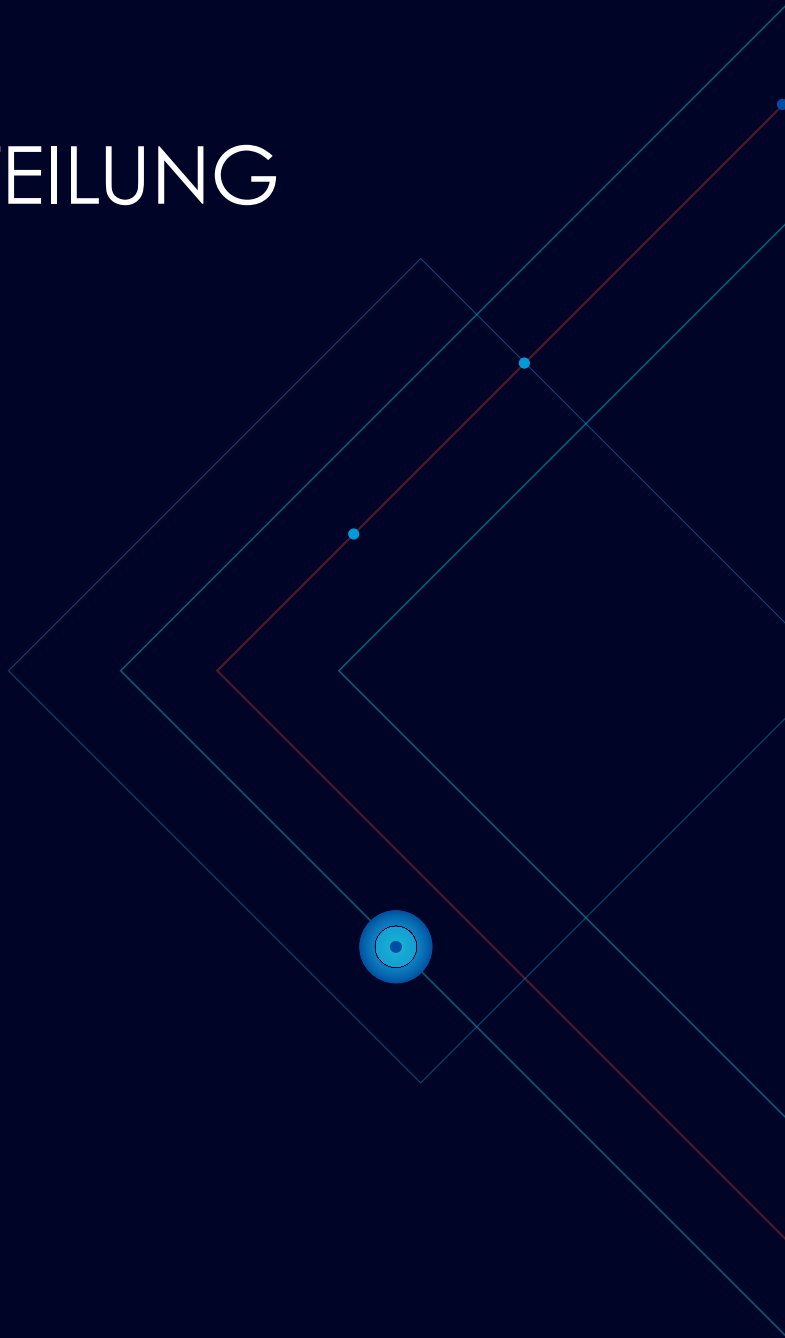
VARONIS DATENRISIKOBEURTEILUNG

AM BEISPIEL: ACME

Wo befinden sich Ihre größten Datensicherheitsbedrohungen?

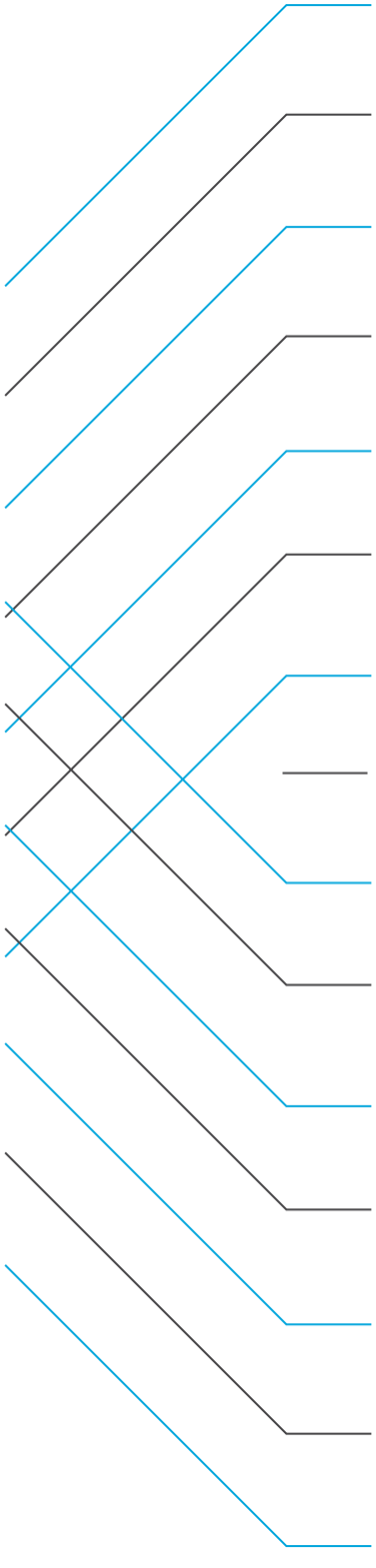
Wir zeigen es Ihnen.

Die Varonis Datenrisikobeurteilung bietet Ihnen einen ausführlichen Bericht über Teile Ihrer Unternehmensdaten:
Risikoanalyse, Stärken, Schwachstellen, Sicherheitslücken und Empfehlungen für Gegenmaßnahmen.



VARONIS

IM DETAIL:



UMFANG DER DATENRISIKOBEURTEILUNG

Der Bericht basiert auf einer Stichprobe eines Teils der Datenspeicher in Ihrem Unternehmen: inklusive Daten, Ordnern, Dateien und Berechtigungen, Benutzer und Gruppenkonten. Hervorgehobene Risikobereiche sind beispielsweise zu leicht zugängliche sensible Daten, Probleme in der Zugriffskontrolle und ähnliches.

ÜBERWACHTE FILESERVER UND DATENQUELLEN

- CIFS_FS_1
- CIFS_FS_2
- CIFS_FS_3
- CIFS_FS_4
- CIFS_FS_5
- NS_FS_1
- EXCH_1
- SP_1

INHALTE

- 331,237 GB Daten
- 90,348,156 Ordner
- 1,617,176,767 Dateien
- 701,387,576 Berechtigungseinträge

ACTIVE DIRECTORY

- 8,580 Benutzerkonten
- 14,427 Gruppen
- 9,268 Computer-Konten
- 420 deaktivierte Benutzer

Datenmaterial von ACME, das im Hinblick auf Risiken in den folgenden Bereichen analysiert wurde:

- Übermäßig exponierte, gefährdete und klassifizierte Daten
- Zugriffsrechte und Berechtigungen
- Überwachen von privilegierten Benutzer- und Endbenutzerzugriffen
- Active Directory
- Struktur der NTFS-Einträge und geteilter Berechtigungen
- Fähigkeit zur Datenhaltung/Datenspeicherung
- Compliance mit geltenden Bestimmungen

Anz. der Ordner mit offenem Zugriff

66.5 Millionen Ordner mit globalem Gruppenzugriff

Anz. der sensitiven Dateien mit offenem Zugriff

339.213.456 sensitive Dateien mit offenem Zugriff

Anz. der Ordner mit veralteten Daten

85.377.723 Ordner mit selten benutze

Dateien mit sensiblen Daten

950.534.645 Dateien enthalten sensible Daten

Anz. der Ordner mit inkonsistenten Berechtigungen

58,419

58.419 Ordner haben inkonsistente Berechtigungen

Benutzerkonten mit niemals ablaufenden Passwörtern

1,182

Benutzerkonten mit niemals ablaufenden Passwörtern

GLOBALER GRUPPENZUGRIFF:

Globale Gruppen erlauben es allen Mitarbeitern einer Organisation, auf diese Ordner zuzugreifen. Globale Gruppen sind Gruppe wie Jeder, Domänen-Benutzer und Authentifizierte Benutzer.

Zu frei verfügbare Daten sind eine weit verbreitete Sicherheitslücke. Den Schätzungen von IT-Experten zufolge dauert es im Durchschnitt ca. 6 bis 8 Stunden pro Ordner, um Gruppen mit globalen Berechtigungen zu finden und manuell zu löschen. Sie müssen die Benutzer identifizieren, die den Zugriff wirklich benötigen, neue Gruppen erstellen und anwenden und diese dann mit den richtigen Benutzern füllen.

RISIKOÜBERBLICK:

Gering | Mittel | Hoch

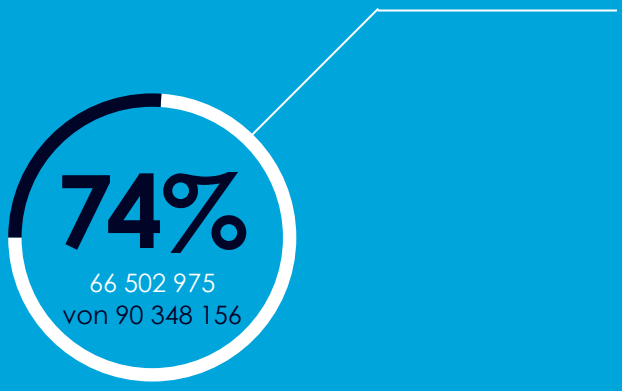
- Eine der wichtigsten Ursachen von Datenschutzverletzungen sind zu großzügige Zugriffsberechtigungen.
- Offenliegende sensible und kritische Daten stellen ein erhebliches Sicherheitsrisiko dar.
- Veraltete Benutzerberechtigungen können von Eindringlingen missbraucht werden.

EMPFOHLENE AKTIONEN:

- Entfernen von globalen Zugriffsberechtigungsgruppen, um die Ordner zu identifizieren, die für diese Gruppen offenliegen.
- Einordnen der Benutzer in neue Gruppen.
- Ersetzen der globalen Zugriffsgruppe in der ACL mit der neuen Gruppe.

Über 66.5 Millionen

Ordner mit globalem Gruppenzugriff



AUFTEILUNG DER GLOBALEN GRUPPENZUGRIFFE

- CIFS_FS_2 11%
- CIFS_FS_3 7%
- CIFS_FS_4 20%
- SP_FS_1 44%
- EXCH_FS_1 18%

SENSIBLE DATEIEN MIT GLOBALEM GRUPPENZUGRIFF

- CIFS_FS_2 2%
- CIFS_FS_3 1%
- CIFS_FS_4 2%
- SP_FS_1 82%
- EXCH_FS_1 13%

SENSITIVE DATEN:

Zahlreiche Dateien enthalten kritische Informationen über Mitarbeiter, Kunden, Projekte, Klienten oder sonstige geschäftsrelevante Informationen. Diese Daten unterliegen häufig Branchenvorschriften wie SOX, HIPAA, PCI, DSGVO, GLBA und weiteren.

Sensible Daten, die für globale Gruppen zugänglich sind, stellen ein erhebliches Risiko für das Unternehmen dar. Sie sollten identifiziert und neue Berechtigungen vergeben werden, damit nur angemessene Benutzer auf sie zugreifen können.

RISIKOÜBERBLICK:

Gering | Mittel | Hoch

- Sensible Daten enthalten häufig die persönlichsten und begehrtesten Informationen: Personenbezogene Daten, Kreditkartendaten, geistiges Eigentum, E-Mails usw.
- Eine der wichtigsten Ursachen von Datenschutzverletzungen sind zu unangemessene Berechtigungen von sensiblen Daten
- Zugriffsberechtigungen
- Unangemessen berechtigte sensible und kritische Daten

EMPFOHLENE AKTIONEN:

- Sensible Daten scannen, klassifizieren und überwachen (wo sie liegen, wer auf sie zugreifen kann und wer tatsächlich auf sie zugreift)
- Erstellen und verwalten eines Modells nach dem Prinzip der notwendigsten Berechtigung
- Pflegen einer datenzentrierten Sicherheitsrichtlinie zum Erfüllen aller gesetzlichen Auflagen im Hinblick auf sensible Daten

Über 950 Millionen

Dateien enthalten sensible Daten (950.534.645)

Über 339 Millionen

(339.213.456) sensible Dateien liegen für globale Gruppen offen

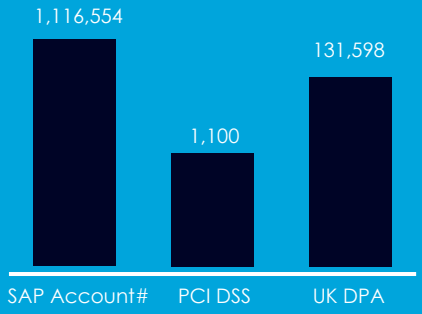
Über 50 % der sensiblen Daten liegen auf einem Dateiserver: SP_FS_1

AUFTEILUNG SENSIBLER DATEN

- CIFS_FS_2 13%
- CIFS_FS_3 12%
- CIFS_FS_4 8%
- SP_FS_1 54%
- EXCH_FS_1 13%

GESAMTANZAHL DER TREFFER NACH TYP

- SAP Acc# 1,116,554
- PCI DSS 1,100
- UK DPA 131,598



VERALTETE DATEN:

Veraltete Daten – d. h. Daten, die über eine festgelegte Aufbewahrungsfrist hinaus aufbewahrt oder bereits seit längerem nicht genutzt wurden – verursachen Kosten für Speicherung und Verwaltung und stellen ein erhöhtes (und unnötiges) Sicherheitsrisiko dar.

RISIKOÜBERBLICK

Gering | Mittel | Hoch

- Veraltete Daten werden schnell zu einem Sicherheitsrisiko und verursachen unnötige Speicherkosten.
- Veraltete Daten stellen ein unnötiges Sicherheitsrisiko dar und lassen Tür und Tor für Diebstahl oder Manipulation offen.

EMPFOHLENE AKTIONEN:

- Identifizieren der veralteten Daten, um zu entscheiden, welche Daten verschoben, archiviert oder gelöscht werden können.
- Erstellen und Umsetzen einer einheitlichen Richtlinie für den Umgang mit veralteten Daten.

253.168 GB
veraltete Daten

Über 85 Millionen
(85.377.723)
Ordner enthielten veraltete Daten

Über 75 % aller in diesem Szenario beurteilten Daten sind veraltete.

MENGE VERALTETER DATEN

- CIFS_FS_2 25%
- CIFS_FS_3 22%
- CIFS_FS_4 8%
- SP_FS_1 29%
- EXCH_FS_1 16%

VERALTETE DATEN MIT SENSIBLEN INFORMATIONEN

- CIFS_FS_2 14%
- CIFS_FS_3 11%
- CIFS_FS_4 9%
- SP_FS_1 53%
- EXCH_FS_1 13%

BENUTZERKONTEN

- 1.182 Benutzerkonten haben Passwörter, die auf unbegrenzte Zeit vergeben wurden.
- 2.555 Benutzerkonten sind veraltet, aber aktiviert.
- 46% (4.635) der Benutzerkonten sollten entfernt werden – so die Empfehlung.

GRUPPEN

- 14% der Sicherheitsgruppen haben keine Benutzer (2.034).
- 26% der Domain-Gruppen sind leer.

1.182

Benutzerkonten haben Passwörter, die nie ablaufen

KONTEN & BENUTZER:

Benutzer mit Passwörtern mit unbegrenzter Gültigkeit

Konten mit Passwörtern, die nie ablaufen, sind ein Sicherheitsrisiko.

Veraltete, aber aktivierte Benutzer

Veraltete, aber aktivierte Konten behalten alle Zugriffsberechtigungen, die ihnen während ihrer aktiven Zeit zugeteilt wurden. Damit sind sie ein Ziel für missbräuchliche und böswillige Verwendung.

Leere Sicherheitsgruppen

Leere Sicherheitsgruppen werden nicht mehr benötigt und können missbraucht werden, um Zugriff auf Daten und Ressourcen zu erlangen.

RISIKOÜBERBLICK:

Gering | Mittel | Hoch

- Veraltete Benutzerberechtigungen und veraltete Konten können für bösartige Zwecke missbraucht werden.
- Benutzer mit unnötigem Zugriff auf sensible Daten stellen ein großes Risiko für das Unternehmen dar.
- Veraltete, aber aktivierte Konten sind ein vermeidbares Sicherheitsrisiko.

EMPFOHLENE AKTIONEN:

- Veraltete, aktivierte Konten überprüfen, um zu ermitteln, ob sie gebraucht werden.
- Konten nach Bedarf löschen oder deaktivieren.
- Konten auf eine strikte Passwortrichtlinie umstellen, die regelmäßige Passwortwechsel vorschreibt.

ORDNER

- 277.277.027 Ordner mit nicht aufgelösten SIDs
- 58.419 Ordner enthalten konsistente Berechtigungen
- 1.040.040 Ordner mit einmaligen Berechtigungen

BERECHTIGUNGEN

- 423.872 Ordner wurden mit direkten Benutzer-ACEs ermittelt
- 25.551 geschützte Ordner

277 027
Nicht aufgelöste SIDs

ORDNER UND BERECHTIGUNGEN:

Nicht aufgelöste SIDs

Nicht aufgelöste Sicherheitskennungen (SIDs) treten dann auf, wenn ein Konto auf einer Zugriffskontrollliste aus dem Active Directory gelöscht wird. Nicht aufgelöste SIDs verursachen Komplexität und können ausgenutzt werden.

Inkonsistente Berechtigungen

Inkonsistente Berechtigungen treten auf, wenn Ordner oder Dateien zusätzliche Einträge für die Zugriffskontrolle von übergeordneten Instanzen erben oder dieser Vererbungsvorgang fehlschlägt. Benutzern kann unbeabsicht Zugang eingeräumt oder aberkannt werden.

RISIKOÜBERBLICK:

Gering | Mittel | Hoch

- Durch inkonsistente Vererbung werden Daten für Benutzer zugänglich, die nicht auf sie zugreifen können sollten, oder verhindern den Zugriff von Personen, die diese Daten benötigen.
- Nicht aufgelöste SIDs und inkonsistente Berechtigungen sind ein vermeidbares Sicherheitsrisiko.
- Ordner mit inkonsistenten Berechtigungen legen Daten potenziell für Insider, Hacker und andere Personen offen.

EMPFOHLENE AKTIONEN:

- Analyse der Berechtigungsstruktur, um zu überprüfen, ob individuelle Regelungen für Ordner erforderlich sind. Wenn dies nicht der Fall ist, erneutes Vererben der übergeordneten Berechtigungen durch Ordner zulassen, um individuelle ACEs zu ersetzen.
- Ordner mit nicht aufgelösten SIDs identifizieren und aus den ACLs löschen.
- Ordner mit direkten Benutzerberechtigungen identifizieren, Benutzer in die passende Gruppe einordnen und die Benutzer-ACE aus der ACL löschen.

AM HÄUFIGSTEN AUSGELÖSTE BENACHRICHTIGUNGSKATEGORIEN

- Eindringung 5
- Privilege Escalation 9
- Exfiltration 2

VERTEILUNG DER SENSIBLEN DATEIEN

- CIFS_FS_2 13 %
- CIFS_FS_3 12 %
- CIFS_FS_4 8 %
- SP_FS_1 54 %
- EXCH_FS_1 13 %

BENUTZERAKTIVITÄT

- 423.110 Öffnen von Dateien
- 182.335 Ändern von Dateien
- 65.120 Löschen von Dateien
- 22.965 Berechtigungsänderungen

750,000+

Audit-Ereignisse 950 Ereignisse mit sensiblen Daten

BENUTZERAKTIVITÄT:

Benutzeraktivität und -verhalten

Die Benutzeraktivität setzt sich aus Datei- und Berechtigungsaktivitäten mit Daten, die von Benutzern innerhalb des Unternehmens vorgenommen werden , zusammen. Dazu gehören Datei- und Berechtigungsaktivitäten, E-Mail- oder SharePoint-Aktivitäten und Aktivitäten zum Ändern von Benutzern und Gruppen in der Organisation.

Varonis überwacht und analysiert das Basisverhalten von Benutzern und Entitäten, um Ihnen Einblick in potenziell verdächtiges Verhalten und ungewöhnliche Aktivitäten zu geben

Anhand der Analysen werden ungewöhnliche Verhaltensweisen identifiziert und gemeldet, Risiken hervorgehoben und Insider-Risiken, Ransomware und zahlreiche weitere Gefahren erkannt.

RISIKOÜBERBLICK:

Gering | Mittel | Hoch

- Versuche, unbefugt auf Datenressourcen zuzugreifen oder Änderungen an ihnen vorzunehmen sind häufig ein Hinweis auf Malware, Insider-Risiken oder Cyber-Angriffe.
- Ungewöhnliche Verhaltensweisen (im Vergleich zu Nutzern der gleichen Berechtigungsgruppe) signalisieren eine potenzielle Übernahme des Kontos, Datenexfiltration und Versuche, Daten zu manipulieren.
- Auffällige Zugriffe auf sensible Daten sind ein Kennzeichen dafür, dass die Daten gefährdet und anfällig für Datenschutzverletzungen sind.

EMPFOHLENE AKTIONEN:

- Überwachung von Benutzerverhalten und Dateiaktivitäten.
- Erkennen und Melden von Sicherheitsverstößen, verdächtigen Verhaltensweisen und ungewöhnlichen Aktivitäten.
- Erstellen von Notfallplänen und Untersuchungsverfahren für den Umgang mit potenziellen Datenschutzverletzungen.

GERINGES RISIKO:

Je komplexer die Struktur eines Dateisystems, desto größer das Risiko von übermäßig exponierten Daten und Schwachstellen in punkto Sicherheit. Ein Zugriffsmanagement mit vereinfachten Prozeduren und Standards hilft, sensible Daten vor einer potenziellen Offenlegung und Insiderbedrohungen zu schützen.

1.040.040 ORDNER MIT EINMALIGEN BERECHTIGUNGEN

Empfehlung:
Die Berechtigungsstruktur überprüfen, um festzustellen, ob einmalige Berechtigungen für Ordner erforderlich sind. Andernfalls dem Ordner ermöglichen, die übergeordneten Berechtigungen erneut zu erben, die einmalige ACEs ersetzen.

277.027 ORDNER MIT NICHT AUFGELÖSTEN SIDS

Empfehlung:
Ordner mit nicht aufgelösten SIDs identifizieren und aus den ACL entfernen.

423.872 ORDNER MIT DIREKTEN BENUTZER-ACES

Empfehlung:
Ordner mit direkten Benutzerberechtigungen identifizieren, Benutzer in die entsprechende Gruppe platzieren und den Benutzer-ACE aus der ACL entfernen.

MITTLERES RISIKO:

Veraltete Daten– ob Dateien, Benutzer oder Gruppen – werden schnell zu einer Sicherheitsbelastung und verursachen überflüssige Speicherkosten. Für eine sichere Umgebung ist eine kontinuierliche und automatisierte Pflege notwendig. Effiziente Nutzung der Ressourcen sicherstellen und Sicherheitslücken schließen, die für Brute-Force-Angriffe anfällig werden.

VERALTETE DATEN: 85.377.723 ORDNER MIT VERALTETEN DATEN; 4.381.574 VERALTETE, SENSIBLE DATEIEN

Empfehlung:
Veraltete Daten identifizieren und die Daten bestimmen, die verschoben, archiviert oder gelöscht werden können. Konsistente Richtlinien erstellen und umsetzen, um veraltete Daten zu verwalten.

1.182 BENUTZER HABEN PASSWÖRTER, DIE NICHT ABLAUFEN

Empfehlung: Konten aktualisieren, um eine strenge Passwortrichtlinie zu etablieren, einschließlich regelmäßiger Passwortänderungen.
Service Accounts mit Passwörtern, die auf unbegrenzte Zeit vergeben wurden, sollten auf ein Minimum beschränkt werden.

455 VERSCHACHTELTE GRUPPEN

Empfehlung:
Verschachtelte Gruppen können den Absturz von Anwendungen verursachen, exzessiv Verarbeitungsressourcen verbrauchen und sich unerwartet verhalten, da viele Anwendungen und Skripte die Gruppenmitgliedschaft rekursiv aufzählen. Um Abhilfe zu schaffen, sollten die verschachtelten Gruppen identifiziert und die Zyklusbedingungen entfernt werden.

HOHES RISIKO:

Übermäßige Zugriffsrechte auf Daten ist eine der Hauptursachen für Datenschutzverstöße: Übermäßig exponierte sensible und kritische Daten stellen ein belastendes Sicherheitsrisiko dar.

Veraltete Benutzerberechtigungen werden zur Zielscheibe für Datenmissbrauch. Um ein „Least Privilege"-Zugriffsmodell umzusetzen, ist es entscheidend, den Zugriff auf die Personen zu beschränken, die diese Daten benötigen: Benutzer verwalten, unterbrochene Vererbungen und inkonsistente Berechtigungen beseitigen und sensible Daten „verschließen".

66.502.975 ORDNER MIT GLOBALEN ZUGRIFFSGRUPPEN

Empfehlung:
Berechtigungen von globalen Zugriffsgruppen entfernen, um die Ordner zu identifizieren, die für einen globalen Gruppenzugriff und ihre aktiven Benutzer freigegeben sind: Aktive Benutzer in eine neue Gruppe verlegen und die globale Zugriffsgruppe in der ACL durch die neue Gruppe ersetzen.

9.213.456 SENSIBLE DATEN SIND FÜR EINEN GLOBALEN GRUPPENZUGRIFF FREIGEGEBEN

Empfehlung:
Sensible Daten sollten durchsucht, klassifiziert und überwacht werden, damit sie in allen Netzwerken geschützt bleiben.

30.000 ORDNER MIT DEFEKTER ACL

Empfehlung:
Inkonsistente Berechtigungen durch Wiederherstellung der NTFS-Vererbung dort, wo die Vererbungsstruktur inkonsistent wird.

2.555 VERALTETE, ABER AKTIVIERTE BENUTZER

Empfehlung:
Veraltete, aber aktive Konten auf ihre Notwendigkeit hin überprüfen. Je nach Bedarf Konten löschen oder deaktivieren.

.

GRAD	FÄHIGKEIT
VOLLSTÄNDIG	• Änderungen in Active Directory verfolgen und berichten (Gruppenmitgliedschaft, GPO usw.)
TEILWEISE	• Änderungen der Access Control List verfolgen und melden • Potenziellen Zugriff für Datei-Container-Objekte analysieren • Potenziellen Zugriff für E-Mail-Container-Objekte analysieren • Identifizieren sensibler und/oder regulierter Inhalte • Veraltete, ungenutzte Inhalte identifizieren
KEINE	• Dateinutzung verfolgen und melden (Erstellen, Ändern, Löschen usw.) • E-Mail-Nutzung nachvollziehen und melden (Senden, Empfangen, Senden als usw.) • Ungewöhnliche Datei- und E-Mail-Aktivitäten ermitteln • Analysieren wo Benutzer oder Gruppen potenziell auf Datei-Container zugreifen können • Analysieren wo Benutzer oder Gruppen potenziell auf E-Mail-Speicher zugreifen können • Genehmigungsprozess für Zugriffsanfragen an Dateneigentümer übertragen

OPERATIVER ABLAUF

Varonis hat bei der Zusammenarbeit mit Tausenden Organisationen eine bewährte und effiziente Methode für Unternehmen zur Überwachung, dem Schutz und der Verwaltung ihrer Daten entwickelt. Unser datenzentrierter Ansatz mindert Risiken, ist effizienter und hilft, Vorschriften wie PCI, HIPAA und die DSGVO zu erfüllen.

ERKENNEN: 1. VORBEREITEN

- Bereitstellung von Varonis
- Priorisieren und Bewerten von Risiken

Dieser vorläufige Bericht ist eine kleine Stichprobe aus dem ersten Schritt der operativen Umsetzung mit Varonis.

ERKENNEN: 2. OPERATIONALISIEREN

- Erstellen eines auf Benachrichtigungen basierten Ereignisreaktionsplans, inklusive Automatisierung
- Grundlagenschulung der Mitarbeiter – Verwalten von Berechtigung und Entdecken verlorener Dateien

VERHINDERN: 3. REPARIEREN

- Reparieren defekter ACLs
- Löschen globaler Zugriffe auf sensible Daten
- Entfernen von verbleibenden globalen Zugriffsgruppen
- Löschen nicht benötigter AD-Artifakte (nicht genutzte Sicherheitsgruppen, unbegrenzt gültige Passwörter usw.)
- Isolieren/Archivieren/Löschen veralteter Daten

VERHINDERN: 4. REORGANISIEREN

- Identifizieren von Ordnern, für die Eigentümer benötigt werden
- Dateneigentümer identifizieren
- Vereinfachen der Berechtigungsstruktur
- Bereitstellen von Berichten für Eigentümer über ihre Daten

PFLEGEN: 5. AUTOMATISIEREN

- Automatisieren des Autorisierungsworkflows über Daten-Eigentümer
- Automatisieren der regelmäßigen Anspruchsprüfungen
- Automatisieren von Disposition, Quarantäne, Richtliniendurchsetzung

PFLEGEN: 6. OPTIMIEREN

- Kontinuierliche Verbesserung durch regelmäßige Überprüfung von Risiken, Benachrichtigungen und Prozessen

SCHRITT EINS:

- Bereiche hohen Risikos mit Alarmmeldungen, Bedrohungsmodellen, Datenklassifizierung und DatAdvantage-Modellierung und Commit- Funktionen identifizieren und beseitigen.
- Probleme mit der DatAdvantage GUI lösen.
- Umfangreiches Reporting auf Basis von ACME-Anforderungen ausbauen (vollständiges Inventory bei definiertem Umfang).
- Dashboard einrichten, um die Wiederherstellung zu nachzuverfolgen.

SCHRITT ZWEI:

- Die ‚Everyone'-Gruppe entfernen und ein „Least Privilege"-Modell in der Windows Share-Umgebung implementieren.
- Gruppenbasiertes Zugriffsmodell bei Basisordnern/Shares auf eine Gruppe „Lesen" und eine Gruppe „Modifizieren" ändern.
- Verantwortliche Business Units und Dateneigentümer für Datensets in ACME identifizieren und kennzeichnen.

SCHRITT DREI:

- Alarme bei Abweichungen von sanierten Ressourcen einrichten.
- Datenhaltung/Datenspeicherung und Migration anhand von Regeln, Umfang und Tiered Storage in Data Transport Engine automatisieren.
- Bereitstellungsprozess für Dateifreigaben automatisieren und regelmäßige Audits und Re-Zertifizierungen von Berechtigungen für Datensets mit DataPrivilege durchführen.

BEGRIFFSERKLÄRUNG:

Inaktive / veraltete Daten:

Daten, bei denen 180 Tage kein Dateisystemereignis registriert wurde.

Offener / globaler Zugang:

Instanz(en), bei denen der Zugang zu einer Entität für Gruppen freigegeben wurde und eine große oder nicht definierte Anzahl von Nutzern Zugang hat.

Sensible Daten:

Zu sensiblen Dateien zählen regulierte Daten (PCI, PII, HIPAA usw.), geistiges Eigentum und vertrauliche Dateien.

Veraltete aktivierte Benutzer:

Benutzerkonten mit Zugangsberechtigungen, die nicht deaktiviert und zur Domain-Anmeldung nicht verwendet wurden.

Benutzer zur Entfernung empfohlen:

Benutzer mit Zugriffsberechtigungen für Daten, die in ihren vorherigen Rollen erforderlich waren, für die sie aber keinen Zugang mehr brauchen.

Leere Sicherheitsgruppen:

Active Directory Gruppen ohne Benutzer.

Nicht aufgelöste SIDs:

Nicht aufgelöste Sicherheits-IDs treten auf, wenn einer Gruppe oder ein Benutzer- ACE direkt berechtigt ist auf einen Ordner zuzugreifen und diese Gruppe oder das mit dem Benutzer verbundene Active Directory-Konto gelöscht wird.

Ordner mit einmaligen Berechtigungen:

Ein Ordner, der seine ACL von einem übergeordneten Ordner erbt und für diese zusätzliche ACEs hat.

Geschützte Ordner:

NTFS-Ordner mit einer explizit definierten ACL, der keine ACEs von den übergeordneten Ordnern erbt.

ÜBER VARONIS

Varonis ist ein führender Technologieanbieter auf dem Gebiet der Datensicherheit und -analyse, spezialisiert auf Software für Datensicherheit, Governance, Compliance, Klassifizierung und Analysen. Varonis erkennt Insider-Risiken und Cyberangriffe durch Analysieren der Dateiaktivitäten und des Benutzerverhaltens, beugt durch Sperren sensibler Daten Katastrophen vor und sorgt durch Automatisierung für einen sicheren Zustand.

Wir unterstützen tausende von Kunden dabei, sich vor Sicherheitsverletzungen zu schützen.

LIVE-DEMO

Richten Sie Varonis in Ihrer eigenen Umgebung ein. Schnell und mühelos

info.varonis.com/trial-de

DATENRISIKOBEURTEILUNG

Sie erhalten eine individuelle Risikobeurteilung, reduzieren Ihr Risikoprofil und beheben Sicherheitsprobleme.

info.varonis.com/express-assessment-de

SETZEN SIE SICH MIT UNS IN VERBINDUNG

Haben Sie noch Fragen? Dann rufen Sie uns an.

sales-germany@varonis.com
tel:+49-89-3803-7990

VARONIS

VC8012C