich einen Überblick über die Situation und die Kenntnisse der Mitarbeiter und schulte das Personal im richtigen Umgang mit den neuen Produkten. Dank des neuen Systems kann sich das Unternehmen jetzt auf Projekte konzentrieren, die zur Weiterentwicklung und zum Wachstum beitragen. Benutzer erhalten ihrer Rolle entsprechend Zugriff auf die benötigten Informationen, während gleichzeitig für die Richtlinieneinhaltung gesorgt ist.

3

3. Szenario: Sicherheits- und Schwachstellenmanagement

Ihr Unternehmen ist sowohl externen als auch internen Bedrohungen ausgesetzt. Unsere Technologien ermöglichen Ihnen ein effektiveres Risikomanagement – unabhängig von der Quelle der Bedrohung. Novell ist ein führender Anbieter von Security Information and Event Management (SIEM) – einem Service für die lückenlose Überwachung der gesamten Unternehmensaktivität. Hierbei wird laufend überprüft, ob die einzelnen Aktivitäten normal oder ungewöhnlich und riskant sind. Die Kombination dieses Service mit den anderen Funktionen unserer Compliance Management-Lösungen gibt Ihnen die Gewissheit, dass Ihre Systeme sicher und richtlinienkonform sind.

Situation des Kunden

Ein bekannter europäischer Finanzmakler wollte Missbrauch und Betrug verhindern und sowohl die Kunden als auch das Unternehmen vor finanziellen Verlusten bewahren. Bei der Suche nach einer Compliance- und Sicherheitslösung stellte das Unternehmen jedoch fest, dass es diesen Lösungen in der Regel an Homogenität mangelte, wodurch das Security Information and Event Management (SIEM) noch komplizierter wurde. Hinzu kam, dass in der Branche immer mehr und immer komplexere Sicherheits- und Compliance-Auflagen zu erfüllen waren. So verlangen die Branchenvorschriften u. a., dass das Unternehmen die Sicherheit des Netzwerks und der gespeicherten Daten gewährleistet, zuverlässige Maßnahmen für das Zugriffsmanagement implementiert, Netzwerke regelmäßig überwacht und testet sowie umfassende Richtlinien zur Informationssicherheit durchsetzt.

Da das Unternehmen über Millionen von Kunden, Tausende von internen Benutzern und Hunderte von Anwendungen verfügt, war die Erstellung von Compliance-Berichten mit einem beträchtlichen Zeit- und Arbeitsaufwand verbunden. Compliance wurde auf Abteilungsebene geregelt, was ineffizient war und einen einheitlichen Ansatz und einheitliche Strategien für das gesamte Unternehmen unmöglich machte. Um Kosten und Aufwand für Compliance zu sparen und die Sicherheitsberichterstattung zu verbessern, benötigte das Unternehmen eine automatisierte, zentralisierte Ressource für die Überwachung und Verwaltung von Sicherheit, Informationen und Ereignissen.

Die Lösung

Durch den Einsatz von Novell Technologien zur Zentralisierung und Optimierung der Netzwerksicherheitsüberwachung und Berichterstattung stärkt das Unternehmen den Schutz vor unbefugten Zugriffen. Um die reibungslose und effiziente Implementierung und Verwaltung der neuen Novell Lösung sicherzustellen, suchte das Unternehmen die Unterstützung eines lokalen Novell Partners.

Novell ersetzte die manuelle, abteilungsinterne Überwachung verschiedener Netzwerkelemente durch eine automatisierte, unternehmensweite Softwarelösung für die Echtzeitüberwachung und Sicherheitsberichterstattung – gesteuert von einem einzigen zentralen Punkt. So verhilft Novell dem Unternehmen nicht nur zur Verbesserung von Sicherheitsstandards, sondern trägt darüber hinaus zur Verringerung der Kosten für Sicherheit und Compliance bei, da die Mitarbeiter der einzelnen Abteilungen keine Überwachungsaufgaben mehr wahrzunehmen haben.

Vor allem jedoch versetzte Novell das Unternehmen in die Lage, den Prozess der Sicherheitsberichterstattung zu vereinfachen und gleichzeitig die Genauigkeit der Informationen zu erhöhen. Das Unternehmen kann den Nachweis über die Einhaltung von Branchenrichtlinien nun deutlich leichter erbringen. Die Novell Lösung ist die einzige Technologie auf der Grundlage eines SIEM-Produkts, die eine Verwaltung der Reaktion auf Vorfälle ermöglicht. Damit werden die Nachverfolgung und Weitermeldung von Vorfällen und Richtlinienverstößen sowie die Reaktion darauf automatisiert und formalisiert, und zwar vom Augenblick des Auftretens bis zur Lösung. Neben der Fähigkeit zur wechselseitigen Integration in führende Problembereichsysteme bietet unsere Technologie außerdem Funktionen zur Überwachung von Systemaktivitäten zu Audit-Zwecken.

„Novell ist als einziger Anbieter in der Lage, den aktuellen Geschäftsanforderungen mit einer umfassenden Echtzeitlösung zur Einhaltung von Vorschriften gerecht zu werden. Bei dieser Lösung können Menschen, Systeme und Prozesse als Einheit zusammenarbeiten.“

Chris Christiansen
Program Vice President
Security Products and Services Group
IDC

„Dank der Lösung von Novell konnten wir unsere Sicherheits-Workflows optimieren und Zeit sparen, da die manuelle Überprüfung der Protokolldateien auf Hunderten von Systemen entfällt.“

Oliver Eckel
Head of Corporate Security
bwin International Ltd.



IDENTITÄTS- UND ZUGRIFFSMANAGEMENT

Jeder Klick lässt sich verfolgen. Lösungen für das Identitäts- und Zugriffsmanagement umfassen eine Reihe von Unternehmenstechnologien, mit denen sich geschäftsorientierte Prozesse zur Verwaltung der Sicherheit von Unternehmensanwendungen und -ressourcen und des Zugriffs darauf automatisieren lassen.

Wir bieten Lösungen für Identitätslebenszyklus-Management, Zugriffsmanagement, Single Sign-on im Unternehmen und Passwortmanagement. Mit diesen Lösungen verwalten Sie Ihre gesamte Identitätsinfrastruktur und regeln den Zugriff auf unternehmenskritische Anwendungen – sicher, einfach und kostengünstig.

- 1. Szenario:**
Identitätslebenszyklus-Management:
Benutzer-Provisioning
- 2. Szenario:**
Identitätslebenszyklus-Management:
Rollenmanagement
- 3. Szenario:**
Identitätslebenszyklus-Management:
Storage-Management
- 4. Szenario:**
Zugriffsmanagement
- 5. Szenario:**
Single Sign-on im Unternehmen
- 6. Szenario:**
Passwortmanagement



„Dank des automatisierten Benutzer-Provisioning mit Novell Identity Manager konnten wir den Zeit- und Arbeitsaufwand erheblich verringern. Außerdem kommt es jetzt zu weniger Verzögerungen für Benutzer.“

Henrik Jordt
Enterprise Architect
Central Denmark Region

1

1. Szenario: Identitätslebenszyklus-Management: Benutzer-Provisioning

Mit Novell Lösungen für das Identitäts- und Zugriffsmanagement können Sie die Zugriffsrechte für einzelne Benutzer vom Tag ihrer Einstellung bis zu ihrem Ausscheiden aus dem Unternehmen verwalten. Durch die richtige Kombination von Provisioning, De-Provisioning, Rollenmanagement und automatischen Richtlinien können Sie die Effizienz von Abläufen verbessern, die Produktivität steigern und die Risiken manueller Prozesse minimieren.

Situation des Kunden

Der Mutterkonzern eines großen internationalen Fertigungsunternehmens erweitert sein Portfolio regelmäßig durch neue Übernahmen, und das Fertigungsunternehmen selbst kooperiert mit zahlreichen Partnern innerhalb und außerhalb des Konzerns. Beide Faktoren tragen dazu bei, dass sich die Zusammensetzung der Benutzergruppe, die Zugriff auf eine Vielfalt unterschiedlicher Ressourcen benötigt, ständig ändert. Ohne eine standardisierte Lösung für das Identitätsmanagement kann das Unternehmen nur mit großem Aufwand sicherstellen, dass die richtigen Personen (ob Mitarbeiter, Partner oder Kunden) Zugriff auf die erforderlichen Ressourcen und Systeme erhalten.

Das Unternehmen stand vor der Aufgabe, den Prozess des Provisioning neuer Benutzer und der Zuweisung von Zugriffsrechten zu vereinfachen, ohne die Sicherheit zu gefährden. Das vorhandene Identitätsmanagementverfahren war ein manueller Prozess, bei dem das IT-Personal auf Anfrage der Bereichsleiter die Rechte für neue Benutzer einrichtete. Da klare, zentral verwaltete Sicherheitsrichtlinien fehlten, war es äußerst schwierig, Benutzeraktivitäten zu überwachen und die Einhaltung gesetzlicher Auflagen nachzuweisen.

Die Lösung

Das Unternehmen verschaffte sich mit Unterstützung von Novell Services einen Überblick über die aktuelle Infrastruktur. Sobald dem Unternehmen eine detaillierte Aufstellung der Assets vorlag, begann es gemeinsam mit einem preisgünstigen Offshore-CSI-Anbieter mit der Implementierung und Verwaltung der Technologie. Die Benutzer-Provisioning-Funktion – Teil eines umfassenderen Systems für das Identitätslebenszyklus-Management – verwaltet Benutzerinformationen über mehrere Systeme hinweg und schafft einen zentralen Kontrollpunkt für die Verwaltung des Zugriffs auf Unternehmensdaten und -anwendungen. Mithilfe von Benutzer-Provisioning lassen sich Benutzerkonten schneller und effizienter erstellen und löschen, woraus sich für das schnell wachsende Unternehmen zahlreiche Vorteile ergeben.

In der zweiten Lösungsphase delegierte das gemeinsame Team von CSI und Novell Services die Benutzerverwaltung aus der Verantwortung der IT-Experten an die Bereichsmanager. Qualifizierte IT-Mitarbeiter werden so entlastet und können sich auf strategisch wichtigere Projekte konzentrieren. Außerdem werden Abteilungsleiter durch Benutzer-Provisioning in die Lage versetzt, das Provisioning für die Benutzer in ihrem Arbeitsbereich selbst durchzuführen. Anstatt darauf warten zu müssen, dass IT-Mitarbeiter das Benutzer-Provisioning zentral für das gesamte Unternehmen vornehmen, können Bereichsmanager jetzt eigenständig Konten für neue Mitarbeiter oder neue Partnerbeziehungen einrichten. Dies führt zu einem deutlich schnelleren Benutzer-Provisioning und zur Erhöhung der Flexibilität und Reaktionsfähigkeit des Unternehmens.

Die nächste Phase des Prozesses bestand in der Erstellung von Workflows zur Automatisierung des Benutzer-Provisioning und des rollenbasierten Zugriffs auf Ressourcen. Wenn ein Manager ein neues Benutzerkonto über ein bestimmtes Profil einrichtet, stellt die Novell Lösung automatisch und reibungslos den Zugriff auf alle relevanten Ressourcen bereit. Der Entzug der Zugriffsrechte wird ebenfalls automatisiert. Hierdurch wird sichergestellt, dass vertrauliche Daten und Systeme nur befugten Benutzern zugänglich sind.

Durch Benutzer-Provisioning erhält das Unternehmen einen zentralen Steuerungspunkt für das Identitäts- und Zugriffsmanagement. Das Unternehmen ist nun in der Lage, Mitarbeiter, Partner und Kunden rasch und mit minimalem Verwaltungsaufwand mit den erforderlichen Systemen und Informationsressourcen zu verbinden. Manager können innerhalb kürzester Zeit Benutzerkonten in den eigenen Arbeitsbereichen erstellen, verwalten oder entfernen und damit sofort auf neue Geschäftsanforderungen reagieren.

2

2. Szenario: Identitätslebenszyklus-Management: Rollenmanagement

Der Erfolg Ihres Unternehmens hängt nicht zuletzt davon ab, dass Benutzer bei Bedarf auf alle erforderlichen Ressourcen zugreifen können. Da Novell Technologien auf den Rollen Ihrer Benutzer und Ihren Geschäftsrichtlinien aufbauen, können Sie sicher sein, dass Ihre Sicherheitsverfahren konsequent eingehalten werden. Die Funktionen des Identitätslebenszyklus-Management ermöglichen eine schnelle und konsistente Zuweisung von Zugriffsberechtigungen. Außerdem lassen sich sehr einfach Daten für den Compliance-Nachweis sammeln. Dies führt einerseits zu niedrigeren Verwaltungskosten und andererseits zu höherer Sicherheit und Produktivität.

Situation des Kunden

Über das IT-System eines Fertigungsunternehmens in den USA wird eine große Zahl von Mitarbeitern, Partnern und Lieferanten verwaltet, die allesamt Zugriff auf die Systeme des Unternehmens benötigen. Angesichts häufiger Änderungen der Benutzergruppe und erhöhter Anforderungen an das Identitäts- und Sicherheitsmanagement suchte das Unternehmen eine IT-Lösung, mit der Benutzern automatisch Rechte in Abhängigkeit von ihrer Rolle im System zugewiesen werden können. Außerdem sollte diese Lösung das Zugriffsmanagement sowie die Überwachung und Berichterstattung bei Sicherheitsvorfällen ermöglichen. Da eine zentralisierte Verwaltung im Unternehmen fehlte, mussten IT-Mitarbeiter das Provisioning manuell vornehmen. Dies war nicht nur kostspielig und zeitaufwändig, sondern setzte das gesamte Unternehmen einem erhöhten Risiko aus.

Die Lösung

Durch strengeres Rollenmanagement mithilfe der Funktionen des Identitätslebenszyklus-Managements erhielt das Unternehmen eine komplette, integrierte Lösung, mit der die Anforderungen an Sicherheit, Governance, Risikomanagement und Compliance erfüllt wurden – ohne zusätzlichen Arbeitsaufwand für die Benutzer. Aufgrund der Dynamik des Benutzerstamms musste das Unternehmen sicherstellen, dass das neue System den richtigen Benutzern die korrekten Zugriffsrechte gewähren würde. In direkter Zusammenarbeit mit Novell IT Consulting erfasste das Unternehmen die bereits verfügbaren Assets und ermittelte, wie sich die neue Lösung auf die vorhandenen Komponenten auswirken würde. Darüber hinaus stellte Novell gemeinsam mit dem Unternehmen sicher, dass das richtige Geschäftsprozessmodell verwendet wurde. Das Ergebnis dieser Zusammenarbeit war eine Novell Lösung, die genau auf die spezifischen Anforderungen des Unternehmens abgestimmt war.

Weil der Zugriff auf vertrauliche Informationen von der Benutzerrolle abhängt und weil System- und Überwachungstools Berichte zu Sicherheitsvorfällen in Echtzeit erstellen, sind die Systeme des Unternehmens nicht länger Sicherheitsrisiken ausgesetzt. Sind die Systeme des Unternehmens nicht länger Sicherheitsrisiken ausgesetzt, sind die Systeme des Unternehmens nicht länger Sicherheitsrisiken ausgesetzt. Das Unternehmen kann nun komplexe Provisioning-Prozesse automatisieren, was Benutzern den unmittelbaren – und angemessenen – Zugriff auf Ressourcen ermöglicht. Dank unserer Technologie kann das Unternehmen seinen Benutzern anhand von Rollen und Richtlinien die nötigen Ressourcen zuweisen. Neue Mitarbeiter und Partner erhalten gleich am ersten Arbeitstag Zugriff auf alle erforderlichen Ressourcen. Abteilungen können den Benutzerzugriff ihren eigenen Anforderungen entsprechend selbstständig verwalten, anstatt auf die Hilfe eines Netzwerkadministrators angewiesen zu sein. Wird einem Mitarbeiter eine andere Rolle zugewiesen, werden seine Zugriffsrechte automatisch aktualisiert. Beim Ausscheiden eines Mitarbeiters oder Zulieferers werden alle Zugriffsrechte in Echtzeit widerrufen. Dank des rollenbasierten Provisioning gehören Sicherheitsrisiken der Vergangenheit an, und das Unternehmen kann die Nutzung von Daten und Ressourcen problemlos verfolgen.

Darüber hinaus steht dem Unternehmen jetzt ein kostengünstiges Verfahren für den Nachweis der Einhaltung gesetzlicher Auflagen zur Verfügung. Ein weiterer Vorteil besteht in der optimierten Nutzung der vorhandenen IT-Hardware- und Softwareinvestitionen dank nahtloser Interoperabilität mit Windows, UNIX und Linux.

Der unbegrenzte Zugriff (rund um die Uhr an 365 Tagen im Jahr) auf das Novell Support Center sorgt dafür, dass alle technischen Fragen schnellstmöglich beantwortet werden. Außerdem kann das Unternehmen von einer weiteren wertvollen Ressource Gebrauch machen: einem Assigned Support Engineer (ASE). Der ASE befindet sich zwar nicht am Standort, ist jedoch mit der Implementierung vertraut und bestens für die Beantwortung der unternehmensspezifischen Fragen gerüstet. Durch das Rollenmanagement, das Teil einer umfassenderen Lösung für Identitäts- und Zugriffsmanagement ist, lässt sich zuverlässig sicherstellen, dass nur autorisierte Benutzer auf vertrauliche Daten und Systeme Zugriff haben.

„Die Mitarbeiter, Schüler und Eltern, die unseren großen und dynamischen Benutzerstamm bilden, verfügen alle über unterschiedliche Rechte für den Zugriff auf verschiedene Anwendungen in unserer IT-Umgebung. Bei unserem vorigen System waren für die manuelle Verwaltung und Sicherung von Benutzerkonten Hunderte von Mitarbeitern erforderlich. Gleichzeitig mussten wir den angemessenen Zugriff und die nötige Skalierbarkeit bei Änderungen der Benutzergruppe sicherstellen. Dank der Identitäts- und Sicherheitsmanagementlösungen von Novell ist es uns gelungen, unsere Identitätsinfrastruktur zu automatisieren.“

Ted Davis

Director of Enterprise Information Services
Fairfax County Public Schools



„Die Steuerung des Zugriffs auf vertrauliche Informationen und geistiges Eigentum ist für unser Unternehmen unerlässlich. Mit Novell schützen wir unsere Daten und sorgen gleichzeitig dafür, dass unsere Benutzer leicht auf die erforderlichen Informationen zugreifen können – unabhängig von ihrem Standort.“

Marguerite Whited

Enterprise Client Services Manager
Fairchild Semiconductor

3

3. Szenario: Identitätslebenszyklus-Management: Storage-Management

Jedes Unternehmen mit einem Netzwerk verfügt über Storage-Systeme, in denen alle Mitarbeiter – Endbenutzer, IT-Personal und Führungskräfte – ihre kritischen Dateien und Informationen ablegen. Selbst in unserer hoch technologisierten Welt kann sich Storage leider nicht selbst verwalten. Im Zentrum des Novell Ansatzes für das Storage-Management steht daher die Automatisierung des kompletten Lebenszyklus von Benutzer- und Gruppen-Storage über identitätsbasierte Richtlinien, die im Verzeichnis gespeichert werden.

Situation des Kunden

Einem wachsenden Schulbezirk in den USA standen nur begrenzte Personal- und Finanzressourcen für die Lösung der Probleme im Bereich Identitäts- und Storage-Management zur Verfügung. Im Bezirk waren mehr als 3.500 Schüler, Lehrer und Mitarbeiter über mehrere Schulstandorte verstreut. Erschwerend kam hinzu, dass unterschiedliche Systeme verwendet wurden. Daher mussten mehr als 3.000 Schülerkonten manuell eingerichtet, aktualisiert und verwaltet werden – ein Prozess, der mit einem hohen Zeit- und Verwaltungsaufwand verbunden war. Der Bezirk suchte eine Lösung zur Automatisierung der Verwaltung von Benutzeridentitäten und Storage-Anforderungen, um das Management insgesamt zu vereinfachen und unnötige IT-Kosten zu vermeiden.

Die Lösung

Um das Benutzer-Provisioning zu automatisieren, Benutzerinformationen im gesamten Unternehmen zu synchronisieren und Schülern, Lehrern und Mitarbeitern identitätsbasierte Storage-Funktionen bereitzustellen, entschieden sich die Bezirksverantwortlichen für den Einsatz der Novell Identitäts- und Zugriffsmanagementlösungen. Mit Novell eDirectory hatten sie bereits Erfahrungen gesammelt, und der Einsatz dieser Technologie sollte auf alle Systeme ausgeweitet werden. Dank eDirectory und weiterer Novell Technologien war es möglich, verteilte Systeme zu verbinden und im Handumdrehen neue Anwendungen in die Umgebung einzubinden.

Novell eDirectory lässt sich problemlos in das Schülerdatensystem des Bezirks integrieren und fungiert als zentrales Repository für Informationen zur Benutzeridentität. Außerdem synchronisiert Novell Identity Manager diese Benutzerinformationen automatisch über mehrere Anwendungen hinweg und automatisiert das Benutzerkonten-Provisioning. Eine manuelle Aktualisierung ist daher nicht länger erforderlich.

Ein weiterer Vorteil für Schüler und IT-Mitarbeiter besteht in der einfachen Verwaltung von elektronischen Schülerportfolios mit Novell Storage Manager. Wenn Schüler jetzt die Klasse wechseln oder Lehrer an eine neue Schule versetzt werden, ist der Zugriff auf die Daten weiterhin gewährleistet. Außerdem können Schüler von der Grundschule bis zum Schulabschluss einfach und sicher auf ihr ePortfolio zugreifen.

Die Nutzung von identitätsgesteuertem Storage gab dem Bezirk die Möglichkeit, den kompletten Lebenszyklus des Benutzer- und Gruppen-Storage über in Novell eDirectory gespeicherte Richtlinien zu automatisieren. Die jeweilige Storage-Aktion richtet sich nach der Benutzeridentität, den im Verzeichnis definierten Ereignissen und diesen Richtlinien. Wenn beispielsweise ein neuer Lehrer an einer bestimmten Schule eingestellt wird, entnimmt das Storage-System der Richtlinie für diesen Standort, wie viel Storage für ihn erstellt werden muss, welche Zugriffsrechte für gemeinsam genutzte Storage-Bereiche einzurichten sind und sogar, welche Dokumente am ersten Arbeitstag im Basisverzeichnis des Lehrers abgelegt werden sollen.

Die Bezirksverantwortlichen planen die Integration weiterer Anwendungen, z. B. der Bibliotheks- und Transportsysteme, um den Zeitaufwand für die Verwaltung weiter zu senken. Da routinemäßige Verwaltungsaufgaben wie Identitäts- und Storage-Management wegfallen, können die IT-Mitarbeiter mehr Zeit auf Aktivitäten mit höherem Wertschöpfungspotenzial verwenden, etwa auf die Anleitung im Umgang mit Computern im Unterricht.

4

4. Szenario: Zugriffsmanagement

Zur Einhaltung von Compliance-Standards müssen Sie stets darüber informiert sein, wer auf Ihre Systeme zugreift – selbst wenn Sie über eine heterogene Umgebung verfügen. Sie müssen kontinuierlich für den sicheren und möglichst unkomplizierten Zugriff auf Webanwendungen sorgen, und zwar auch für Mitarbeiter und Partner außerhalb der Firewall. Eine weitere wichtige Aufgabe ist die unternehmensweite intelligente Durchsetzung von Sicherheitsrichtlinien auf der Grundlage präziser Informationen.

Situation des Kunden

Ein Gesundheitsdienstleister in Südamerika ist auf besondere Leistungen spezialisiert. Im Gesundheitswesen ist der direkte, sichere Zugriff auf Daten die Voraussetzung für eine effiziente Patientenbetreuung. Aufgrund der zahlreichen verschiedenen Systeme mussten sich Ärzte und andere Mitarbeiter des Unternehmens viele unterschiedliche Benutzernamen und Passwörter für den Zugriff auf die Klinikapplikationen merken.

Ziel der Einrichtung war es, Benutzern die Verwendung der Technologielösungen zu erleichtern und dafür zu sorgen, dass die richtigen Personen schnell Zugang zu den richtigen Daten erhielten, wann immer nötig. Außerdem sollte auch Remotebenutzern bequemer und sicherer Zugriff bereitgestellt werden, unabhängig davon, wo sie sich befinden – an einem anderen Standort, in der Wohnung eines Patienten oder auf Reisen.

Die Lösung

Das Unternehmen prüfte die Lösungen verschiedener Softwareanbieter, bevor es sich für ein Novell System entschied. Um die Kosten zu senken, wollte man die Produkte selbst implementieren. Allerdings wurde Novell damit beauftragt, aus Gründen der Gütesicherung regelmäßig eine Qualitätsprüfung durchzuführen. Nach der Implementierung der Zugriffsmanagement-Technologie übertrug das Unternehmen Novell außerdem die Aufgabe, kundenspezifische Verbindungsschnittstellen zu entwickeln. Das Novell Custom Development-Team, Teil von Novell Services, entwickelte spezielle Identitätsmanagement-Verbindungsschnittstellen für das Unternehmen, um die Lösung exakt auf die besonderen Anforderungen abzustimmen.

Seit der Einrichtung des Portals gewährleisten die Novell Lösungen für Identitäts- und Zugriffsmanagement den sicheren, identitätsbasierten Zugriff auf das neue Portal. Dies wiederum gibt Benutzern die Möglichkeit, schnell auf eine Reihe von Anwendungen zuzugreifen, z. B. Klinikverwaltung, Finanzen, Kalender und eMail.

Dank des identitätsbasierten Portals kann das Unternehmen den Benutzern nun je nach Rolle und Verantwortungsbereich personalisierte Ansichten der Informationen bereitstellen. Dadurch verkürzt sich die Zeit des Zugriffs auf wichtige Informationen für Benutzer um fast 90 Prozent. Auch die Tatsache, dass jeder Mitarbeiter eine einzige Benutzer-ID und nur ein Passwort erhält, beschleunigt den Datenzugriff und führt außerdem zu einer Verringerung der passwortbezogenen Helpdeskanfragen um 80 Prozent. Die richtigen Personen haben nun jederzeit Zugriff auf alle erforderlichen Informationen, damit sie im Interesse der Patienten die bestmöglichen Entscheidungen treffen können.

Novell Lösungen ermöglichen den effektiven Einsatz des IT-Personals im Unternehmen und ebnen den Weg zu einer höheren Leistung bei gleichbleibendem Ressourcenaufwand. Ohne den umständlichen Prozess zur Anwendungsbereitstellung kann das IT-Personal das Unternehmen ganz einfach auf dem neuesten Stand halten.



„Angesichts der zahlreichen Anwendungen, die wir einsetzen, blieb uns nur Single Sign-on. Viele unserer Benutzer mussten sich bisher acht bis zwölf Passwörter merken. Jetzt sind fast alle Anwendungen über einen einzigen Benutzernamen und ein einziges Passwort zugänglich.“

John Jahne

Vice President für Network Services

Webster Bank

5

5. Szenario: Single Sign-on im Unternehmen

Fällt es Ihrer IT-Abteilung immer schwerer, sämtliche passwortbezogenen Anfragen zu bearbeiten? Leidet die Produktivität der Benutzer unter Problemen mit Passwörtern? Die Sekunden oder Minuten, die für die Anmeldung bei verschiedenen Systemen benötigt werden, scheinen auf den ersten Blick unerheblich. In der Summe können diese Augenblicke jedoch Stunden und Tage verlorener Produktivität bedeuten. In dieser Situation hilft Single Sign-on im Unternehmen.

Situation des Kunden

Eine Kreditgesellschaft mit Sitz in Asien stand vor der Herausforderung, die Sicherheit der Identitäten von Benutzern und Kunden möglichst kostengünstig zu gewährleisten. Ein unternehmensweites Audit ergab, dass eine gründliche Überholung des Identitätsmanagementsystems erforderlich war. Mitarbeiter, denen mehrere Identitäten in verschiedenen Formaten zugewiesen waren, verwendeten häufig bis zu acht Passwörter für den Zugriff auf Auftragserfassungs-, Kreditverwaltungs- und Finanzanwendungen. Das IT-Personal befürchtete, dass sich aus der Fragmentierung des Identitätsmanagementsystems große Sicherheitsrisiken für das Unternehmen ergeben könnten.

Außerdem sah das Unternehmen seinen Ruf als herausragender Serviceanbieter gefährdet. Kundendienstmitarbeiter verbrachten mehr Zeit mit der Bearbeitung von IT-Problemen als mit der Kundenbetreuung, und IT-Mitarbeiter widmeten etwa 20 Prozent ihrer Arbeitszeit der Behebung von Problemen beim Passwort- und Identitätsmanagement. Diese Zeit hätten sie sinnvoller auf echte strategische Initiativen verwenden können, z. B. auf das Management der Kundenbeziehungen.

Die Lösung

Um den Sicherheits- und Produktivitätsanforderungen gerecht zu werden, implementierte das Unternehmen in Form von Novell SecureLogin eine Identitätsmanagement- und Single Sign-on-Lösung von Novell. Dank Novell SecureLogin müssen sich die Benutzer des Unternehmens jetzt nur noch bei einer Anwendung anmelden, und dies geschieht bei der täglichen Anmeldung an der Workstation zu Beginn des Arbeitstags. Sind Benutzer einmal angemeldet, erkennt SecureLogin die Eingabe von Passwörtern und fragt, ob das betreffende Passwort für die nächste Anmeldung gespeichert werden soll. Stimmt der Benutzer zu, kümmert sich SecureLogin um alles Weitere, d. h., Benutzer sind nicht mehr gezwungen, sich mehrere Passwörter zu merken.

Dank dieses Prozesses erhalten Benutzer überall und jederzeit Single Sign-on-Zugriff auf Unternehmensressourcen in einer sicheren Umgebung. Das Unternehmen muss nicht länger eine für alle Unternehmensanwendungen gültige Anmeldung bereitstellen, sondern kann Benutzern eine einfache und effiziente Möglichkeit zum Erstellen eigener sicherer Passwörter an die Hand geben. Diese innovative Funktion verhilft dem Unternehmen nicht nur zur Senkung der Verwaltungskosten und Steigerung der Benutzerproduktivität, sondern außerdem zu einer deutlichen Erhöhung der Sicherheit und einer Verbesserung der Compliance.

In Verbindung mit Novell Identity Manager und als Teil der umfassenden Lösung für Identitäts- und Zugriffsmanagement ermöglicht es das unternehmensweite Single Sign-on den Benutzern, verloren gegangene oder vergessene Passwörter zurückzusetzen. Hierzu steht eine Self-Service-Funktion zur Verfügung. Darüber hinaus profitiert das IT-Team von einer Vereinfachung der Benutzerverwaltung. Das Team kann problemlos Zugriffsrechte für Anwendungen nach Benutzern oder Gruppen gewähren sowie Anzeige- und Bearbeitungsfunktionen für die einzelnen Benutzer festlegen.

Seit der Implementierung der Novell Lösungen erhielt das Unternehmen äußerst positives Feedback von Mitarbeitern, die sich für den Zugriff auf ihre Anwendungen nicht länger mehrere Passwörter merken müssen. Die Zahl der Passwörter pro Benutzer wurde von acht auf eins verringert. Dank unserer Produkte kann das Unternehmen den mit passwortbezogenen Problemen verbundenen Zeit- und Kostenaufwand reduzieren, während Produktivität und ROI steigen. Die Firma rechnet mit der Amortisierung der Investition in etwa 10 Monaten. Damit nicht genug: Im Folgejahr könnten sogar Einsparungen von bis zu 440.000 US-Dollar erzielt werden.

6

6. Szenario: Passwortmanagement

Mit den Ansprüchen an die Zuverlässigkeit wächst auch die Notwendigkeit strengerer Authentifizierungsanforderungen. Dies kann zu komplexeren Passwortrichtlinien führen, die von Benutzern eine häufigere Änderung der Passwörter verlangen. Wenn sich Benutzer zahlreiche Passwörter für viele verschiedene Anwendungen merken müssen, ist die Wahrscheinlichkeit hoch, dass sie mindestens eines davon vergessen. Werden Passwörter vergessen, resultiert dies in Produktivitätseinbußen und höheren Verwaltungskosten, da Benutzer sich an den Helpdesk wenden müssen, um die Passwörter zurücksetzen zu lassen. Mit Novell Technologien können IT-Abteilungen Passwortrichtlinien im gesamten Unternehmen durchsetzen, Benutzer mit Self-Service-Funktionen für das Passwortmanagement ausstatten, Kosten senken und die Produktivität steigern.

Situation des Kunden

In einem großen medizinischen Zentrum in Nordamerika traten Probleme bei der Anmeldung von Benutzern auf. Die Mitarbeiter mussten sich im Laufe des Tages bei mehreren Anwendungen anmelden, jedes Mal mit einem anderen Passwort. Da die Benutzer Schwierigkeiten hatten, sich alle Passwörter zu merken, stieg die Anzahl passwortbezogener Helpdeskanfragen auf monatlich über 800 an. Generische Anmeldungen hatten außerdem eine Verringerung der Systemsicherheit zur Folge, da der Internetzugriff und die Workstation-Nutzung nicht effektiv überwacht werden konnten. Von der Automatisierung des Identitäts- und Passwortmanagements erhoffte sich das IT-Personal neben der Verringerung des Zeitaufwands für die Verwaltung einen besseren Schutz vertraulicher Informationen.

Die Lösung

Die Verantwortlichen im Zentrum erkannten schnell, dass ein Upgrade der Systeme erforderlich war. Neue Funktionen für das Passwortmanagement sollten Benutzern Frustration ersparen und den Zeit- und Kostenaufwand für den Support verringern. Auch Produktivitätseinbußen sollten auf diese Weise minimiert werden, da Mitarbeiter in der Lage sein würden, Passwörter zurückzusetzen, ohne sich an den Helpdesk zu wenden.

Nach Einrichtung eines Auswahlgremiums zur Bewertung verschiedener Anbieter von Passwort- und Identitätsmanagementlösungen entschied sich das Zentrum für die Novell Identitäts- und Zugriffsmanagementlösungen, die Funktionen für das Passwortmanagement umfassen. Über das Komplettpaket aus Produkten und Services wird das Zentrum mit Technologie und Support aus einer Hand versorgt. Die Implementierung ermöglicht es dem Zentrum, Single Sign-on für Anwendungen bereitzustellen, was die Benutzerfreundlichkeit verbessert und zur Erhöhung der Sicherheit beiträgt. Dank des neuen Systems können Benutzer, die sich nicht mehr an ihr Passwort erinnern, dieses nun mithilfe des Passwort-Self-Service zurücksetzen.

Das Zentrum implementierte die Lösung auch, um Benutzerinformationen über Verzeichnisdienste hinweg verwalten zu können. So wurde z. B. aus dem Personalsystem die zentrale Datenbank für Informationen zur Benutzeridentität. Diese Implementierung eröffnete dem Zentrum die Möglichkeit, Personaländerungen automatisch an andere Systeme zu übermitteln. Eine manuelle Aktualisierung war nicht mehr erforderlich. Die manuellen Prozesse, die mit der Vergabe und dem Entzug von Zugriffsrechten verbunden waren, wurden abgeschafft. Neue Benutzerkonten können nun schnell und effizient eingerichtet werden. Das IT-Personal kann außerdem sofort nach dem Ausscheiden eines Mitarbeiters die Zugriffsrechte entziehen, um sowohl die Sicherheit des Netzwerks als auch die des Zugangs zu den 1.500 Kontrollpunkten für die kritische Infrastruktur zu gewährleisten.

Weiterhin ist das Zentrum in der Lage, Benutzern einfach und sicher Zugriff auf wichtige Netzwerkressourcen zu gewähren – von jedem Standort aus. Auf diese Weise können Mitarbeiter, die nicht vor Ort arbeiten oder auf Dienstreise sind, auf wichtige Daten zugreifen oder Informationen aktualisieren, ohne dass es im medizinischen Zentrum zu Verzögerungen oder Ausfällen kommt.

Mit den Passwortmanagementfunktionen der Novell Lösung und den maßgeschneiderten Vor-Ort-Schulungen für das IT-Personal ist es dem Zentrum gelungen, das Identitäts- und Passwortmanagement zu zentralisieren und zu automatisieren. Die IT-Mitarbeiter konnten den Zeitaufwand für das Benutzer-Provisioning um 60 Prozent senken und die Einrichtung neuer Benutzerkonten um 90 Prozent beschleunigen. Benutzer erhalten jetzt sicheren Single Sign-on-Zugriff auf Anwendungen, was nicht nur zur Erhöhung der Sicherheit, sondern auch zur Steigerung der Mitarbeiterproduktivität beiträgt. Durch die Automatisierung des Identitätsmanagements und die Schulung der Endbenutzer konnten sowohl die Zahl der Helpdeskanfragen als auch die damit verbundenen Kosten bereits um etwa 70 Prozent gesenkt werden. Die IT-Mitarbeiter sind nun in der Lage, sich Projekten mit höherem Wertschöpfungspotenzial zu widmen, anstatt sich mit routinemäßigen Verwaltungsaufgaben beschäftigen zu müssen.

„Wenn ein einheitliches Verfahren für den Zugriff auf das Netzwerk existiert, erhöht das die Sicherheit und verringert den Aufwand für Benutzer.“

Carl Vercio
WHS Program Manager
OSD

„Vor der Implementierung der Novell Lösung gab es zahllose unterschiedliche Methoden für das Benutzer-Provisioning. Wir hätten nie gedacht, dass wir diesen Prozess ohne eine deutliche Verstärkung unserer Personaldecke straffen könnten. Dank Novell verfügen wir jetzt über eine hochwertige und dennoch kostengünstige Lösung, die viele unserer Mitarbeiter entlastet, sodass sie sich anderen Projekten widmen können.“

Eric Leader
Chief Technology Architect
Catholic Healthcare West

Dank unserer Infrastruktursoftware und unseres Partnernetzwerks sind wir bei Novell in der Lage, heterogene IT-Umgebungen harmonisch miteinander zu verbinden, sodass Menschen und Technologien als Einheit zusammenarbeiten können.

Die meisten Unternehmen arbeiten mit heterogenen IT-Umgebungen. Diese Tatsache darf sich jedoch nicht negativ auf die Wettbewerbsfähigkeit auswirken. Wir unterstützen Unternehmen auf der ganzen Welt bei der Verwaltung heterogener IT-Umgebungen mit dem Ziel, Kosten, Komplexität und Risiken zu verringern. Ganz gleich, nach welcher Art von Lösung Sie suchen – Identität und Sicherheit, Data Center oder Enduser-Computing – bei uns finden Sie die richtigen Tools zur Ausschöpfung von Leistungspotenzialen und Nutzung von Geschäftschancen. „Making IT Work As One“ heißt das Rezept, mit dem wir auch Ihnen zum Erfolg verhelfen.

novell.com/security

Novell Making IT Work As One

Novell.

Novell GmbH |
Nördlicher Zubringer 9-11 |
40470 Düsseldorf |
Tel: +49-211-56 31-0 |
Fax: +49-211-56 31-250 |
www.novell.de

Novell GmbH |
Heiligenstädter Lände 27c |
A-1190 Wien |
Tel: +43-1-367 74 44 |
Fax: +43-1-367 74 44 20 |
www.novell.at

Novell (Schweiz) AG |
Leutschenbachstrasse 41 |
CH-8050 Zürich |
Tel: +41-43-299 78 00 |
Fax: +41-43-299 75 01 |
www.novell.ch