8MAN

Access Rights Management. Only much Smarter.

WHITEPAPER DSGVO

Wie Sie mit 8MAN Ihr Unternehmen absichern.

MANAGEMENT SUMMARY

Die Datenschutzgrundverordnung (DSGVO) kommt und damit eine Reihe von neuen Anforderungen an Ihr Unternehmen. Neben den zentralen Informationen zur eigentlichen Regulatorik zeigt Ihnen das vorliegende Whitepaper, wie Sie mit 8MAN die zentralen Punkte der DSGVO umsetzen und damit Ihr Unternehmen sicher in die Zukunft führen. Die DSGVO dient dem Schutz personenbezogener Daten. Damit vertritt sie einerseits die Rechte von Verbrauchern und setzt andererseits Maßstäbe für den Schutz von Unternehmen.

Konkret schützt die Umsetzung Ihr Unternehmen vor Daten-, Informations- und Wissensdiebstahl. So wie Sie vertrauliche Papiere im Safe aufbewahren, sollten Sie auch mit Ihren digitalen Daten umgehen. Ohne Schutzvorkehrungen werden diese unerkannt kopiert und im schlimmsten Fall verkauft. Statt nur vom Datenschutz, sprechen Experten von einem Datenschatz. Diesen abzusichern, bedeutet gleichzeitig Ihr Unternehmen zu schützen.

Im Kapitel sechs dieses Whitepapers sind einige Prüffragen aufgeführt. Machen Sie den Test in Ihrem Unternehmen und prüfen Sie, wie schnell Ihre IT und die Geschäftsbereiche zufriedenstellende Antworten finden. Sollten Sie noch keine Lösung für ein professionelles Access Rights Management im Einsatz haben, freuen wir uns, Ihnen kostenfrei eine Teststellung von 8MAN anzubieten.

Kontaktieren Sie uns! Wir sind jederzeit bereit, 8MAN in Ihrem Unternehmen vorzuführen.

Stephan Brack, CEO **Sven Reinhardt,** CTO **Matthias Schulte-Huxel,** CSO

1. Hintergrund zur DSGVO

Mit der DSGVO regelt die Europäische Kommission die Verarbeitung personenbezogener Daten. Die Verordnung trat am 25.05.2016 in Kraft und wird zum 25.05.2018 geltendes Recht. Damit wird die aus dem Jahr 1995 stammende Datenschutz-Richtlinie 95/46/EG vollkommen ersetzt. Als supranationales EU-Recht wirkt die Regulation unmittelbar und bedarf keiner weiteren nationalen Beschlüsse.

Damit verfolgt die Kommission Datenschutzverstöße mit immer mehr Nachdruck. Ausdruck der Ernsthaftigkeit der EU-Initiative sind die neuen Bußgelder bei Verstoß gegen die Regulierung. Rangierten die Strafzahlungen vor der Novelle zwischen 50.000 und 300.000 Euro, erhebt die EU mit der DSGVO bis zu 20 Millionen Euro oder 4 Prozent des Jahresumsatzes (DSGVO Art. 83 Abs. 4 und Abs. 5).

Das Datenschutzrecht bietet jeder in der EU sich aufhaltenden, natürlichen Person Schutz vor der Verarbeitung ihrer Daten und reguliert Unternehmen und Institutionen weltweit bei der Handhabung personenbezogener Daten.

Personenbezogene Daten zeichnen sich durch einen Bezug zwischen der Person und einer anderen Person, Sache oder einem Ereignis aus. Konstitutiv für personenbezogene Daten ist die Möglichkeit, die Daten einer bestimmten Person zuzuordnen. Beispiele für personenbezogene Daten sind Kfz-Kennzeichen, Kontonummern, Rentenversicherungsnummern, Matrikelnummern, E-Mail- und IP Adressen. Maßgeblich für die Gültigkeit der Novelle ist nicht der Standort des Unternehmens, sondern der Aufenthaltsort der Person, deren Daten erfasst wurden.

2. Zentrale Anforderungen aus der DSGVO

Die DSGVO ist komplex. Sie verfügt über insgesamt elf Kapitel, die wiederum in 99 Artikel aufgegliedert sind. Experten diskutieren vor allem die Artikel 5 und 32. Diese repräsentieren die zentralen Neuanforderungen der DSGVO im Vergleich zu vorherigen Datenschutzrichtlinien.

Artikel 5: Grundsätze für die Verarbeitung personenbezogener Daten
(1) Abschnitt e) Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit");

(2) Der Verantwortliche ist für die Einhaltung des § 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht").

Artikel 32 Sicherheit der Verarbeitung

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

3. Anforderungen an Ihr Access Rights Management

Die Artikel 5 und 32 implizieren eine Reihe von Anforderungen an das Access Rights Management in Ihrem Unternehmen.

Artikel 5: Implizite Anforderungen

1. Datensicherheit und Integrität herstellen: Ressourcen, die personenbezogene Daten erhalten, dürfen nur vertrauenswürdigen Personen zugänglich sein. Ferner müssen die Verzeichnisse einem kontinuierlichen Monitoring unterliegen. Damit ist gewährleistet, dass Kopiervorgänge und Modifikationen an den Dateien jederzeit nachvollziehbar sind. Im Falle eines Sicherheitsvorfalls sind sowohl die Geschäftsbereiche als auch die IT auskunftsfähig und in der Lage, den Vorfall aufzuklären.

2. Dokumentation von Zugriffsrechten: Insbesondere die im Artikel 5 Absatz 2 festgehaltene Rechenschaftspflicht fordert von datenverarbeitenden Institutionen, jederzeit verzeichnisgenau die Zugriffsrechtehistorie und das tatsächliche Zugriffsverhalten aus der Vergangenheit nachweisen zu können.

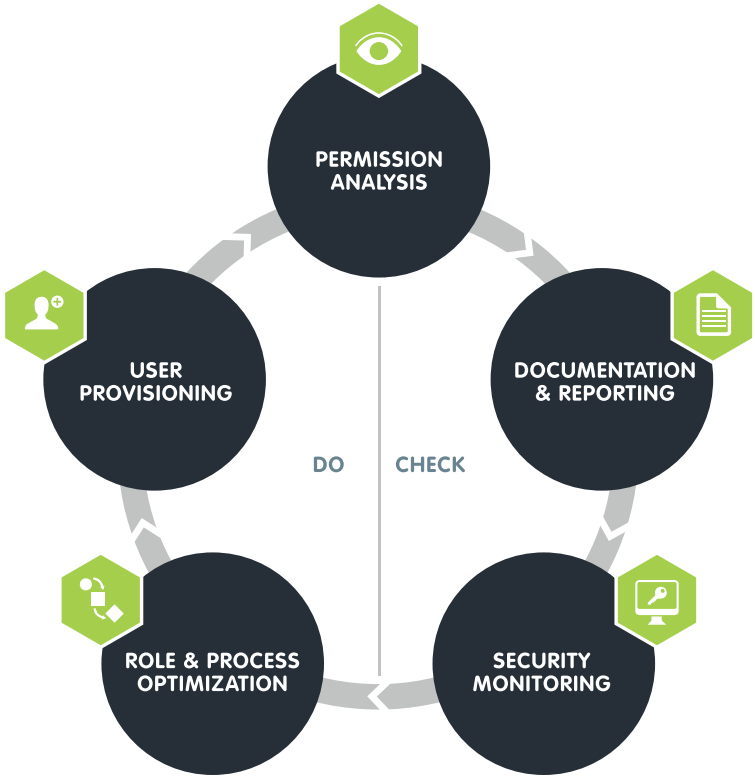
3. Pflege der Berechtigungssituation: Insbesondere im Joiner, Mover und Leaver-Prozess (also dem Lebenszyklus eines Nutzerkontos im Firmennetzwerk) müssen die IT und die Fachabteilungen die Berechtigungen des Mitarbeiters im Blick behalten und sehr schnell ändern können. Datendiebstahl erfolgt meist in der Leaver-Phase. Zu diesem Zeitpunkt muss die Fachabteilung dem Mitarbeiter alle Zugriffsrechte auf sicherheitskritische Verzeichnisse entzogen haben.

Artikel 32: Implizite Anforderungen

4. Data Owners einführen: Die DSVGO fordert klare Verantwortlichkeiten im Umgang mit personenbezogenen Daten. Dazu ist die Einführung der Rolle „Data Owner" zentral. Data Owners sind Führungskräfte, die innerhalb ihrer Abteilung über Daten wachen. Sie wissen welche Verzeichnisse geschützt werden müssen und welche Mitarbeiter vertrauenswürdig sind. Die Einführung von neuen Rollen, wie die des Data Owners, verlangt gleichzeitig nach neuen Prozessen der Zusammenarbeit und der Dokumentation vorgenommener Aktivitäten.

4. Mit 8MAN zentrale DSGVO Anforderungen umsetzen

8MAN verfügt über fünf zentrale Disziplinen. Diese bilden in ihrer Gesamtheit ein klares und schnell zu implementierendes System für ein DSGVO konformes Access Rights Management.



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 der zentralen DSGVO-Anforderungen ist **Permission Analysis**. 8MAN zeigt die Berechtigungssituation in Ihrem Netzwerk bidirektional: Entweder wählen Sie eine Ressource mit personenbezogenen Daten und lassen sich anzeigen, wer darauf Zugriff hat oder Sie lassen sich die Zugriffsrechte eines Nutzers auf sämtliche Ressourcen anzeigen. Mit diesem Wissen ist die Anforderung (1) „Datensicherheit und Integrität herstellen" schnell umsetzbar.

Die Zugriffsrechtesituation, die Aktivitäten in den geschützten Verzeichnissen und die Praxis der Berechtigungsvergabe bereitet **Documentation & Reporting** für Sie in einfach lesbaren und strukturierten Reporten auf. Diese lassen sich automatisiert und verzeichnisspezifisch an die beteiligten Rollen im Unternehmen versenden. Die Anforderung (2) „Dokumentation von Zugriffsrechten" ist damit automatisch erfüllt.

Neben der Zugriffsrechtesituation sind vor allem die tatsächlichen Vorgänge mit den personenbezogenen Daten relevant. Mit dem **Security Monitoring** vertiefen Sie das Sicherheitsniveau und erfassen Aktivitäten innerhalb der Verzeichnisse, in denen die personenbezogenen Daten gespeichert sind. Darüber hinaus erfasst die AD Analyse auch außerhalb von 8MAN vorgenommene Änderungen an der Berechtigungssituation. Damit sind temporäre Gruppenmitgliedschaften und daraus resultierende unkontrollierte Berechtigungsvergaben sofort nachvollziehbar. 8MAN informiert Sie proaktiv über die Alerts Funktion, sollte jemand versuchen, die Sicherheitsgruppe zu manipulieren.

8MAN bietet mit Role & Process Optimization eine Reihe von Best Practice Prozessen, deren Implementierung für ein DSGVO-konformes Access Rights Management essentiell ist. Die Kontrolle und Pflege von Zugriffsrechten auf personenbezogene Daten muss prozessual im Unternehmen definiert sein. **Role & Process Optimization** schafft dafür den geeigneten Rahmen. Zentral ist in der Konzeption die Rolle des Data Owners: Anforderung (4) „Data Owners einführen". Die Führungskraft wacht über die Zugriffsrechtesituation im eigenen Bereich und entscheidet, wer auf die personenbezogenen Daten Zugriff haben soll. Im Rahmen einer periodischen Rezertifizierung kann der Data Owner – auch ohne weitreichende IT Kenntnisse – Berechtigungen entfernen oder bestehen lassen.

Auch bei einer vierteljährlich gesetzten Rezertifizierung bleibt die Adhoc-Pflege der Berechtigungssituation eine wichtige Anforderung. Verlässt ein Mitarbeiter das Unternehmen, müssen frühzeitig seine Zugriffsrechte auf personenbezogene Daten bzw. sonstiges Unternehmenwissen entfernt werden. Dies erfolgt durch den Data Owner oder Administrator via Drag & Drop im **User Provisioning**. Anforderung (3): Pflege der Berechtigungssituation.

5. Schritte für die Implementierung einer DSGVO-konformen Sicherheitsarchitektur im Unternehmen

Das folgende Kapitel zeigt Ihnen die wichtigsten Schritte auf dem Weg zu einem DSGVO-konformen Access Rights Management. Die Dokumentation der genannten Services finden Sie in unserem Anwenderhandbuch.

5.1 Data Owners nominieren und ihnen Ressourcen zuweisen

Um die IT-Sicherheit Ihrer personenbezogenen Daten zu erhöhen, ist es notwendig die entsprechenden Strukturen in Ihrem Unternehmen zu verankern. Ziel ist es, die Sicherheitskompetenz im Unternehmen zu dezentralisieren. Nominieren Sie dazu Data Owners in den Bereichen, wo personenbezogene Daten verwendet werden. In der Regel zählt dazu der Einkauf, der Vertrieb und natürlich die Personalabteilung.

DATA OWNERS, DATENSCHUTZBEAUFTRAGTE UND DER AUDITOR

Typischerweise ernennen Geschäftsführer ihre Abteilungsleiter zu Data Owners. Sie kennen die schützenswerten Daten ihrer Abteilung und wissen, wer darauf Zugriff haben sollte.

Der Data Owner ist die „First Line of Defense". Er reportet an den Datenschutzbeauftragten und wird über weitere Rechte und Pflichten durch ihn beraten („Second Line of Defense").

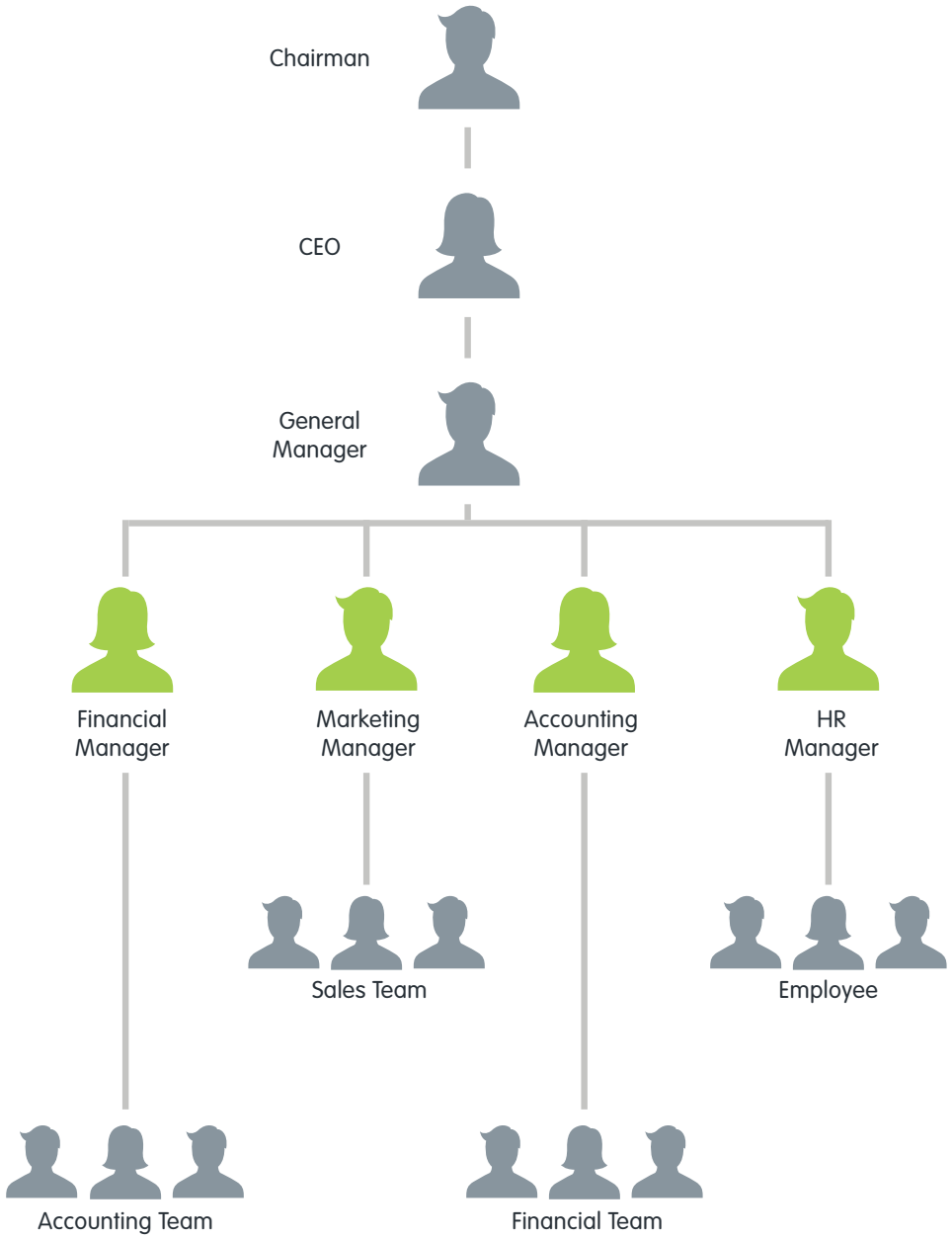
Die „Third Line of Defense" ist üblicherweise das interne oder externe Audit. Sowohl der Datenschutzbeauftragte als auch der interne Auditor sollten durch automatisierte Reporte regelmäßig über die Berechtigungssituation informiert werden. Alternativ können Sie den Sicherheitsrollen im Unternehmen auch einen Lese-Account in 8MAN anlegen (**D013**). (s. Abb. S.9)

8MAN DISZIPLIN: ROLE & PROCESS OPTIMIZATION

Verkürzt Ihren Access Rights Management Prozess und involviert nur die notwendigen Akteure.

Auszuführende(r) Service(s):

- ✓ **D002** Einen Data Owner definieren und ihm Ressourcen zuweisen
- ✓ **D003** Einem Data Owner die Verzeichnisrechte-Verwaltung übertragen
- ✓ **D013** Einen 8MAN Account für eine Sicherheitsrolle anlegen


Chairman
CEO
General Manager
Financial Manager
Marketing Manager
Accounting Manager
HR Manager
Sales Team
Employee
Accounting Team
Financial Team

5.2 Personenbezogene Daten lokalisieren und zentralisieren

Jeder Data Owner durchsucht im nächsten Schritt seine zugewiesenen Ressourcen nach personenbezogenen Daten. Sollten sich diese in unterschiedlichen Verzeichnisbäumen befinden, empfehlen wir die Daten zentral zu speichern. (s. Abb. S.11)

5.3 Zugriffsrechte auf die personenbezogenen Daten reduzieren

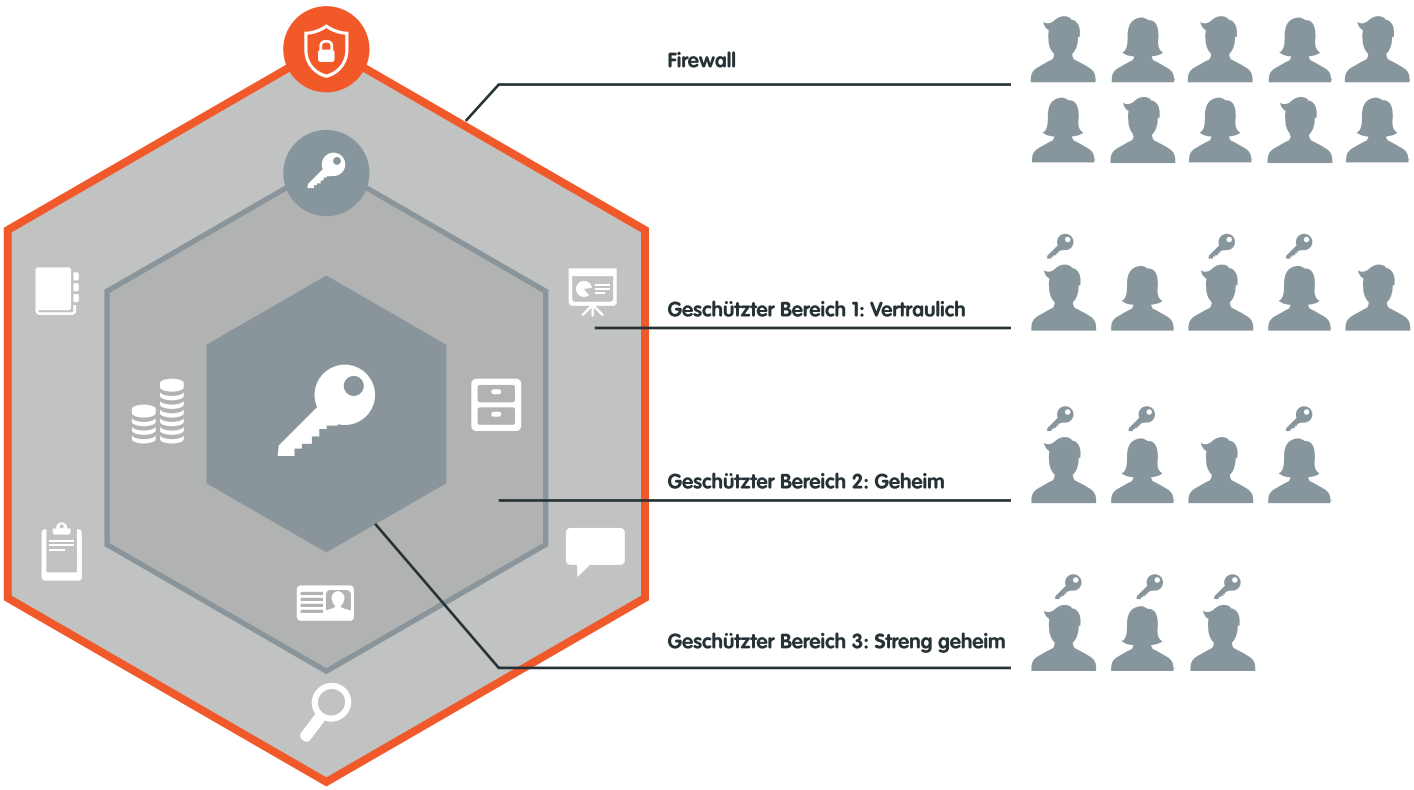
Erstellen Sie eine AD Sicherheitsgruppe und berechtigen Sie darüber alle zugriffsberechtigten Personen auf das sicherheitskritische Verzeichnis (**E001**). Anschließend identifizieren Sie etwaige Mehrfachberechtigungen und entfernen diese, sodass der Zugriff auf das Verzeichnis nur durch die Sicherheitsgruppe erfolgen kann (**E017**). Entfernen Sie anschließend die Zugriffsrechte von Personen, die nicht zwingend Einblick in die personenbezogenen Daten brauchen (**E015**). Hierbei gilt das „Principle of least Privilege". Es besagt, dass sicherheitsrelevante Daten nur den Personen zugänglich seien sollten, die auf deren Verarbeitung wirklich angewiesen sind.

8MAN DISZIPLIN: USER PROVISIONING

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

Auszuführende(r) Service(s):

- ✓ **E001** Gruppen anlegen und Benutzer hinzufügen
- ✓ **E017** Mehrfachberechtigungen auf Verzeichnissen entfernen
- ✓ **E015** Verzeichnisberechtigungen für Mitarbeiter erteilen und entziehen



Personenbezogene Daten gehören zum Bereich „Geschützter Bereich 1". Nur wenige Mitarbeiter sollten darauf zugreifen können.

5.4 Verzeichnisse und Gruppen mit Hilfe des Security Monitorings überwachen

Im nächsten Schritt wenden Sie das Security Monitoring an. Liegen Ihre personenbezogenen Daten auf dem Fileserver, empfehlen wir die tatsächlichen Zugriffe auf das Verzeichnis regelmäßig zu analysieren (**C009**). Senden sie den Report mit den Dateizugriffen automatisiert an den Datenschutzbeauftragten und die interne Revision. Damit involvieren Sie ohne weiteres Zutun die weiteren Sicherheitsrollen in ihrem Unternehmen. Ihre AD Gruppe sichern Sie mit der Alerts Funktion ab (**C005**). Sollte jemand diese manipulieren, erhalten der Data Owner, Datenschutzbeauftragte und Geschäftsführer sofort einen E-Mail Alert.

8MAN DISZIPLIN: SECURITY MONITORING
Überwacht sicherheitsrelevante Aktionen im Active Directory und auf Ihren Fileservern.

Auszuführende(r) Service(s):
- ✓ **C009** Die Zugriffe auf sensible Dateien ermitteln
- ✓ **C005** Alarme für AD Konten und Gruppen anlegen, bearbeiten und löschen

5.5 Die Sicherheitsrollen im Unternehmen automatisiert mit Reporten involvieren

Die Reporte über die Berechtigungssituation oder über die Dateizugriffe auf personenbezogene Daten sollten periodisch dem Datenschutzbeauftragten und dem internen Auditor zur Verfügung gestellt werden. 8MAN erlaubt es, die Reporte verzeichnisspezifisch zu definieren und automatisiert den Beteiligten via E-Mail zu senden (**D020**). Insbesondere die Services (**B034, B014, C009**) sind dabei zentral.

8MAN DISZIPLIN: DOCUMENTATION & REPORTING / SECURITY MONITORING
Erfasst Access Rights Aktivitäten im Logbuch und erstellt revisionssichere Reporte / überwacht sicherheitsrelevante Aktionen im Active Directory und auf Ihren Fileservern.

Auszuführende(r) Service(s):
- ✓ **D020** Reporte automatisch zusenden lassen
- ✓ **B034** Wo haben Benutzer / Gruppen Zugriff? (Fokus Verzeichnis)
- ✓ **B014** Wer hat wo Zugriff? (Fokus Mitarbeiter)
- ✓ **C009** Die Zugriffe auf sensible Dateien ermitteln

5.6 Die Berechtigungssituation für Verzeichnisse mit personenbezogenen Daten im Blick behalten

Die Berechtigungen auf sicherheitskritische Verzeichnisse müssen regelmäßig durch die Data Owners geprüft werden. Die durch den Administrator zu aktivierende 8MAN Rezertifizierungsfunktion (**D023**) fordert die Data Owners periodisch zur Einhaltung ihrer Prüfpflicht auf. In einer einfachen Ansicht können Sie schnell und verzeichnisspezifisch die Zugriffsrechte entweder bestehen lassen oder entziehen (**D024**).

8MAN DISZIPLIN: ROLE & PROCESS OPTIMIZATION
Verkürzt Ihren Access Rights Management Prozess und involviert nur die notwendigen Akteure.

Auszuführende(r) Service(s):
- ✓ **D023** Den Rezertifizierungsprozess aktivieren (Administrator)
- ✓ **D024** Bestehende Zugriffsrechte rezertifizieren (Data Owner)

5.7 Verzeichnisberechtigungen vor dem Abteilungswechsel oder Unternehmensaustritt entfernen

Sobald ein Mitarbeiter die Abteilung wechselt, bedarf es eines sofortigen Entzugs seiner abteilungsspezifischen Zugriffsrechte. Dies können Data Owners bequem im Webclient erledigen. In der „Leaver-Phase" gilt: Je früher die Berechtigungen auf sicherheitskritische Verzeichnisse entfernt werden (**E052**), desto besser.

8MAN DISZIPLIN: USER PROVISIONING
Regelt die Anlage neuer Nutzerkonten, die Rechteverwaltung und die Bearbeitung von Kontodetails.

Auszuführende(r) Service(s):
- ✓ **E052** Berechtigungen im Webclient entfernen

6. Prüffragen an Ihre IT und Geschäftsbereiche

1. Wo sind unsere personenbezogenen Daten gespeichert und wer hat darauf Zugriff?

2. Wo hat Herr Mustermann überall Zugriff?

3. Wer hat im Zeitraum XY was im Verzeichnis XY gemacht?

4. Welches sind unsere besonders sicherheitsrelevanten AD- Gruppen, auf welche Daten berechtigen diese und wer ist darin Mitglied?

5. Wie bekomme ich Bescheid, wenn eine AD Sicherheitsgruppe oder ein Nutzerkonto manipuliert wurden?

6. Wer erstellt mir schnell einen verständlichen Report über die Zugriffsrechtesituation in meinem Unternehmen?

7. Wer ist in seinem Fachbereich verantwortlich für die Überwachung sicherheitsrelevanter Verzeichnisse?

8. Wann hatten wir unsere letzte Rezertifizierung von Zugriffsrechten?

7. Über 8MAN

8MAN ist eine führende Lösung für Access Rights Management (ARM) in Microsoft-Umgebungen und schützt damit Unternehmen vor unberechtigten Zugriffen auf sensible Daten. Die in Deutschland von Protected Networks entwickelte Software-Lösung setzt Maßstäbe für professionelle Netzwerksicherheit und agile IT-Organisation und bündelt modernste Funktionalität mit der Erfüllung gängiger Sicherheits- und Compliance-Richtlinien. Die 8MAN Kerndisziplinen umfassen: Permission Analysis, Documentation & Reporting, Security Monitoring, Role & Process Optimization und User Provisioning.

WIE SIE IHR UNTERNEHMEN SICHERN

Die Einführung von 8MAN ist kein Projekt, sondern ein Griff zum Telefon. Vereinbaren Sie einen Termin und ein zertifizierter Techniker wird die Installation und Konfiguration bei Ihnen im Unternehmen vornehmen. Je nach den Möglichkeiten in Ihrem Unternehmen kann die Installation vollständig via Remote Access vorgenommen werden.

8. Kontakt

Andreas König
Head of Sales Engineering
& Professional Services

T: +49 30 390 63 45-77
M: +49 160 661 56 27
koenig@8man.com

Kostenloses Webinar Starten Sie mit einer 30-minütigen Führung und sehen Sie den 8MAN in Aktion. Als Teilnehmer bleiben Sie untereinander anonym. Sie haben die Möglichkeit, am Ende der Präsentation im Chat Fragen zu stellen.

Kostenlose Teststellung Testen Sie 8MAN mit einer 21 Tage gültigen kostenlosen Testlizenz und Sie haben genug Zeit, sich von unserer Lösung in Ruhe zu überzeugen.

8MAN | Protected Networks GmbH

Alt-Moabit 73
10555 Berlin
Germany

T: +49 30 390 63 45 - 0
E: info@8man.com
W: www.8man.com

Autor:
Fabian Fischer
Knowledge Manager

+49 30 390 63 45-41
fabian@8man.com