MicroNova
Software und Systeme

ManageEngine

Whitepaper

# Sicherheit für das Active Directory: Sicherheits-Audits richtig nutzen, um kritische Schwachstellen aufzudecken


von

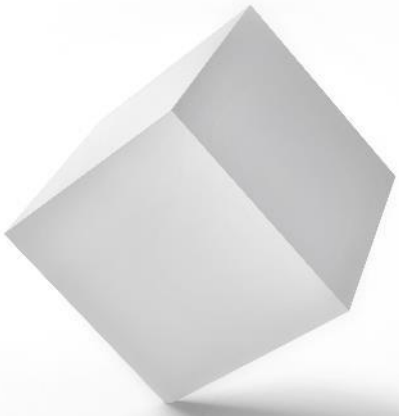
Derek Melber

Group Policy und Active Directory MVP
ManageEngine AD Solutions Technical Evangelist

und

Boris Slavik

Systems Engineer, MicroNova AG

# 1 Abstract

Das Active Directory (AD) ist in vielen Unternehmen zugleich Verzeichnisdienst, zentrales Tool zur Verwaltung der firmenweiten Benutzerrechte und Rückgrat der IT-Infrastruktur – und damit ein „lohnendes" Angriffsziel für Hacker und Cyberattacken. Der Microsoft-Dienst enthält unter anderem eine Art Generalschlüssel zu Gruppen- und Benutzerkonten; bei einem Ausfall wäre zudem der Zugriff der meisten Mitarbeiter auf wichtige Dienste lahm gelegt. Das Active Directory ist im wahrsten Sinne unternehmenskritisch und sollte von IT-Abteilungen daher so gut wie möglich abgesichert werden. Ein regelmäßiges Sicherheits-Audit schafft eine gute Basis, um potentielle Schwachstellen frühzeitig aufzuspüren und zu beheben.

In der Regel wird der Windows-Verzeichnisdienst allerdings nur einmal im Jahr, im Rahmen allgemeiner IT-Audits, genauer unter die Lupe genommen. Als Datengrundlage dient dabei eine Momentaufnahme zum Zeitpunkt der Reporterstellung. Welche Änderungen zwischen den jährlichen Audits durchgeführt werden, lässt sich mit dieser Methode nicht nachvollziehen. Besser für ein transparentes Änderungs-Management sind kontinuierliche Audits, die jede Änderung im AD dokumentieren und in übersichtlichen Reports zusammenfassen.

Dieses Whitepaper stellt zunächst Möglichkeiten vor, die Sie bei der Erstellung von AD-Sicherheits-Audits nutzen können, und erklärt die jeweiligen Vor- und Nachteile. Wie Sie ein kontinuierliches AD-Auditing möglichst effizient einrichten, und wie Sie vorgehen können, um die Sicherheit Ihrer AD-Umgebung zu verbessern, erläutert der zweite Teil des Whitepapers am Beispiel der AD-Auditing- und -Reporting-Lösung ADAudit Plus von ManageEngine.

# 2 Verschiedene Arten von AD-Audits

Insgesamt stehen Unternehmen drei verschiedene Audit-Arten zur Überprüfung des Active Directory zur Verfügung: Am beliebtesten sind derzeit die sogenannten, meist einmal jährlich durchgeführten Standard-Audits. Allerdings gelten diese bei AD-Experten inzwischen als veraltet, da sie nur den aktuellen Zustand des Active Directory zum Zeitpunkt der Reporterstellung betrachten und dadurch den Großteil der am Verzeichnisdienst vorgenommenen Änderungen außer Acht lassen – ein großes Sicherheitsrisiko für das Unternehmen.

Eine weitere Möglichkeit, das AD zu überwachen, bietet das sogenannte kontinuierliche Auditing. Hierbei sollen – so die Idee – alle Modifikationen berücksichtigt werden. In der Praxis gibt es allerdings etliche Auditing-Lösungen, die zwar ein kontinuierliches Reporting versprechen, tatsächlich aber nur regelmäßige, meist monatliche Momentaufnahmen des AD erstellen.

Daneben existieren jedoch auch Lösungen, die ein wirklich kontinuierliches Auditing der Active-Directory-Umgebung ermöglichen und alle daran vorgenommenen Änderungen ohne Ausnahme zuverlässig aufzeichnen. Idealerweise sollten solche Tools für ein effizientes Monitoring zusätzlich über integrierte und leicht verständliche Berichte, Berechtigungskonzepte mit mehreren Rollen sowie eine Alarmierungsfunktion verfügen.

## 2.1 Standard-Audits für das Active Directory

AD-Standard-Audits enthalten in der Regel Informationen zur bestehenden Infrastruktur. Sie werden meist auf Initiative von Auditoren erstellt, die dazu bei der IT-Abteilung diverse Reports zum aktuellen Zustand der Server anfordern. Um die für das Audit als wichtig erachteten Daten bereitstellen zu können, nutzen die Administratoren verschiedene in Windows integrierte oder von Drittanbietern bereitgestellte Tools zur Reporterstellung.

Um ein möglichst aussagekräftiges Endergebnis zu erhalten, sollten einige wichtige Komponenten des Active Directory im Standard-Audit auf jeden Fall berücksichtigt werden. Welche das sind und was es sonst noch bei der Erstellung von AD-Standard-Audits zu beachten gilt, erläutern die folgenden Absätze.

### 2.1.1 Den Audit-Umfang ermitteln

Wenn Sie ein internes oder externes Audit des Active Directory durchführen wollen, müssen Sie zunächst die Größe der AD-Umgebung sowie alle Details zur Infrastruktur ermitteln. Sie benötigen mindestens die folgenden Informationen, um den Audit-Umfang abschätzen zu können:

- Anzahl der Active Directory Forests
- Anzahl der Active Directory Domains
- Anzahl der Domain-Controller pro Domain

- Anzahl der Vertrauensstellungen (Trust Relationships) pro Domain
- NetBIOS- und DNS-Namen pro Domain
- Struktur der Organisationseinheiten pro Domain

Die meisten Unternehmen beziehen sinnvollerweise auch Windows-Server in ihre Audits ein. Um sich einen Überblick über die relevanten Server zu verschaffen, sind folgende Informationen erforderlich:

- Anzahl der Windows-Server pro Domain
- Liste der wichtigsten Anwendungen pro Server (Personalwesen, Finanzen, immaterielle Güter, persönliche Daten usw.)
- Liste der Betriebssysteme pro Windows-Server
- Liste der physischen Standorte des Unternehmens
- Aufschlüsselung der IT-Struktur pro Standort
- Sicherheitsplanung und -umsetzung durch Gruppenrichtlinien und Organisationseinheiten, sofern vorhanden

### 2.1.2 Das Audit-Programm entwickeln

Die Entwicklung des Audit-Programms hängt in der Regel von vier Faktoren ab: Umfang des Audits, Anzahl der Stichproben, vorhandene Compliance-Vorgaben und Anzahl der untersuchten Sicherheitseinstellungen. Änderungen an nur einem dieser Faktoren können Auswirkungen auf das gesamte Audit-Programm haben. Darüber hinaus sollten auch die für das Audit zur Verfügung stehenden Ressourcen berücksichtigt werden. Ausschlaggebend sind hier vor allem der Zeitaufwand und damit verbunden die Anzahl der benötigten Personen.

Bei den meisten Audits stehen Compliance-Vorgaben im Vordergrund: Sie müssen durch das Endergebnis erfüllt werden, um Strafzahlungen oder zusätzlichen Aufwand zur Nachbesserung zu vermeiden. Die Compliance-Vorgaben lassen sich dabei meist nicht reduzieren, da sie verpflichtend vorgeschrieben sind und eingehalten werden müssen. Allerdings sollte ein gutes Audit-Programm idealerweise eine gute Balance zwischen den oben genannten vier Faktoren berücksichtigen.

Je mehr Stichproben von unterschiedlichen Servern in das Audit einbezogen werden, desto verlässlicher sind die Ergebnisse. Bei großen Umgebungen mit mehreren Domänen ist es allerdings oft erforderlich, die insgesamt aufgewendete Audit-Zeit zu erhöhen; alternativ kann die Anzahl der untersuchten Sicherheitseinstellungen reduziert werden. Bei kleineren Umgebungen mit einer relativ geringen Anzahl an Stichproben können hingegen mehr Sicherheitseinstellungen untersucht und somit größere Bereiche der Windows-Umgebung abgedeckt werden.

Letztendlich gilt es folglich, die verschiedenen Faktoren gegeneinander abzuwägen und einen ausgewogenen Kompromiss für die individuellen Anforderungen des eigenen Unternehmens zu finden. Ergebnis dieser Überlegungen ist ein Audit-Programm, das aus einer Liste von Berichten für jeden Server besteht.
Idealerweise deckt das Audit-Programm unter anderem folgende Informationen ab:

- Tool zum Erstellen des Berichts
- Spezielle Anweisungen zum Tool, z. B. Befehlszeilenbeispiele, Speicherort auf dem Server, auszuwählende Menüs, Optionen usw.
- Server, auf denen das Tool ausgeführt werden soll
- Format, in dem der Bericht erstellt werden soll (.doc, .xls, .txt usw.)
- Name des Reports

### 2.1.3 Analyse und Audit-Bericht

Anschließend gilt es, die erstellten Berichte anhand verschiedener Kriterien zu analysieren; diese können von Unternehmen zu Unternehmen stark variieren, da jede Firma unterschiedlich hohe Anforderungen an die einzelnen Zugriffsberechtigungen hat.

Bevor Sie die Analyse durchführen können, benötigen Sie die folgenden Dokumentationen:

- Protokoll der Befragung des Administrators
- Unternehmensdokumentation hinsichtlich Sicherheitskonfigurationen und -kontrollen
- Dokumentation zum Server-Aufbau
- Microsoft-Branchenstandards für Sicherheitskontrollen
- Alle Berichte zum Audit-Programm

Auf Grundlage dieser Dokumente können Sie die Analyse durchführen. Das Ergebnis ist eine Liste mit Sicherheitseinstellungen, die nicht den Sicherheitsrichtlinien und -konfigurationen des Unternehmens entsprechen. Im Abschlussbericht werden diese unzureichenden Sicherheitssteuerungen in der Regel als

Abweichungen ausgewiesen. Der Bericht sollte für jede Ausnahme angeben, was erwartet und was ermittelt wurde. Normalerweise werden die Ausnahmen für jedes Gerät einzeln aufgelistet. Weitreichende Ausnahmen, die größere Bereiche betreffen, müssen allerdings im Bericht nur einmal mit einem entsprechenden Hinweis aufgeführt werden.

Die meisten Berichte enthalten neben einer Liste der Sicherheitseinstellungen und der gefundenen Probleme auch Hintergrundinformationen zu den einzelnen Abweichungen sowie empfohlene Lösungen.

### 2.1.4 Bedenken gegenüber Standard-AD-Audits

Da bei den meisten AD-Audits die gleichen Verfahren und Prozesse eingesetzt werden, arbeiten die Auditoren oft unter ähnlichen Bedingungen – unabhängig davon, mit welcher Umgebung sie es zu tun haben. Vor diesem Hintergrund ist es wenig erstaunlich, dass sich die Bedenken der Auditoren ähneln. Ein Großteil davon mag unbegründet, aber nicht von der Hand zu weisen sein, v. a. folgende Punkte sind jedoch durchaus gerechtfertigt:

- **Zugriffsberechtigungen werden nur für das Audit geändert**
  Derartige Bedenken sind zwar in der Regel unbegründet, es gibt jedoch einzelne Administratoren, die so vorgehen. Dagegen lässt sich nur wenig unternehmen: Denn selbst wenn Sie dabei sind, wenn der Administrator den Bericht erstellt, können Sie nicht sicher sein, ob im Vorfeld bestimmte Modifikationen durchgeführt wurden. Die einzig sinnvolle Möglichkeit, um das auszuschließen, bieten kontinuierliche Audits, die alle Änderungen zuverlässig erfassen.

- **Textdokumente sind nicht zuverlässig**
  Dieser Einwand ist zwar berechtigt, aber die dahinter stehende Annahme ist falsch: Viele Auditoren gehen davon aus, dass ein Screenshot zuverlässiger sei als eine Textdatei. Dabei lassen sich Screenshots fast ebenso leicht verändern wie Textdateien. Gleichzeitig haben Screenshots einen entscheidenden Nachteil: Wenn Sie für das Audit ausschließlich Bilddateien erhalten, kann der Zeitaufwand für die Datenanalyse im Vergleich zu durchsuchbaren Textdateien nahezu doppelt so hoch sein.

- **Fehlerhafte Berichte**
  Auditoren befürchten oft, dass sie falsche Informationen erhalten. Die Hauptbedenken sind dabei, dass der Administrator einzelne Daten vor dem Erstellen des Berichts geändert hat (siehe oben) oder dass nicht die korrekten Informationen zur Verfügung gestellt werden. Da die Arbeit mit einer falschen Datenbasis reine Zeitverschwendung ist, sind korrekte und präzise Daten von zentraler Wichtigkeit. Die Berichte, mit denen Sie arbeiten, müssen daher auf jeden Fall die richtigen Informationen enthalten – und das unabhängig davon, ob Sie vor Ort sind, das Audit remote durchführen oder darauf vertrauen müssen, dass Ihnen die richtigen Informationen bereit gestellt werden.

- **Änderungen zwischen den Audits werden nicht erfasst**
  Ein Standard-Audit ist immer nur eine Momentaufnahme des Active Directory. Das bedeutet, dass im Audit keine Änderungen berücksichtigt sind, die vor oder nach der Reporterstellung durchgeführt wurden bzw. werden. In der Praxis nehmen IT-Abteilungen allerdings auch zwischen den Audits zahlreiche Modifikationen am Active Directory vor. Diese werden – wie auch die zugehörigen Berechtigungskontrollen – nicht erfasst und bleiben dadurch unbemerkt. Das macht das gesamte Netzwerk und damit auch das Unternehmen verwundbar für Angriffe.

  Abbildung 1 zeigt, wie ein Standard-Audit auf dem Zeitstrahl aussieht.

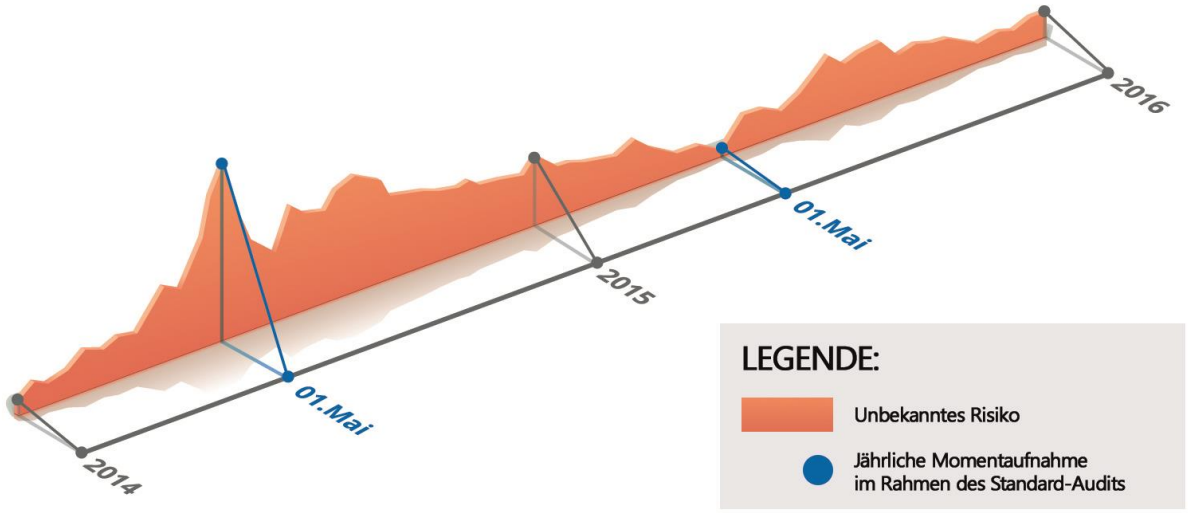



*Abbildung 1: Standard-Audit mit Momentaufnahme des Active Directory im zeitlichen Verlauf*

## 2.2 Kontinuierliches Auditing

Um die Mängel des Standard-Audits zu beheben, bei dem lediglich Momentaufnahmen des Active Directory ausgewertet werden, hat die Auditing-Community besagtes Konzept der kontinuierlichen Audits entwickelt. Dieses Konzept ist genial, die typische Umsetzung ist es in der Regel leider nicht: Häufig verwenden IT-Abteilungen weiterhin die vorhandenen Tools, nur einfach häufiger oder regelmäßig. Das Endergebnis kommt einem kontinuierlichen Auditing möglicherweise zwar relativ nahe, da mehrere Berichte für jede Sicherheitseinstellung erstellt werden. Doch es gibt einen gravierenden Nachteil: Die einzelnen Berichte müssen meist manuell und damit zeitaufwändig auf Änderungen untersucht werden, und zwar durch den Vergleich mit den zuvor erstellten Reports.

Abbildung 2 zeigt ein typisches kontinuierliches Auditing auf einem Zeitstrahl.

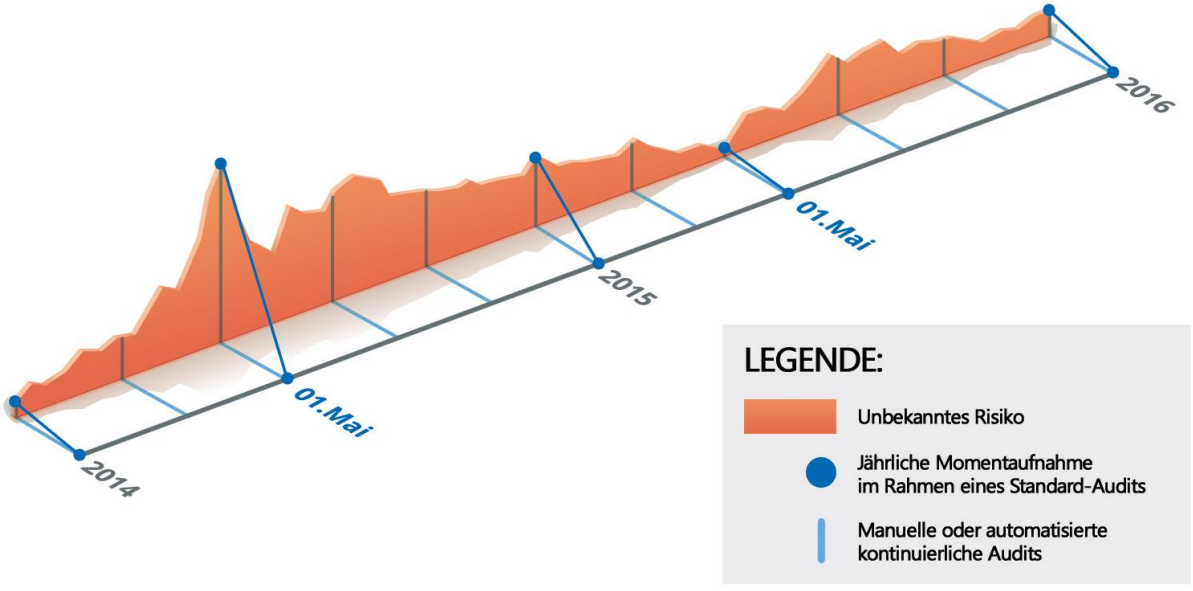



*Abbildung 2: Kontinuierliches Auditing im zeitlichen Verlauf*

Es gibt etliche Tools, mit denen Administratoren Berichte regelmäßig erstellen und planen können. Diese Werkzeuge sind in der Regel kostenlos oder sehr kostengünstig erhältlich, wie beispielsweise:

- Active-Directory-Benutzer und -Computer: Gespeicherte Abfragen
- DumpSec (GUI- und Befehlszeilenoptionen)
- PowerShell (Basis-PowerShell und Active-Directory-Modul für PowerShell)
- PowerGUI (ein Tool von Dell/Quest basierend auf deren ActiveRoles Management Shell for Active Directory)
- Geplante Aufgaben (in jeden Windows-Computer integriert)

## 2.3 Echtes kontinuierliches AD-Audit

Im Gegensatz zu den bereits vorgestellten Audit-Arten ermöglicht nur ein wirklich kontinuierliches Auditing die lückenlose Überwachung des Active Directory. Denn weder ein jährliches noch ein in kürzeren Abständen regelmäßig durchgeführtes Momentaufnahmen-Audit kann Änderungen an den AD-Sicherheitseinstellungen konstant überwachen; beide Audit-Arten setzen die Unternehmensumgebung dadurch hohen potentiellen Risiken aus.

Ein wirklich kontinuierliches Auditing bedeutet, dass ein lückenloses Erfassen und Melden sicherheitskritischer AD-Änderungen die Momentaufnahmen durchgängig ersetzt.

Lösungen für ein – im wahrsten Sinne des Wortes – kontinuierliches Auditing zeichnet folgende Funktionen aus:

- Alle im Active Directory vorgenommenen Änderungen werden erfasst (siehe Abbildung 3).
- Die Berichte geben eindeutig wieder, ob und wann Sicherheitseinstellungen geändert wurden, inklusive Einzelheiten dazu, wann, von wem und was genau geändert wurde.
- Es ist möglich, bestimmten Personen Lesezugriff zu geben, so dass Auditoren Berichte jederzeit nach eigenem Ermessen erstellen können.
- Benutzerdefinierte Berichte können zu bestimmten Usern, Computern und Gruppen definiert werden.
- Durch das Anlegen von Alarmen wird der Administrator bei Änderungen an wichtigen Zugriffsberechtigungen sofort informiert.

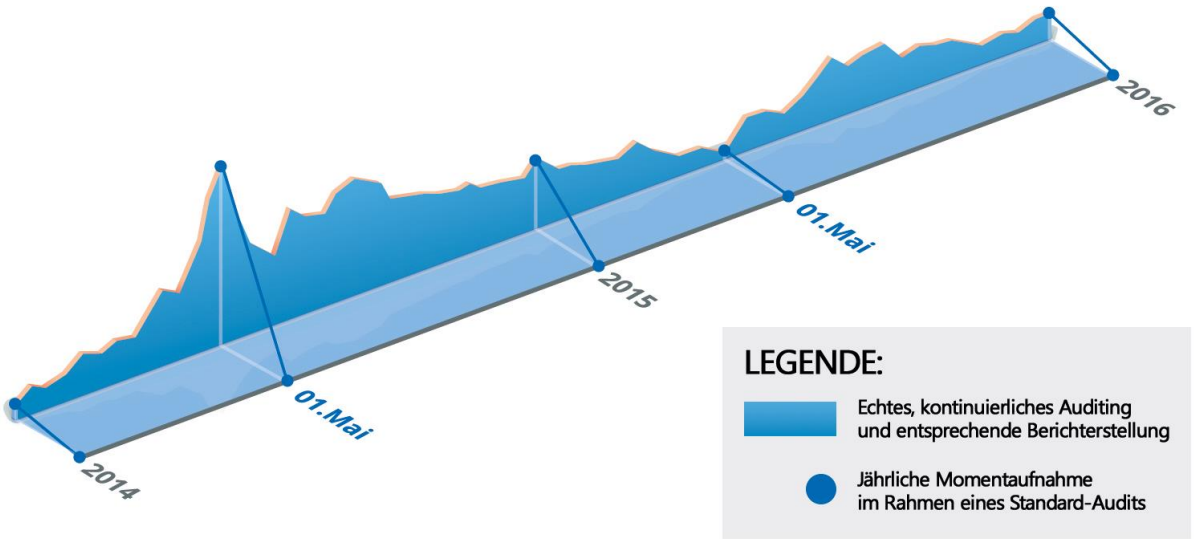



*Abbildung 3: Echtes kontinuierliches Auditing im zeitlichen Verlauf*

# 3 ADAudit Plus

Derzeit gibt es nur wenige Angebote auf dem Markt, mit denen ein wirklich kontinuierliches AD-Auditing möglich ist. Eines davon ist ADAudit Plus von ManageEngine. Mit der webbasierten Lösung können IT-Administratoren das Active Directory mit relativ geringem Aufwand dauerhaft überwachen und Änderungen lückenlos auswerten. Eine Alarmfunktion informiert die AD-Verantwortlichen zudem unmittelbar, wenn wichtige Zugriffsrechte geändert werden. Auf diese Weise können IT-Abteilungen die Sicherheit ihrer AD-Umgebung einfach und effizient erhöhen.

Wie das genau funktioniert und welchen Reports IT-Administratoren dabei besondere Aufmerksamkeit schenken sollten, erfahren Sie in den nächsten Absätzen.

## 3.1 Jede AD-Änderung wird erfasst und dokumentiert

Um alle AD-Änderungen dauerhaft dokumentieren und auswerten zu können, nutzt ADAudit Plus unter anderem die Log-Dateien der diversen Windows Domain Controller. Diese Sicherheitsprotokolle bieten umfangreiche Informationen zu Änderungen an AD-Objekten. Windows überschreibt diese allerdings bereits nach einer relativ kurzen Zeit, da Microsoft den zur Verfügung stehenden Speicherplatz auf vier Gigabyte beschränkt hat. ADAudit Plus speichert die Protokolle in einer eigenen Datenbank, ehe sie überschrieben werden, und bereitet sie so auf, dass sie für die verschiedenen Berichte nutzbar sind.

Insgesamt bietet ADAudit Plus mehr als 150 Berichte mit unterschiedlicher Detailtiefe zu AD-Änderungen an Benutzern, Gruppen, Organisationseinheiten, Gruppenrichtlinien sowie User-Log-ons. Die sogenannten Summary Reports ermöglichen einen schnellen Überblick über die AD-Umgebung. Per Mausklick lassen sich bei Bedarf ausführliche Informationen darüber anzeigen, was im Active Directory genau geändert wurde und wer die Änderung wann vorgenommen hat; zudem stellt die Lösung die alte Konfiguration der neuen gegenüber.

Um bei der Vielzahl an Informationen nicht den Überblick zu verlieren, bietet das Dashboard von ADAudit Plus gerade für neue Nutzer eine gute Orientierungshilfe. Es fasst die wichtigsten Informationen zu AD-Änderungen komprimiert zusammen und hilft so, Anomalien schnell und einfach aufzuspüren. Standardmäßig enthält es Grafiken zu folgenden Punkten (weitere können individuell hinzugefügt werden):

- **Account Management**: An welchen Computern , Gruppen oder Usern wurden Änderungen vorgenommen?
- **Top User Log-on Failures**: Bei welchen Benutzer-Accounts sind die meisten Anmeldefehler aufgetreten?
- **Log-on Failures – Error Code**: Was war die Ursache für die fehlgeschlagenen Log-on-Versuche?
- **Log-on Peak Hour Usage**: Zu welchen Uhrzeiten wurden besonders viele Anmeldeversuche vorgenommen?
- **Account Locked Out Users**: Wurden über einen bestimmten Zeitraum besonders viele Anwenderkonten gesperrt?

Auch hier können sich Administratoren per Klick auf die jeweilige Grafik detaillierte Informationen anzeigen lassen.

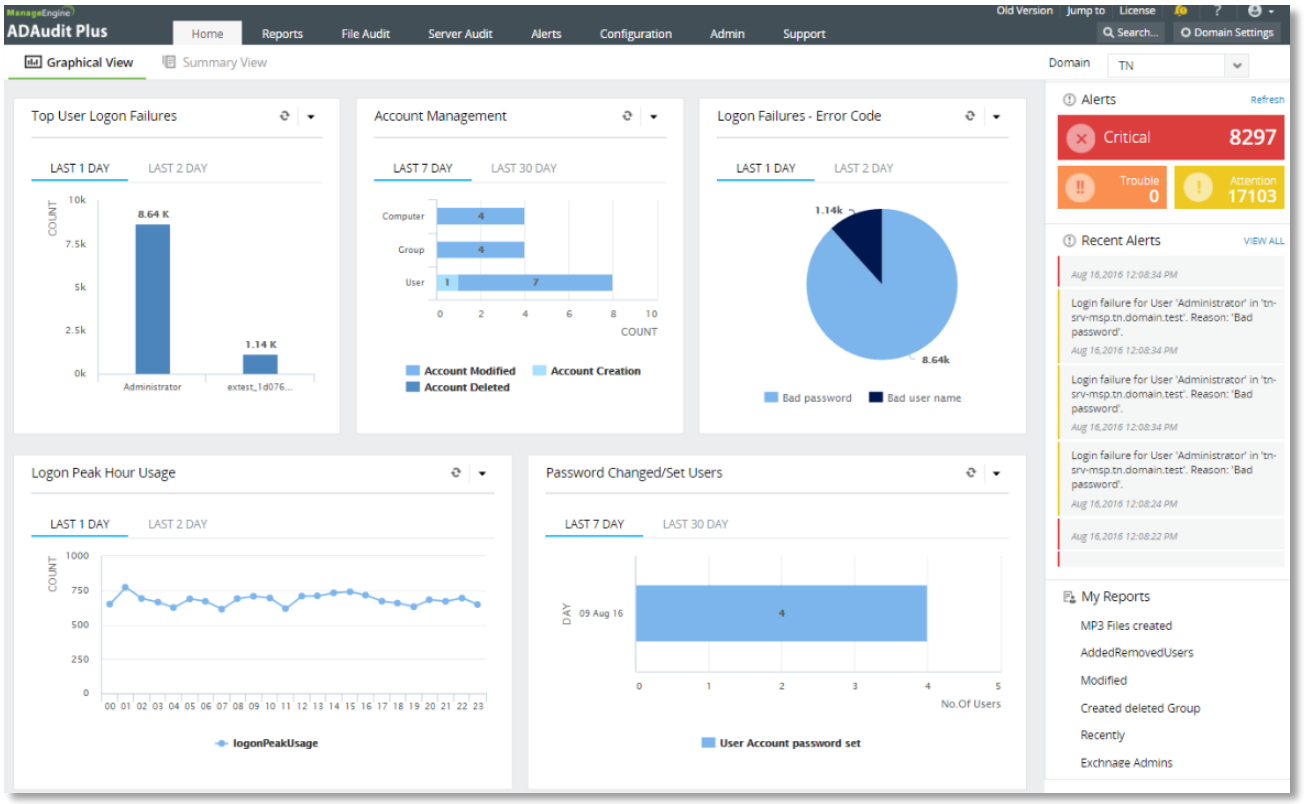



*Abbildung 4: Das Dashboard von ADAudit Plus ermöglicht IT-Administratoren einen schnellen Überblick über die wichtigsten AD-Änderungen.*

## 3.2 Lesezugriff für alle Berichte

Ein weiterer wichtiger Aspekte beim AD-Auditing ist die Möglichkeit, mit verschiedenen Rollen und Zugriffsberechtigungen zu arbeiten. Denn auf diese Weise lässt sich einfach gewährleisten, dass jeder Anwender nur die Berechtigungen erhält, die er für seine Aufgaben tatsächlich benötigt – sei es für die Sicherheitskonfiguration, die Reporterstellung oder das Auditing. Idealerweise sollten sich die Rollen sowohl durch Windows-Berechtigungen als auch durch das AD-Auditing-Tool steuern lassen.

In ADAudit Plus können Sie die Rolle eines Anwenders schnell und leicht festlegen. Um beispielsweise einem Auditor Zugriff auf die Berichte zu ermöglichen, weisen Sie dessen Profil einfach die Berechtigung „Operator" zu. Anschließend kann der Auditor auf alle Berichte zugreifen, jedoch nicht auf die Konfiguration und den Admin-Bereich, wie in Abbildung 5 dargestellt; eine Installation von ADAudit Plus ist dazu nicht erforderlich.

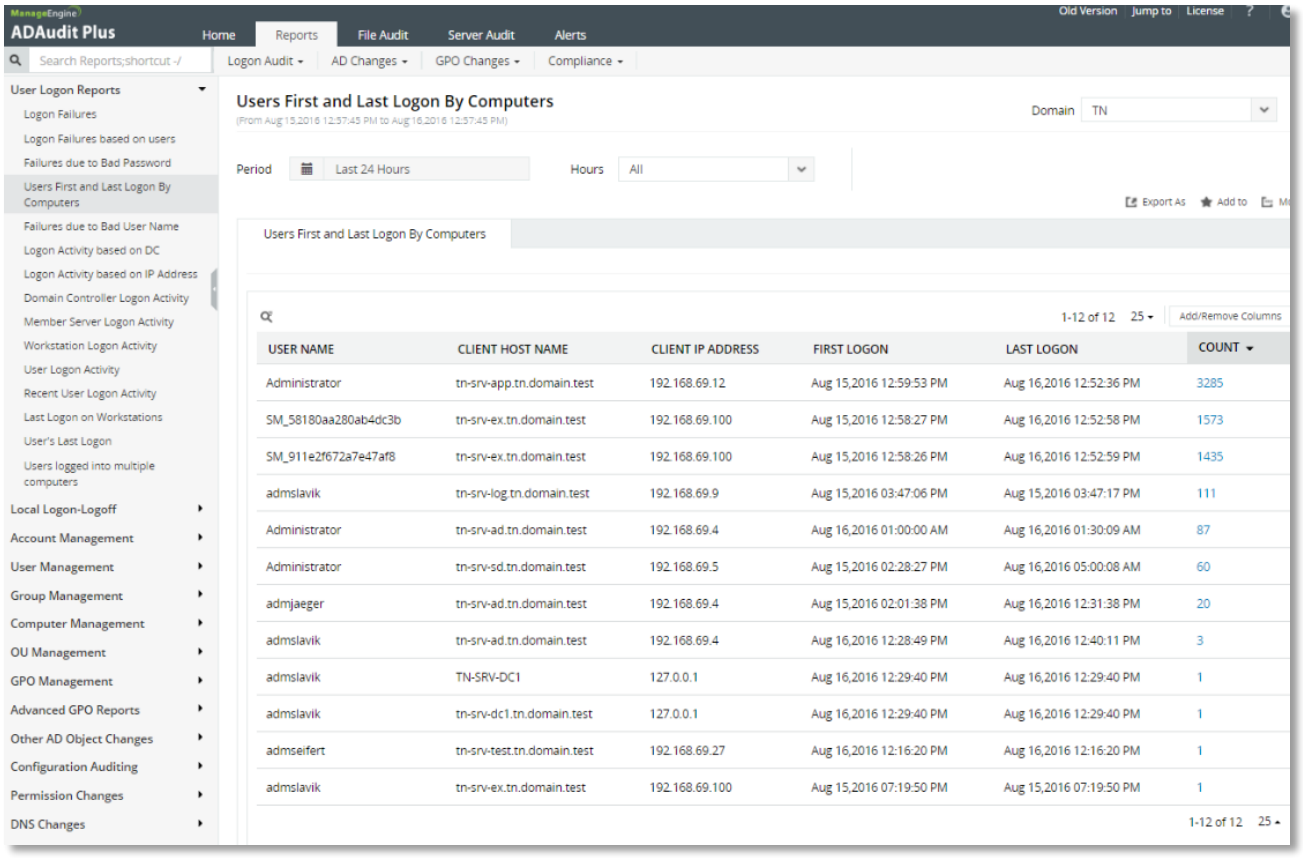



*Abbildung 5: ADAudit Plus ermöglicht Lesezugriff auf Berichte.*

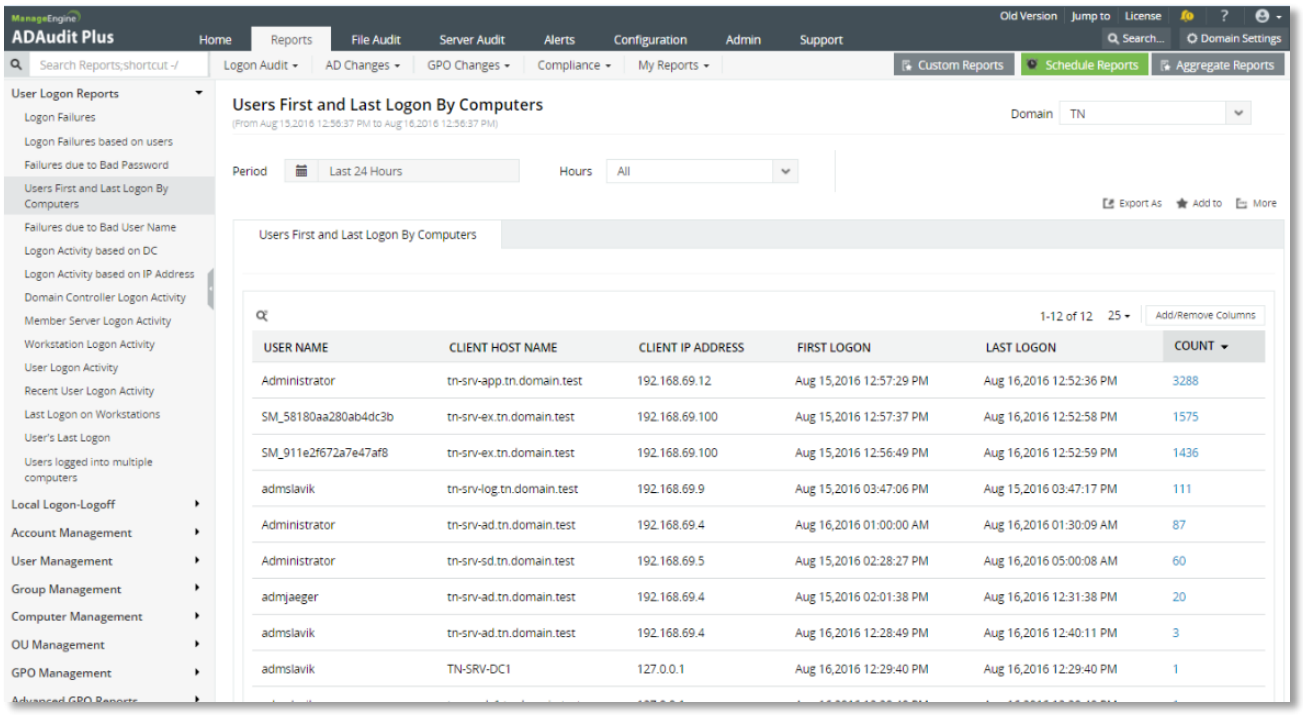



*Abbildung 6: Administratorsicht von ADAudit Plus: Dem Administrator stehen oben zusätzlich die Reiter „Konfiguration“ und „Admin“ zur Verfügung.*

## 3.3 Erstellung benutzerdefinierter Berichte

Jede Active-Directory-Installation verfügt über spezifische Benutzer, Gruppen, Servicekonten etc. Diese Accounts müssen genau wie alle anderen integrierten Benutzer und Gruppen überwacht werden. Mit ADAudit Plus können Sie dies mit Hilfe individueller Reports einfach bewerkstelligen.

## 3.4 Einfach zu erstellende Alarme

Ein weiteres wichtiges Feature einer echten kontinuierlichen AD-Auditing-Lösung ist eine zuverlässige Alarmfunktion, die den IT-Administrator bei kritischen Modifikationen des Active Directory umgehend informiert.

In ADAudit Plus können Sie für jeden vorkonfigurierten oder benutzerdefinierten Report einfach und schnell einen individuellen Alarm festlegen (siehe Abbildung 7). Dabei lässt sich für jedes Ereignis einstellen, ob der Alarm auf dem Dashboard von ADAudit Plus angezeigt oder per E-Mail an einen oder mehrere Empfänger versendet werden soll.

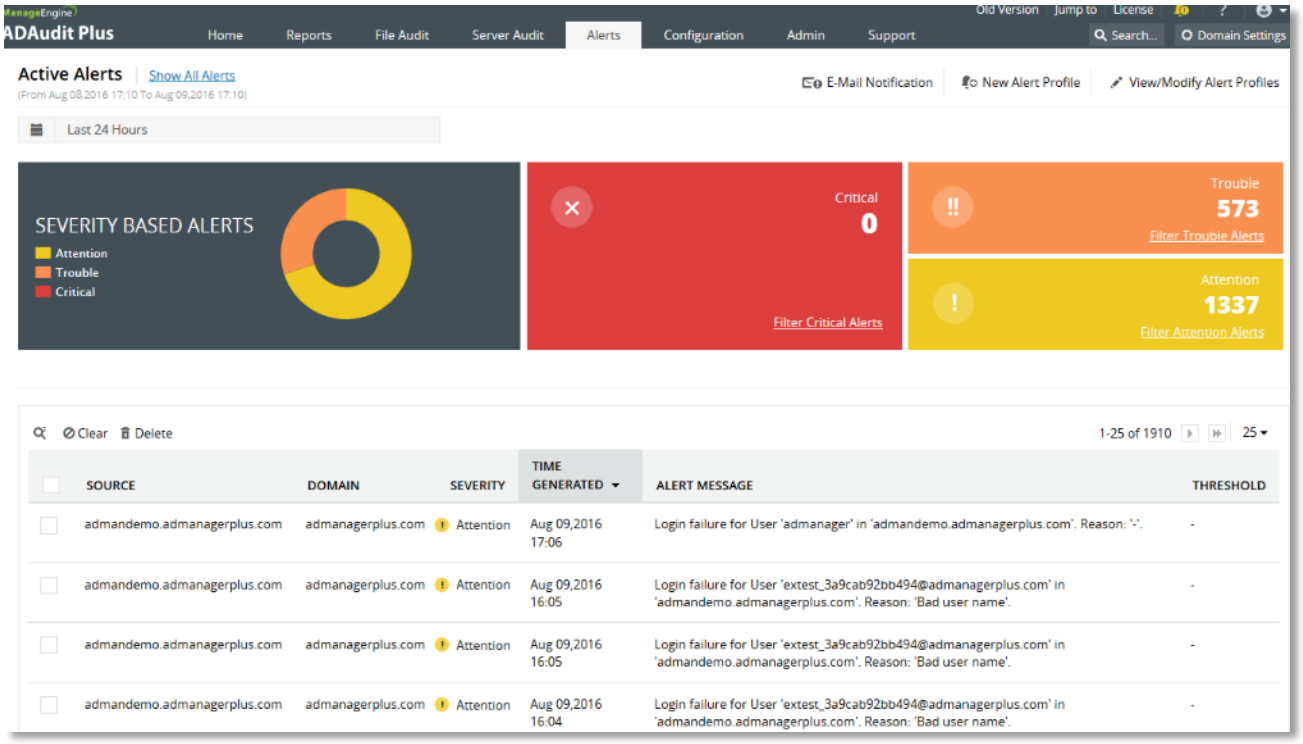



*Abbildung 7: Alarme ermöglichen Ihnen Einblicke in Änderungen an AD-Objekten in Echtzeit.*

## 3.5 Eine Auswahl an AD-Berichten

Änderungen können weitreichende Auswirkungen auf die Sicherheit des Active Directory haben – Sie als IT-Administrator bzw. IT-Verantwortlicher werden diese daher genau unter die Lupe nehmen wollen. ADAudit Plus ist ein sehr umfangreiches und mächtiges Reporting-Tool, das kontinuierlich aufzeichnet, was Sie überprüfen möchten. Jedes Unternehmen hat eigene Sicherheitsrichtlinien festgelegt. Um die Einhaltung der Sicherheitsvorschriften zu überwachen, bietet ADAudit Plus eine Vielzahl an Reports für verschiedene Bereiche. Aus diesen können Sie genau die Reports auswählen, die Ihre Anforderungen genau erfüllen, und so die Sicherheit der AD-Umgebung verbessern.

Im Folgenden stellen wir beispielhaft einige Reports vor, mit denen Sie AD-Änderungen mit recht geringem Aufwand im Auge behalten können.

### Alarmkonfiguration

ADAudit zeichnet die von Ihnen ausgewählten AD-Änderungen, die als Ereignisse in den Eventlogs der Domain-Controller und anderer Server zu finden sind, vollständig auf. Das erspart die Notwendigkeit, die auditierten Ereignisse aktiv, auf eigene Initiative hin nach kritischen Vorfällen zu durchsuchen. Sie können sich selbstverständlich durch ADAudit Plus alarmieren lassen, wenn es zu Ereignissen kommt, die Sie besonders interessieren.

Dafür ist lediglich ein sogenanntes „Reportprofil" erforderlich – im Grunde ein Ereignisfilter. ADAudit stellt Ihnen dazu eine Vielzahl bereits vorkonfigurierter Profile zur Verfügung. Sollte zu einem bestimmten Ereignis kein passendes Profil vorhanden sein, können Sie sich auf einfache Weise ein eigenes erstellen.

Wir empfehlen dabei folgende Vorgehensweise:

## Schritt 1: Erstellung eines neuen Reportprofils

Zunächst erstellen Sie ein neues Reportprofil („New Report Profile" im Reiter „Configuration"), vergeben möglichst einen „sprechenden Namen" und fügen eine Beschreibung hinzu (siehe Abbildung 8). Danach wählen Sie die Ereigniskategorie aus, in die das zu überwachende Ereignis einzuordnen ist, und wählen die passende Aktion (‚Actions') aus. Nun brauchen Sie nur noch festzulegen, welche Nutzer oder Gruppen Sie speziell im Visier haben – und schon ist Ihr Profil einsatzbereit.

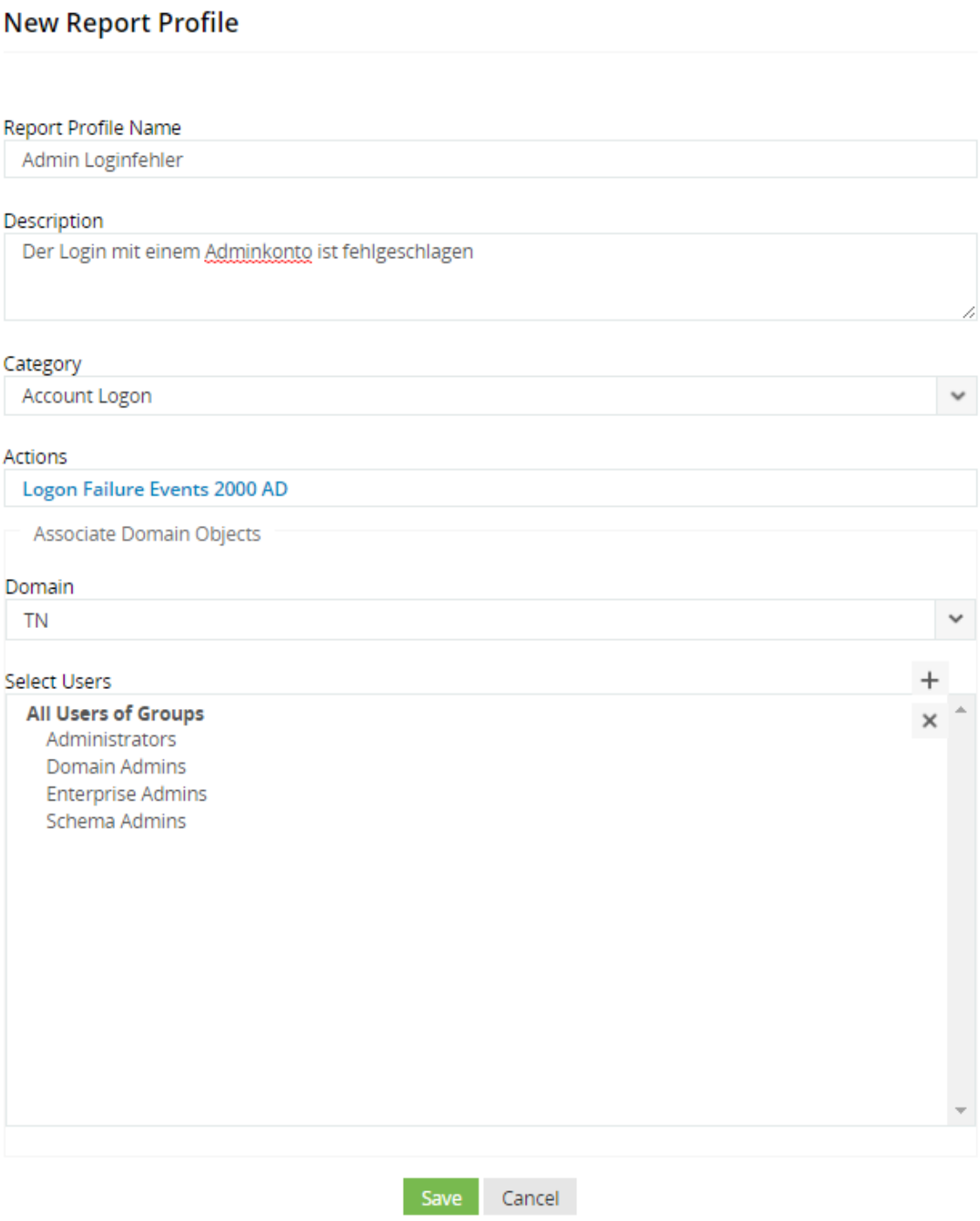



*Abbildung 8: So erstellen Sie ein Reportprofil für fehlgeschlagene Login-Versuche von Administratoren in ADAudit Plus.*

## Schritt 2: Erstellung des Alarmprofils

Im zweiten Schritt erstellen Sie das Alarmprofil („New Alarm Profile" im Reiter „Alerts"). Dabei gehen Sie ähnlich vor wie beim Reportprofil. Bei „Category" geben Sie das Profil an, mit dem Sie die Ereignisse filtern (z. B. das gerade von Ihnen erstellte) und tragen ein, wer die Alarm-E-Mail erhalten soll (siehe Abbildung 9).

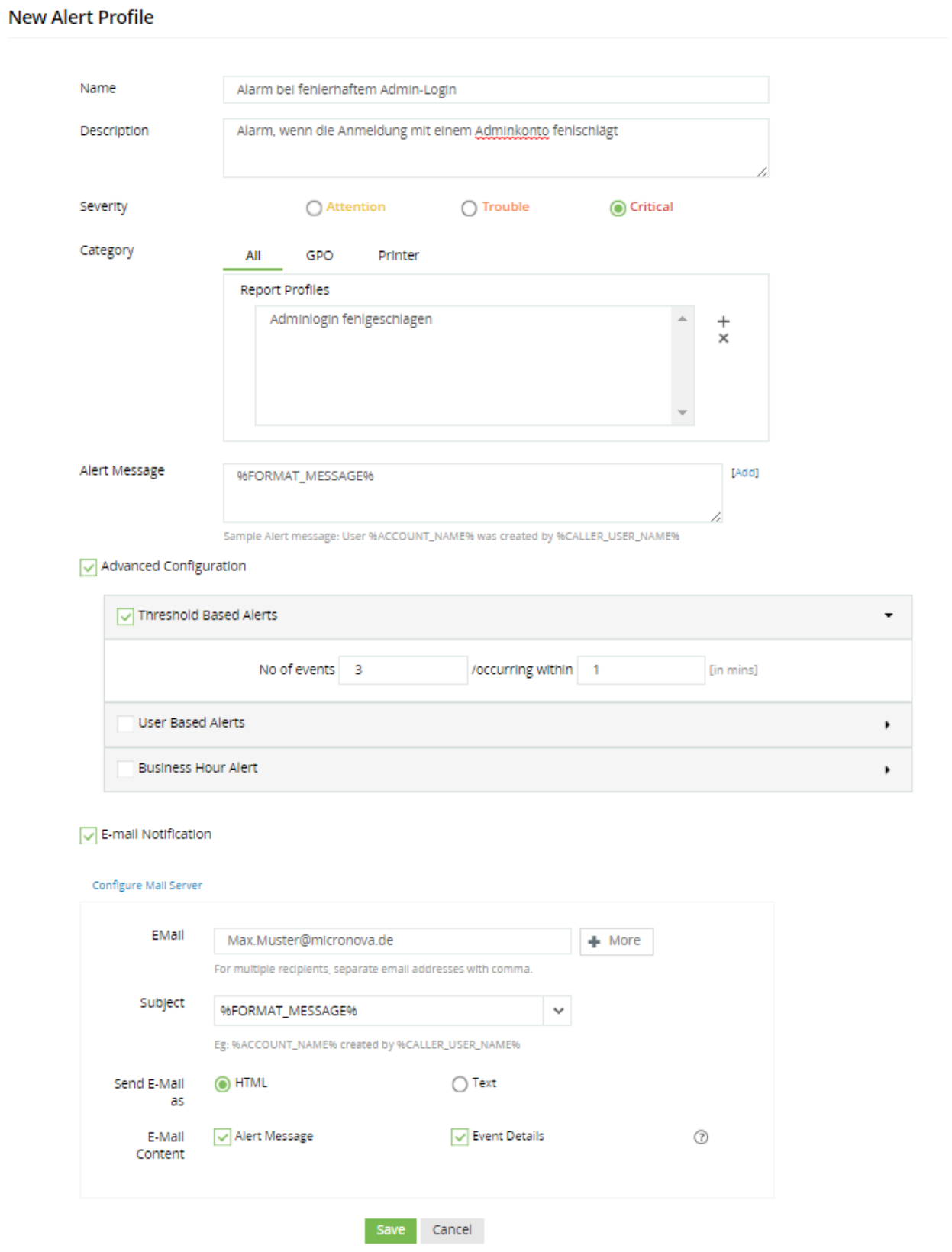



*Abbildung 9: Erstellung eines neuen Alarmprofils für die Kategorie „Administrator Login fehlgeschlagen" in ADAudit Plus.*

Sobald Sie das Alarmprofil angelegt haben, informiert ADAudit Sie automatisch, wenn das zu überwachende Ereignis eintritt. Im Abbildung 10 sehen Sie beispielsweise, wie ein von ADAudit per E-Mail versendeter Bericht zu fehlgeschlagenen Log-ons nach Usern aussehen würde.

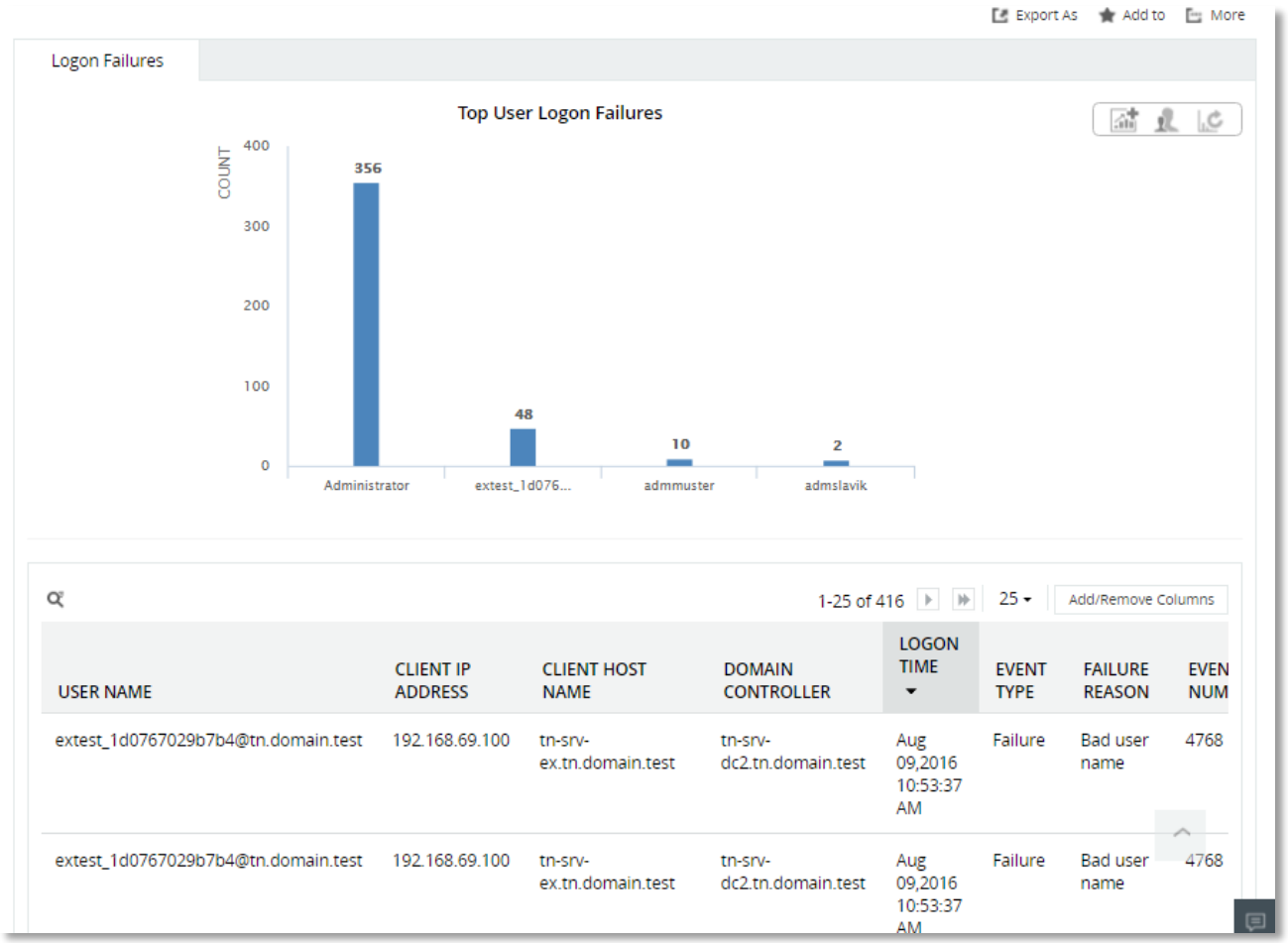



*Abbildung 10: Der „Top User Log-on Failures"-Report zeigt Ihnen die fehlgeschlagenen Log-ons nach Usern.*

## Weitere Berichtsbeispiele:

### Bericht über neu erstellte Freigaben

Erstellt ein Administrator eine neue Verzeichnisfreigabe, gewährt er damit auch einer oder mehreren Personen Zugriff auf bestimmte Dateien. Vor diesem Hintergrund möchten Sie sicher auf dem Laufenden bleiben, welche Freigaben existieren und welche neu hinzugekommen sind, um diese gegebenenfalls z. B. auf Konformität zu bestehenden Sicherheitsrichtlinien zu prüfen. Auch hier hilft ein entsprechender Bericht.

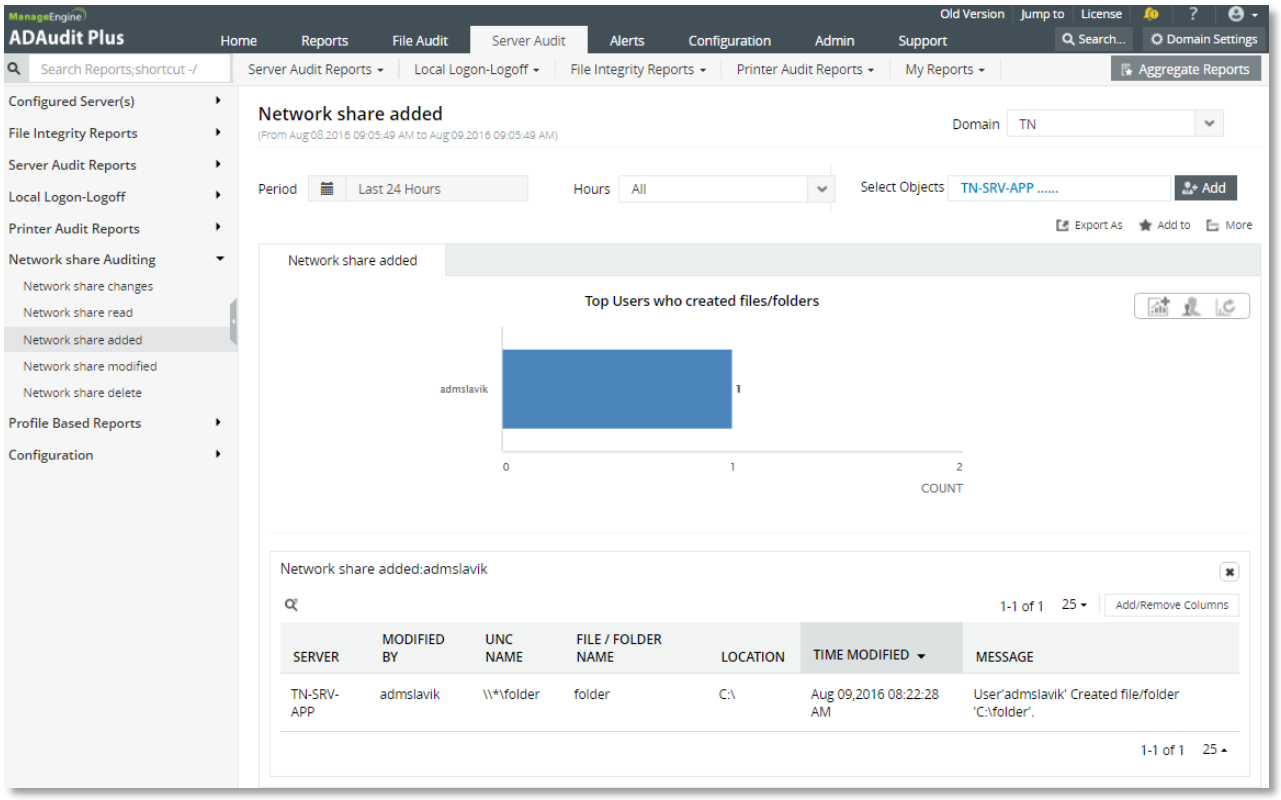



*Abbildung 11: Der Report „Network share added" listet auf, welche Freigaben in den letzten 24 Stunden erteilt wurden.*

## Bericht über Änderungen in Sicherheitsgruppen

Um Änderungen an Ihren Sicherheitsgruppen zu dokumentieren und somit auch nachvollziehen zu können, eignet sich beispielsweise der Bericht „Recently Added Members to Security Groups". Mit diesem Report sehen Sie auf einen Blick, welche Mitglieder neu in Sicherheitsgruppen aufgenommen wurden – Informationen, die Ihnen helfen können, beispielsweise einer Schattenadministration den Riegel vorzuschieben.

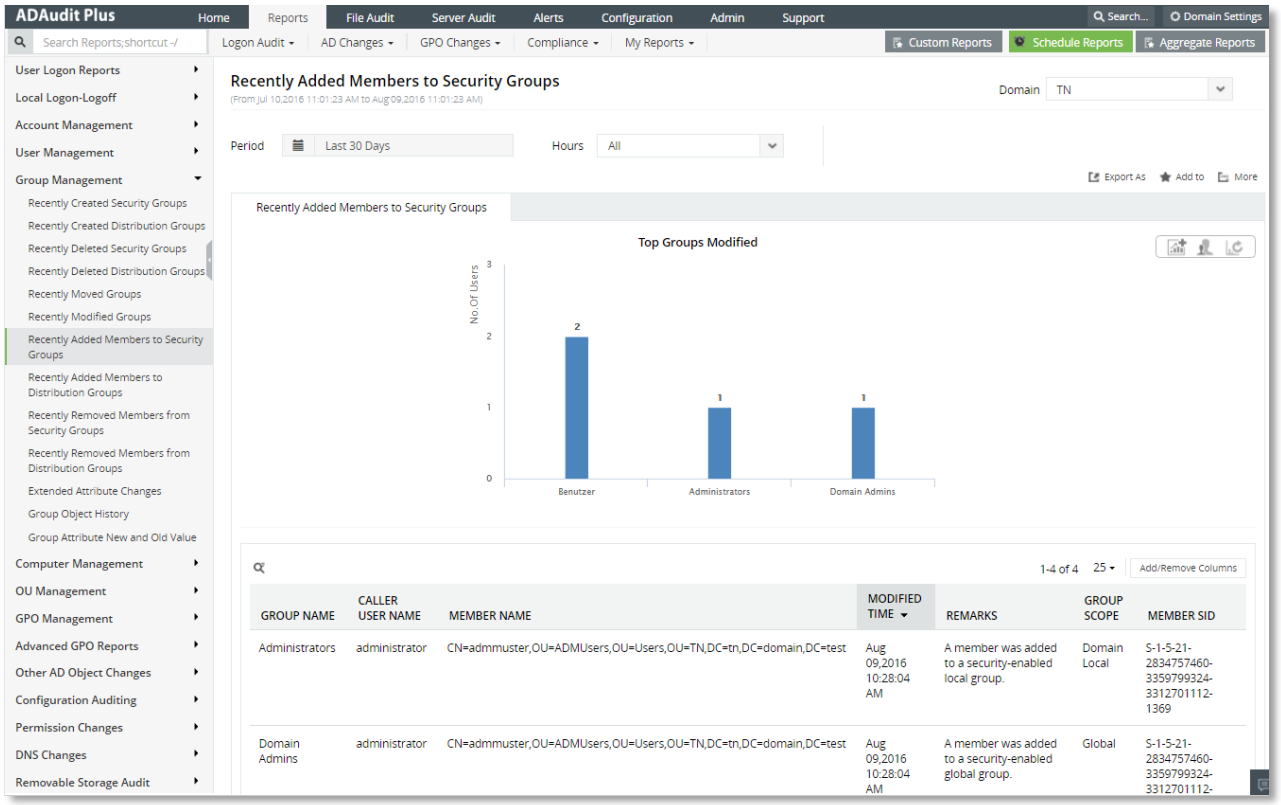



*Abbildung 12: Der Report „Recently Added Members to Security Groups" zeigt alle in den letzten 30 Tagen neu in Sicherheitsgruppen hinzugefügten Mitglieder.*

Die vorgestellten Berichte sind nur eine kleine Auswahl an Überwachungsmöglichkeiten, die Ihnen in ADAudit Plus zur Verfügung stehen. Sie können alle Berichte übrigens individuell an die spezifischen Anforderungen Ihres Unternehmen anpassen und wie beschrieben bei Bedarf einfach erweitern.

## 3.6 Zusammenfassung

Ein reibungslos funktionierendes und gut abgesichertes Active Directory entscheidet nicht nur über die Benutzerproduktivität, sondern trägt auch maßgeblich zur Unternehmenssicherheit bei. Sie sollten daher umfangreiche Maßnahmen ergreifen, um die Sicherheit und Zuverlässigkeit des AD zu gewährleisten.

AD-Standard-Audits sind hierbei ineffizient und unzureichend, da sie nicht alle Änderungen am Active Directory berücksichtigen – und damit das Risiko von Angriffen auf das Unternehmensnetzwerk erhöhen. Wesentlich besser eignen sich wirklich kontinuierliche Lösungen wie ADAudit Plus: Sie zeichnen zuverlässig sämtliche Änderungen an AD-Objekten auf. Damit liefern sie alle Informationen, die Sie zum Überwachen und Sichern Ihrer Active-Directory-Umgebung benötigen. Selbst wenn Ihnen nur begrenzte Ressourcen zur Verfügung stehen, verbessert ADAudit Plus als kostengünstige und effiziente Lösung die Sicherheit Ihres Active Directory. Eine gute Basis schaffen Sie dabei bereits, wenn Sie die für Ihr Unternehmen wichtigsten AD-Reports regelmäßig überprüfen, um Anomalien oder potentielle Angriffe frühzeitig aufspüren zu können.