

Prozessautomatisierung in der IT-Security

Automation statt Reaktion

Ausgelöst durch die Forderung nach erhöhter Effizienz, besseren Service Levels und strikterer Kostenkontrolle in der IT, überlegen Unternehmen, wie sie ihre IT-Prozesse besser definieren und implementieren können. Das Mittel der Wahl ist die IT-Prozess-Automatisierung. Nicht eingeführte oder nur partiell umgesetzte Prozesse schmälern den Nutzen und die Effektivität der IT-Sicherheit.

Warum investieren Unternehmen in IT-Security? Ein wesentlicher Grund ist die Tatsache, dass die IT als gesamte Abteilung eine Dienstleistung für den eigentlichen Geschäftszweck des Unternehmens liefert. Dies bedingt, dass diese Dienste sicher, zuverlässig und verfügbar sind. Nun stellt sich die Frage: Wie ist es möglich, die IT-internen Funktionen wie Service-Desk, Incident- und Problem-Management auf die IT-Security auszuweiten? Tatsache ist, dass es in vielen Unternehmen noch immer viel zu wenig Interaktion zwischen dem IT-Betrieb und der IT-Security-Abteilung gibt.

auch nicht sinnvoll, denn einige Hersteller sind besonders gut im Bereich der Firewalls, andere glänzen bei Content-Protection-Systemen.

Mittlerweile setzen viele Unternehmen IT-Security-Management-Lösungen ein, um die einzelnen Tools („Security Point Products“ genannt) herstellerunabhängig in zentralisierten Systemen zu managen. Lösungen für das Security-Information- and Event-Management (SIEM), Compliance-, Vulnerability- und Configuration-Management sind einige Beispiele dafür. Zum Einsatz kommen diese Management-Systeme

in der IT-Security-Abteilung. Denn einerseits erfordern diese Systeme Expertise und Spezialwissen in der IT-Security, andererseits benötigt die IT-Security-Abteilung diese Lösungen für viele ihrer täglichen Aufgaben.

An sich ist diese Situation nicht falsch, gäbe es nicht den erwähnten Mangel an Interaktion zwischen IT-Betrieb und IT-Security. Die Existenz dieses Mangels ist nicht verwunderlich, denn die Lösungen des IT-Security-Managements sind nicht IT-Operations-tauglich. Wie also lösen wir dieses Dilemma? Und: Wollen wir dieses Dilemma überhaupt lösen?

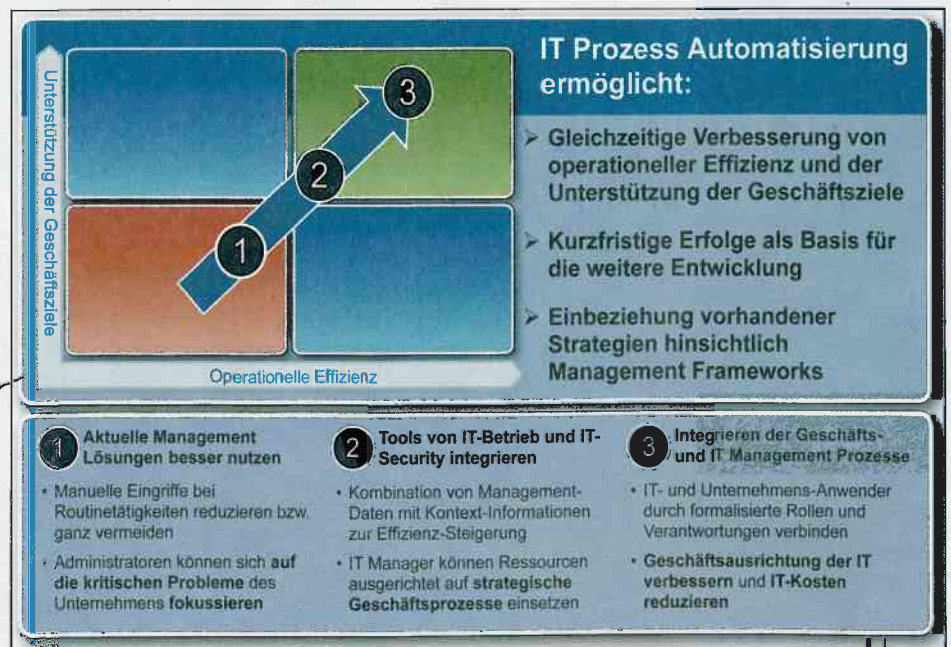
Die Antwort auf die zweite Frage lautet: unbedingt! Führende Analysten wie Gartner sagen, dass ein höherer Reifegrad in der IT-Security nur durch Operationalisierung und Automatisierung erreichbar ist. Die IT muss einen umfassenden, verfügbaren und sicheren Service liefern können.

Der Begriff „Operationalisierung“ bedarf einer Erläuterung. Unter Operationalisierung versteht man die Einbindung oder Verlagerung von Aktivitäten in den IT-Betrieb. Dort ist der Service-Desk und in der Regel auch ein mehr oder weniger ITIL-konformes (IT Infrastructure Library) Incident- und Problem-Management beheimatet. Hier laufen also die Fäden der IT zusammen. Der Service-Desk ist eine Funktion,

Die „gute alte“ reaktive Zeit

In der „guten alten Zeit“ sahen sich Unternehmen einer konkreten Gefahr ausgesetzt und investierten in eine IT-Security-Lösung zu deren Eliminierung: Firewalls der neuesten Generation, Lösungen für Identitäts- und Zugriffsverwaltung, Verfahren zur Änderungskontrolle und Host-gestützte Techniken gegen versuchtes Eindringen folgten. Alles in allem war dies ein sehr reaktives Vorgehen.

Und so nahm das Chaos seinen Lauf: Die Security-Produkte bekämpften zwar die aufgetretenen Probleme, stellten jedoch meist nur einen Verbund von Insellösungen dar. Schließlich wird es nicht gelingen, sämtliche IT-Security-Tools von nur einem einzigen Hersteller zu erwerben. Dies wäre



Automation bringt nicht nur im IT-Betrieb Vorteile, sondern auch im IT-Security-Bereich. Bild: NetIQ/Attachmate

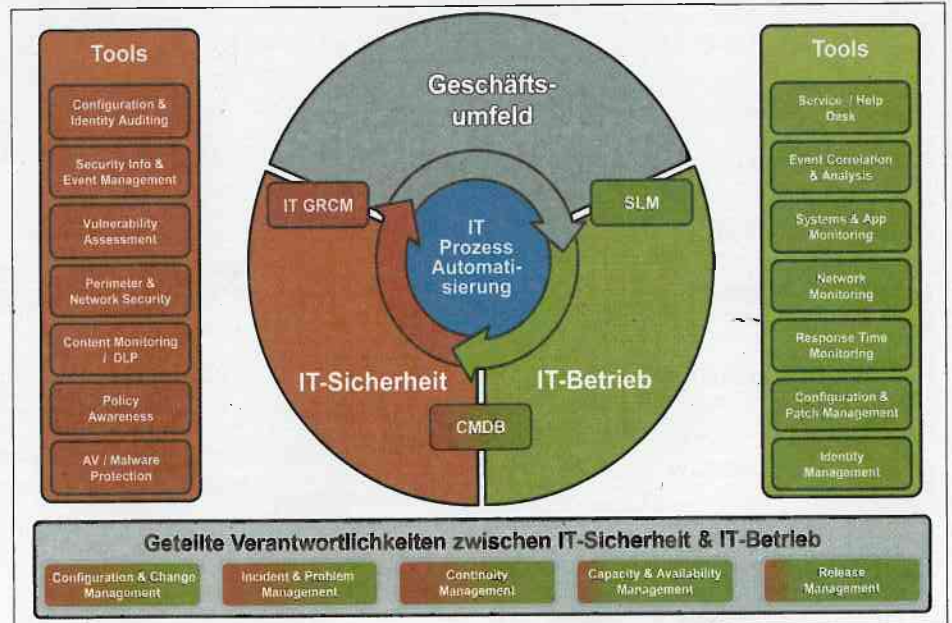
um auftretende Störungen, Change Requests etc. kosteneffizient zentral zu bearbeiten. Die Operationalisierung der IT-Security umzusetzen heißt also, den IT-Betrieb in die IT-Security derart einzubinden, dass das alltägliche Incident-Management sicherheitsrelevanter Vorfälle ebenfalls dort aufläuft. Dies reduziert die Kosten für das Unternehmen und befreit die Fachkräfte in der IT-Security-Abteilung von diesen täglichen Routineaufgaben.

Doch ein Bindeglied fehlt hier: die IT-Prozess-Automatisierung. Die Basis für die Automatisierung der IT-Prozesse bildet die formale Beschreibung des Prozessablaufs: Was soll automatisiert werden? Wer wird einbezogen, zum Beispiel durch automatisierte Benachrichtigungen? Ist ein Genehmigungsverfahren Bestandteil des Prozesses? Welche IT- und Sicherheitslösungen sind an dem Prozess beteiligt?

Ausgehend von dieser Prozessbeschreibung kann man ein Diagramm erstellen, das den Prozess grafisch darstellt und im Idealfall direkt in der IT-Prozess-Automatisierung umgesetzt wird. Diese Software steuert sämtliche definierten Prozesse und deren Instanzen. Sie kontrolliert alle angebotenen IT-Management-Lösungen wie die Security-Management-Tools und die Lösungen des IT-Betriebs wie beispielsweise die Service-Desk-Software.

IT-Prozess-Automatisierung bringt nicht nur Vorteile für die Zusammenarbeit von IT-Betrieb und IT-Security im Rahmen so genannter Makroprozesse, sondern bietet auch innerhalb der IT-Security erhebliche Vorteile bei der täglichen Arbeit durch Umsetzung von Mikroprozessen. Beispiele dafür sind:

- Benachrichtigungen an die zuständigen IT-Sicherheitsmitarbeiter weiterleiten, zum Beispiel auf Basis von Dienst- und Einsatzplänen und der Expertise der Mitarbeiter, inklusive automatischer Eskalation, falls innerhalb definierter Servicezeiten keine Bearbeitung erfolgt ist,
- Tickets in ein Ticketsystem für Vorfälle einstellen,
- den Umfang der Überwachung kritischer Systeme aufgrund eines Ereignisses oder einer Schwachstelle vorübergehend ändern,



Mittels IT-Prozessautomatisierung greifen Abläufe ineinander, die den IT-Betrieb, die IT-Security und das Business betreffen. Bild: NetIQ/Attachmate

- Reaktion auf Sperren/Rücksetzen eines Kennworts,
- Reaktion auf Eintragen in eine Gruppe mit hohen Rechten,
- Vorfälle in Korrelation mit einer Konfigurations- oder Compliance-Richtlinie bringen und einen Arbeitsvorgang für forensische Zwecke anlegen,
- Berichte über Benutzerzugriffsberechtigungen in Reaktion auf eine Rechtsverletzung eines Benutzers erstellen sowie
- prüfen, ob ein Benutzer, der sich beim System anmeldet, überhaupt noch dem Unternehmen angehört (oder unterwegs oder im Urlaub ist).

Betrachten wir einmal einen Prozessablauf im Detail an einem Beispiel. Auf einem Windows-Domänen-Controller stellt das SIEM-System einen Vorfall fest: Ein Benutzer wird in die Gruppe der Domänenadministratoren aufgenommen. Diesen Vorfall müsste nun eigentlich ein IT-Security-Mitarbeiter manuell bearbeiten. Durch die Anbindung an die IT-Prozess-Automatisierung wird allerdings ein Prozess gestartet, der als erstes im Service-Desk-System ermittelt, ob es einen Change Request für diese Änderung gibt. Falls solch ein Ticket existiert, prüft die Software das Ticket: Sie stellt fest, welches Benutzerkonto dort genannt ist, und vergleicht es mit der Information aus dem Sicherheitsvorfall. Ist im Ti-

cket ein anderes Benutzerkonto angegeben als das der Gruppe hinzugefügte, liest die Software den Eigentümer des Tickets aus und schickt diesem eine E-Mail mit dem Hinweis darauf, dass er den falschen Benutzer ausgewählt hat. Die Frage, ob das Automationssystem diesen Fehler korrigieren soll, beantwortet der Ticket-Eigentümer zum Beispiel durch eine E-Mail-Antwort mit dem Stichwort „genehmigt“. Daraufhin entfernt die Software den falschen Benutzer automatisch, nimmt den richtigen Benutzer auf und schließt den Sicherheitsvorfall. Das Beispiel zeigt, dass der formale Ablauf dieses Prozesses vollkommen ohne Einbeziehung der IT-Security-Abteilung funktioniert und erfolgreiche Operationalisierung zu entsprechender Kosteneinsparung führen kann.

Die IT-Prozess-Automatisierung bringt auch im Security-Umfeld handfeste Vorteile und zahlt sich für Unternehmen schnell aus. Bei definierten Prozessen lassen sich konkrete Zeiteinsparungen ablesen, die den Mehrwert einer Automationslösung schnell verdeutlichen. Die Effizienz steigt, die Kosten sinken, Risiken werden reduziert.

Jörn Dierks/wg

Jörn Dierks ist Chief Security Strategist EMEA bei NetIQ/Attachmate.