CARO-Suite
Best Practices

Für effektives Bereinigen Ihrer Zugriffsrechte

Mit der CARO-Suite können Sie Berechtigungsfehler und Risiken von Zugriffsrechten analysieren und automatisiert bereinigen. Sparen Sie Zeit und Geld durch saubere Berechtigungsstrukturen dank Risikobewertung von Experten für Ihre IT-Sicherheit.

CUSATUM Service GmbH

Hauptsitz
Wiesenweg 16
16548 Glienicke / Nordbahn

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

CARO – RISK ASSESS © - *Für Ihren Durchblick*

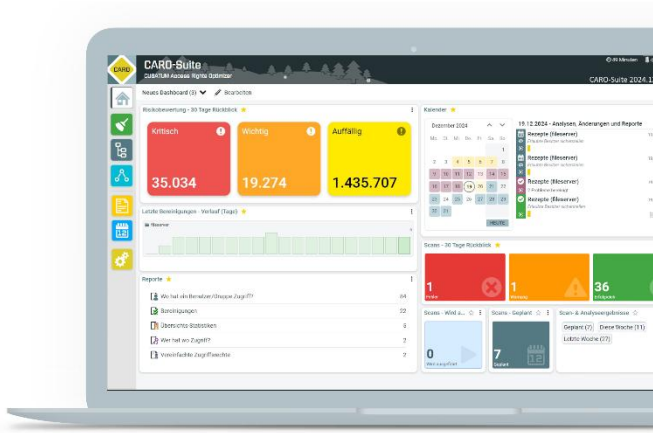
Übersicht durch Experten-Risikobewertung und umfangreiche Berechtigungsanalysen.

CARO - AUTOMATE © - *Für Ihre Entlastung*

Effizienz durch detaillierte Handlungsempfehlungen und automatisiertes Bereinigen.

CARO - SECURE © - *Für Ihre Kontrolle*

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



CARO-SUITE IM DETAIL

- Risikobewertung mit Expertenwissen
- Detaillierte Analysen für Berechtigungsfehler
- Führt Analysen für hybriden Szenarien aus
- Umfangreiche Handlungsempfehlungen zum Bereinigen
- Für Filesystem, Active Directory und Entra ID
- Hoch performante Scans und umfangreiche Analysen zur Änderung Ihrer problematischen Zugriffsrechte
- Planbarkeit von Scans und Änderungen für einen beliebigen Zeitpunkt
- Globale Ressourcen-Ansicht der Zugriffsrechte mit Gruppenmitgliedschaften
- Integration in andere Systeme über Rest-API
- Automatisierung von Mitarbeiterprozessen mit dem Zusatzmodul C-MAN
- Basis-Reporte im PDF-Format, durch Word-Office-Report-Vorlagen einfach an eigene Corporate-Identity anpassbar
- Revisionssichere Protokollierung aller durchgeführten Änderungen
- Mehrsprachiger Web-Client mit Multi-User-Support
- Datenspeicherung in MS-SQL-Datenbank
- Einfaches Lizenzmodell

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.

Bereinigungsschritte

Reihenfolge	Analyse-Bausteine	Technologie	Sinnvolle Einstellung in der CARO-Suite
1 Domänen-Scan als Grundvoraussetzung	ARCA	AD, Entra ID	Täglich scannen, Mindestens inaktive Benutzer suchen
2 Freigabe-Berechtigungen überprüfen	SARA	FS	1x pro Woche
3 Tote SIDs finden und entfernen	TEUS	FS, AD	1x pro Woche
4 Besitzer korrigieren	BAKS	AD, FS	*Damit ggf. die durch CREATOR_ONWER erzeugten Direktberechtigungen durch spätere ERBE-Bereinigungen bestehen bleiben. Alle 1-2 Wochen
5 Direkte Berechtigungen aufräumen	DARS	FS	1x pro Woche
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.
7 Direkte ungewollte Berechtigungen entfernen	DUKE	FS, AD	1x pro Woche

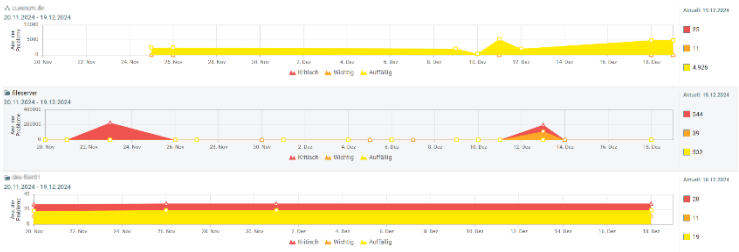
Best Practices

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

👁 – wird derzeit nur als Audit-Baustein angeboten

Risikobewertung von Experten

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.



Risikoeinstufung der Zugriffsrechte-Probleme

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	Bereinigungsbausteine	Erklärung	Analysen
Kritisch	VASS, ARCA, RAPA, DUKE, DARS, BAKS, SARA	Diese Analysen finden Berechtigungsfehler, die von unseren Experten als kritisch eingestuft werden. Kritische Fehler entstehen durch unzulässige Zugriffsrechte und sollten vorrangig bereinigt werden.	Erlaubte Besitzer-Analyse Direkte Benutzerberechtigung Redundante Zugriffsrechte Unterbrochene Vererbung Inaktive Computer Kennwort läuft nie ab Aktivierte Vererbung in Shares Offene Freigaben Privilegierte Rollen Globale Administrator-Rolle Anzahl Globale Admins Ablaufende Clientschlüssel
Wichtig	ERBE, MARS, VASS, ARCA, LARS, SARA	Diese Analysen finden weitere als wichtig eingestuften Probleme in Ihrem System. Solche relevanten Probleme sollten zeitnah behoben werden.	Ersteller-Besitzer Mindest-Berechtigungen Verschobene Verzeichnisse Ungewollte Konten Inaktive Benutzer Listgruppenanalyse Jeder-Vollzugriff Freigaben Gruppen-Rollenzuweisungen Cloud-Native Konten Rollenzuweisungen Inaktive Gastbenutzer Inaktive Anwendungen
Auffällig	TEUS, ARCA, SARA	Es werden Sicherheits-auffälligkeiten in den Zugriffsrechten gefunden. Diese Auffälligkeiten sollten nach unserer Erfahrung durch Ihre Administratoren überprüft werden.	Verwaiste Kontoreferenzen Veraltetes Kennwort Deaktivierter Benutzer Nie angemeldete Benutzer Leere Gruppen Gruppen ohne Beschreibung Nicht-administrative Freigaben Inaktive Cloud-Native Benutzer Cloud-Native Benutzer

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

Kritisch

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

Kritisch

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

Wichtig

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

Kritisch

Verschobene Verzeichnisse Finden

Wichtig

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

Auffällig

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

Wichtig

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

Wichtig

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

Wichtig

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

Kritisch

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

Freigabe-Berechtigungen überprüfen

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.

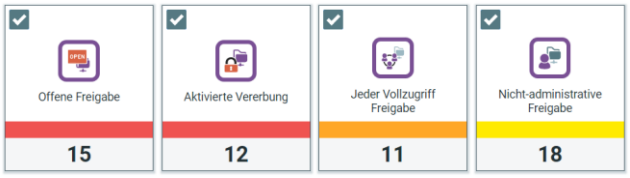
(2) Freigaben werden überprüft, ob authentifizierte Konten (AD und lokal) mindestens das Lese-Zugriffsrecht haben. Dann gelten diese Freigaben als **offene Shares**. Damit kann ein unkontrollierter Datenabfluss erfolgen.

(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.

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

Active Directory (AD)

- Inaktive Benutzer- oder Computerkonten
- Deaktivierte Benutzer, auch mit Prüfung nach x Tagen inaktiv
- Noch nie angemeldete Benutzer
- Nie angemeldete Benutzer
- Leere Gruppen und Gruppen ohne Beschreibung
- Konten mit nie ablaufenden Kennwörtern
- Benutzer mit veraltetem Kennwort

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

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!

Die CUSATUM Service GmbH am Standort Berlin/Brandenburg ist ein Software- und Beratungsunternehmen mit dem Fokus auf Berechtigungsmanagement und Automatisierung von Mitarbeiterprozessen. Als „Macher der ersten Stunde" haben wir den 8MAN von Protected Networks entwickelt. Dieser heißt jetzt SolarWinds-ARM und ist bis heute ein großer Erfolg im deutschsprachigen Raum.

Unsere Erfahrungen aus eineinhalb Jahrzehnten im Berechtigungsmanagement haben wir in unserer CARO-Suite eingebracht. Sie ist die notwendige Ergänzung zum ARM, die bisher gefehlt hat! Die CARO-Suite unterstützt Unternehmen im Berechtigungsmanagement zur Erfüllung gängiger Sicherheits- und Compliance-Richtlinien.

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

Hauptsitz
Wiesenweg 16
16548 Glienicke / Nordbahn

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

Support

Telefon +49 30 94 86 3401
Mobile +49 175 221 11 04

E-Mail support@cusatum.de

Stand: Januar 2025

SECURITY MADE IN GERMANY