

Lizenz zum Aufpassen.



8MAN **Sicherheitskonzepte**

Christian Schönfeld und Christian Zander

Haftungsausschluss

Die in diesem Handbuch gemachten Angaben können sich jederzeit ohne vorherige Ankündigung ändern und gelten als nicht rechtsverbindlich.

Die beschriebene Software **8MAN** wird von protected-networks.com im Rahmen einer Nutzungsvereinbarung zur Verfügung gestellt und darf nur in Übereinstimmung mit dieser Vereinbarung eingesetzt werden.

Dieses Dokument darf ohne die vorherige schriftliche Erlaubnis von protected-networks.com weder ganz noch teilweise in irgendeiner Form reproduziert, übermittelt oder übersetzt werden, sei es elektronisch, mechanisch, manuell oder optisch.

Dieses Dokument ist in einer Einheit zu denen auf der Website von protected-networks.com veröffentlichten rechtlichen Hinweisen AGB, EULA und der Datenschutzerklärung zu sehen.

Urheberrecht

8MAN ist eine geschützte Bezeichnung für ein Programm und die entsprechenden Dokumente, dessen Urheberrechte bei protected-networks.com GmbH liegen.

Marken und geschäftliche Bezeichnungen sind – auch ohne besondere Kennzeichnung – Eigentum des jeweiligen Markeninhabers.

protected-networks.com GmbH
Alt-Moabit 73
10555 Berlin
Tel.: +49 (30) 390 63 45 - 0
Web: www.protected-networks.com

Hot-Line
Support: susi.support@protected-networks.com
Tel.-Support: +49 (30) 390 63 45 - 0
Zu den üblichen Bürozeiten

Veröffentlichung: Juli 2010

8MAN Sicherheitskonzepte

1. Entwicklungsteam des Herstellers

Zahlreiche Mitarbeiter im Entwicklungsteam der protected-networks.com GmbH haben in ihrer bisherigen beruflichen Laufbahn in sicherheitskritischen Bereichen (Telekommunikation, Serveradministration) gearbeitet. Dazu kommen junge Mitarbeiter, die ständig versuchen, fantasievoll das eigene Produkt zu unterwandern und damit Sicherheitslöcher zu finden. Dies geschieht alles unter unserer Maxime, dass Sicherheit und Stabilität unbedingte Priorität vor neuer Funktionalität genießt.

Die protected-networks.com GmbH kooperiert mit den Herstellern der zugrunde liegenden Systemsoftware (Microsoft, NetApp). Informationen aus erster Hand helfen uns, sämtliche Unklarheiten in kürzester Zeit auszuräumen und zu korrekten und sicheren Lösungen zu gelangen.

2. Ein Wort zur Verschlüsselung

Zusätzlich zu den üblichen Verschlüsselungsmethoden, wie zum Beispiel md5, wird für 8MAN ein mehrstufiges Verfahren verwendet, um das Auslesen wichtiger Informationen zu verhindern. Dieses legen wir aus Sicherheitsgründen hier nicht näher dar.

3. Schutz vor Angriff von außen

Einmal installiert, muss sich 8MAN im laufenden Betrieb fortwährend gegen äußere Manipulationen schützen und sicherstellen, dass keine schadhafte Komponenten ausgeführt und keine internen Speicherinhalte ausgelesen werden können.

3.1. Installation

3.1.1. Signatur des Installationspaketes mit dem Zertifikat eines anerkannten Zertifikatsausstellers (VeriSign)

Diese Zertifikate, verfügbar ab Herbst 2010, garantieren die Authentizität der Datenquelle.

3.1.2. Privater Übertragungskanal vom Hersteller zum Kunden

Die protected-networks.com GmbH stellt dem Kunden auf Anfrage einen privaten Übertragungskanal zur Verfügung. Dies kann in Form eines Mediums (z. B. CD) oder mittels eines zeitlich begrenzten und idealerweise kennwortgeschützten Speicherbereichs geschehen. Insbesondere die letzte Variante kommt zunehmend zum Einsatz, wobei wir einen „Download-Link“ auf den eigenen Server oder einen angemieteten Bereich im Internet verschicken.

3.2. Installationsort

3.2.1. Installationscomputer

Der Installationscomputer muss Mitglied einer Domäne des Unternehmensnetzwerks sein, um 8MAN ausführen zu können. Dies garantiert dem Unternehmen die volle Kontrolle über die einstellbaren globalen Sicherheitsrichtlinien. Ein domänenfremder Computer entzieht sich vollständig diesem Sicherheitssystem und befindet sich somit in einem Graubereich, der ein immenses Sicherheitsrisiko darstellt.



3.2.2. Installationsordner

Die 8MAN Installation erfolgt im Standardordner für alle Programme, die mittels System-Sicherheitsrichtlinien gegen unberechtigte Zugriffe geschützt sind. Alle Daten im Installationsordner sind unveränderlich, dies gilt insbesondere für die Programmdateien und die Konfigurationsdateien mit den Standardeinstellungen.

Alle vom Benutzer vorgenommenen Änderungen an den Standardeinstellungen der Konfiguration sind in einem gesonderten Bereich für Programmeinstellungen des Betriebssystems gespeichert. Alle sensiblen Konfigurationsdaten (z.B. Kennwörter) sind zusätzlich verschlüsselt.

Weitere Konfigurationsdaten werden später in der angebotenen MS SQL Datenbank abgelegt. Diese Datenbank verfügt über ein Benutzer- und Zugriffssystem, um nur berechtigte Zugriffe zu gestatten. Wie schon bei den im Dateisystem abgelegten sensiblen Konfigurationsdaten, sind auch solche Informationen in der Datenbank verschlüsselt.

3.3. Zur Laufzeit von 8MAN

Ist die Installation erfolgreich durchgeführt, muss 8MAN fortwährend seine eigene Sicherheit gewährleisten. Dazu genügt es nicht, ausschließlich auf die Zugriffsschutzmechanismen des Betriebssystems auf der Ebene der Installationsordner zu vertrauen. Dazu berücksichtigt 8MAN jeden der nachfolgenden Punkte.

3.3.1. Schutz gegen Dekompilation

Bei diesem Mechanismus geht es nicht primär um den Schutz des geistigen Eigentums des Herstellers, als vielmehr um den Schutz des Unternehmens, welches die Software einsetzt. Wer Kenntnis von den genauen Programmabläufen erlangt, kann Verschlüsselungsmechanismen analysieren und aufdecken sowie kleinste Schwachstellen ausnutzen, die nur mit diesem detaillierten Wissen möglich sind.

Neben den Programmdateien müssen auch alle zusätzlichen Dateien – wie z. B. SQL Skripte für die Datenverarbeitung – auf sichere Weise gegen unberechtigten Zugriff geschützt sein. Die protected-networks.com GmbH verschlüsselt diese.

3.3.2. Schutz gegen Laufzeit-Debugger

Bei Laufzeit-Debuggern handelt es sich um Software, mit der sich die schrittweise Ausführung von Programmen, insbesondere deren Zugriffe auf Speicherinhalte, verfolgen lassen. Somit ließen sich Kennwörter oder sensible Kundendaten ausspionieren. 8MAN unterbindet dies und beendet sich gegebenenfalls selbst, sofern ein Unterbinden nicht möglich ist.

3.3.3. Signierung aller Komponenten

Unsere erweiterbare Softwarearchitektur basiert auf dynamisch nachladbaren Komponenten. Welche Komponenten tatsächlich zum Einsatz kommen, wird durch die Konfiguration und die jeweilige Situation bestimmt. Alle zu ladenden Komponenten müssen mit einem privaten Schlüssel signiert sein und es jedem anderen Softwarehersteller – egal ob legal oder illegal – unmöglich machen, Komponenten zu manipulieren bzw. eigene zu erstellen. Dies garantiert, dass ausschließlich vertrauenswürdige Komponenten ausgeführt werden.



4. Schutz vor Angriff von innen

Im Gegensatz zu äußeren Angreifern kommen innere Angreifer aus dem Unternehmen, welches die Sicherheitssoftware einsetzt oder haben zumindest eine Vertrauensstellung im Unternehmen. Hierbei sind prinzipiell zwei Arten von Angriffen zu unterscheiden. In beiden Fällen ist die Sicherheitssoftware im laufenden Betrieb und nicht manipuliert (siehe Äußere Angriffe).

4.1. Schutz gegen missbräuchliche Programmnutzung

Die erste Art des Angriffs ist das simple Nutzen der Sicherheitssoftware. Fehler oder andere Sicherheitslücken könnten einem Benutzer Informationen liefern, die auf normalem Weg nicht zugänglich sind.

Um eine Sicherheitssoftware nach innen sicher zu machen, gibt es viele Konzepte, die von zahlreichen anderen Produkten bis hin zu der Systemsoftware selbst angewendet werden.

4.1.1. Zugangssicherung nur für berechtigte Benutzer und Gruppen

8MAN verfügt über eine Benutzerverwaltung. Diese erlaubt eingeschränkten Benutzergruppen, die Funktionen oder nur Teile davon zu verwenden. Welche Benutzer welche Funktionen verwenden dürfen, wird über die Konfiguration festgelegt.

4.1.2. Feingranulare Aufgaben mit dedizierten Zugangsinformationen

Mit 8MAN werden vielfältige Aufgaben abgearbeitet. Dies beginnt mit der Konfiguration des laufenden Systems selbst, setzt sich über die verschiedensten Datensammelaktivitäten fort und gipfelt schließlich in sicherheitskritischen Änderungen an sensiblen Einstellungen im Unternehmensnetzwerk.

Jede von 8MAN ausgeführte Aufgabe wird mit den minimal nötigen Zugriffsberechtigungen durchgeführt. Dies beugt Missbrauch vor und erhöht das Vertrauen.

Im Normalfall sind allen möglichen Aufgaben die nötigen Zugangsdaten über die Konfiguration zugeordnet. In streng vertraulichen Bereichen des Unternehmensnetzwerks sind die Standardzugangsdaten in der Regel nicht mehr ausreichend. Für diese Zwecke werden temporäre Zugangsdaten eingesetzt, die der Benutzer direkt eingeben kann und die sofort nach Abschluss der Aufgabe wieder gelöscht werden.

4.2. Schutz gegen unentdecktes Ausspähen sensibler Daten

Die zweite Art des inneren Angriffs ist das unentdeckte Ausspähen sensibler Unternehmensdaten. Dazu bietet ein modernes Softwaresystem zahlreiche Angriffspunkte. Die folgenden Punkte beschreiben die bekannten Ansätze.

4.2.1. Überwachung des Nachrichtenverkehrs im Netzwerk

Es existiert eine Vielzahl von frei zugänglichen Werkzeugen zum Aufzeichnen und Analysieren des Nachrichtenverkehrs im Netzwerk. Dies geschieht, ohne dass dies entdeckt werden könnte. Sobald an einem Knoten im Unternehmensnetzwerk der Datenverkehr abgegriffen werden kann, besteht ein potentielles Risiko.

Um diesem Risiko zu begegnen, wird die gesamte Kommunikation zwischen den einzelnen Komponenten der Sicherheitssoftware ausnahmslos verschlüsselt. Zudem müssen die Softwarekomponenten der Kommunikationspartner vertrauenswürdige (d.h. signierte und versionierte) Komponenten sein.

Zusätzlich werden alle Zugangsinformationen doppelt verschlüsselt übertragen, um diese sensiblen Daten zu schützen.



4.2.2. Zugriff auf Programmdateien im Dateisystem

Die Ablageorte für die sensiblen Daten können konfiguriert und anschließend mit den Mitteln der Systemsoftware vor Fremdzugriffen geschützt werden. Sicherheitskritische Daten werden nur verschlüsselt abgelegt, um im Falle einer Sicherheitslücke in der Systemsoftware keine verwendbaren Informationen zugänglich zu machen.

Im Idealfall ist 8MAN auf einem eigenen Computersystem installiert, welches sich innerhalb des Unternehmensnetzwerks abschotten lässt und somit ungewollte Zugriffe von vornherein unterbindet.

4.2.3. Zugriffe auf Programmdateien in der Datenbank

Alle erfassten Daten werden in einer Datenbank des Herstellers Microsoft (MS SQL) gespeichert. Diese Datenbank verfügt über eine effektive Benutzerverwaltung, mit der sich Benutzer und deren Berechtigungen auf einzelne Datenbanken steuern lassen.

Wie im Dateisystem oder beim Netzwerkverkehr, sind auch hier sicherheitskritische Informationen wie z.B. Zugangsdaten, zusätzlich verschlüsselt – liegen also nie im Klartext vor.

Die Installation der Sicherheitssoftware und der Datenbank auf einem gemeinsamen Computersystem trägt zur Steigerung der Sicherheit bei, weil somit potentielle Angriffspunkte nicht mehr existieren.

4.2.4. Zugriffe auf Protokolle

Zum Abschluss ist festzustellen, dass sämtliche Programmprotokolle – ob in Form einfacher Textdateien oder des Systemprotokolls – keine sensiblen Informationen enthalten. Die Programmprotokolle dienen zur Überwachung des Systemzustands der Sicherheitssoftware und im Falle eines Fehlers zur Problemsuche. Dafür müssen diese Protokolle an den Hersteller gesandt werden und dürfen daher keine wichtigen Unternehmensdaten beinhalten.

8MAN. Und Berechtigungen bleiben sauber.



Über protected-networks.com GmbH

Die protected-networks.com GmbH mit Sitz in Berlin entwickelt integrierte Lösungen für das Berechtigungsmanagement in Server-Umgebungen für Unternehmen aller Branchen. Integrated Data Security Management heißt der Ansatz, den protected-networks.com verfolgt und Unternehmen eine einheitliche Lösung für die Verwaltung von Berechtigungen und Daten bietet. Die Lösung **8MAN** ermöglicht das Visualisieren, Administrieren, Dokumentieren und Optimieren aller Berechtigungen, die innerhalb der IT-Umgebung bestehen. Damit erweitert und optimiert **8MAN** nicht nur die Funktionen der Microsoft-Dienste wie Active Directory, Fileserver, SharePoint und Exchange, sondern auch die Funktionen vieler anderer Serversysteme. Die protected-networks.com GmbH wurde Anfang 2009 gegründet und ist durch die Investitionsbank Berlin sowie dem High Tech Gründerfonds finanziert.



protected-networks.com GmbH

Alt-Moabit 73

10555 Berlin

Tel. 030 / 390 63 45 - 50 | Fax 030 / 390 63 45 - 51

info@protected-networks.com

www.protected-networks.com

