8MAN intern – Sicherheit & Datenschutz

8MAN erhöht durch seinen Einsatz die Sicherheitsstandards und Transparenz im Berechtigungsmanagement nachhaltig. Wie sieht es aber mit 8MAN selbst aus? Ist das Produkt auch im Einsatz sicher und welche Maßstäbe legt der Hersteller an sein Produkt in dieser Hinsicht? Das ein wenig zu beleuchten, ist das Ziel des folgenden Artikels, der sich auf Angaben des Herstellers stützt.

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 Verfahren wird aus Sicherheitsgründen hier nicht näher beschrieben. Die Signatur des Installationspaketes erfolgt mit dem Zertifikat eines anerkannten Zertifikatausstellers (VeriSign). Diese Zertifikate, verfügbar seit Herbst 2010, garantieren die Authentizität der Datenquelle.

Personalisierter Übertragungskanal vom Hersteller zum Kunden
Die protected-networks.com GmbH stellt dem Kunden auf Anfrage einen personalisierten Übertragungskanal zur Verfügung. Das 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 vom Hersteller ein „Download-Link" auf den eigenen Server oder einen angemieteten Bereich im Internet verschickt wird.

Installationscomputer
Der Installationscomputer muss Mitglied einer Domäne des Unternehmensnetzwerks sein, um 8MAN ausführen zu können. Das garantiert dem Unternehmen die volle Kontrolle über die einstellbaren globalen Sicherheitsrichtlinien. Ein domänenfremder Computer entzieht sich vollständig diesem Sicherheitssystem und befindet sich somit in einer Grauzone, die ein immenses Sicherheitsrisiko darstellt. Die 8MAN-Installation erfolgt im Standardordner für alle Programme, die mittels System-Sicherheitsrichtlinien gegen unberechtigte Zugriffe geschützt sind. Alle Daten im Installationsordner sind unveränderlich, das gilt insbesondere für die Programm- und 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 angebundenen 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.

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

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. So lassen sich Kennwörter oder sensible Kundendaten ausspionieren. 8MAN unterbindet das und beendet sich gegebenenfalls selbst, sofern ein Unterbinden nicht möglich ist.

Signierung aller Komponenten
8MANs 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 – gleichgültig, ob legal oder illegal – unmöglich machen, Komponenten zu manipulieren bzw. eigene zu erstellen. Damit wird garantiert, dass ausschließlich vertrauenswürdige Komponenten ausgeführt werden.

Zugangssicherung nur für berechtige 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.

Zugriff auf Programmdaten 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 separaten Computersystem installiert, welches sich innerhalb des Unternehmensnetzwerks abschotten lässt und somit ungewollte Zugriffe von vornherein unterbindet.

Zugriffe auf Programmdaten 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 potentielle Angriffspunkte nicht mehr existieren.

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.

aikux.com GmbH
Oldenburger Str. 37
10551 Berlin

Geschäftsführer: Thomas Gomell
Tel.: +49 (30) 8095010-40
Fax: +49 (30) 8095010-41
Email: info@aikux.com

www.aikux.com