8MAN

Access Rights Management. Only much Smarter.

ANFORDERUNGEN DES BSI UMSETZEN

Protected Networks

8MAN: ANFORDERUNGEN DES BSI UMSETZEN

Hintergrund: Der Grundschutzkatalog

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) vertritt mit dem Grundschutzkatalog eine Reihe von Anforderungen für den sicheren Betrieb von IT-Systemen. Darin enthalten sind technische, organisatorische, personelle und infrastrukturelle Maßnahmen, die für die Zertifizierung von IT-Systemen relevant sind.

Als zentrale Zertifizierungsstelle für IT-Sicherheit in Deutschland legt das BSI ein besonderes Augenmerk auf die Verwaltung von Zugriffsrechten. So heißt es in Maßnahme M 4.41 Einsatz angemessener Sicherheitsprodukte für IT-Systeme, dass häufig "vorhandene Sicherheitsfunktionalitäten" nicht ausreichten und "geeignete Sicherheitsprodukte" für die Zugriffsrechteverwaltung eingesetzt werden sollten. In der zentralen Maßnahme **M 2.8 Vergabe von Zugriffsrechten** gibt das BSI mit "Prüffragen" den Betreibern von IT-Systemen die Möglichkeit, das Sicherheitsniveau im Netzwerk selbst zu erörtern.

Bundesamt
für Sicherheit in der
Informationstechnik

Die Prüffragen der M 2.8 "Vergabe von Zugriffsrechten"

1. Werden nur die Zugriffsrechte vergeben, die für die jeweiligen Aufgaben erforderlich sind?
2. Liegt eine aktuelle Dokumentation der vergebenen Zugriffsrechte vor?
3. Werden beantragte Zugriffsrechte oder Änderungen erteilter Zugriffsrechte von den Verantwortlichen bestätigt und geprüft?
4. Existiert ein geregeltes Verfahren für den Entzug von Zugriffsrechten?

(Quelle: BSI, 14. EL Stand 2014)

8MAN Access Rights Management und BSI-Anforderungen

8MAN verfügt über fünf zentrale Services. Diese bilden in Ihrer Gesamtheit ein klares und schnell zu implementierendes System für eine professionelle Zugriffsrechteverwaltung in Ihrem Unternehmen.

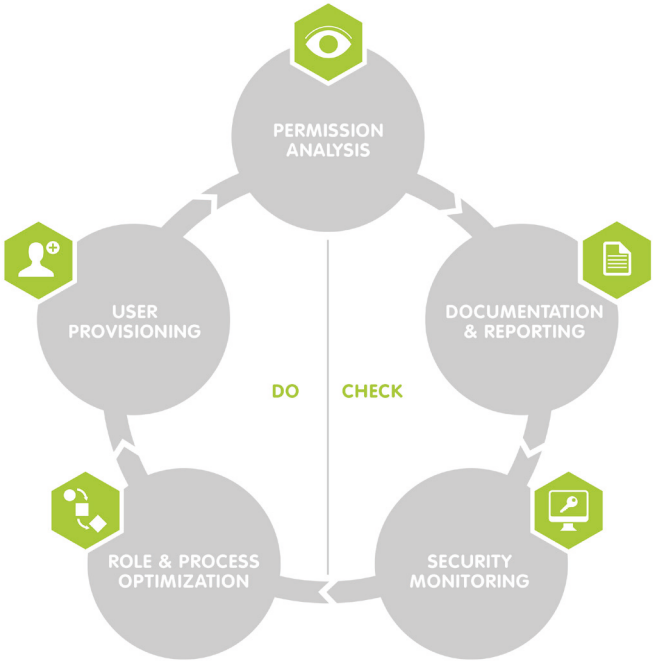
PERMISSION ANALYSIS
Zeigt ressourcenübergreifend die Berechtigungssituation in Ihrem Unternehmen.

DOCUMENTATION & REPORTING
Erfasst Access Rights Aktivitäten im Logbuch und erstellt revisionssichere Reporte.

SECURITY MONITORING
Überwacht sicherheitsrelevante Aktionen im Active Directory und auf Ihren Fileservern.

ROLE & PROCESS OPTIMIZATION
Verkürzt Ihren Access Rights Management Prozess und involviert nur die notwendigen Akteure.

USER PROVISIONING
Regelt die Anlage neuer Nutzerkonten, die Rechteverwaltung und die Bearbeitung von Kontodetails.



Zentral für die Erfüllung des Grundschutzes ist **Permission Analysis**. 8MAN zeigt die Berechtigungssituation in Ihrem Netzwerk bidirektional: Entweder wählen Sie eine sicherheitskritische Ressource und lassen sich anzeigen wer darauf Zugriff hat, oder Sie lassen sich die Zugriffsrechte eines Nutzers anzeigen. Die Anforderung (1), nur die Zugriffsrechte zu vergeben, die für die Mitarbeiter-Rolle notwendig sind, ist damit schnell umsetzbar.

Eine klare Dokumentation der Zugriffsrechte (2) schafft 8MAN mit **Documentation & Reporting**. Jede mit 8MAN vergebenen oder entzogenen Rechte sind im Logbuch erfasst und können in verständlichen Reporten dargestellt werden. Sie erkennen sofort, wer welche Rechte an wen vergeben hat. Bei sicherheitsrelevanten Aktionen verlangt 8MAN immer die Eingabe eines Kommentars. Mit einer kurzen Begründung oder Ticketnummer ist auch nach langer Zeit nachvollziehbar, weshalb ein Zugriffsrecht geändert wurde. Mit dem **Security Monitoring** können Sie das Sicherheitsniveau vertiefen und Aktivitäten erfassen, die außerhalb von 8MAN vorgenommen wurden.

Zugriffsrechte regeln die Verteilung von Firmenwissen. Sie sind geschäftskritisch und sollten nicht vom Administrator vergeben werden. Mit **Role & Process Optimization** wird die Verwaltung von Zugriffsrechten zu einem optimierten Business-Prozess. Data Owner (Führungskräfte) ordnen die Zugriffsrechte ihren Mitarbeitern zu. Diese wissen im Gegensatz zum Administrator, welche die schützenswerten Informationen in der Abteilung sind und wer darauf Zugriff haben sollte. Über individuelle Freigabe-Workflows (3) ist die Verantwortung eindeutig geklärt.

Sicherheitsrelevante Prozesse, wie die geregelte Vergabe und der Entzug (4) von Zugriffsrechten, scheitern häufig an der Effizienz-Hürde. Genau an dieser Stelle setzt **User Provisioning** an: Nutzerkonten und deren Zugriffsrechte können auch durch nicht IT-versierte Business Units schnell und einfach verändert werden.

Quelle: BSI (2014): IT Grundschutzkatalog. M 2.8 Vergabe von Zugriffsrechten,
URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02008.html

Anhang: Weitere BSI Anforderungen und dazugehörige 8MAN Services

Im Folgenden erhalten Sie Anforderungen des BSI Grundschutz zum Thema Access Rights Management. 8MAN unterstützt mit spezifischen Services bei der Umsetzung folgender Maßnahmen:

Katalognummer	BSI IT Grundschutz „Prüffragen"	Mit welchen Services* unterstützt 8MAN?
M 2.31 **Dokumentation der zugelassenen Benutzer und Rechteprofile.**	Sind die zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile dokumentiert?	**Documentation & Reporting** Reporte: B006: OU Mitglieder und Gruppenzugehörigkeiten aufzeigen B018: Wer kann wo über welche Berechtigungsgruppen zugreifen? B034: Wo haben Benutzer und Gruppen Zugriff? B014 Wer hat wo Zugriff?
	Wird die Dokumentation der zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile regelmäßig auf Aktualität überprüft?	**Documentation & Reporting** 8MAN erstellt alle Reporte automatisiert und in frei konfigurierbaren Intervallen.
	Ist die Dokumentation der zugelassenen Benutzer, Benutzergruppen und Rechteprofile vor unbefugtem Zugriff geschützt?	**Documentation & Reporting** Die Reporte lassen sich in geschützte Bereiche speichern oder an ausgesuchte Personenkreise verschicken.
	Wird die Dokumentation der zugelassenen Benutzer, Benutzergruppen und Rechteprofile - sofern sie elektronisch erfolgt - in das Datensicherungs-verfahren einbezogen?	N/A
M 2.8 **„Vergabe von Zugriffsrechten"**	Werden nur die Zugriffsrechte vergeben, die für die jeweiligen Aufgaben erforderlich sind?	**Permission Analysis** A004: Überberechtigte Benutzer anhand des Kerberos Tokens identifizieren A014: Ein Verzeichnis und die Berechtigungen darauf identifizieren A015: Einen Benutzer und seine Berechtigungen identifizieren A017: Mehrfachberechtigungen auf Verzeichnissen identifizieren
	Liegt eine aktuelle Dokumentation der vergebenen Zugriffsrechte vor?	**Documentation & Reporting** Reporte: B014: Wer hat wo Zugriff? B016: Wo haben Mitarbeiter eines Managers Zugriff? B034: Wo haben Benutzer und Gruppen Zugriff? B018: Wer kann wo über welche Berechtigungsgruppen zugreifen? B033: 8MAN Access Rights Management Aktivitäten erfassen (Logbuch Report)
	Werden beantragte Zugriffsrechte oder Änderungen erteilter Zugriffsrechte von den Verantwortlichen bestätigt und geprüft?	**Role & Process Optimization** D001: Die Verzeichnisrechte Verwaltung an einen Data Owner (Führungskraft) delegieren D011: Den Freigabeprozess definieren D014: GrantMA: Als Mitarbeiter FS-Zugriffsrechte beim DO bestellen

Katalognummer	BSI IT Grundschutz „Prüffragen“	Mit welchen Services* unterstützt 8MAN?
	Existiert ein geregeltes Verfahren für den Entzug von Zugriffsrechten?	**User Provisioning** E003:Gruppenmitgliedschaften bearbeiten E010: Einen Nutzer und seine Berechtigungen löschen E012: Einen Nutzer mittels „Soft Delete“ löschen
M 3.6 **Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern.**	Sind die Aktivitäten, die beim Weggang oder Funktionswechsel von Mitarbeitern durchzuführen sind, klar geregelt?	N/A
	Werden die zuständigen Stellen über das Ausscheiden eines Mitarbeiters rechtzeitig unterrichtet?	N/A
	Wird sichergestellt, dass sämtliche Zutrittsrechte, Zugangsberechtigungen und Zugriffsrechte einer ausscheidenden Person entzogen und gelöscht werden?	**User Provisioning** **Zutrittsrechte** lassen sich bei AD administrierten Tür-Systemen über 8MAN regeln. E003: Gruppenmitgliedschaften bearbeiten **Zugangsrechte und Zugriffsrechte** zu administrieren bedeutet AD Konten löschen oder temporär zu deaktivieren. 8MAN verfügt über zwei Services dazu: E010: Einen Nutzer und seine Berechtigungen löschen E012: Einen Nutzer mittels „Soft Delete“ löschen
	Wird sichergestellt, dass sämtliche institutionseigenen Werte (z.B. Unterlagen, Schlüssel, Rechner, Speichermedien) von einer ausscheidenden Person zurückgefordert und eingezogen werden?	N/A
M 4.24 **Sicherstellung einer konsistenten Systemverwaltung.**	Werden alle nötigen Vorgaben zur Sicherstellung einer konsistenten Systemverwaltung umgesetzt?	N/A
	Werden administrative Tätigkeiten und Systemeingriffe dokumentiert?	**Documentation & Reporting** *Dokumentation von Tätigkeiten, die mit 8MAN durchgeführt wurden:* B001: Ressourcenübergreifen die Eventhistorie nachvollziehen **Security Monitoring** *Dokumentation von Tätigkeiten, die auch außerhalb von 8MAN durchgeführt wurden:* C001: Änderungen im AD überwachen C002: Temporäre Gruppenmitgliedschaften erkennen C003: Anmeldeversuche mit Kontosperrung identifizieren C004: Kennwortzurücksetzungen überwachen C006: Die Berechtigungshistorie für ein sicherheitsrelevantes Verzeichnis analysieren C008: Temporäre Berechtigungsänderungen auf dem Fileserver nachweisen C009: Die Zugriffe auf sensible Dateien ermitteln

Katalognummer	BSI IT Grundschutz „Prüffragen“	Mit welchen Services* unterstützt 8MAN?
M 4.135 **Restriktive Vergabe von Zugriffsrechten auf Systemdateien.**	Wird der Zugriff auf Systemdateien auf einen möglichst kleinen Kreis von Administratoren beschränkt?	**Permission Analysis** A014 Ein Verzeichnis und die Berechtigungen darauf identifizieren A015 Einen Benutzer und seine Berechtigungen identifizieren
	Sind Systemverzeichnisse so eingerichtet, dass sie den Benutzern nur die benötigten Privilegien zur Verfügung stellen?	**Permission Analysis** A014 Ein Verzeichnis und die Berechtigungen darauf identifizieren A015 Einen Benutzer und seine Berechtigungen identifizieren
	Erfolgt die Vergabe von Zugriffsrechten restriktiv und im Einklang mit den organisationseigenen Sicherheitsrichtlinien?	N/A
	Wird die Rechtevergabe aller Programme inklusive der von diesen aufgerufenen weiteren Programme überprüft?	N/A
	Wird der Zugriff auf Systemdateien immer protokolliert?	**Security Monitoring** C009: Die Zugriffe auf sensible Dateien ermitteln
M 4.247 **Restriktive Berechtigungsvergabe bei Client-Betriebssystemen ab Windows Vista.**	Wurden alle Berechtigungen restriktiv nach den so genannten Need-to-know- oder Least-Privilege-Prinzipien vergeben?	**Permission Analysis** A015 Einen Benutzer und seine Berechtigungen identifizieren
	Wurde für Anwendungen unter Windows ein restriktives Berechtigungskonzept definiert und umgesetzt?	N/A
	Wurde der Sicherheitsgruppe „Jeder“ das Schreibrecht innerhalb von Systemordnern entzogen?	**Documentation & Reporting** B023 Das Konto„Jeder“ auf Berechtigungen prüfen
	Werden Freigabeberechtigungen nicht an integrierte Systemgruppen wie Authentifizierte Benutzer oder Jeder erteilt?	**Documentation & Reporting** B023 Das Konto„Jeder“ auf Berechtigungen prüfen B032 Das Konto „Authentifizierte Benutzer“ auf Berechtigungen prüfen
	Sind die restriktiven Berechtigungen mit dem Patchmanagement und dem Netz- und System-management abgestimmt?	N/A

Katalognummer	BSI IT Grundschutz „Prüffragen“	Mit welchen Services* unterstützt 8MAN?
M 4.309 **Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste.**	Wurden die Zugriffsrechte der Benutzer- und Administratorgruppen gemäß der erstellten Sicherheitsrichtlinie konfiguriert?	N/A
	Wurden die sich tatsächlich ergebenden effektiven Rechte auf die Zielobjekte stichprobenartig kontrolliert?	**Permission Analysis** A014 Ein Verzeichnis und die Berechtigungen darauf identifizieren
	Sind die Administratorrollen und die Delegation von Administrationsrechten konsistent konfiguriert?	**Permission Analysis** A015 Einen Benutzer und seine Berechtigungen identifizieren **Documentation & Reporting** B004 Kontodetails von Nutzern anzeigen
M 4.312 **Überwachung von Verzeichnisdiensten.**	Wurde ein bedarfsgerechtes Überwachungskonzept zum Verzeichnisdienst entworfen und umgesetzt?	**Permission Analysis** C001 Änderungen im AD überwachen
	Werden wichtige Systemereignisse des Verzeichnisdienstes protokolliert und regelmäßig ausgewertet?	**Security Monitoring** C002 Temporäre Gruppenmitgliedschaften erkennen C003 Anmeldeversuche mit Kontosperrung identifizieren C004 Kennwortzurücksetzungen überwachen C005 Alarme für AD Gruppen anlegen, bearbeiten und löschen
	Werden die Überwachungsparameter des Verzeichnisdienstes im Rahmen eines Testbetriebs überprüft und gegebenenfalls angepasst?	N/A

***** Die Angaben beziehen sich auf Active Directory & Fileserver. Fragen Sie unseren Vertrieb für die Integration weiterer Ressourcen.