HORNETSECURITY

365 PERMISSION MANAGER

HEBEN SIE IHRE COMPLIANCE FÜR M365 AUF'S NÄCHSTE LEVEL

VERMEIDEN SIE DATENLECKS UND COMPLIANCE-PROBLEME IN MICROSOFT 365 DURCH EFFEKTIVES BERECHTIGUNGSMANAGEMENT

Das wichtigste und sensibelste Gut eines Unternehmens sind seine Daten. In einer traditionellen IT-Infrastruktur werden alle Daten in der Regel an einem zentralen Ort gespeichert, was es für CISOs einfach macht, Daten zu überwachen, Änderungen zu verfolgen oder die Freigabe und Löschung von Daten zu beschränken. Aber die Arbeitsweise ändert sich!

Mit der meistgenutzten Office-Suite für Unternehmen, Microsoft 365, können Mitarbeiter nun selbst Zugriffsrechte festlegen und Daten nach eigenem Ermessen freigeben. Und genau das ist das Problem, vor dem immer mehr CISOs stehen: Sie haben keinen Überblick über die Berechtigungen, die innerhalb und außerhalb ihres Unternehmens geteilt werden. Sie sind blind, was die Zugriffsrechte auf Unternehmensdaten angeht.

Diese Tatsache sollte nicht fahrlässig ignoriert werden, denn das kann zu katastrophalen Datenlecks und Datenschutzverstößen führen.

Wie CISOs die Kontrolle über Berechtigungen in M365 zurückgewinnen:

- ✔ Sie müssen einen leicht verständlichen Überblick über alle erteilten Genehmigungen erhalten.
- ✔ Sie benötigen ein Tool, mit dem sie SharePoint-, OneDrive- und Teams-Sites Freigabe-Richtlinien zuweisen können.
- ✔ Sie müssen in der Lage sein, Benutzern, die sich nicht an die festgelegten Richtlinien halten, die Zugriffsrechte zu entziehen.
- ✔ Sie brauchen ein Tool, das automatisch Richtlinien prüft und Warnungen an CISOs, Administratoren und Site-Besitzer sendet, wenn eine Richtlinie verletzt wurde.

365 Permission Manager schafft wieder Klarheit und minimiert das Risiko von Datenverlusten

- ✔ Der benutzerfreundliche und schnell zu implementierende GRC (Governance, Risk and Compliance) / DLP (Data Loss Prevention)-Dienst ermöglicht CISOs und Administratoren die mühelose Verwaltung von Microsoft 365-Berechtigungen, volle Transparenz, Durchsetzung von Compliance-Richtlinien und Überwachung von Verstößen.
- ✔ 365 Permission Manager trägt durch eine benutzerfreundliche Oberfläche, die einen umfassenden Überblick über die Berechtigungen bietet, zum besseren Schutz sensibler Informationen bei.
- ✔ CISOs und Administratoren sparen Zeit und Mühe, da sie Massenaktionen zur Verwaltung von Berechtigungen durchführen, Best-Practice-Richtlinien zuweisen oder benutzerdefinierte Compliance-Richtlinien für SharePoint-Sites und OneDrive erstellen können.
- ✔ Eine Audit-Funktion ermöglicht die einfache Genehmigung oder Zurückweisung möglicher Verstöße, indem die Einstellungen der Site entsprechend der zugewiesenen Compliance-Richtlinie zurückgesetzt oder Benutzern und Gruppen der Zugriff entzogen wird.

JETZT TESTEN!

ELOVADE

Kontaktdaten für Deutschland & Österreich

ELOVADE Deutschland GmbH
hornetsecurity@elovade.com
DE: +49 6441 67118 842
AT: +43 820 0010 36
elovade.com/hornetsecurity

Kontaktdaten für die Schweiz

ELOVADE Swiss AG
sales@elovade.ch
CH: +41 55 552 27 92
elovade.ch/hornetsecurity

365 PERMISSION MANAGER IST AUCH TEIL VON 365 TOTAL PROTECTION

E-MAIL-SECURITY, BACKUP, COMPLIANCE, AI RECIPIENT VALIDATION
UND SECURITY AWARENESS IN EINER LÖSUNG

PLAN 1	PLAN 2	PLAN 3	PLAN 4
BUSINESS	ENTERPRISE	BACKUP	COMPLIANCE & AWARENESS
SPAM & MALWARE PROTECTION	ADVANCED THREAT PROTECTION	BACKUP & RECOVERY OF MAILBOXES & TEAMS	PERMISSION MANAGEMENT
			PHISHING & ATTACK SIMULATION
			COMMUNICATION PATTERN ANALYSIS
EMAIL ENCRYPTION	EMAIL ARCHIVING	BACKUP & RECOVERY OF ONEDRIVE & SHAREPOINT	PERMISSION ALERTS
			SECURITY AWARENESS
			AI RECIPIENT VALIDATION
EMAIL SIGNATURES & DISCLAIMERS	EMAIL CONTINUITY	BACKUP & RECOVERY OF ENDPOINTS	PERMISSION AUDIT
			ESI® REPORTING
			SENSITIVE DATA CHECK

- **Effektives Management von Berechtigungen** – Quick Actions zur Korrektur von Berechtigungen für mehrere Sites auf einmal. Erweiterte Filterung zur schnellen Überprüfung und Aufschlüsselung verschachtelter Gruppen, um einen transparenten Überblick über die effektiven Zugriffsrechte zu erhalten.
- **Alerts** - Tägliche Zusammenfassung kritischer Berechtigungsänderungen in Ihrem M365-Tenant in Bezug auf die Freigabe von Websites, Dateien und Ordnern innerhalb und außerhalb Ihrer Organisation.
- **Audit-Funktion** - zur Freigabe oder Zurückweisung möglicher Verstöße durch Rückgängigmachung der Site-Einstellungen gemäß der zugewiesenen Compliance-Richtlinie oder Entzug des Zugriffs.
- **Phishing-Simulation** - Individuell angepasste Phishing-Szenarien führen zu gefälschten Anmeldeseiten, enthalten Anhänge mit Makros und E-Mails mit Antwort-Threads.
- **Security Awareness Service** - Vollautomatisiertes Awareness-Benchmarking, Spear-Phishing-Simulation und E-Training zur Sensibilisierung und zum Schutz der Mitarbeiter vor Cyber-Bedrohungen.
- **ESI® reporting** - Der ESI® Awareness Benchmark ermöglicht eine standardisierte, transparente Messung des Sicherheitsverhaltens auf Unternehmens-, Gruppen- und Benutzerebene.
- **Analyse von Kommunikationsmustern** – Lernt automatisch Ihre E-Mail-Kommunikationsmus ter und hilft, Ihre ausgehende Kommunikation innerhalb und außerhalb des Tenants zu sichern.
- **AI Recipient Validation** - analysiert E-Mails auf der Grundlage früherer Kommunikation und löst in verschiedenen Fällen Warnungen aus. (E-Mail-Texte und Anhänge werden nicht an die Server von Hornetsecurity übertragen. Die Analyse dieser wird im lokalen Outlook-Client durchgeführt).
- **Sensitive data check** - Benutzer werden sofort benachrichtigt, wenn die E-Mail, die sie zu senden versuchen, sensible Informationen wie personenbezogene Daten enthält.