nevisReports – Governance Dashboards

Kurzbeschreibung

Governance-Dashboards machen die Verwaltung Ihrer Sicherheitsinfrastruktur einfacher denn je. Intuitive Grafiken zeigen frühere und aktuelle Daten aller Produkte an. Normales und anomales Verhalten lässt sich somit auf einen Blick erkennen.

Vorteile

nevisReports bietet detaillierte Governance Dashboards, die die Nutzung aller Produkte Ihrer NEVIS Security Suite in nahezu Echtzeit anzeigen. So können Sie **normales und anomales Verhalten sofort erkennen**, ein entscheidender Vorteil, um **potenzielle Bedrohungen** entdecken zu können.

nevisReports führt Protokolldaten und Informationen aus verschiedenen Quellen in optisch ansprechenden Dashboards zusammen, die Ihnen einen **besseren Überblick über die Arbeit des Systems** gestatten. Dank der skalierbaren Architektur können auch grosse Datenmengen verarbeitet und visualisiert werden.

Darüber hinaus lassen sich die Governance Dashboards benutzerspezifisch anpassen, so dass Sie stets die für Sie am wichtigsten Elemente im Blick haben. Die Dashboards können massgeschneidert an die Anforderungen jeder Organisation angepasst werden, die Wert darauf legt, die Nutzungsmuster ihrer NEVIS-Umgebung zu visualisieren und entsprechend zu analysieren.

Worum geht es?

Sicherheit erfordert heutzutage einen ganzheitlichen Blick auf gewährte Autorisierungen, Authentisierungsprozesse und Identitäten. Sie müssen Ihre Geschäftsanwendungen an jedem einzelnen Tag schützen, Prozesse für Neuzugänge und ausscheidende Mitarbeitende verwalten und andere wichtige sicherheitsrelevante Handlungen ausführen.

Ohne ein Tool, mit dem sich alle diese Ereignisse zusammenfassen lassen, kann es zu einer Sisyphusaufgabe werden, die Komplexität Ihres Systems im Griff zu behalten.

nevisReports löst dieses Problem. Das Governance Dashboard von nevisReports zeigt ausgewählte Informationen zu wichtigen Ereignissen aller Produkte Ihrer NEVIS Security Suite an. Sie müssen die Berichte der einzelnen Produkte also nicht mehr manuell auswerten. Das Governance Dashboard zeigt ihnen die Daten in einheitlicher Form an.

Die Berichtsdaten werden in optisch ansprechender Form zusammengefasst. Wichtige Zahlen zu Ihrer NEVIS-Infrastruktur werden in einer sich selbsttätig aktualisierenden Grafik dargestellt.

So erhalten Sie einen verständlichen Überblick über die gesamte Systemaktivität und können einfacher definieren, was als „normales" Systemverhalten anzusehen ist. Dadurch erkennen Sie auch, was „anomales" Verhalten ist und wo potenzielle Bedrohungen, Konfigurationsprobleme oder Fehlfunktionen des Systems vorliegen könnten.

Wichtigste Merkmale

- Viele Produkte – ein Dashboard.
- Vergleich früherer und aktueller Daten, um Anomalien zu erkennen.
- Dashboards basieren jeweils auf den neuesten Daten (Reporting nahezu in Echtzeit).
- Sichtbarkeit der Dashboards kann auf bestimmte Benutzergruppen beschränkt werden.
- Interaktive Diagramme mit Quickinfos.
- Probleme mit einzelnen Geschäftsanwendungen schnell auffindbar.
- Überblick über inaktive Konten und ungenutzte Autorisierungen.
- Anzeige der zugrunde liegenden Daten (detaillierte Event-Logs) unter Verwendung der Governance-Berichte von nevisReports.

Dashboard

Das Governance Dashboard in Abbildung 1 hat viel zu bieten: Die grosse Vielfalt der Dashboard-Anzeigen zeigt die Leistungsfähigkeit von nevisReports. Intuitive Grafiken bieten Ihnen einen leicht verständlichen Überblick für die einfache Verwaltung Ihrer Geschäftsanwendungen.

Schweiz ▪ AdNovum Informatik AG ▪ Röntgenstrasse 22 ▪ 8005 Zürich ▪ Schweiz ▪ +41 44 272 6111 ▪ info@nevis-security.ch ▪ www.nevis-security.ch
Singapur ▪ AdNovum Singapore Pte. Ltd. ▪ 3 Shenton Way ▪ #23-03 Shenton House ▪ Singapore 068805 ▪ +65 6536 0668 ▪ info@adnovum.sg ▪ www.nevis-security.sg
Deutschland ▪ NEVIS Security GmbH ▪ Maximilianstraße 35 A ▪ 80539 München ▪ Deutschland ▪ +49 89 2421 8180 2 ▪ info@nevis-security.de ▪ www.nevis-security.de

-

Anwendungsfälle

Anwendungsfall 1 – Normales und anomales Verhalten erkennen

Sie erhalten die Aufgabe, das Verhalten Ihrer Anwendungen hinsichtlich gleichzeitig geöffneter Sitzungen zu überprüfen.

Die in Abbildung 2 gezeigte Detailansicht zeigt, wie viele Sitzungen in den letzten 24 Stunden im Vergleich zu früheren Zeiträumen gleichzeitig aktiv waren. Die schwarze Linie zeigt die Aktivität während der vergangenen 24-Stunden-Periode an. Die grauen Linien stehen für das Verhalten an den Tagen davor.

Dies zeigt sehr gut, wie Sie normales und anomales Verhalten erkennen können. Solange die schwarze Linie dem gleichen Muster folgt wie mehrere graue Linien, liegt normales Verhalten vor.

Vor rund zwölf Stunden jedoch verhielt sich die schwarze Linie vollkommen abweichend. Sie erkennen hier anomales Verhalten, dessen Ursache untersucht werden sollte. Es könnte sich um eine Sicherheitsbedrohung, eine Fehlfunktion des Systems oder um ein Konfigurationsproblem handeln.

Mit der Quickinfo-Funktion erhalten Sie nähere Informationen zu dieser Anomalie (oder zu jedem anderen Datenpunkt). Die betreffenden Informationen helfen Ihnen, in den Governance-Berichten von nevisReports noch weiter nachzuforschen.

Möglicherweise finden Sie dort mehr als nur ein Muster. Im Augenblick sieht es beispielsweise so aus, als sei die graue Linie unten im Diagramm eine weitere, frühere Anomalie. Sollten aber noch weitere Linien einen ähnlichen Verlauf aufweisen, könnte es sich um eine zweite normale Situation handeln, die beispielsweise am Wochenende auftritt.

Schweiz ▪ AdNovum Informatik AG ▪ Röntgenstrasse 22 ▪ 8005 Zürich ▪ Schweiz ▪ +41 44 272 6111 ▪ info@nevis-security.ch ▪ www.nevis-security.ch
Singapur ▪ AdNovum Singapore Pte. Ltd. ▪ 3 Shenton Way ▪ #23-03 Shenton House ▪ Singapore 068805 ▪ +65 6536 0668 ▪ info@adnovum.sg ▪ www.nevis-security.sg
Deutschland ▪ NEVIS Security GmbH ▪ Maximilianstraße 35 A ▪ 80539 München ▪ Deutschland ▪ +49 89 2421 8180 2 ▪ info@nevis-security.de ▪ www.nevis-security.de

Anwendungsfall 2 – Inaktive Konten und ungenutzte Autorisierungen

Für einen Risk and Compliance Officer ist es wichtig zu wissen, ob bestehende Konten und Autorisierungen noch benötigt werden. Dies trägt dazu bei, die aktuelle Anfälligkeit des Unternehmens für Bedrohungen einzuschätzen und durch geeignete Massnahmen zu minimieren.

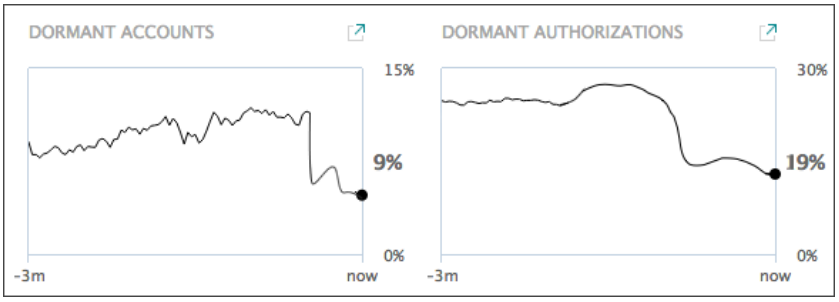
Nehmen wir an, dass Sie seit etwa zweieinhalb Monaten Anstrengungen unternommen haben, um die Zahl der inaktiven Konten und ungenutzten Autorisierungen auf unter 10% zu drücken.

Die Dashboard-Anzeige "Dormant Accounts" zeigt, wie sich die Anzahl der freigegebenen Konten, die während einer bestimmten, benutzerspezifisch einstellbaren Zeit nicht aktiv waren, in den letzten Monaten entwickelt hat.

In diesem Fall können Sie erkennen, dass die Massnahmen, die Sie ergriffen haben, Früchte tragen. Die Anzahl inaktiver Konten wurde auf 9% des gesamten Kontenbestands gesenkt.

Über das Dashboard-Element für "Dormant Authorizations" ist in ähnlicher Weise die Anzahl ungenutzter Autorisierungen pro geschützter Geschäftsanwendung und pro Benutzer erkennbar.

Im vorliegenden Fall ist zu sehen, dass auch diese sich verringert hat, auch wenn angesichts der 19% noch Verbesserungsmöglichkeiten bestehen. Sie könnten sich dafür entscheiden, noch weitere ungenutzte Autorisierungen einzuziehen, um die Angriffsfläche Ihres Unternehmens zusätzlich zu verkleinern.



Architektur – wie funktioniert es?

Abbildung 4 vermittelt einen Überblick über die Funktion des Governance Dashboard von nevisReports.

nevisReports überwacht und sammelt statistische Daten aus nevisProxy, nevisAuth und nevisIDM. Es hat jedoch nur minimalen Einfluss auf deren Betrieb.

Mit den erfassten Daten erstellt nevisReports anschliessend ein Governance Dashboard, auf das die Benutzer über das Web zugreifen können

Schweiz ▪ AdNovum Informatik AG ▪ Röntgenstrasse 22 ▪ 8005 Zürich ▪ Schweiz ▪ +41 44 272 6111 ▪ info@nevis-security.ch ▪ www.nevis-security.ch
Singapur ▪ AdNovum Singapore Pte. Ltd. ▪ 3 Shenton Way ▪ #23-03 Shenton House ▪ Singapore 068805 ▪ +65 6536 0668 ▪ info@adnovum.sg ▪ www.nevis-security.sg
Deutschland ▪ NEVIS Security GmbH ▪ Maximilianstraße 35 A ▪ 80539 München ▪ Deutschland ▪ +49 89 2421 8180 2 ▪ info@nevis-security.de ▪ www.nevis-security.de