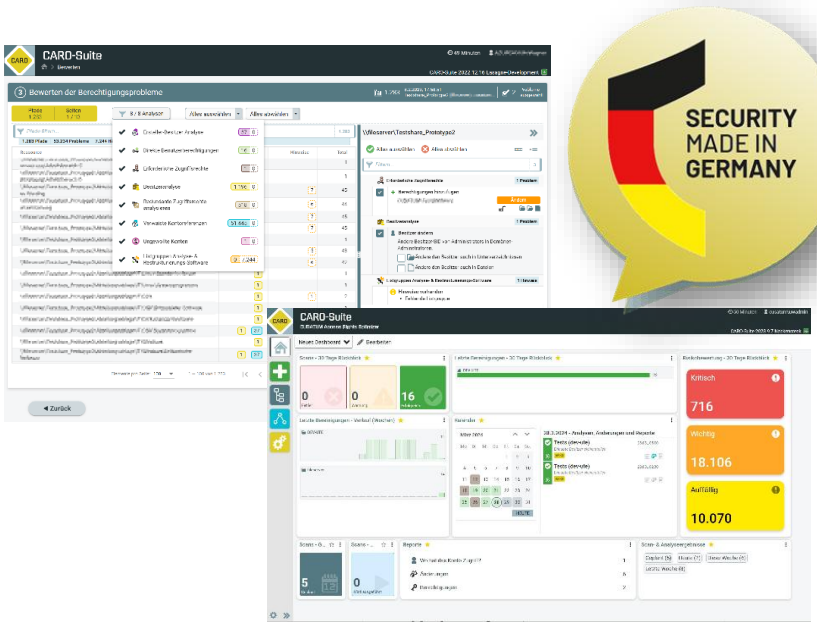
CARO-Suite Best Practices

Automatisierte Bereinigung von Berechtigungen

In vielen Unternehmen kämpfen IT-Administratoren mit zeitfressenden Prozessen, um Zugriffsrechte zu vergeben. Deswegen haben wir die CARO-Suite entwickelt, die das Berechtigungsmanagement automatisiert und sowohl schneller als auch sicherer macht. IT-Admins reduzieren damit den Aufwand, sichern die Kontrolle der Zugriffsrechte und vermeiden Sicherheitsrisiken für das Unternehmen.



CUSATUM Service GmbH

Wiesenweg 16
16548 Glienicke / Nordbahn
www.cusatum.de

E-Mail: info@cusatum.de

Best Practices

CARO-Suite - Zugriffsrechte sicher im Griff!

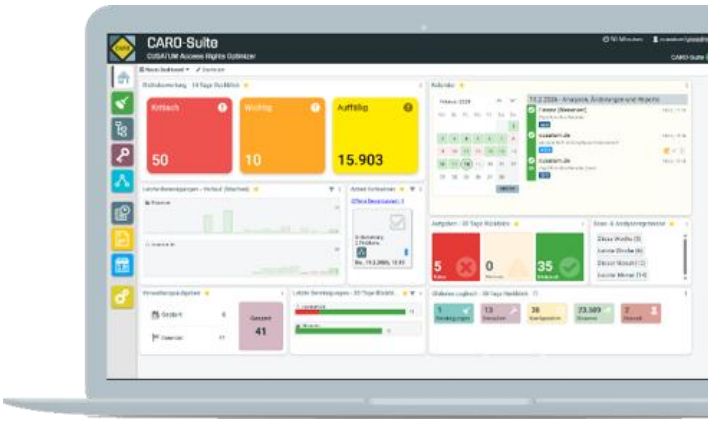
Historisch gewachsene Berechtigungsstrukturen gehören mit CARO der Vergangenheit an. Sicherheitslücken werden beseitigt und automatisch reduziert. CARO sorgt in Ihren IT-Strukturen für Ordnung!

ANALYSIEREN – *Risiken verstehen*

Übersicht durch Experten-Risikobewertung und umfangreiche Berechtigungsanalysen.

AUTOMATISIEREN – *Höchste Effizienz*

Effizienz durch detaillierte Handlungsempfehlungen und automatisiertes Bereinigen.



KONTROLLIEREN - *Volle Kontrolle*

Sie haben Ihre Berechtigungen im Griff; Mit compliance-konformen Reporten und revisionssicherer Protokollierung.

DOKUMENTIEREN – *Compliance jederzeit belegbar*

Zugriffsrechte und Konten live einsehen und verwalten. Keine Wartezeiten mehr. Echtzeit statt Datenbank.

Best Practices

Für das Bereinigen ist es sinnvoll, bestimmte Analysen nacheinander zu starten. Sehen Sie in der folgenden Übersicht eine empfohlene Reihenfolge von CARO-Analysen für ein effizientes Aufräumen.

Empfehlung für eine Bereinigungs-Reihenfolge

Reihenfolge	Analyse-Bausteine	Technologie	Einstellung in der CARO-Suite	Automatisierte Bereinigung
1 Domänen-Scan als Grundvoraussetzung	ARCA	AD, Entra ID	Täglich scannen, Mindestens inaktive Benutzer suchen	Teilweise
1 **Alternativ:** IST-Datenstand erfassen	EBIS	FS, AD, Ex, Entra ID	Alternativ, wenn Sie nur CARO nur zur Anzeigen und zum Reporten nutzen wollen	
2 Freigabe-Berechtigungen überprüfen	SARA	FS	1x pro Woche	
3 Tote SIDs finden und entfernen	TEUS	FS, AD	1x pro Woche	Ja
4 Besitzer korrigieren	BAKS	AD, FS	*Damit ggf. die durch CREATOR_ONWER erzeugten Direktberechtigungen durch spätere ERBE-Bereinigungen bestehen bleiben. Alle 1-2 Wochen	Ja
5 Direkte Berechtigungen aufräumen	DARS	FS	1x pro Woche	Ja

6	Problematische Ersteller-Besitzer korrigieren	BAKS DARS ERBE	FS	*Darf laufen, wenn BAKS gelaufen ist **ODER** auf dem System ein Gruppenkonzept eingesetzt wird **UND** DARS keine Hinweise liefert, d.h. es fehlen keine Berechtigungsgruppen.	Ja
7	Direkte ungewollte Berechtigungen ent7fernen	DUKE	FS, AD	1x pro Woche	
8	Redundante Berechtigungen beseitigen	RAPA	FS	1x pro Woche	
9	Mindest-Berechtigungen überprüfen und korrigieren	MARS	FS	Alle 1-2 Wochen	
10	Unterbrochene Vererbungen finden und beseitigen, Verschobene Verzeichnisse finden und korrigieren	VASS	FS	Immer am Ende der Aufräumprozesse durchführen. Alle 1-2 Wochen	
✓	Listberechtigungen überprüfen	LARS	FS	Immer am Ende der Aufräumprozesse durchführen. Alle 1-2 Wochen	

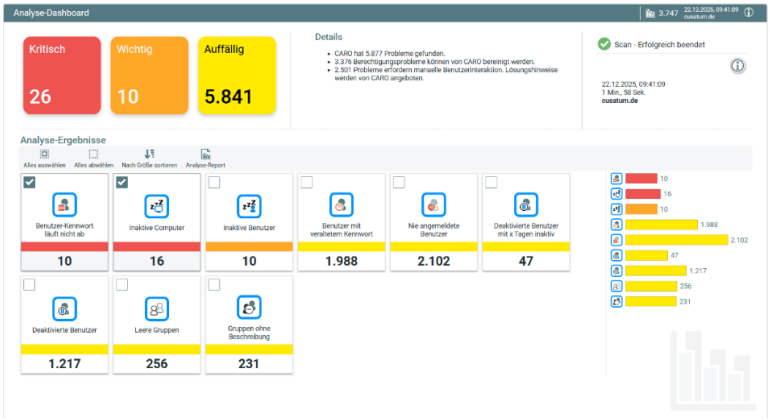
Best Practices

	Bei Bedarf			
✓	Prüfen und Austausch von Zugriffsrechten	EAPE	FS	Bei Bedarf
✓	Verzeichnisnamens-Längen oder Pfad-Längen prüfen, Freigaben mit Verweis auf lokale Laufwerke prüfen, Benutzerpostfächer überprüfen	FRAK	Ex, FS 👁	Bei Bedarf

👁 wird in der Technologie nur als Audit-Baustein angeboten

Risikobewertung

Mit dem Risiko-Dashboard erkennen Sie auf einen Blick, wo genau bei Ihnen die größten Berechtigungsprobleme zu finden sind und wie Sie diese mit wenigen Klicks automatisiert bereinigen können.
Mit der CARO-Suite erhalten Sie 14 Analyse- und Bereinigungsbausteine mit insgesamt 50 einzelnen Analysen.



Risikostufen nach BSI-Standard

Die erkannten Probleme aus den Analysen der CARO-Suite werden analog zur Risikobewertung zur BSI-Risikomatrix in 3 Kategorien eingestuft: kritische, wichtige und auffällige Probleme von Zugriffsrechten.
Quelle: Matrix zur Einstufung von Risiken, BSI-Standard 200-3, www.bsi.bund.de/grundschutz, v 1.0.

Risiko-bewertung	Erklärung
Kritisch	Kritische Fehler entstehen durch unzulässige Zugriffsrechte und sollten vorrangig bereinigt werden.
Wichtig	Analysen finden weitere als wichtig eingestuften Probleme in Ihrem System. Solche relevanten Probleme sollten zeitnah behoben werden.
Auffällig	Es werden Sicherheits-auffälligkeiten in den Zugriffsrechten gefunden. Diese Auffälligkeiten sollten nach unserer Erfahrung durch Ihre Administratoren überprüft werden.

Analysen mit Risikoeinstufung: kritisch

Kategorie	Risiko	Beschreibung	Technologie
Inaktive Computer	Kritisch	Analysiere alle Computer, ob sie zu lange inaktiv waren.	Active Directory
Benutzer-Kennwort läuft nicht ab	Kritisch	Analysiere alle Benutzer mit nie ablaufenden Kennwörtern	Active Directory
Unterbrochene Vererbung	Kritisch	Sucht Ordner mit deaktivierter Vererbung.	Filesystem
Direkte Benutzerberechtigungen	Kritisch	Erkenne und analysiere direkte Benutzerzugriffsrechte.	Filesystem
Erlaubte Besitzer	Kritisch	Erlaubte Besitzer Analyse	Filesystem
Redundante Zugriffsrechte	Kritisch	Erkenne und analysiere redundante Zugriffsrechte für Konten.	Filesystem
Ablaufende Clientschlüssel	Kritisch	Analysiere alle Anwendungs-Registrierungen nach ablaufenden Clientschlüsseln.	Entra ID
Globale Administratoren	Kritisch	Analysiere alle Globalen Administratoren.	Entra ID
Globale Administrator-Rolle	Kritisch	Best Practices für die Anzahl an Globalen Administratoren.	Entra ID
Privilegierte Rollen	Kritisch	Best Practices für Anzahl an privilegierten Rollenzuweisungen.	Entra ID
Aktivierte Vererbung	Kritisch	Die Vererbung von NTFS-Zugriffsrechten auf Freigaben sollte deaktiviert sein. Das Ändern vererbter NTFS-	Filesystem

		Berechtigungen aus der Ferne löscht alle Zugriffsrechte und macht die Freigabe unbrauchbar.	
Offene Freigabe	Kritisch	Alle authentifizierten Konten (Active Directory und lokal) haben mindestens das Lese-Zugriffsrecht auf die Informationen der Dateisystem-Freigabe. Damit kann ein unkontrollierter Datenabfluss erfolgen.	Filesystem
Nicht-administrative Laufwerks-Freigaben	Kritisch	Prüft auf nicht-administrative Freigaben mit Verweis auf komplette lokale Laufwerke.	Filesystem

Analysen mit Risikoeinstufung: wichtig

Kategorie	Risiko	Beschreibung	Technologie
Inaktive Benutzer	Wichtig	Analysiere alle Benutzer, ob sie zu lange nicht angemeldet waren.	Active Directory
Ersteller-Besitzer	Wichtig	Entferne Ersteller-Besitzer-Berechtigungen.	Filesystem
Erforderliche Zugriffsrechte	Wichtig	Sicherstellen, dass Konten erforderliche Zugriffsrechte haben.	Filesystem
Verschobene Objekte	Wichtig	Erkenne und analysiere verschobene Objekte.	Filesystem
Zugriffsrechte ungewollter Konten	Wichtig	Prüfe bei allen Zugriffsberechtigungen, ob das berechtigte Konto	Filesystem

		eines der ungewollten Konten ist.	
Inaktive Anwendungen	Wichtig	Analysiere alle Anwendungen, ob sie zu lange nicht angemeldet waren.	Entra ID
Inaktive Gast-Benutzer	Wichtig	Analysiere alle Gast-Benutzer, ob sie zu lange nicht angemeldet waren.	Entra ID
Cloud-Native Konten Rollen-zuweisungen	Wichtig	Best Practices für die ausschließliche Nutzung von Cloud-Native Konten für Rollenzweisungen.	Entra ID
Gruppen-Rollen-zuweisungen	Wichtig	Best Practices für die ausschließliche Nutzung von Gruppen für Rollenzuweisungen.	Entra ID
Jeder Vollzugriff Freigabe	Wichtig	Das Jeder-Konto sollte maximal Ändern-Zugriffsrecht auf der Freigabe haben. Bei Vollzugriff besteht das Risiko, dass bei erweiterten NTFS-Zugriffsrechten Anwender unbewusst Schaden anrichten können.	Filesystem
List-Berechtigungen	Wichtig	Analyse aller Zugriffsberechtigungen von Verzeichnisbäumen hinsichtlich der Erreichbarkeit aller Verzeichnisse	Filesystem

Analysen mit Risikoeinstufung: auffällig

Kategorie	Risiko	Beschreibung	Technologie
Gruppen ohne Beschreibung	Auffällig	Alle Gruppen analysieren, die keine Beschreibung besitzen.	Active Directory
Leere Gruppen	Auffällig	Alle Gruppen analysieren, die keine Mitglieder besitzen.	Active Directory
Deaktivierte Benutzer	Auffällig	Analysiere alle Benutzer, die deaktiviert sind.	Active Directory
Deaktivierte Benutzer - x Tage inaktiv	Auffällig	Deaktivierte Benutzer, die mindestens x Tage nicht angemeldet waren.	Active Directory
Deaktivierte Benutzer in einer OU löschen	Auffällig	Überprüft alle Benutzer aus der konfigurierten OU, die deaktiviert sind und mindestens X Tage nicht geändert wurden.	Active Directory
Nie angemeldete Benutzer	Auffällig	Analysiere alle Benutzer, ob sie noch nie angemeldet waren.	Active Directory
Benutzer mit veraltetem Kennwort	Auffällig	Analysiere alle Benutzer, ob sie zu lange nicht ihr Kennwort verändert haben.	Active Directory
AD-Objekte mit RC4-Verschlüsselung	Auffällig	Alle Objekte mit RC4-Verschlüsselung analysieren (Rivest Cipher).	Active Directory
AD-Objekte mit KDC-Fallback auf Domänen-Standard	Auffällig	Alle Objekte mit KDC-Fallback auf Domänen-Standard analysieren (oft RC4).	Active Directory
Verwaiste Kontoreferenzen	Auffällig	Prüfe bei allen Zugriffsberechtigungen, ob das berechtigte Konto noch existiert.	Filesystem
Abgelaufene Clientschlüssel	Auffällig	Analysiere alle Anwendungs-Registrierungen nach abgelaufenen Clientschlüsseln.	Entra ID
Ablaufende Abonnements	Auffällig	Ablaufende Abonnements	Entra ID

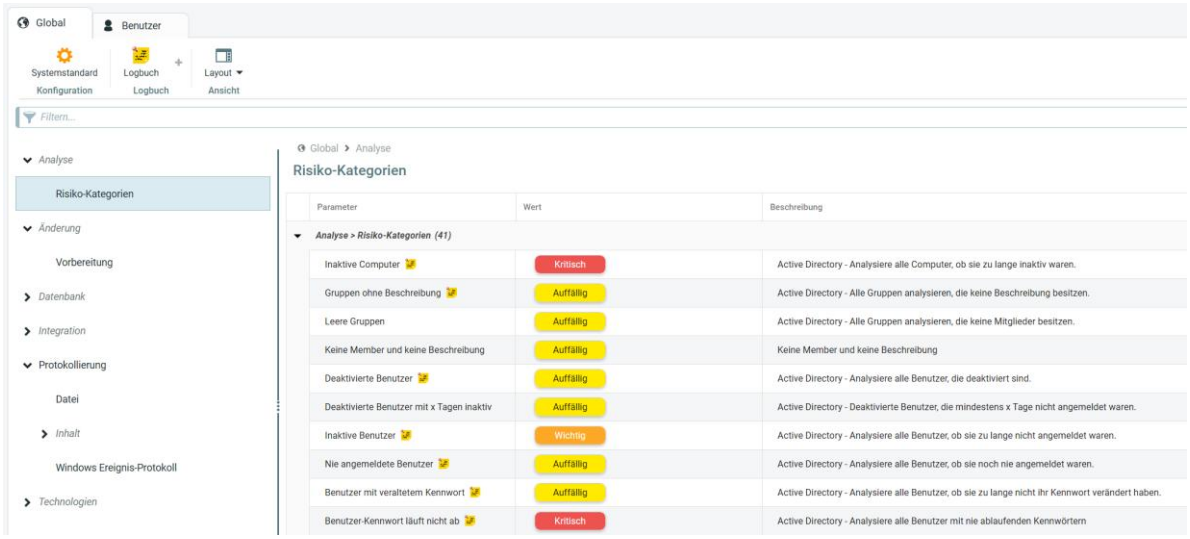
Best Practices

Cloud-Native Benutzer	Auffällig	Analysiere alle Benutzer, die nicht mit einem On-Prem-AD synchronisiert sind.	Entra ID
Inaktive Cloud-Native Benutzer	Auffällig	Analysiere alle inaktiven Benutzer, die nicht mit einem On-Prem-AD synchronisiert sind.	Entra ID
Inaktive OnPrem-Benutzer	Auffällig	Analysiere alle inaktiven Benutzer, die mit einem On-Prem-AD synchronisiert sind.	Entra ID
Nicht-administrative Freigabe	Auffällig	Server auf die Existenz von Freigaben prüfen. Administrative Freigaben (C$, etc.) werden ignoriert. Freigaben können unkontrollierten Zugriff auf kritische Informationen ermöglichen.	Filesystem
Austausch von Berechtigungen	Auffällig	Analyse der Berechtigung, um diese gegen ein gewünschtes Zugriffsrecht auszutauschen. Zur Vereinheitlichung für ein sauberes Berechtigungsmanagement-Konzept.	Filesystem
Freigegebene Postfächer	Auffällig	Analysiere alle freigegebenen Postfächer, denen keine Berechtigungen zugewiesen sind.	Exchange
Benutzer-postfächer	Auffällig	Analysiere alle Benutzerpostfächer, für die mehrere Konten Berechtigungen haben.	Exchange
Aktive Abwesenheits-notizen	Auffällig	Erkennt Postfächer mit aktivierter Out-of-Office-Konfiguration.	Exchange
Postfachgröße	Auffällig	Analysiere alle Postfächer, die eine bestimmte Größe überschreiten.	Exchange

Prüft CARO-Zugriffsgruppen	Auffällig	Prüft alle ACEs der CARO-Zugriffsgruppen	Filesystem
SID-Historie überprüfen	Auffällig	Prüfe alle ACEs, ob eine bestimmte Domänen-SID enthalten ist.	Filesystem
Verzeichnis-namenslänge	Auffällig	Prüft die Länge von Verzeichnisnamen.	Filesystem
Verzeichnis-pfadlänge	Auffällig	Prüft die Länge von Verzeichnispfaden.	Filesystem

Anpassung der Risikoeinstufungen

Die Risikoeinstufung für die einzelnen Analysen können Sie mit der CARO-Suite unter ***Globale Einstellungen*** an Ihre Vorgaben im Berechtigungsmanagement anpassen:



CARO-Analysen und Anwendungsfälle

FRAK

FRAK

EAPE

Flexible-**R**essourcen-**A**nalyse und **K**orrektur

Filesystem

- Prüft die Länge von Verzeichnisnamen
- Prüft die Länge von Verzeichnispfaden
- Prüft auf nicht-administrative Freigaben mit einem Verweis auf komplette lokale Laufwerke
- Prüft CARO-Zugriffsgruppen auf ihre ACEs
- SID-Historie überprüfen

Die Verzeichnis-Analysen sind individuell anpassbar.

Anwendungsfall: Es gibt Projekt-Ordner, die von Data-Ownern verwaltet werden. Ein Projekt-Laufwerk „P:" ist für alle Anwender als "Projekt$" freigegeben. Damit kommen einige IDM/IAM oder Berechtigungsmanagement-Tools nicht zurecht. Mit FRAK können diese Laufwerke schnell gefunden werden. Langwierige Fehlersuchen werden damit vermieden, z.B. dass ein Report nicht die gewünschten Daten anzeigt.

Exchange

- Analysiere alle Benutzerpostfächer, wo für mehrere Konten Berechtigungen existieren
- Analysieren alle freigegebenen Postfächer, denen keine Berechtigung zugewiesen sind
- Finde Postfächer mit aktivierter Abwesenheitsnotiz
- Überprüfung der Postfachgrößen

Anwendungsfall: Nach dem Least Privilege sollten möglichst nur wenige Personen/Identitäten Zugriff haben, desto kleiner ist das Angriffsrisiko. Mit einer einzigen verantwortlichen Person ist klar, wer Änderungen vornimmt oder E-Mails im Auftrag sendet. Das erleichtert Prüfungen. Ausnahmen sollten nur Shared Mailboxes sein.

Verzeichnisnamens-Länge überprüfen

Verzeichnispfad-Länge überprüfen

Nicht-administrative Laufwerks-freigaben überprüfen

Benutzerpostfächer überprüfen

Aktive Abwesenheitsnotizen finden

Postfachgrößen überprüfen

EAPE

Exchange-**A**ccess **Pe**rmissions

- Prüft auf bestimmte Zugriffsrechte und tauscht diese mit einem anderen Zugriffsrecht aus
- Eine Konten-Ausschlussliste kann konfiguriert werden (Skip-Liste)
- Ebenfalls können Attribute angegeben werden, nach denen nur bestimmte Konten zum Check einbezogen werden sollen (White-Liste)

Anwendungsfall: Prüfen auf das Zugriffsrecht *Ändern* und tauscht dieses mit dem Zugriffsrecht *Eingeschränktes Ändern* aus.

Austausch von bestimmten Zugriffsrechten

Automatische Bereinigung möglich

Best Practices

CARO-Analysen und Anwendungsfälle

DARS

DUKE

BAKS

VASS

DARS

Direktzugriff **A**nalyse- und **R**estrukturierungs-**S**oftware

- Identifiziert Direktberechtigungen von Usern
- Korrigiert effizient diese Einträge

Anwendungsfall: Wilma Gucken ist Mitglied in der Gruppe Finanzabteilung und hat zusätzlich direkten Zugriff auf Geschäftsdaten. Nachdem Wilma nicht mehr in der Finanzabteilung ist, hat sie trotzdem noch Zugriff! DARS findet schnell alle Gruppen- und direkten Benutzerzugriffe und löscht diese überflüssigen Zugriffsrechte effektiv. Für andere Benutzer mit direkten Zugriffsrechten werden Hinweise erzeugt.

Direkte Berechtigungen checken

Automatische Bereinigung möglich

DUKE

Direktzugriffsrechte **U**ngewollter **K**onten **E**ntfernen

- Identifiziert alle Zugriffsrechte der konfigurierten ungewollten Konten und entfernt diese
- Reduziert Sicherheitsrisiken durch das Entfernen von unbekannten und unkontrollierbaren Zugriffsberechtigungen

Anwendungsfall: Administratoren bekommen durch die UAC einen Vollzugriff gewährt. Mit DUKE werden diese direkten Einträge entfernt und die Gruppenmitgliedschaft über die Administratoren-Gruppe wird wieder hergestellt.

Direkte ungewollte Berechtigungen entfernen

Automatische Bereinigung möglich

BAKS

Besitzer-**A**nalyse- und **K**orrektur-**S**oftware

- Stellt zulässige Besitzer sicher, damit administrative Konten Ihre Berechtigung behalten, z.B. damit Backup-Tools funktionieren
- Analysiert Sicherheitsrisiken durch das Entfernen von unerlaubten und unkontrollierbaren Zugriffsberechtigungen

Anwendungsfall: Durch das Erstellen von Verzeichnissen und Dateien bekommen „normale" Benutzer das Besitzrecht. Dadurch sind diese Benutzer in der Lage, die Berechtigung selbst zu verändern. Im schlimmsten Fall werden hier die Administratoren, Service Accounts und Benutzer ausgesperrt. Best-Practice ist es, diese Benutzer durch die lokalen Fileserver-Administratoren auszutauschen.

Besitzer korrigieren

Automatische Bereinigung möglich

VASS

Vererbung-**A**nalyse- und **S**anierungs-**S**oftware

- Identifiziert veränderte Berechtigungen in Ordner-Hierarchien
- Findet verschobene Verzeichnisse
- Angleichung der Berechtigungen durch Vererbung oder andere systemspezifische Werkzeuge

Anwendungsfall: Das Aufbrechen von Vererbung unterhalb der zu administrierenden Verzeichnisebenen ist oft ungewollt und führt dazu, dass Benutzer dort nicht mehr zugreifen können. Best-Practice ist, dass nach der Administrationsebene alle Berechtigungen durchvererbt sind. CUSATUM empfiehlt maximal 4 Ebenen.

Aufgebrochene Vererbungen wieder-herstellen

Verschobene Verzeichnisse Finden

Automatische Bereinigung möglich

Best Practices

CARO-Analysen und Anwendungsfälle

TEUS

LARS

ERBE

MARS

TEUS

Tool zur **E**ntfernung **U**nbekannter **S**IDs

- Entfernt tote SIDs und macht die Dokumentation Ihrer Berechtigungen wieder leichter lesbar und verständlich
- Reduziert die Nachfragen Ihrer Revision und dokumentiert, dass Sie die volle Kontrolle haben
- Bietet mehr Sicherheit, da weniger Angriffsfläche für SID History Injection

Anwendungsfall: Nach dem Löschen von Benutzern und Gruppen im Active Directory werden diese in den berechtigten Ressourcen-ACL's nicht automatisch mit entfernt. Zurück bleibt auf den Ressourcen die verwaiste oder tote SID. Diese Einträge machen notwendige Audit-Reporte schwer lesbar und werden auch als Sicherheitsproblem eingestuft.

Unbekannte SIDs entfernen

Automatische Bereinigung möglich

LARS

Listgruppen **A**nalyse- und **R**estrukturierungs-**S**oftware

- Analyse der Berechtigungen in Ordner-Hierarchien
- Verwalten von List-Berechtigungen in übergeordneten Ordnern

Anwendungsfall: Benutzer sollen zu den „Arbeitsverzeichnissen" navigieren können. Best-Practice sieht dafür eine Listberechtigung vor, die über Active Directory-Gruppen gesteuert wird. Durch die tägliche Arbeit werden oft Verzeichnisse verschoben, neu erstellt, umbenannt oder gelöscht. Dabei müssten die Listberechtigungen mit korrigiert werden, damit die Benutzer weiterhin problemlos zu den Verzeichnissen gelangen. Weder die Administratoren noch auf dem Markt befindliche Software z.B. SolarWinds-ARM, Tenfold oder IDM/IAM-Systeme korrigieren diese Probleme nachhaltig.

Fehler in Listgruppen analysieren

ERBE

ERsteller-**B**esitzer auf Dateisystemen **E**ntfernen

- Entfernt den Ersteller-Besitzer und verhindert das Entstehen von neuen toten SIDs
- Erlaubt damit eine saubere Migration, z.B. in die Cloud

Anwendungsfall: Standard-Einstellung von Microsoft beim Einbinden neuer Festplatten ist es, die Ersteller-Besitzer-Berechtigung mit Vollzugriff zu vergeben. Dadurch entstehen direkte Berechtigungen, die bei einem Löschen des Benutzers zu einer verwaisten SID führt. Zusätzlich kann der Benutzer die Administratoren, Service Accounts und Benutzer auszusperren. Best-Practice von CUSATUM ist, diesen Eintrag zu entfernen und mit einer Gruppenberechtigung zu arbeiten.

Ersteller-Besitzer entfernen

Automatische Bereinigung möglich

MARS

Mindestberechtigungen **A**nalyse und **R**estrukturierungs-**S**oftware

- Prüft alle Dokumente und Ordner auf erforderliche Zugriffsrechte für Konten und berücksichtigt dabei sowohl direkte als auch indirekte Zugriffsrechte
- Setzt fehlende Berechtigungen

Anwendungsfall: Sie wollen die Mindestberechtigung für einen Benutzer überprüfen, ob z.B. ein Benutzer oder ein Service Account überall mindestes Modify hat. Oft sind entweder keine Berechtigungen oder eine zu geringe Berechtigung vergeben.

Mindest-Berechtigungen überprüfen

Automatische Bereinigung möglich

Best Practices

CARO-Analysen und Anwendungsfälle

RAPA

Redundant **A**ccount **P**ermision **A**nalysis

- Identifiziert redundante Berechtigungen
- Überprüfen von Gruppenmitgliedschaften mit gleichzeitiger Direktberechtigung

Anwendungsfall: Wenn ein Benutzer eine direkte und eine gleichwertige oder höhere Gruppenberechtigung bekommen hat, ist die direkte Berechtigung redundant. In diesem Fall kann die direkte Berechtigung entfernt werden. Somit vermeidet man auch das verwaiste-SID-Problem und kann den Leaver-Prozess einfacher und effektiver gestalten.

Redundante Berechtigungen beseitigen

Automatische Bereinigung möglich

RAPA

SARA

SARA

Share **A**ccess **R**ights **A**nalysis

Analyse von Freigabe-Zugriffsrechten

- Prüfen auf vererbte NTFS-Zugriffsrechte
- Suchen von **offenen Shares** für authentifizierte Konten
- Suchen von Jeder-Vollzugriff Freigaben
- Prüfen auf die Existenz von nicht-administrativen Freigaben

Anwendungsfälle:

(1) Die Vererbung von NTFS-Zugriffsrechten auf Freigaben sollte deaktiviert sein. Das Ändern vererbter NTFS-Berechtigungen aus der Ferne löscht alle Zugriffsrechte und macht die Freigabe unbrauchbar.

(2) Freigaben werden überprüft, ob authentifizierte Konten (AD und lokal) mindestens das Lese-Zugriffsrecht haben. Dann gelten diese Freigaben als **offene Shares**. Damit kann ein unkontrollierter Datenabfluss erfolgen.

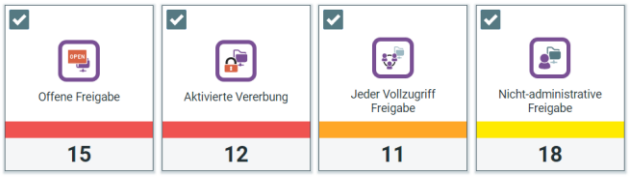
(3) Das Jeder-Konto sollte maximal Ändern-Zugriffsrecht auf der Freigabe haben. Bei Vollzugriff besteht das Risiko, dass bei erweiterten NTFS-Zugriffsrechten Anwender unbewusst Schaden anrichten können.

(4) Ihre Server werden auf die Existenz von nicht-administrativen Freigaben geprüft. Administrative Freigaben (C$, etc.) werden dabei ignoriert. Freigaben können unkontrollierten Zugriff auf kritische Informationen ermöglichen.

Freigabe-Berechtigungen überprüfen

SARA

CARO überprüft riskante Zugriffsrechte auf Fileserver-Freigaben und findet Ihre ***offenen Freigaben***.



Daten können somit nicht mehr unbemerkt abgegriffen werden.
Durch die Möglichkeit der täglichen Überprüfung Ihrer Systeme, unterstützt Sie CARO dort, wo Access Rights Management- und IDM-Systeme an ihre Grenzen stoßen.

CARO-Analysen und Anwendungsfälle

ARCA

ARCA

Account **R**isk- und **C**ompliance-**A**ssessment

- Analysiert Konto-basierend auf Best Practice-Kriterien
- Für Active Directory und Entra ID

Viele Analysen sind individuell anpassbar.

Active Directory (AD)

- Inaktive Benutzer- oder Computerkonten *
- Deaktivierte Benutzer, auch mit Prüfung nach x Tagen inaktiv *
- Nie angemeldete Benutzer *
- Leere Gruppen und Gruppen ohne Beschreibung
- Konten mit nie ablaufenden Kennwörtern
- Benutzer mit veraltetem Kennwort
- Konten mit RC4-Verschlüsselung
- Konten mit KDC-Fallback auf Domänen-Standard

Anwendungsfall: Das BSI und andere IT-Auditierungen, wie TISAX und BAFIN, überprüfen sicherheitskritische KPI's im Active Directory. Dadurch kann die Qualität der Mitarbeiterprozesse und die IT-Sicherheit überprüft und gewährleistet werden. Im ARCA-Modul sind die wichtigsten AD-Analysen zusammengefasst und können individuell angepasst werden.

Entra ID – Zugriffsüberprüfungen in der Cloud

- Globale Administratoren auf zulässige Anzahl und Mitglieder prüfen*
- Anzahl der privilegierte Rollenzuweisungen überprüfen
- Ausschließliche Nutzung von Gruppen in Rollenzuweisungen
- Überprüfen, dass nur Cloud-Native-Konten für Rollenzuweisungen genutzt werden
- Ablaufende Clientschlüssel in den App-Registrierungen finden*
- Ablaufende Abonnements finden *
- Finden von inaktiven Gastbenutzern, die sich über einen längeren Zeitraum nicht angemeldet haben *
- Finden aller inaktive Cloud-Native Benutzer, die nicht mit einem On-Prem-AD synchronisiert sind
- Finden von inaktiven On-Prem-Benutzern, die nicht mit einem On-Prem-AD synchronisiert sind
- Inaktive Anwendungen finden*
- Überprüfen der Anzahl von privilegierten Rollenzuweisungen

Anwendungsfall: Mit CARO können Sie jetzt Ihre Zugriffe für cloudbasierte und hybride Ressourcen auf Entra ID überprüfen und bereinigen. CARO integriert dabei Best Practices für Microsoft Entra-Rollen*.

*Eine ausführliche Beschreibung der Microsoft Best Practices finden Sie hier: https://learn.microsoft.com/de-de/entra/identity/role-based-access-control/best-practices

Account Risk- und Compliance Analysen für Active Directory und Entra ID

Automatische Bereinigung möglich

Berechtigungen anzeigen und dokumentieren

EBIS

EBIS

Erfassung der **B**erechtigungs-**I**st-**S**ituation

- Zeichnet die Berechtigungslage auf Fileservern und im Active Directory auf
- Analysiert u.a. auf unterbrochenen Vererbungshierarchien, verschobene Verzeichnisse oder Null-DACL
- Zeigt im Detail die geänderten Berechtigungen unterhalb an, wie hinzugekommene oder entfernte Zugriffsrechte

Anwendungsfall: Sie wollen regelmäßig Ihre Berechtigungen in der globalen Ressourcen-Ansicht überprüfen oder Berechtigungsreporte erstellen, wie Wer-hat-Wo-Zugriffs-Report, Use-Case-Report oder einen Berechtigungs-Differenz-Report.

IST-Situation erfassen und Berechtigungen reporten

Best Practices

CUSATUM – Gemeinsam für mehr Sicherheit!

Mit über 25 Jahren Erfahrung im Berechtigungsmanagement und der Automatisierung von Mitarbeiterprozessen sind wir seit 2017 als eigenständiges Unternehmen für unsere Kunden da.

Unser Ziel: Ordnung ins Berechtigungschaos bringen!

Mit unserer CARO-Suite, dem CUSATUM Access Rights Optimizer, bieten wir eine smarte Lösung für automatisiertes Berechtigungsmanagement, mit der Sie Daten- und Zugriffsrechte schnell, sicher und automatisiert managen können.

Kurz gesagt: Weniger Klicks, weniger Chaos, mehr Sicherheit.

Mike Wiedemann, CEO
Seine Leidenschaft ist Kundenzufriedenheit. Für zufriedene Kunden geht er auch die „extra Meile"!

Ute Wagner, CDO
Ein User Interface muss nicht nur einfach zu bedienen sein, es muss auch Freude machen, es zu nutzen!

Christian Schönfeld, CEO
Meine Erfahrungen direkt umwandeln in CARO - das ist mein Anspruch! Für alles gibt es eine Lösung. Packen wir es an!

CUSATUM

Herausgeber

CUSATUM Service GmbH
Wiesenweg 16
16548 Glienicke / Nordbahn

www.cusatum.de
E-Mail: info@cusatum.de

Support

Telefon +49 (0)3305 678 3090
E-Mail: support@cusatum.de

Stand: September 2026

SECURITY MADE IN GERMANY