Business White Paper
IT-MANAGEMENT-SOFTWARE

www.novell.com

Schutz und Management Ihres Unternehmens: Ein integrierter Ansatz

Novell

Inhaltsverzeichnis:

Vereinfachung des Managements im gesamten Unternehmen

Viele IT-Administratoren betrachten Sicherheits- und Systemmanagement als separate Bereiche. Diese Unterscheidung besteht in den meisten IT-Abteilungen nach wie vor.

In Ihrem Unternehmen kommen unzählige Plattformen, Verzeichnisse, Systeme und Anwendungen zum Einsatz, die alle verwaltet und betreut werden müssen. Sie müssen für eine ordnungsgemäße Verwaltung dieser komplexen Infrastruktur sorgen, da Ihre wertvollen Ressourcen ansonsten im Laufe der Zeit erhöhten Verwaltungsaufwand und zusätzliche Kosten verursachen. Wenn Ihr Managementprogramm nicht umfassend genug ist, stellen ungeschützte Geräte womöglich sogar eine Sicherheitsbedrohung für Ihre gesamten Systeme dar.

Es stellt sich also die Frage, wie sich die einzelnen Managementaufgaben integrieren und automatisieren lassen und wie Sie gleichzeitig Herausforderungen hinsichtlich Governance, Risiko und Compliance (GRC) bewältigen können. Die Antwort ist die Novell Lösung für Sicherheits- und Systemmanagement. Hierbei handelt es sich um eine Lösung, die Sie beim Schutz und beim Management Ihres Unternehmens vom Desktop bis zum Rechenzentrum unterstützt. Von den Vorteilen in Form von niedrigeren Kosten, geringerer Systemkomplexität und minimiertem Risiko profitieren Sie fast umgehend.

Auf dem Papier ist die Erfolgsformel denkbar einfach:

Integration + richtliniengest. Automatisierung = Einfachheit

In der Praxis ist diese Formel zunächst nur schwer umzusetzen, doch genau hier kommt Novell ins Spiel. Wir realisieren dieses Konzept mithilfe eines gemeinsamen unternehmensweiten Richtlinienspeichers, der eine einheitliche Anwendung der Richtlinien gewährleistet. Darüber hinaus bieten wir eine Reihe richtliniengesteuerter Komponenten zur Automatisierung routinemäßiger Abläufe des Sicherheits- und Ressourcen-Managements.* Diese Komponenten sind vollständig integriert und unterstützen Ihre IT-Abteilung bei der Bewältigung von Management-Herausforderungen. Mit dieser Lösung sind Sie in der Lage, sich auf das Wesentliche zu konzentrieren – das Wachstum Ihres Unternehmens.

Entscheidung für Integration

Viele IT-Administratoren betrachten Sicherheits- und Systemmanagement als separate Bereiche. Das liegt vor allem daran, dass den beiden Bereichen unterschiedliche Aufgaben zugeteilt sind. Zum Systemmanagement gehören zum Beispiel die Nachverfolgung physischer Geräte, die Konfiguration und das Provisioning von Geräten, die Kontrolle von Softwarelizenzen, die Installation von Patches und die Implementierung von Upgrades. Das Sicherheitsmanagement umfasst u. a. Identitäts- und Zugriffsmanagement sowie den Schutz vor Bedrohungen, unbefugtem Zugriff und Malware.

Diese Unterscheidung besteht in den meisten IT-Abteilungen nach wie vor. Eine Gruppe von Mitarbeitern beschäftigt sich z. B. mit der Frage, wie Anwendung X auf Gerät Y bereitgestellt gestellt werden kann, während ein anderes Team vor dem Problem steht, welche Benutzer von Gerät Y Zugriff auf Anwendung X erhalten sollen.

Bei diesem zweigleisigen Ansatz werden die Abhängigkeiten zwischen Sicherheits- und Systemmanagement nicht berücksichtigt. In der folgenden Abbildung sind die komplexen Abhängigkeiten dargestellt:

* *Diese Komponenten sind am Ende dieses White Papers aufgeführt.*

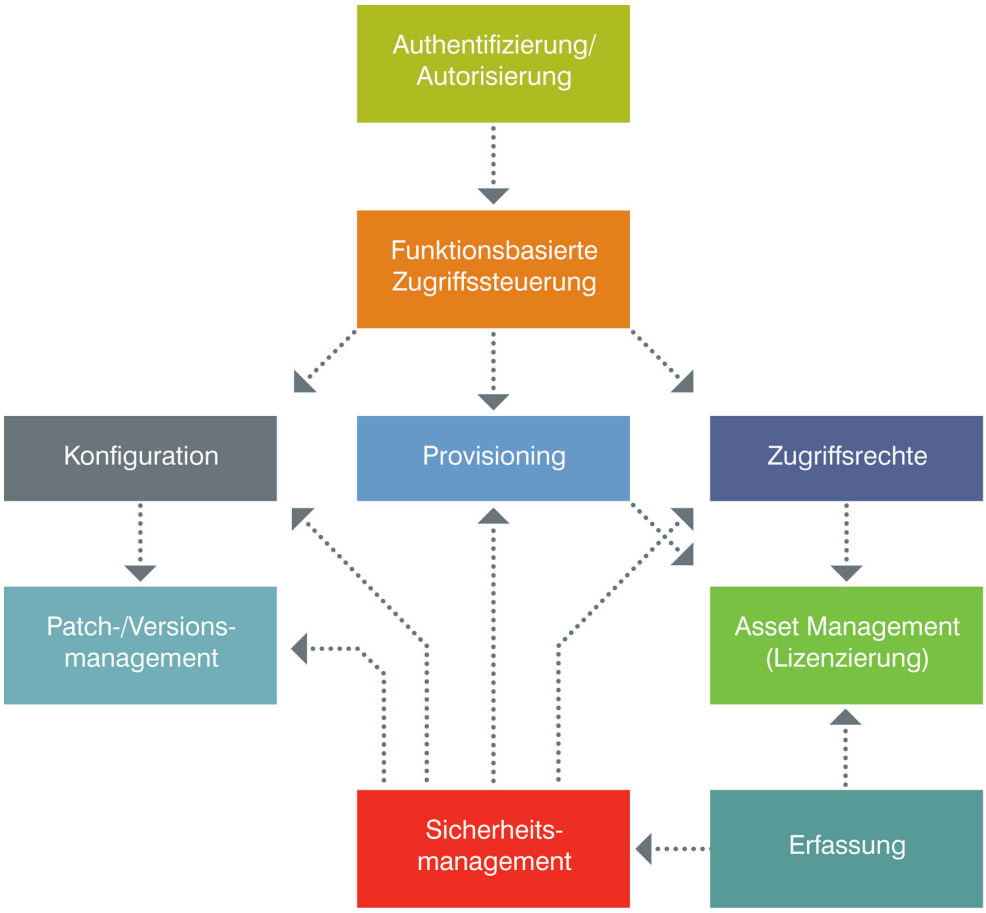

Abb. 1. *Sicherheits- und Systemmanagement wurden lange Zeit als separate Bereiche behandelt, doch wie aus dieser Abbildung hervorgeht, existieren zahlreiche Abhängigkeiten – was eindeutig für einen integrierten Ansatz spricht.*

In einem integrierten System wird ein Upgrade automatisch als Reaktion auf eine Sicherheitswarnung durchgeführt, wodurch die Systemsicherheit und die Produktivität aller Beteiligten gewährleistet werden.

Wenn wechselseitige Beziehungen nicht berücksichtigt werden, können Situationen eintreten, in denen viele Probleme nicht angegangen werden, weil die Zusammenarbeit zwischen den Sicherheits- und Systemmanagement-Teams nicht effektiv genug ist. Es könnte zum Beispiel passieren, dass das Sicherheitsmanagement-Team eine ungewöhnliche Aktivität – möglicherweise einen Sicherheitsverstoß – an einem Endgerät feststellt, jedoch nicht weiß, dass das Systemmanagement-Team ein Upgrade besitzt, mit dem ein solcher Sicherheitsverstoß unterbunden werden kann. Die Mitarbeiter des Systemmanagement-Teams wiederum verfügen über dieses Tool, haben es aber noch nicht implementiert, weil sie noch nicht über diese potenzielle Sicherheitsgefährdung informiert wurden. In einem integrierten System wird ein Upgrade automatisch als Reaktion auf eine Sicherheitswarnung durchgeführt, wodurch die Systemsicherheit und die Produktivität aller Beteiligten gewährleistet werden.

Hier ein weiteres Beispiel für die Effizienz eines integrierten Systems: Ein Sicherheitssystem erfasst einen Benutzer, der versucht, ohne entsprechende Zugriffsberechtigung sensitive Daten abzurufen. In diesem Fall würden die Zugriffsrechte des Benutzers den Unternehmensrichtlinien gemäß automatisch einer internen Prüfung unterzogen.

Identitäts- und Systemmanagement von Novell bietet eine umfassende Lösung für Herausforderungen im Bereich Governance, Risk und Compliance (GRC).

Identitätsgesteuertes Sicherheits- und Ressourcen-Management verringert den Arbeitsaufwand Ihrer IT-Mitarbeiter, die sich somit auf strategisch wichtigere Aspekte konzentrieren können.

Umsetzung des Potenzials richtliniengesteuerter Automatisierung

Der Mangel an integrierten Programmen für Sicherheits- und Systemmanagement ist nicht die einzige Herausforderung, mit der sich Ihr Unternehmen konfrontiert sieht. Ihre IT-Abteilung wendet womöglich wertvolle Ressourcen für zeitintensive Prozesse auf, die sich mit einer identitätsbasierten Sicherheits- und Systemmanagementlösung problemlos automatisieren ließen.

Der Transfer eines Benutzers in eine neue Gruppe ist ein typisches Beispiel. Wenn Benutzer neue Zugriffsrechte und eine neue Arbeitsplatzlizenz erhalten, werden ihnen häufig die alten Rechte entzogen. Da das Sicherheitsmanagement-Team den Entzug der alten Zugriffsrechte, das Systemmanagement-Team jedoch die Erteilung einer neuen Lizenz abwickelt, ist für die Einrichtung von Benutzerkonten für neue Gruppenmitglieder ein eMail-Austausch zwischen dem Gruppenleiter und zwei verschiedenen IT-Abteilungen erforderlich. Doch dabei bleibt es nicht: Beim Transfer von Benutzern müssen oftmals auch höhere Entscheidungsebenen bei der Genehmigung von Zugriffsrechten oder Lizenzen einbezogen werden. Möglicherweise muss ein Administrator die Zugriffsliste manuell ändern und die Arbeitsplatzlizenz aktivieren, was zusätzlichen Zeitaufwand bedeutet (neben Verzögerungen, die auftreten, wenn der für die Genehmigung zuständige Abteilungsleiter zu beschäftigt oder nicht anwesend ist).

Diese kostspieligen manuellen Prozesse können durch die Integration von Sicherheits- und Systemmanagement umgangen werden. Wenn ein Mitarbeiter in eine andere Abteilung wechselt, braucht der neue Abteilungsleiter lediglich eine entsprechende Anfrage über das Unternehmensportal zu stellen, wodurch eine Workflow-Sequenz gestartet wird – und der Mitarbeiter kann fast ohne Verzögerung produktiv eingesetzt werden.

Governance, Risk und Compliance

Identitäts- und Systemmanagement von Novell bietet eine umfassende Lösung für Herausforderungen im Bereich Governance, Risk und Compliance (GRC):

- **Governance obliegt nunmehr den Personen, die die Anforderungen ihrer Mitarbeiter kennen.** *Unternehmensrichtlinien werden nicht mehr anhand von Softwareparametern, sondern auf der Grundlage von Unternehmenszielen erstellt.*
- **Das Risiko wird verringert.** *Mit automatisierten Workflows werden keine Arbeitsschritte ausgelassen, und alle Ressourcen sind sicher und zugänglich. Unzufriedene Mitarbeiter können keine Systemschäden verursachen, nur weil ihnen der Zugriff auf eine Datenbank versehentlich nicht entzogen wurde.*
- **Unternehmensrichtlinien und rechtliche Vorschriften werden eingehalten.** *Dank automatisierten Richtlinien und Berichten wird Compliance durch eine Reihe von Prozessen erreicht, die einfach zu implementieren und nachzuverfolgen sind.*

Governance

Mit dem richtigen Governance-System können Sie das IT-Management vereinfachen und die Gesamtkosten senken.

Verringerung des IT-Verwaltungs- und Wartungsaufwands

Identitätsgesteuertes Sicherheits- und Ressourcen-Management verringert den Arbeitsaufwand Ihrer IT-Mitarbeiter, die sich somit auf strategisch wichtigere Aspekte konzentrieren können. Wenn die Zugriffsrechte den Unternehmensrichtlinien gemäß zugewiesen werden, ist die Governance nicht länger von eingeschränkten Softwarefunktionen abhängig. Einzelne Geschäftseinheiten können selbst darüber entscheiden, welche Benutzer Zugriff auf welche Ressourcen erhalten, sodass sich die IT-Abteilung ihrer eigentlichen Aufgabe widmen kann: der Implementierung.

Da die Zugriffsrechte beim identitätsgesteuerten Sicherheits- und Ressourcen-Management auf der Grundlage von Richtlinien zugewiesen werden können, lässt sich der Verteilungsprozess automatisieren

(wobei auch halbautomatisierte oder manuelle Workflows möglich sind). Auf diese Weise werden viele zeitintensive und fehleranfällige manuelle Prozesse umgangen. Mit integriertem Sicherheits- und Systemmanagement lassen sich die richtigen Images und Funktionen über Workflows auf den richtigen Desktops, Notebooks oder mobilen Geräten bereitstellen. Außerdem weist ein integriertes System den Benutzern die Zugriffsrechte zu, was eine weitere Verringerung des Arbeitsaufwands bedeutet. Dies alles führt zu höherer IT-Effizienz und größerer Benutzerfreundlichkeit.

Zur weiteren Vereinfachung der Verwaltungsprozesse ist eine Übernahmefunktion verfügbar, mit der bestimmte Ressourcen und Rechte allen Mitarbeitern einer bestimmten Arbeitsgruppe oder Geschäftseinheit zugewiesen werden.

Kostensenkungen

Die Automatisierung manueller Arbeitsabläufe macht sich unmittelbar in Form von Kosteneinsparungen für IT-Abteilungen bemerkbar, da die Bereitstellung des richtigen Computers und die Zuweisung der richtigen Zugriffsrechte weniger Zeit im Anspruch nimmt.

Auch der verbesserte Überblick über die Ressourcenauslastung, vor allem über die Nutzung von Softwarelizenzen, verhilft Ihrem Unternehmen zu Einsparungen. Dank Berichten, mit deren Hilfe Daten zur Lizenzierung, Installation und Nutzung an einem Ort zusammengefasst werden, und detaillierten Daten zu Desktops, Servern und anderen Netzwerkressourcen haben IT-Manager die Möglichkeit, Lizenzen an individuelle Anforderungen anzupassen und auf diese Weise Ausgaben für nicht genutzte Softwarelizenzen zu vermeiden.

Kosten für das Passwortmanagement lassen sich mithilfe identitätsgesteuerten Sicherheits- und Ressourcen-Managements senken. Durch eine Kombination aus Single Sign-on (geringere Wahrscheinlichkeit, dass Benutzer ihre Passwörter vergessen) und Self-Service (Benutzer können ihre Passwörter selbst zurücksetzen) wird außerdem die Anzahl von Helpdesk-Anfragen zu Passwortrücksetzungen um 30–90 Prozent verringert.

Risiko

Moderne Unternehmen wollen keine unnötigen Risiken eingehen. Darum entscheiden sich viele für identitätsgesteuertes Sicherheits- und Ressourcen-Management.

Besseres Risikomanagement

Die Sicherheit spielt beim Risikomanagement eine entscheidende Rolle, wobei der Schutz vertraulicher Daten und die Verhinderung der Ausnutzung von Schwachstellen zu den größten Herausforderungen gehören. Identitätsgesteuertes Sicherheits- und Ressourcen-Management ist eine wirksame Waffe im Kampf gegen Datenmissbrauch aufgrund von Sicherheitsverstößen.

Beim identitätsgesteuerten Sicherheits- und Ressourcen-Management wird automatisch sichergestellt, dass ausschließlich autorisierte Personen Zugriff auf vertrauliche Daten, Anwendungen und andere Ressourcen erhalten.

Außerdem haben Sie die Möglichkeit, das Risikomanagement mithilfe integrierter Sicherheits- und Ereignisüberwachung zu verbessern. Sie können sämtliche sicherheitsrelevante Daten, die ununterbrochen von Netzwerkgeräten generiert werden, zusammenführen und korrelieren, eine integrierte Echtzeit-Ansicht zum Netzwerkstatus abrufen und automatisierte Reaktionen anderer Systemkomponenten einrichten, z. B. das De-Provisioning eines Kontos oder das Aktualisieren von Software.

Und zu guter Letzt lassen sich mit identitätsgesteuertem Systemmanagement Sicherheitslücken schließen. Es ermöglicht die Deaktivierung ungenutzter Software- und Hardwareressourcen und den Schutz der zahlreichen Netzwerkendgeräte. Endpoint Security Management schützt Daten durch festplattenübergreifende Datenverschlüsselung für Notebooks und verhindert, dass Benutzer vertrauliche Daten auf USB- oder Bluetooth-Speichergeräte übertragen.

Compliance

Die Sicherheit Ihrer Systeme muss nachweisbar sein, und darum benötigen Sie identitätsbasiertes Sicherheits- und Systemmanagement.

Die Automatisierung manueller Arbeitsabläufe macht sich unmittelbar in Form von Kosteneinsparungen für IT-Abteilungen bemerkbar, da die Bereitstellung des richtigen Computers und die Zuweisung der richtigen Zugriffsrechte weniger Zeit im Anspruch nimmt.

Identitätsbasiertes Sicherheits- und Systemmanagement stellt eine integrierte, automatisierte und sichere Lösung für die routinemäßige Verwaltung Ihrer IT-Ressourcen dar. Es bietet Zuverlässigkeit, Flexibilität und Skalierbarkeit für die IT-Abteilung, ganze Geschäftseinheiten und individuelle Benutzer.

Verbesserung der Compliance

Die Einhaltung rechtlicher Vorschriften zur Sicherheit umfasst zwei Komponenten:

- *Implementierung von Sicherheitsrichtlinien und -abläufen wie Zugriffssteuerung, integrierte Sicherheits-/Ereignisüberwachung und Endpoint Security Management.*
- *Dokumentierter Nachweis darüber, dass das Unternehmen die erforderlichen Richtlinien und Abläufe einhält*

Wenn Zugriffsanforderungen und andere Sicherheitsangelegenheiten per eMail erledigt werden, ist es außerordentlich schwierig, Compliance nachzuweisen und die Abläufe zu dokumentieren. Durch automatisierte Sicherheitsabläufe mit einer zentralisierten, richtliniengesteuerten Engine sind Sie hingegen in der Lage, Mitarbeiter und Ressourcen nachzuverfolgen, die konsequente Durchsetzung von Gesetzen und Vorschriften wie HIPAA und SOX zu gewährleisten sowie Abläufe lückenlos zu dokumentieren.

Zusätzliche Vorteile

Es gibt viele weitere gute Gründe für die Implementierung eines identitätsbasierten Sicherheits- und Systemmanagements.

Höhere Benutzerproduktivität

Manuelles Provisioning und mangelhafte Integration können zu Ausfallzeiten und damit zu kleineren Gewinnspannen führen. Ihr Unternehmen muss sicherstellen, dass Benutzer schnellen und ununterbrochenen Zugriff auf die benötigten Daten und Funktionen haben. Automatisiertes Provisioning und Single Sign-on (SSO) tragen zu einer Steigerung der Benutzerproduktivität bei.

Automatisierte Verwaltung des Rechenzentrums

Ein erfolgreiches Systemmanagement schafft die Voraussetzung für die größere Verbreitung virtueller Computer und eine ressourcensparende Arbeitsweise. Bei einer automatisierten Verwaltung des Rechenzentrums lassen sich physische und virtuelle Computer je nach Bedarf neu konfigurieren. Server können beispielsweise so konfiguriert werden, dass sie am Monatsende die Anforderungen eines Finanzsystems bewältigen oder während einer Vertriebspromotion überdurchschnittlich hohen Netzwerkverkehr abwickeln.

System- und prozessübergreifende Konsistenz

Zu den Hauptvorteilen von Information Technology Infrastructure Library (ITIL) gehört, dass es prozessübergreifende Konsistenz ermöglicht. Bei ITIL handelt es sich um eine Sammlung von Best Practices für IT-Management in 11 Funktionsbereichen: Helpdesks, Anfragen, Probleme, Änderungen, Konfiguration, Releases, Verfügbarkeit, Kapazität, Finanzen, Service Level Agreements (SLAs) und Kontinuität.
Mit der Bindung des identitätsgesteuerten Sicherheits- und Ressourcen-Managements an die ITIL-Standards wird die optimale Leistung Ihrer IT-Ressourcen gewährleistet.

Identitätsbasiertes Sicherheits- und Systemmanagement stellt eine integrierte, automatisierte und sichere Lösung für die routinemäßige Verwaltung Ihrer IT-Ressourcen dar. Es bietet Zuverlässigkeit, Flexibilität und Skalierbarkeit für die IT-Abteilung, ganze Geschäftseinheiten und individuelle Benutzer. Identitätsgesteuertes Sicherheits- und Ressourcen-Management muss nicht in einer einzigen, groß angelegten Initiative implementiert werden – dies ist auch in kleinen, überschaubaren Schritten möglich. Im folgenden Abschnitt geht es um die Funktionen, die für den Erfolg in den einzelnen Funktionsbereichen ausschlaggebend sind.

Einsatz von Schlüsselfunktionen

Wir sind uns der Tatsache bewusst, dass viele Unternehmen bereits einige dieser Funktionen verwenden. Unsere eigenen Angebote basieren jedoch auf offenen Standards und sind mit Web-Services-Funktionen kompatibel. Deshalb lassen sich Novell Produkte problemlos in vorhandene Tools und Systeme integrieren. Doch unabhängig von den Systemen, die in Ihrem Unternehmen derzeit zum Einsatz kommen, spielen die folgenden Funktionen für Ihren Erfolg eine entscheidende Rolle.

Erfassen

Erfassung/Asset Management

Das IT-Team kann kein Gerät verwalten, von dessen Existenz es nichts weiß. Durch den Überblick über Ressourcen und vor allem lizenzierte Anwendungen sind Benutzer in der Lage, bessere Entscheidungen bezüglich Lizenzierungsanforderungen zu treffen und somit erhebliche Kosteneinsparungen zu erzielen. Der erste Schritt bei der Verbesserung des Sicherheits- und Systemmanagements besteht darin, die Systeme im Netzwerk zu erfassen, die geschützt und verwaltet werden müssen. Zu den wichtigsten Funktionen im Bereich Erfassung/Asset Management gehören:

- *Automatische Erkennung und Erfassung von Netzwerkgeräten*
- *Routinemäßige Erfassung von Anwendungen*
- *Erkennung von Anwendungssuiten*
- *Ununterbrochener Überblick über Computer-Images und Anwendungsversionen*
- *Import von Lizenz- und Kaufdaten für den Softwareabgleich*

Verwalten

Konfigurationsmanagement

In einem optimierten System ist die gerätespezifische Anwendungsbereitstellung in das Provisioning von Zugriffsrechten integriert. Zu den wichtigsten Funktionen im Bereich Konfigurationsmanagement gehören:

- *Änderungskontrolle für Remote-Management und Implementierung von Anwendungs-Updates*
- *Patchkontrolle für Remote-Management von Sicherheitspatches*
- *Integration in Sicherheitsüberwachungssysteme zur Aktivierung automatischer Reaktionen auf Sicherheitslücken*

Bereitstellen

Zentralisierte Richtlinien-Engine

Eine zentralisierte Engine sorgt für unternehmensweite Konsistenz und Verringerung des IT-Arbeitsaufwands. Zu den wichtigsten Funktionen im Bereich der zentralisierten Richtlinien-Engine gehören:

Durch den Überblick über Ressourcen und vor allem lizenzierte Anwendungen sind Sie in der Lage, bessere Entscheidungen bezüglich Lizenzierungsanforderungen zu treffen und somit erhebliche Kosteneinsparungen zu erzielen.

- *Verknüpfung von Zugriffsrechten mit Benutzerfunktionen (wie von Geschäftseinheiten definiert)*
- *Dynamische Zuweisung und automatische Modifizierung von Zugriffsrechten auf der Grundlage geänderter Benutzerfunktionen*
- *Automatische, manuelle oder gemischte Zuweisung von Funktionen und Rechten*
- *Gliederung der Berichte nach Funktionen, mit Funktionen verknüpften Rechten und mit Benutzern verknüpften Funktionen*

Integrierter Identitätsspeicher

Wenn mehrere Datenquellen vorhanden sind, greift Novell auf autorisierte Quellen zurück und trägt so zur Vermeidung politischer Konflikte bezüglich des Dateneigentums bei. Die meisten Systeme verwenden einen sogenannten „Last-Commit“-Ansatz, d. h. kritische Daten werden jeweils von der Quelle kontrolliert, die zuletzt einen Eintrag in die Datenbank vorgenommen hat. Bei Verwendung einer autorisierten Quelle hingegen können Daten ausschließlich über eine einzige Quelle geändert werden. Auf diese Weise wird sichergestellt, dass Datenverantwortliche und -eigentümer sich auf die Fehlerfreiheit ihrer Daten verlassen können. Zu den Schlüsselfunktionen im Bereich des integrierten Identitätsspeichers gehören:

- *Konnektivität mit mehreren Datenspeichern und somit Gesamtansicht eines Benutzers*
- *Verwendung einer autorisierten Quelle zur Vermeidung von Konflikten bezüglich des Dateneigentums*
- *Bidirektionale Verbindung mit Systemen (sodass Geschäftsabläufe integriert werden und IT-Abteilungen bei der Festlegung autorisierter Datenquellen flexibel agieren können)*

Bei Verwendung einer autorisierten Quelle können Daten ausschließlich über eine einzige Quelle geändert werden. Auf diese Weise wird sichergestellt, dass Datenverantwortliche und -eigentümer sich auf die Fehlerfreiheit ihrer Daten verlassen können.

Compliance-Auditing spielt bei der alltäglichen IT-Verwaltung eine immer wichtigere Rolle. Daher sind Funktionen zur Einhaltung rechtlicher Vorschriften und Erleichterung der Compliance unverzichtbar.

- *Echtzeit-Erkennung und -Reaktion als Voraussetzung für einen präventiven Ansatz bei Sicherheitsfragen*
- *Ermittlung von Richtlinienverstößen bei der nicht autorisierten Verwendung zweier oder mehrerer Systeme durch einen Benutzer*
- *Umfassende Durchsetzung von Unternehmensrichtlinien, auch für Super-Administratoren und andere vertrauenswürdige Benutzer*

Passwortmanagement

Unternehmensweites Passwortmanagement ist die Voraussetzung für die Implementierung eines Single Sign-on-Systems. Zu den Schlüsselfunktionen im Bereich Passwortmanagement gehören:

- *Self-Service für Benutzer über das Internet, ohne Anmeldung beim Netzwerk*
- *Implementierung unternehmensweit gültiger Passwortrichtlinien*
- *Unternehmensweite Passwortsynchronisierung (einschließlich älterer Systeme)*
- *Single Sign-on mit erweiterten Authentifizierungsoptionen wie Biometrie, Smartcards und Token*

Workflow

Ein effizienter und benutzerfreundlicher Workflow, bei dem alle Abläufe so weit wie möglich automatisiert sind (und dennoch manuelle Eingriffe erlaubt sind) führt zu einer signifikanten Steigerung der Produktivität und senkt den IT-Verwaltungsaufwand merklich. Zu den Schlüsselfunktionen im Bereich Workflow gehören:

- *Benutzerfreundliche Designtools für die Erstellung und Verwaltung von Workflow-Anfragen*
- *Detailliertes, automatisiertes Dokumentationstool*
- *Dynamisches Routing von Workflow und Genehmigungen an die richtigen Funktionen/Personen auf der Grundlage bestimmter Unternehmensdaten*
- *Möglichkeit zur Delegierung der Genehmigungsautorität*
- *Automatische Eskalation von Anfragen an einen alternativen Genehmiger (bei Zeitüberschreitung)*
- *Integrierte Verwaltungskonsole für das Identitäts- und Zugriffsmanagement*

Zugriff

Zugriffsmanagement

Ein technisch ausgereiftes Zugriffsmanagement ist für die Senkung des Sicherheitsrisikos und die Einhaltung rechtlicher Vorschriften unerlässlich. Zu den Schlüsselfunktionen im Bereich Zugriffsmanagement gehören:

- *Web- und clientbasiertes Single Sign-on*
- *Endgerät-Authentifizierung für Desktops, Notebooks und mobile Geräte*
- *Federated Provisioning für interne und externe Partner*
- *Einhaltung branchenüblicher/offener Standards*
- *Schutz privater Benutzerdaten*
- *Sichere Abläufe zur Übermittlung von Änderungen an Zugriffsrechten über das Internet*
- *Berichte zu Ereignissen und Änderungen im Zusammenhang mit Benutzerrechten*

Sicherheit

Sicherheitsmanagement

Trotz verfügbarer Sicherheitsdaten besteht für Sie die Herausforderung darin, diese Daten auszuwerten und effektiv auf die damit verbundenen Bedrohungen zu reagieren. Zu den Schlüsselfunktionen im Bereich Sicherheitsmanagement gehören:

- *Aggregation von Daten aus unterschiedlichen Quellen*
- *Datenkorrelation auf der Grundlage von Zeit, Ort, Benutzer, Gruppe und Prozess oder komplexeren Beziehungen*
- *Vorgefertigte und individuell anpassbare Berichterstellung*
- *Ereignisbasiertes Design*
- *Automatisierte Reaktionen auf Sicherheitslücken*

Compliance, Dashboard, Berichte und Auditing

Compliance-Auditing spielt bei der alltäglichen IT-Verwaltung eine immer wichtigere Rolle. Daher sind Funktionen zur Einhaltung rechtlicher Vorschriften und Erleichterung der Compliance unverzichtbar. Zu den Schlüsselfunktionen des Bereichs Compliance, Dashboard, Berichte und Auditing gehören:

- *Aktive Dashboards, die den Compliance- und Risikostatus anzeigen*

- *Schwerpunkt auf Richtlinienverstößen und Auffälligkeiten*
- *Berichte für Geschäftsführer und IT-Manager*
- *Integration abgeschotteter Daten zum besseren Verständnis des genauen Systemstatus*

Endpoint Security Management

Sie schützen die anfälligsten Bereiche Ihrer Systeme: die Endgeräte. Endpoint Security Management sorgt für integrierte Sicherheit am Endgerät zur Kontrolle von USB- und Wireless-Geräten, Daten und Anwendungen. Zu den Schlüsselfunktionen im Bereich Endpoint Security Management gehören:

- *Unterbindung des Zugriffs nicht autorisierter USB-Geräte*
- *Datenverschlüsselung auf Endgeräten zum Schutz vor Diebstahl*
- *Standorterkennung für Wireless Security*
- *Verwaltung von Sicherheitsrichtlinien*

Koordination

Automatisierung des Rechenzentrums

Mit der Automatisierung des Provisionings von Rechenzentrumsressourcen sind Sie eher in der Lage, wechselnden Geschäftsanforderungen gerecht zu werden. Zu den Schlüsselfunktionen im Bereich der Automatisierung des Rechenzentrums gehören:

- *Anpassung an Workload-Anforderungen, Hardwarezustand und Unternehmensrichtlinien*
- *Integriertes Management physischer und virtueller Computer*

Planung der Implementierung: Best Practices und Projektmeilensteine

Wenn Sie die Implementierung vereinfachen wollen, benötigt Ihre IT-Abteilung klar definierte Ziele. Mithilfe der folgenden Best Practices und empfohlenen Meilensteine können Sie mit der Implementierung des identitätsgesteuerten Sicherheits- und Ressourcen-Managements beginnen und Ihre Vorstellung eines integrierten, effizienten Unternehmens in die Praxis umsetzen.

Abstimmung der IT-Funktion auf die Geschäftstätigkeit

- ❑ Bedienen Sie sich bei der Leitung des Projekts eines Prozessmodells wie ITIL oder Cobit.
- ❑ Versichern Sie sich der Unterstützung aus der Führungsebene.
- ❑ Beziehen Sie IT-Führungskräfte bei geschäftliche Fragen mit ein.

Auswertung und Gestaltung

- ❑ Bestimmen Sie vor dem Projektstart, ob bestehende Gegebenheiten angepasst werden müssen.
- ❑ Entwickeln Sie eine Lösungs-Roadmap, um festzulegen, welche Kriterien das Unternehmen nach Abschluss des Projekts erfüllen soll.
- ❑ Berücksichtigen Sie beim Ausschreibungsprozess Geschäftseinheiten wie Personalabteilung oder Buchhaltung, die eigene Anwendungen besitzen.
- ❑ Legen Sie die zu automatisierenden Geschäftsabläufe fest.
- ❑ Zeichnen Sie das bestehende Modell Ihrer Unternehmensdaten auf.

Machbarkeitsnachweis

- ❑ Konzentrieren Sie sich auf den Zugriff auf ältere oder abgeschottete Anwendungen.
- ❑ Ermitteln Sie die Anforderungen des Anbieters hinsichtlich spezifischer Anpassungen.
- ❑ Ziehen Sie in Erwägung, in einen detaillierteren Machbarkeitsnachweis zu investieren – wobei der Preis auf den endgültigen Erwerb angerechnet wird.
- ❑ Legen Sie Erfolgsfaktoren auf der Grundlage von Geschäftsanforderungen fest, nicht auf der Grundlage technischer Details.

Produktionsvorbereitung, Pilotphase und Rollout

- ❑ Setzen Sie realistische Deadlines.
- ❑ Stellen Sie sicher, dass die Lösung Ihrer Wahl ein Rollback unterstützt.
- ❑ Erstellen Sie ein zentralisiertes Identitätsdepot.
- ❑ Bestimmen Sie Projektleiter aus Benutzergruppen und schulen Sie diese zuerst.

Installation

- ❑ Installieren Sie die Software.
- ❑ Richten Sie die verbundenen Systeme ein.
- ❑ Nehmen Sie die Software in Betrieb.
- ❑ Konfigurieren Sie das Passwortmanagement.
- ❑ Konfigurieren Sie die Berechtigungen.

Mit der Automatisierung des Provisionings von Rechenzentrumsressourcen sind Unternehmen eher in der Lage, ständig wechselnden Geschäftsanforderungen gerecht zu werden.

www.novell.com

- ❑ Konfigurieren Sie Audit- und Berichterstellung.
- ❑ Konfigurieren Sie Workflow- und Benutzeranwendungen auf der Grundlage der Unternehmensrichtlinien.

Dokumentation

- ❑ Stellen Sie sicher, dass die Dokumentation den Anforderungen hinsichtlich Audits und Compliance entspricht.
- ❑ Automatisieren Sie die Dokumentierung.

Weitere Anmerkungen

- ❑ Identitäts- und Zugriffsmanagement-projekte sind vor allem dann erfolgreich, wenn sie schrittweise umgesetzt werden.
- ❑ Zu Beginn sind möglicherweise nicht alle Technologien erforderlich; letztendlich kommen jedoch die meisten zum Einsatz.
- ❑ Vermeiden Sie den Einsatz von Lösungen, deren Implementierung eine Unterbrechung der bestehenden Systeme zur Folge hätte.
- ❑ Beginnen Sie mit Projektkomponenten, die auf primäre Geschäftsfaktoren ausgerichtet sind, sodass Sie einen schnellen ROI erzielen und intern Unterstützung für das Projekt gewinnen.
- ❑ Konzentrieren Sie sich auf die Gesamt-kosten des Projekts, nicht nur auf die Kosten für Software oder Support.

Unternehmenswachstum dank Integration und Automatisierung

Governance, Risk und Compliance (GRC) stellen mittlerweile die größten Herausforderungen für IT-Abteilungen dar. Der Novell Ansatz zur Bewältigung dieser Herausforderung (das identitätsgesteuerte Sicherheits- und Ressourcen-Management) ist eine integrierte, automatisierte und richtliniengesteuerte Lösung, mit der nicht nur GRC-Probleme angegangen werden können, sondern die darüber hinaus zur Senkung von Kosten, Erreichung von Geschäftszielen, Verbesserung der Benutzerproduktivität und Förderung der Konsistenz im gesamten Unternehmen beiträgt.

Komponenten des identitätsgesteuerten Sicherheits- und Ressourcen-Managements

Novell ZENworks Asset Management	Erfassung aller Unternehmensressourcen, Erstellung von Berichten inklusive Lizenzierung, Installation und Nutzungsdaten
Novell ZENworks Configuration Management	Richtliniengesteuerte Automatisierung von Software-Einrichtung, Updates, Eigenreparatur und Migration
Novell Identity Manager	Systemübergreifende Umsetzung von Unternehmensrichtlinien in IT-Kontrollen und Compliance-Verfügungen
Novell Access Manager	Schutz unternehmenseigener Webressourcen und Durchsetzung einheitlicher, richtlinienbasierter Authentifizierungs- und Zugriffsmethoden
Sentinel von Novell	Integration identitätsbasierter Systeme in andere Systeme und damit Gewährleistung der Einhaltung von Unternehmensrichtlinien
Novell ZENworks Orchestrator	Automatisierung des Provisionings physischer und virtueller Rechenzentrumsressourcen zur Erfüllung wechselnder Anforderungen

Weitere Informationen darüber, wie Novell Sie bei der Sicherung und Verwaltung Ihres Unternehmens unterstützen kann, finden Sie unter www.novell.com/innovationline.

Novell Services
Informationen zu den Novell Services wie Consulting, Training und Support erhalten Sie im Internet unter:
www.novell.com/consulting
www.novell.com/training
www.novell.com/support

Weitere Informationen
Informationen zu Novell Produkten erhalten Sie beim Novell Fachhandelspartner oder besuchen Sie uns im Internet unter: www.novell.com/products

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

Novell GmbH
Heiligenstädter Lände 27c
A - 1190 Wien
Tel: +43-(0)1-367 74 44
Fax: +43-(0)1-367 74 44 20
www.novell.at

Novell (Schweiz) AG
Leutschenbachstrasse 41
CH - 8050 Zürich
Tel: +41-(0)43-299 78 00
Fax: +41-(0)43-299 75 01
www.novell.ch

Novell