8MAN

DAS INFORMATION SECURITY ASSESSMENT IM FOKUS

Mit 8MAN Anforderungen des VDA umsetzen

Vorwort

Als Marktführer im Access Rights Management arbeiten wir eng mit besonders schutzbedürftigen Industriezweigen zusammen. Ein wichtiger Bereich ist die Automobilindustrie, die sich innerhalb der letzten Jahre stark globalisiert hat. Mit der Ausweitung der Geschäftsprozesse sind auch die Sicherheitsanforderungen für alle Beteiligten gestiegen.

Insofern begrüßen wir die klaren Anforderungen des Verbandes der Automobilindustrie (VDA), die im Rahmen des Information Security Assessment (ISA) formuliert sind. Darin enthalten sind technische, organisatorische, personelle und infrastrukturelle Maßnahmen, die für die Absicherung von IT-Systemen relevant sind.

8MAN erfüllt die zentralen technischen Anforderungen und geht sogar noch darüber hinaus. Mit der vorliegenden Publikation zeigen wir das Funktionsspektrum von 8MAN und wie unsere Lösung bei der Bewältigung der regulatorischen Anforderungen hilft. Über die eingefügten Links gelangen Sie direkt in unsere Online-Hilfe, in der unser gesamtes Funktionsspektrum dokumentiert ist.

Wir wünschen Ihnen viel Spaß bei der Umsetzung des VDA ISA. Sollten Sie für die Optimierung Ihrer IT professionelle Unterstützung benötigen, sind wir jederzeit für Sie da.

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

Inhaltsverzeichnis

Klicken Sie auf das Whitepaper-Symbol, um den Abschnitt im Original zu lesen.

Als 8MAN-Kunde können Sie sofort handeln: Klicken Sie auf den grünen Pfeil, gelangen Sie direkt in unsere Online-Hilfe zu dem korrespondierenden 8MAN-Service.

1.Das IT Sicherheitskonzept von 8MAN

Mit insgesamt acht Disziplinen verfügt 8MAN über das größte Leistungsportfolio auf dem Markt.

Die fünf Kerndisziplinen bilden in ihrer Gesamtheit ein klares und schnell zu implementierendes System für eine professionelle Zugriffsrechteverwaltung in Ihrem Unternehmen.

Zentral für die Absicherung Ihrer Daten ist **Permission Analysis.** 8MAN zeigt die Berechtigungs-situation 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.

Documentation & Reporting schafft eine klare Dokumentation der Zugriffsrechte. Alle 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** vertiefen Sie das Sicherheitsniveau und erfassen auch Aktivitäten, die außerhalb von 8MAN vorgenommen wurden. Sollte sich ein Mitarbeiter mit Bordmitteln Einblick in geschützte Verzeichnisse verschaffen, löst 8MAN sofort einen Alarm aus. Dateizugriffe, Manipulationen am AD und Eingriffe an ausgewählten Postfächern werden lückenlos dokumentiert.

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 individuell definierbare Freigabe-Workflows ist die Verantwortung eindeutig geklärt.

Die geregelte Vergabe und der Entzug von Zugriffsrechten scheitern häufig an der Effizienzhürde. Genau an dieser Stelle setzt **User Provisioning** an: Nutzerkonten und ihre Zugriffsrechte können auch durch nicht IT-versierte Business Units schnell und einfach verändert werden.

Ein ganzheitliches Berechtigungsmanagement darf sich nicht allein auf die Zugriffsrechte im Active Directory und in Fileservern beschränken. Mit **Resource Integration** folgen wir unserer Vision, immer mehr berechtigungsabhängige Anwendungen in die 8MAN Lösung zu integrieren. Unser Ziel ist eine Oberfläche, mit der Sie alle Anwendungen analysieren und administrieren können. Neben den Basistechnologien Active Directory und Fileserver haben wir MS Exchange, MS SharePoint und MS Dynamics NAV erfolgreich eingebunden. Mit unserer offenen Schnittstelle "Easy Connect" können Sie auch selbst Daten in 8MAN einlesen. Sie gewinnen so die 8MAN-typische Übersicht über die Berechtigungslage weiterer Systeme.

Die Korrektur von Berechtigungsfehlern und Inkonsistenzen ist auf Fileservern nur schwer möglich. Die Umsetzung von Best Practices scheitert an zwei zentralen Hürden: Wissen und Zeit. Darüber hinaus liegt der Fokus im klassischen Access Rights Management (ARM) auf der Verzeichnisebene. Sie ist die zentrale Analyseebene, blendet aber die Dateiebene aus. **Threat & Gap Management** startet einen Prozess, der in einen sicheren und standardisierten Fileserver mündet. Durch eine Reihe klarer Entscheidungen definieren Sie, wie mit Sicherheits- und Strukturproblemen umgegangen werden soll. Ihre Anforderungen und die in 8MAN hinterlegten Best Practices werden automatisch umgesetzt. Darüber hinaus ist die Archivierung veralteter Daten möglich. Denn: je geringer die Dateimasse, desto einfacher die Verwaltung.

Moderne IT-Lösungen müssen in der Softwarelandschaft einer strukturierten IT miteinander vernetzt sein. Insellösungen schaffen Frustration bei Nutzern, Administratoren und IT-Leitern. **8MAN Application Integration** ist die serienmäßig enthaltene WebAPI. Diese lässt sich für die Anbindung an zahlreiche Lösungen nutzen.

2. Das VDA ISA im Überblick

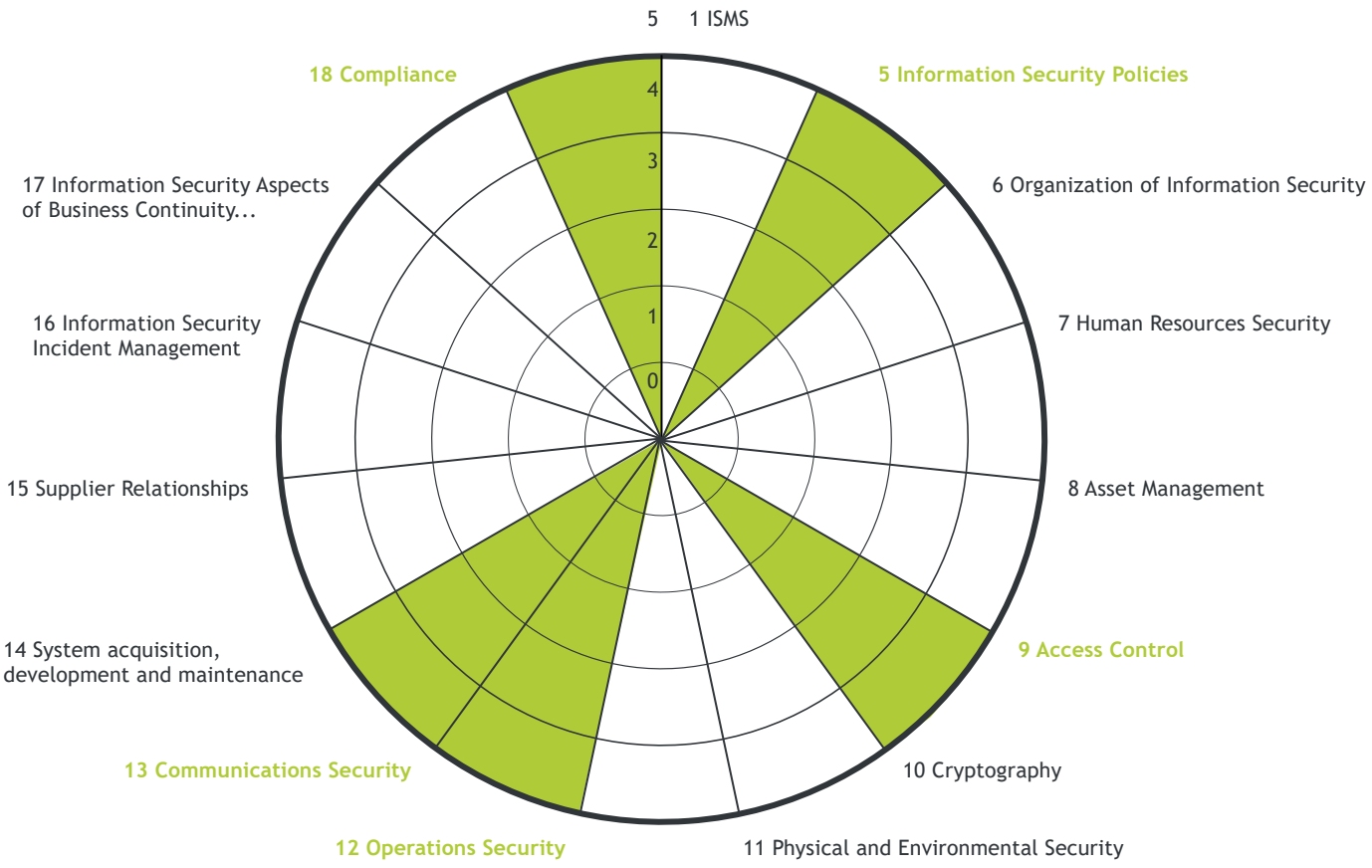
Erstmalig im Jahr 2005 veröffentlichte der VDA Empfehlungen zur Informationssicherheit für die Automobilindustrie. Heute basiert das VDA ISA auf der ISO 27002:2013 und dient vor allem der Informationssicherheitsbewertung.

Mit der systematischen Abfrage zentraler Prüffragen, dient der VDA ISA als Basis für

- Self-Assessments zur Bestimmung der Informationssicherheit in der Organisation
- Audits, z.B. durch interne Fachabteilungen (z. B. Revision, Informationssicherheit)
- die Prüfung nach TISAX (Trusted Information Security Assessment Exchange, https://enx.com/tisax/)

Der VDA ISA ist auf Deutsch und Englisch erhältlich.

Abgefragt werden Ist-Zustände in insgesamt 14 Teilbereichen:



8MAN erfüllt vor allem Anforderungen in den Bereichen:

- Organization of Information Security
- Access Control
- Operations Security
- Communications Security
- Compliance

3.1. Organization of Information Security

3.1.1 Der Baustein im Überblick

#	Thematik	8MAN
6.1	Zuweisung der Verantwortung für Informationssicherheit	X
6.2	Informationssicherheit in Projekten	
6.3	Mobile Endgeräte	
6.4	Rollen und Verantwortlichkeiten bei externen IT-Diensteanbietern	

3.1.2. Prüffragen und 8MAN Funktionalität

VDA ISA Prüffrage(n)	Wie unterstützt 8MAN?
Prüffrage 6.1. Inwieweit sind die Verantwortlichkeiten für Informationssicherheit definiert und zugewiesen?	Mit **Role & Process Optimization** wird die Verwaltung von Zugriffsrechten zu einem optimierten Business-Prozess mit klaren Verantwortlichkeiten. Data Owners (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. **Services** → Die Verzeichnisrechte Verwaltung an einen Data Owner (Führungskraft) delegieren

3.2. Access Control

3.2.1 Der Baustein im Überblick

#	Thematik	8MAN
9.1	Zugang zu Netzwerken und Netzwerkdiensten	
9.2	Benutzerregistrierung	X
9.3	Privilegierte Benutzerkonten	X
9.4	Vertraulichkeit von Authentifizierungsinformationen	
9.5	Zugriff auf Informationen und Applikationen	X
9.6	Trennung von Informationen in gemeinsam genutzten Umgebungen	

3.2.2. Prüffragen und 8MAN Funktionalität

VDA ISA Prüffrage(n)	Wie unterstützt 8MAN?
Prüffrage 9.2 Inwieweit sind Verfahren zur Registrierung, Änderung und Löschung von Benutzern mit den zugehörigen Zugriffsrechten umgesetzt und erfolgt dabei insbesondere ein vertraulicher Umgang mit den Anmeldeinformationen?	**User Provisioning** 8MAN steuert den gesamten Nutzerkonto-Lifecycle (Joiner-, Mover-, Leaver-Prozess). Ein Nutzerkonto wird mit einem Template angelegt. Mit einem Abteilungsprofil wird ein Basissatz an Berechtigungen zugewiesen. In der abteilungsübergreifenden Kollaboration werden Berechtigungen temporär vergeben. Bei Austritt aus dem Unternehmen werden alle Rechte kontrolliert entzogen und das Nutzerkonto deaktiviert. **Services** → Die Nutzeranlage mit Templates standardisieren → Ein neues Abteilungsprofil erstellen (Webclient) → Temporäre Gruppenmitgliedschaften bearbeiten (Webclient) → Benutzer deaktivieren (Cockpit)

3.2.2. Prüffragen und 8MAN Funktionalität

VDA ISA Prüffrage(n)	Wie unterstützt 8MAN?
Prüffrage 9.3 Inwieweit ist die Zuweisung sowie die Nutzung von privilegierten Benutzer- und technischen Konten geregelt und wird diese überprüft?	**Betrieb mit dem AD Servicekonto** 8MAN ist nur passwortgeschützt zu erreichen und lässt sich mit Hilfe eines Servicekontos zum führenden System im Active Directory machen. Eine Arbeit mit Bordmitteln ist dann nicht mehr möglich und das AD ist vor sonstiger Manipulation geschützt. Alle mit 8MAN durchgeführten Operationen werden automatisch dokumentiert.
Prüffrage 9.5 Inwieweit wird der Zugriff auf Informationen und Applikationen auf berechtigte Personen eingeschränkt?	8MAN arbeitet strikt nach dem Need-to-know-Prinzip. Danach sollten immer nur so viele Zugriffsrechte vergeben werden, wie für die Aufgabenwahrnehmung der Rolle notwendig sind. **Permission Analysis** → Überberechtigte Benutzer anhand des Kerberos Tokens identifizieren → Ein Verzeichnis und die Berechtigungen darauf identifizieren → Einen Benutzer und seine Berechtigungen identifizieren → Mehrfachberechtigungen auf Verzeichnissen identifizieren **Documentation & Reporting** → Wer hat wo Zugriff? → Wo haben Mitarbeiter eines Managers Zugriff? → Wo haben Benutzer und Gruppen Zugriff? **User Provisioning** → Gruppenmitgliedschaften bearbeiten → Einen Nutzer und seine Berechtigungen löschen → Einen Nutzer mittels „Soft Delete“ löschen

3.3. Operations Security

3.3.1 Der Baustein im Überblick

#	Thematik	8MAN
12.1	Änderungsmanagement (Change Management)	
12.2	Trennung der Entwicklungs-, Test- und Produktivumgebung	
12.3	Schutz vor Schadsoftware	
12.4	Informationssicherung (Backup)	
12.5	Event-Logging	X
12.6	Protokollierung Administrationstätigkeiten	X

3.3.2. Prüffragen und 8MAN Funktionalität

VDA ISA Prüffrage(n)

Prüffrage 12.5

Inwieweit werden Ereignis-Logs, die z.B. Benutzeraktivitäten, Ausnahmen, Fehler und Sicherheitsereignisse beinhalten können, erzeugt, aufbewahrt, überprüft und gegen Veränderungen abgesichert?

Wie unterstützt 8MAN?

Security Monitoring

Mit dem Security Monitoring vertiefen Sie das Sicherheitsniveau und erfassen auch Aktivitäten, die außerhalb von 8MAN vorgenommen wurden. Sollte sich ein Mitarbeiter mit Bordmitteln Einblick in geschützte Verzeichnisse verschaffen, löst 8MAN sofort einen Alarm aus. Dateizugriffe auf Fileservern, Manipulationen am AD und Eingriffe an ausgewählten Postfächern werden lückenlos dokumentiert.

Services

- Änderungen im Active Directory überwachen
- Alarme für Nutzerkonten anlegen
- Alarme für Gruppen anlegen
- Die Zugriffe auf sensible Dateien ermitteln
- Alarme für Verdachtsfälle auf Ransomware aktivieren (Fileserver)
- Alarme für Datenlöschungen aktivieren (Fileserver)
- Alarme für Verdachtsfälle auf Datendiebstahl aktivieren (Fileserver)

3.3.2. Prüffragen und 8MAN Funktionalität

VDA ISA Prüffrage(n)	Wie unterstützt 8MAN?
Prüffrage 12.6 Inwieweit werden die Aktivitäten von Systemadministratoren und -operatoren protokolliert, die Ablage der Protokolle gegen Veränderungen abgesichert und regelmäßig überprüft?	8MAN protokolliert unabhängig von der ausführenden Rolle sicherheitskritische Aktivitäten. Ob Administrator oder Help Desk. Die Aktivitäten werden in Reporten oder im Logbuch systematisch erfasst. **Services** → Änderungen im Active Directory überwachen (Report) → AD Logga Ereignisse mit dem Logbuch auswerten

3.4. Communications Security

3.4.1 Der Baustein im Überblick

#	Thematik	8MAN
13.1	Verwaltung der Netzwerke	
13.2	Sicherheitsanforderungen an Netzwerke/-dienste	
13.3	Trennung von Netzwerken (Netzwerk-Segmentierung)	
13.4	Elektronischer Austausch von Informationen	X
13.5	Geheimhaltungsvereinbarungen beim Informationsaustausch mit Dritten	

3.4.2. Prüffragen und 8MAN Funktionalität

VDA ISA Prüffrage(n)	Wie unterstützt 8MAN?
Prüffrage 13.4 Inwieweit werden Informationen während des Austauschs oder der Übermittlung geschützt?	8MAN schützt alle Authentisierungsdaten mit dem Advanced Encryption Service (AES).

3.5. Compliance

3.5.1 Der Baustein im Überblick

#	Thematik	8MAN
18.1	Verwaltung der Netzwerke	X
18.2	Sicherheitsanforderungen an Netzwerke/-dienste	X
18.3	Trennung von Netzwerken (Netzwerk-Segmentierung)	
18.4	Elektronischer Austausch von Informationen	

3.5.2. Prüffragen und 8MAN Funktionalität

VDA ISA Prüffrage(n)	Wie unterstützt 8MAN?
Prüffrage 18.1 Inwieweit wird die Einhaltung gesetzlicher (länderspezifisch) und vertraglicher Bestimmungen sichergestellt (z.B. Schutz des geistiges Eigentums, Einsatz von Verschlüsselungstechniken und Schutz von Aufzeichnungen)?	8MAN orientiert sich vor allem an den Sicherheitsanforderungen des Bundesamts für Informationssicherheit (BSI). Das BSI definiert mit dem IT-Grundschutz die zentralen Kriterien für eine sichere IT. Diese umfassen, wie die VDA ISA, Anforderungen der ISO 27002:2013 Whitepaper-BSI IT-Grundschutzkatalog im Fokus
Prüffrage 18.2 Inwieweit werden Vertraulichkeit und Schutz von personenbezogenen Informationen gewährleistet (abhängig von nationalen Gesetzgebungen)?	8MAN erfüllt zentrale DSGVO-Anforderungen. Die Protected Networks GmbH hat die notwendigen Schritte für die konforme Absicherung personenbezogener Daten in einem Whitepaper definiert. Whitepaper-DSGVO

8MAN | Protected Networks GmbH

Alt-Moabit 73
10555 Berlin
Germany

T: +49 30 3906345 - 0
E: info@8man.com
W: www.8man.com

Autor:
Fabian Fischer
Teamlead Product Management

T: +49 30 3906345-41
E: fabian@8man.com