

CyberSafe! Ihr Wissensboost zu Rechtemanagement

Rechtemanagement ist der Schlüssel zu sicherem und effizientem Arbeiten in Unternehmen. Wer Zugriffsrechte strukturiert vergibt und verwaltet, schützt sensible Daten, minimiert Risiken und bleibt handlungsfähig. Machen Sie Rechtemanagement zur Routine – für mehr Cyber-Sicherheit und weniger potentielle Angriffsflächen für Cyber-Kriminelle

Trainingsvideo: Rechtemanagement

Gemeinsam mit unserem IT-Krisendienstleister geben wir praxisnahe Einblicke, worauf es beim Rechtemanagement wirklich ankommt. Erhalten Sie im Expertenvideo konkrete Tipps, wie Sie mit gezielten Maßnahmen Ihr Netzwerk optimal sichern.

Expertentipps zum Nachlesen

Lesen Sie hier die wichtigsten Take-Aways aus dem Expertenvideo:

- **Minimalprinzip (Least Privilege) konsequent umsetzen:** Vergeben Sie Nutzern nur die Rechte, die für die jeweilige Aufgabe wirklich notwendig sind. So reduzieren Sie Angriffsflächen und schützen Ihr Unternehmen.
- **Rollenbasierte Rechtevergabe nutzen:** Bündeln Sie Berechtigungen in Rollen (z.B. nach Abteilung oder Aufgabe) und weisen Sie diese gezielt zu – das erleichtert die Verwaltung und verhindert Fehler.
- **Administrative Konten strikt trennen:** Arbeiten Sie im Alltag ausschließlich mit normalen Nutzerkonten. Admin-Konten sollten nur für administrative Aufgaben genutzt werden.
- **Lokale Administratorrechte kontrollieren und regelmäßig prüfen:** Vergeben Sie lokale Adminrechte nur temporär und rotieren Sie Passwörter regelmäßig.
- **Software und Maschinenrechte kritisch hinterfragen:** Prüfen Sie, ob Anwender wirklich administrative Rechte benötigen. Vermeiden Sie unnötige Berechtigungen, um Schwachstellen zu minimieren.
- **Sicherheitsdomänen klar abgrenzen:** Trennen Sie Zugriffe auf Backup-, Produktiv- und Virtualisierungsumgebungen. So verhindern Sie, dass ein kompromittierter Account das gesamte Unternehmen gefährdet.
- **Onboarding und Offboarding-Prozesse etablieren:** Rechtevergabe und -entzug müssen klar geregelt sein. Entfernen Sie Berechtigungen konsequent, wenn Mitarbeiter das Unternehmen verlassen oder die Rolle wechseln.
- **Regelmäßige Überprüfung und Dokumentation:** Kontrollieren Sie Nutzerkonten und Berechtigungen in festen Intervallen und dokumentieren Sie Prozesse sowie Änderungen für maximale Transparenz.



[Zum Expertenvideo](#)

Hier gelangen Sie zur kompletten Video-reihe „CyberSafe! Ihr Wissensboost für mehr IT-Sicherheit“

[Weitere Videos entdecken](#)

Wissensboost: Rechtemanagement

Rechtemanagement ist mehr als „ein paar Benutzerrechte“ – es ist ein zentraler Baustein für die IT-Sicherheit und einen stabilen Geschäftsbetrieb. Wer Rechte gezielt vergibt, Prozesse klar definiert und regelmäßig prüft, schützt sich vor Datenverlust, Angriffen und Betriebsunterbrechungen.

Was versteht man unter Rechtemanagement?

Rechtemanagement ist die strukturierte Verwaltung, Vergabe und der Entzug von Berechtigungen auf verschiedene Objekte wie Software, Räume, Hardware oder Maschinen. Es erleichtert die Verwaltung von Nutzer- und Rollenrechten, besonders bei vielen Mitarbeitern.

Warum ist Rechtemanagement so wichtig?

Je mehr Personen und Systeme Zugriff auf Ihre IT haben, desto größer ist die Angriffsfläche. Ziel des Rechtemanagements ist, das Risiko von Sicherheitsvorfällen zu minimieren, indem nicht jeder Zugriff auf alles bekommt.

Checkliste: Das sollten Sie prüfen

Ja	Nutzen Administratoren ein normales Benutzerkonto für ihre tägliche Arbeit und ein separates, persönliches Adminkonto für administrative Zugriffe?
Ja	Werden Rechte nach dem Minimalprinzip vergeben und regelmäßig überprüft (Least-Privilege-Prinzip)?
Ja	Werden Zugriffsrechte regelmäßig überprüft und angepasst?
Ja	Werden Passwörter für lokale Admin-Konten zentral verwaltet und regelmäßig erneuert?
Ja	Haben Sie Rollen und Sicherheitsgruppen sinnvoll definiert?
Ja	Gibt es klare Prozesse für Onboarding und Offboarding?

Cyber-Versicherung: Allround-Schutz bei digitalen Risiken

Die genannten Tipps helfen dabei, die Cyber-Sicherheit zu stärken. Leider lässt sich aber auch mit umfassenden Schutzmaßnahmen ein Cyber-Angriff nicht vollständig ausschließen. Um im Ernstfall handlungsfähig zu bleiben, sollten Sie das Restrisiko zusätzlich absichern. Zum Beispiel mit einer Cyber-Versicherung von Hiscox. Als Experte für Cyber-Gefahren und Pionier am deutschen Versicherungsmarkt hält Hiscox Selbstständigen und Unternehmen den Rücken frei – vorbeugend, mitten in der Krise, bei der Schadenregulierung und bei der nachgelagerten Sicherheitsanalyse.

Hiscox

Bernhard-Wicki-Straße 3, 80636 München

Für Makler

T +49 89 54 58 01 100

E hiscox.info@hiscox.de

W makler.hiscox.de/cyber

Für Endkunden

T +49 89 54 58 01 700

E myhiscox@hiscox.de

W hiscox.de/cyber

Hiscox in Social Media

