audicon we care

Überwachung der Windows Sicherheitsprotokolle mit CaseWare™ Monitor

Überblick

Windows-Sicherheitsprotokolle

In den meisten Windows-Umgebungen wird der Nutzen von Überwachungsprotokollen nicht voll ausgeschöpft. Sie werden oft nur zu Untersuchungszwecken herangezogen und gewöhnlich erst, nachdem sich ein Vorfall ereignet hat. Windows-Protokolle haben jedoch einen enormen Wert, sofern sie richtig konfiguriert und effizient überwacht werden.

Systemprotokolle generieren riesige Datenmengen aus verschiedenen Quellen. Folglich kann die Zusammenfassung, Durchsicht und Analyse der Daten oft langwierig und ineffizient sein. Als weitere Erschwernis kommt hinzu, dass Protokolle durch unzulängliche Konfiguration überfüllt sind, überschrieben werden, unvollständig oder unbrauchbar sind.

Es gibt Lösungen, die die Zusammenfassung und Sammlung sowohl von lokalen Protokollen als auch Remote-Protokollen aus dem gesamten Unternehmen mithilfe des Einsatzes von Software-Tools oder Hardware erleichtern. Was bei den derzeitigen Lösungen zur Analyse von Protokollen fehlt, ist die Möglichkeit, relevante Informationen, die zur Bestimmung der hochriskanten Aktivitäten nötig sind, intelligent herauszufiltern, Benachrichtigungen an die entsprechenden Personen, unabhängig von ihren technischen Fähigkeiten, zu versenden, die Auflösung von Auffälligkeiten zu dokumentieren und einen passenden Workflow für die Eskalation von Auffälligkeiten einzuführen.

Überwachungsrichtlinien

Die Überprüfung auf Sicherheitsereignisse in kritischen Computersystemen ist ein wesentlicher Bestandteil einer soliden Sicherheitsstrategie. Die Überwachungsrichtlinie für Windows definiert, für welche Sicherheitsereignisse Aktionen bei Erfolg und/oder Fehlschlagen im Sicherheitsprotokoll geprüft und aufgezeichnet werden. Windows 2003 hat beispielsweise 9 Überwachungsrichtlinien, aber standardmäßig sind nur zwei aktiviert:

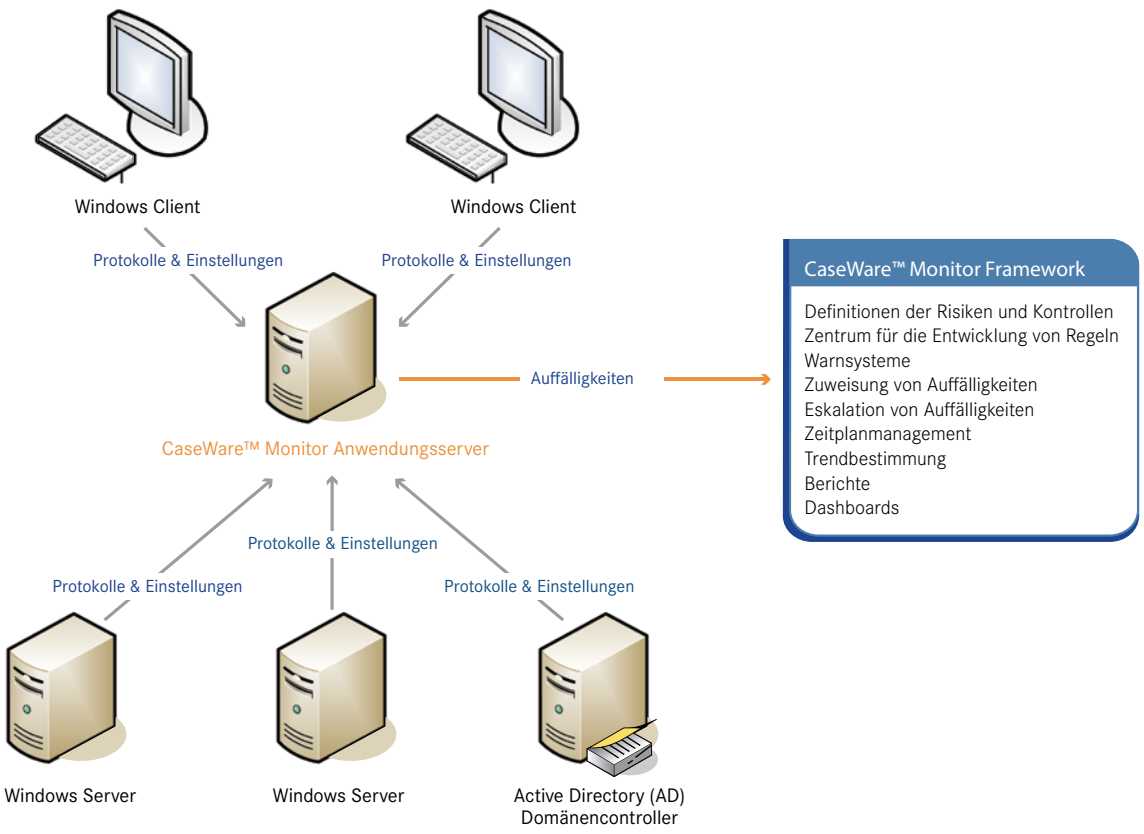
- Anmeldeereignisse an Konten: Erfolgsüberwachung
- Anmeldeereignisse: Erfolgsüberwachung

Bei den anderen Überwachungskategorien (Managementereignisse, Verzeichnisdienstzugriff, Objektzugriff, Richtlinienänderung, Rechteverwendung, Prozessverfolgung und Systemereignisse) ist die Überwachung deaktiviert. Jedes Unternehmen muss seine eigene Position zum Thema Sicherheit definieren und dementsprechende Überwachungen veranlassen. Unabhängig von der Konfiguration der Infrastruktur ist eine effektive Protokollanalyse und -überwachung erforderlich, um sicherzustellen, dass Ziele bezüglich Sicherheit, Risiko und Überwachung erreicht werden können.

CaseWare™ Monitor Lösung

Unsere Lösung konzentriert sich auf die Automatisierung von Analyse, Bericht, Benachrichtigungen und Verwaltung von Auffälligkeiten innerhalb der Windows-Protokollumgebung des Unternehmens. Wie in Abbildung 1 dargestellt, werden Überwachungsrichtlinien über Gruppenrichtlinien konfiguriert und an Clients und Server innerhalb der Umgebung weitergegeben. Die daraus resultierenden Protokolle werden in einem zentralen CaseWare™ Monitor Server zur Analyse und Abfrage zusammengeführt. Einmal eingerichtet, verwendet CaseWare™ Monitor ein Monitoring-Framework, das alle elektronischen Aktivitäten untersucht, um berichtspflichtige Ereignisse zu erkennen und die entsprechenden Personen zu informieren.

Abbildung 1 — Monitoring von Windows-Ereignissen



Workflow und Berichterstellung

Wenn ein entsprechendes Ereignis oder eine Reihe von Ereignissen erkannt wird, werden die entsprechenden Benachrichtigungen ausgelöst und es folgt ein strenger Prozess, der sicherstellt, dass hochriskante Aktivitäten gemäß den Vorgaben der Sicherheitsrichtlinien des Unternehmens bearbeitet werden.

Andere wesentliche Aspekte der Lösung sind die Automatisierung der Berichterstellung und die Visualisierung der Kontrollumgebung.

Das Framework enthält standardisierte Dashboards:

- Datenübergreifende Trendbestimmung der Ergebnisse
- Gruppierung nach Risikoeinstufung
- Gruppierung nach Status (neu, ausstehend, überfällig etc.)
- Vergleiche über Netzwerke und Benutzer hinweg

Beispielberichte und -alarmierungen

Alarmierungen, die auf Handlungen basieren

- Fehlgeschlagene Versuche zur Dateifreigabe
- Neue Konten erstellt
- Aufstellung von neuen Richtlinien und Änderungen an bestehenden Richtlinien
- Zugriff auf Systemresourcen durch Personen in Urlaub
- Zugriff auf Systemresourcen zu ungewöhnlichen Zeiten
- Personen identifizieren, die zu spezifischen Gruppen hinzugefügt wurden, z. B. VPN, Administrator, Consultants, Systembenutzer etc.
- Domänencontroller hinzugefügt
- Benutzer mit mehreren Kontensperrungen innerhalb kurzer Zeit
- Anmeldeversuche an geschützten Arbeitsstationen ermitteln
- Anmeldeversuche mit ungültigem Anmeldetyp ermitteln
- Anmeldeversuche mit abgelaufenen Kennwörtern oder Kennwörtern, die nicht geändert wurden, emitteln

Alarmierungen, die auf Handlungen basieren (Fortsetzung)

- Anmeldeversuche an deaktivierte Konten ermitteln
- Anmeldeversuche mit abgelaufenen Konten ermitteln
- Erneute Anmeldung mit speziellen Rechten ermitteln
- Erfolgreiche Anmeldung mit Servicekonto an Konsole
- Reaktivierte Konten
- Versuchte Anmeldung durch unbekannte Domänennamen ermitteln
- Fehlgeschlagene Authentifizierung des Radius-Server
- Anmeldeversuche mit standardmäßigem Administratorkonto ermitteln
- Fehlgeschlagene Anmeldung mit Benutzernamen des Administrators, aber unbekannter Domäne
- Batch-Anmeldungen durch Konten, die Personen zugeordnet sind, ermitteln
- Benutzer, deren Kennwort die erlaubte Gültigkeitsdauer überschritten hat
- Benutzer mit aktiviertem Fernzugriff zur Server-Anwahl
- Ruhende Computerkonten
- Benutzer ermitteln, denen auf andere Weise die Anmeldung an Computern ermöglicht wird

Benachrichtigungen über die Konfiguration des Active Directorys

- Konten, die keine Anmeldungen aufweisen
- Konten, die abgelaufen sind
- Benutzer, die ihre Kennwörter nicht ändern müssen
- Verwendung der Servicekonten
- Konten, die nicht einem bestimmten Benutzer zugeordnet sind, sondern von einer Gruppe verwendet werden
- Benutzer/unbekannte Objekte in Domänencontroller-Gruppen ermitteln
- Server ermitteln, bei denen die Protokollierung deaktiviert wurde
- Ehemalige Mitarbeiter mit aktiven Konten ermitteln
- Änderungen an Benutzerkonten

Benachrichtigungen über die Konfiguration des Active Directorys (Fortsetzung)

- Änderungen bei Gruppen ermitteln (abgesehen von Löschung, Erstellung oder Änderung der Mitgliedschaft)
- Änderungen an universellen Gruppen mit aktivierter Sicherheit
- Änderungen an der Domäne und den Verhältnissen der Gesamtstrukturvertrauensstellung ermitteln

Vorteile

UNTERNEHMERISCHE HERAUSFORDERUNG	CASEWARE™ MONITOR LÖSUNG
Anforderungen der Stakeholder Eskalation von Risiko- und Compliance-Anforderungen	• Bietet für das ganze Unternehmen eine einheitliche Definition und Überwachung der Kontrollen und die Sicherheit, dass sie über alle Geschäftsprozesse hinweg effektiv angewendet werden.
Automatisierung Das Erkennen und Auflösen von Regelverstößen automatisieren	• Erkennt Regelverstöße an der Datenquelle • Verteilt Daten via Dashboard, E-Mail und SMS im ganzen Unternehmen anhand kundendefinierter Regeln • Bietet einen Workflow für die Beseitigung von Auffälligkeiten einschließlich einer automatischen Erkennung von Fehlerbehebungen • Ermöglicht dem Benutzer, Kontrollen in mehreren Businessprozessen über eine zusammenfassende Übersicht zu definieren • Effizienz wird gesteigert, indem die Analysen wiederholbar gemacht werden mit der Möglichkeit, Toleranzen anzupassen • Geschäftsregeln und Parameter können an Kundenwünsche angepasst werden und vom Unternehmen kann eine neue Logik entwickelt werden • Ermöglicht außerdem die Überwachung von Geschäftskennzahlen • Auffälligkeiten werden erkannt, sobald sie entstehen

Integration Nahtlose Integration in vorhandene Lösungen	• Erfordert keine Änderungen des zugrunde liegenden Systems, das überwacht wird • Bietet nur Lesezugriff auf Daten und Quelldaten können nicht verändert werden. • Benutzer- und Gruppensicherheit durch Unterstützung von LDAP • Starke Verschlüsselung
Prozessoptimierung Der Prozess wird effizienter und kostengünstiger	• Auffälligkeiten werden ohne zeitliche Verzögerung entdeckt • Niedrigere Eintreibungskosten • Höherer Automatisierungsgrad • Compliance und andere Berichte werden automatisch erstellt • Wissen und Fachkenntnisse werden im Kontrollsystem abgebildet und wiederholbar gemacht

CaseWare™ Monitor
Bei CaseWare™ Monitor handelt es sich um eine eingetragene Marke von CaseWare International Inc. Die Audicon GmbH ist exklusiver Distributor von CaseWare™ Monitor in Deutschland.

Über Audicon
Die Audicon GmbH ist der führende Anbieter von Software-Lösungen, methodischem und fachlichem Know-how sowie Dienstleistungen rund um Audit, Risk und Compliance. Die Lösungen richten sich an Wirtschaftsprüfer und Steuerberater, Compliance- und Risiko-Manager sowie Revisoren und Rechnungsprüfer/Kämmerer.
Weitere Informationen: **www.audicon.net**

Sie haben Fragen? Wir helfen Ihnen gerne weiter!

Telefonisch:	Per E-Mail:	Im Internet:
+49 211 5 20 59 - 430	sales@audicon.net	www.audicon.net

Audicon GmbH | Niederlassung Düsseldorf

Neuer Zollhof 3
40221 Düsseldorf
Fon: +49 211 5 20 59 - 0
Fax: +49 211 5 20 59 - 120
E-Mail: info@audicon.net

Audicon GmbH | Niederlassung Stuttgart

Am Wallgraben 100
70565 Stuttgart
Fon: +49 711 78886 - 0
Fax: +49 711 78886 - 180
E-Mail: info@audicon.net