

Faigle FleetManagement: Thema Sicherheit

Die von René Faigle AG eingesetzte Managed-Print-Software stammt vom kanadischen Unternehmen Print-Fleet Inc., welche dieses Produkt im letzten Jahrzehnt erfolgreich vertrieben hat.

PrintFleet Inc. ist auf sichere Softwarelösungen spezialisiert, die in allen Netzwerkkumgebungen eingesetzt werden können.

Nachstehende Erläuterungen beziehen sich auf den Einsatz, der von René Faigle AG genannten **Faigle Fleet Management Software**, nachfolgend **FFM** genannt.

FFM erfasst nur diejenigen Daten des Outputgerätes, die für das Management einer Druckumgebung wichtig sind. Persönliche Daten oder Benutzerinformationen sind hiervon stets ausgenommen.

Thema dieses Dokuments sind Netzwerk- und Informationssicherheit in Bezug auf:

- FFM Enterprise Server-Hardware
- FFM Data Collector Agent Software
- FFM Optimizer Webkonsole
- FFM Softwareprüf- und Freigabeprozess
- FFM Quellcodeschutz

Des Weiteren wird erklärt, warum durch die Nutzung von FFM Softwareapplikationen keines der folgenden Gesetze verletzt wird:

- Gesetz zur Vereinheitlichung des elektronischen Datenverkehrs im Gesundheitswesen sowie der Datensicherheit (Health Insurance Portability and Accountability Act-HIPAA)
- Sarbanes-Oxley
- Gramm-Leach-Bliley Act (Gramm-Leach-Bliley-Gesetz - GLBA)
- Bundesinformations-Sicherheitsmanagement-Gesetz (Federal Information SecurityManagement Act-FISMA)

FFM Data Collector Agent Software

Beim FFM Data Collector Agent (DCA) handelt es sich um eine Softwareanwendung, die überall dort, wo Daten von Outputgeräten zu erfassen sind, auf einem nicht dedizierten Netzwerkservers, installiert wird.

Der DCA läuft als Windows®-Service (oder, optional, als geplante Aufgabe) und kann rund um die Uhr betrieben werden.

Erfasste Informationen

Der FFM DCA versucht bei einem Netzwerkscan folgende Informationen von Outputgeräten zu erfassen:

- IP-Adresse (möglicherweise maskiert)
- Tonerkartuschen-Seriennummer
- Gerätebeschreibung
- Wartungsset-Füllstände
- Seriennummer
- Füllstände (ausgenommen Toner)
- Zählwertablesungen
- Anlagennummer
- Einfarbig oder Farbidentifizierung

Faigle FleetManagement: Thema Sicherheit (Fortsetzung)

Erfasste Informationen (Fortsetzung)

- Standort
- LCD-Ablesung
- MAC-Adresse
- Gerätestatus
- Hersteller
- Fehlercodes
- Firmware
- Tonerfüllstände
- Verschiedenes (gerätespezifisch)

Es werden keine Druckauftrags- oder Benutzerdaten erfasst.

Datenerfassungs- und Übertragungsmethoden

Der DCA erfasst Daten von Outputgeräten in festgelegten Abständen mit Hilfe von SNMP, ICMP und HTTP. Anschliessend überträgt er die Daten über FTP (Port 21/Port 20), HTTP (Port 80) oder HTTPS (Port 443) an die zentralisierte Datenbank.

Übersicht über FFM Security

Den Benutzern wird die Übertragung der Daten über HTTPS empfohlen, da diese Methode die SSL 128-Bit-Verschlüsselung der Daten während der Übertragung beinhaltet. FTP und HTTP bieten keine Verschlüsselung. Eine Übertragung mit HTTPS ist nur möglich, wenn das Gerät, welches die übertragenen Daten empfängt, ein SSL-Sicherheitszertifikat besitzt.

Optionale Fernupdates

Der DCA bietet als optionales Leistungsmerkmal, die Möglichkeit von Fernupdates über die Aktivierung der Optionen Health Check und Intelligent Update. Durch Health Check wird in regelmässigen Abständen sichergestellt, dass der DCA in Betrieb ist; andernfalls erfolgt ein Neustart des DCA-Betriebs. Mit Hilfe von Intelligent Update kann der DCA den Eingang von Software-Updates und DCA-Konfigurationsänderungen prüfen, die von einem Administrator des FFM Enterprise-Servers in Auftrag gegeben worden sind.

Netzwerkverkehr

Der vom DCA generierte Netzwerkverkehr ist minimal und variiert je nach Anzahl gescannter IP-Adressen. Die nachfolgende Tabelle zeigt, die mit dem DCA verbundene Netzwerklast, im Vergleich zu jener, die durch das Laden einer einzelnen Standard Webseite hervorgerufen wird.

Faigle FleetManagement: Thema Sicherheit (Fortsetzung)

Mit dem DCA verbundene Netzwerk-Bytelast	
Laden einer einzelnen Standard Website	60.860
DCA-Scan, IP leer	5.280
DCA-Scan, 1 Drucker	7.260
DCA-Scan, 1 Drucker, 1 Subnet	96.300
DCA-Scan, Netzwerk aus 13 Druckern	111.530

FFM Optimizer Webkonsole

Der FFM Optimizer ist die Online-Schnittstelle für das FFM Enterprise-System.

Erlaubnisbasiertes Benutzermanagement

Der Zugriff auf die FFM Optimizer Webkonsole wird über ein erlaubnisbasiertes Benutzermanagement gesteuert. Benutzer müssen sich beim FFM Optimizer mit Benutzernamen und Passwort anmelden. Ihnen werden eine oder mehrere Rollen zugewiesen, Erlaubnisse definiert und der Zugriff auf eine oder verschiedene Gerätegruppen gewährt.

HTTPS-Zugriff

Auf die Website kann mittels HTTPS zugegriffen werden. Voraussetzung hierfür ist, dass der Webserver mit einem SSL-Sicherheitszertifikat installiert worden ist. Die FFM Enterprise Administratoren verfügen über die Option, Benutzern den Zugriff auf die FFM Optimizer-Website nur mit HTTPS zu gestatten, indem sie eine automatische Weiterleitung für die HTTP-Version der Website einrichten. Dies wird empfohlen, da auf diese Weise, die 128-Bit-Verschlüsselung, der über das Internet übertragenen Daten gewährleistet wird.

FFM Quellcodeschutz

Der FFM Quellcode wird in einem gesicherten Revision Control System aufbewahrt, zu dem nur das FFM Entwicklungsteam Zugang hat. Jede Änderung des Quellcodes wird nachverfolgt, einschliesslich Namen des Entwicklers, welcher die Änderung vornimmt sowie Angabe des Grundes. Produkte werden vor ihrer Auslieferung verschlüsselt.

Die Erfüllung des Gesetzes zur Vereinheitlichung des elektronischen Datenverkehrs im Gesundheitswesen sowie der Datensicherheit (HIPAA) wird durch die Verwendung von FFM Softwareapplikationen nicht beeinträchtigt.

Die Verwendung von FFM Softwareapplikationen stellt für die teilnehmenden Stellen (Covered Entities) keinerlei Verstoß gegen das Gesetz zur Vereinheitlichung des elektronischen Datenverkehrs im Gesundheitswesen sowie der Datensicherheit (HIPAA) dar.

Schliesslich erfassen, speichern oder übertragen FFM Softwareapplikationen keine Informationen zum Inhalt von Druckaufträgen, wodurch auch keine Möglichkeit des Zugriffs bzw. der Speicherung oder Übertragung von geschützten Gesundheitsinformationen (ePHI) besteht, gemäss ihrer Definition durch das HIPAA.

Weitere Informationen zum HIPAA finden Sie auf Website <http://www.hhs.gov/ocr/hipaa/>

Faigle FleetManagement: Thema Sicherheit (Fortsetzung)

Die Erfüllung des Sarbanes-Oxley-Gesetzes wird durch die Verwendung von FFM Softwareapplikationen nicht beeinträchtigt.

Die Software von FFM ist nicht auf ihre Nutzung im Rahmen eines internen Kontrollsystems gemäss der Beschreibung in Abschnitt 404, „Management Assessment of Internal Controls“, ausgelegt und wird somit keine Auswirkungen auf diese Kontrollen haben.

IT-Kontrollsysteme sind ein wichtiger Bestandteil bei der Erfüllung des Sarbanes-Oxley-Acts. Kraft dieses Gesetzes liegt in der Verantwortung der Geschäftsleitung, die Wirksamkeit der internen Kontrolle der Finanzberichterstattung zu gewährleisten, zu bewerten und zu überwachen. Es gibt IT-Systeme auf dem Markt, die speziell auf die Erfüllung dieser Ziele ausgelegt sind. Die FFM Software ist nicht als IT-Kontrollsystem ausgelegt, wirkt sich jedoch auch nicht nachteilig oder gefährdend auf andere, zu Kontrollzwecken dienende Systeme aus.

Weitere Informationen zum Sarbanes-Oxley-Act finden Sie auf Website:

<http://thecaq.aicpa.org/Resources/Sarbanes+Oxley/>

Die Erfüllung des Gramm-Leach-Bliley Acts (GLBA) wird durch die Verwendung von FFM Softwareapplikationen nicht beeinträchtigt.

Die Verwendung von FFM Softwareapplikationen stellt für die teilnehmenden Stellen (Covered Entities) keinerlei Verstoß gegen den Gramm-Leach-Bliley Act (GLBA) dar. Schliesslich erfassen, speichern oder übertragen FFM Softwareapplikationen keine Informationen zum Inhalt von Druckaufträgen, wodurch auch keine Möglichkeit des Zugriffs bzw. Speicherung oder Übertragung persönlicher Finanzinformationen besteht, selbst wenn diese Informationen gedruckt oder anderweitig an Druckgeräte, von FFM Softwareapplikationen überwacht, verschickt werden.

Weitere Informationen zum Gramm-Leach-Bliley Act finden Sie auf Website:

<http://jwww.ftc.gov/jprivacy/privacyinitiatives/jglbact.html>

Die Erfüllung des Bundesinformations-Sicherheitsmanagement Gesetzes (Federal Information Security Management Act - FISMA) wird durch die Verwendung von FFM Softwareapplikationen nicht beeinträchtigt.

FFM Softwareapplikationen sind nicht auf ihre Nutzung innerhalb eines internen Kontrollsystems zur Erfüllung des FISMA ausgelegt und werden somit keine Auswirkungen auf diese Kontrollen haben. Die Verwendung von FFM Softwareapplikationen stellt für die teilnehmenden Stellen (Covered Entities) keinerlei Verstoß gegen den Federal Information Security Management Act (FISMA) dar. Schliesslich erfassen, speichern oder übertragen FFM Softwareapplikationen keine Daten zum Inhalt von Druckaufträgen, wodurch auch keine Möglichkeit des Zugriffs bzw. Speicherung oder Übertragung von Informationen mit hohem Risiko besteht, selbst wenn diese Informationen gedruckt oder anderweitig an Druckgeräte, von FFM Softwareapplikationen überwacht, verschickt werden.

Für weitere Informationen zu FFM-Produkten, setzen Sie sich bitte mit René Faigle AG in Verbindung - Telefon 044 308 43 43 oder besuchen Sie uns auf unserer Website www.faigle.ch