

Faigle FleetManagement: Au sujet de la sécurité

Le Managed-Print-Software utilisé par Faigle est originaire de PrintFleet Inc. une entreprise Canadian, laquelle a distribué ce produit dans les dernières dix ans avec succès.

PrintFleet Inc. est spécialisé dans des solutions de software, lesquelles peuvent être utilisées dans tous les réseaux.

Les explications ci-dessous se réfèrent à l'utilisation de Faigle Fleet Management Software par Faigle, nommé FFM ci-après.

FFM enregistre que des données d'un appareil d'output, lesquelles sont importante pour le management de l'environnement d'impression. Des données personnelles ou des informations sur les utilisateurs en sont non concernées.

La sécurité du réseau et les informations concernant sont le sujet de ce document.

- FFM Enterprise Server-Hardware
- FFM Data Collector Agent Software
- FFM console Web Optimizer
- FFM processus d'examinasson et libration du software
- FFM Protection du code source

De plus c'est expliqué pourquoi aucunes des lois ci-dessous seraient lésées par l'utilisation des applications software FFM :

- Loi sur la généralisation de la circulation technique dans le système de santé ainsi que dans la sécurité des données (Health Insurance Portability and Accountability Act-HIPAA)
- Sarbanes-Oxley
- Actes Gramm-Leach-Bliley (Loi Gramm-Leach-Bliley LGLB)
- Loi sur le management de sécurité des informations de l'état (Federal Information SecurityManagement Act-FISMA)

FFM Data Collector Agent Software

FFM Data Collector Agent (DCA) est une application software qui est installée là où un appareil d'output enregistre des données sur un serveur de réseau ne pas dédié.

Le DCA marche sur Windows®-Service (ou optimal comme devoir voisiné) e peut être exploité non-stop.

Informations enregistrées

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

- Adresse IP (masquées si possible)
- Numéro de série des cartouches des toners
- Description de l'appareil
- Niveau de remplissage de l'entretien

Faigle FleetManagement: Au sujet de la sécurité (Continuation)

- Numéro de série
- Niveau de remplissage (excepté les toners)
- Lecture de la consommation compteur
- Numéro du calculateur électronique
- Unicolore ou identification des couleurs

Informations enregistrées (Continuation)

- Lieu
- Lecture LCD
- Adresse MAC
- État actuel de l'appareil
- Constructeur
- Code des erreurs
- Firmware
- Niveau de remplissage des toners
- Divers (selon l'appareil)

Les données concernant les commandes d'impression ainsi que lesquelles des utilisateurs ne seront pas enregistrées.

Méthodes de la saisie des données ainsi que de la circulation

Le DCA enregistre régulièrement des données des appareils d'output avec SNMP, ICMP et HTTP. Après il les transmette via FTP (Port 21/Port 20), HTTP (Port 80) ou HTTPS (Port 443) à la banque des données centrale.

Vue ensemble sur FFM Security

La transmission des données par HTTPS est recommandée, parce que cette méthode garde le chiffrement 128-Bit des données pendant la transmission. FTP et HTTP n'offrent pas de chiffrement. Une transmission avec HTTPS est possible seulement si l'appareil, lequel reçoit les données, a un certificat de sécurité SSL.

Updates à distance optimales

Le DCA offre comme caractéristique optimale la possibilité de faire des updates à distance en activant les options Health Check et Intelligent Update. Health Check assure régulièrement que le DCA est encore en marche, sinon le DCA se démarre automatiquement. Avec Intelligent Update le DCA peut contrôler l'entrée des updates du software et les changements de configuration du DCA, lesquelles sont fait par un administrateur du serveur FFM Enterprise.

Circulation dans le réseau

La circulation minimal dans le réseau est générée par le DCA et varie selon le nombre des adresses IP scannées. Le tableau ci-dessous montre l'utilisation du réseau connexe avec le DCA comparé avec laquelle que se forme si un seul site standard est chargeant.

Faigle FleetManagement: Au sujet de la sécurité (Continuation)

Utilisation du réseau connexe avec le DCA en bytes	
Charger un seul site standard	60.860
DCA-Scan, IP vide	5.280
DCA-Scan, 1 imprimante	7.260
DCA-Scan, 1 Drucker, 1 réseau soumis	96.300
DCA-Scan, réseau avec 13 imprimantes	111.530

FFM console Web Optimizer

L'Optimizer FFM est une interface en ligne pour le système Enterprise FFM.

Management des utilisateurs s'appuyant sur des permissions

L'accès sur le FFM console Web Optimizer est commandé par un management des utilisateurs s'appuyant sur des permissions. Les utilisateurs doivent se connecter sur l'Optimizer FFM avec un nom d'utilisateur et un mot de passe. Ils obtiendront un ou plusieurs rôles, des permissions et l'accès sur un ou plusieurs groupes d'appareilles.

Accès HTTPS

On peut avoir accès sur le site avec HTTPS. Une condition en est que le serveur Web a été installé avec un certificat de sécurité SSL. Les administrateurs de FFM Enterprise détiennent les options pour régler les permissions des utilisateurs pour le site FFM Optimizer avec HTTPS. Cela se passe en installant une retransmission automatique pour la version HTTPS du site. Comme ça le chiffrement 128-Bit des données est garanti pendant la transmission au travers de l'internet.

FFM Protection du code source

Le FFM code source est gardé dans un Revision Control System. Le team du développement est seule en avant l'accès. Chaque changement du code source est suivi inclu le nom du développeur lequel a fait le changement ainsi que sa raison. Les produits sont chiffrés avant leur livraison.

L'exécution de la loi sur une généralisation de la circulation technique dans le système de santé ainsi que dans la sécurité des données (HIPAA) n'est pas altérée par les applications software de FFM.

L'utilisation des applications software de FFM n'est pas du tout une infraction pour les départements participants (Covered Entities) à la loi sur la généralisation de la circulation technique dans le système de santé ainsi que la sécurité des données (HIPAA).

En effet les applications software de FFM ne gardent pas des informations sur le contenu des ordres d'impression. Veut dire qu'il n'y a aucune possibilité d'en garder et transmettre ou avoir accès sur des informations de santé protégé (ePHI), dit la définition du HIPAA.

Pour d'autres informations sur HIPAA veuillez voir le site <http://www.hhs.gov/ocr/hipaa/>

Faigle FleetManagement: Au sujet de la sécurité (Continuation)

L'exécution de la loi sur Sarbanes-Oxley n'est pas altérée par les applications software de FFM.

Le software de FFM n'est pas fait pour l'utiliser dans le cadre d'un système de contrôle interne selon la description dans la partie 404 „Management Assessment of Internal Controls“. Alors le software n'a pas de effets sur ces contrôles.

Les systèmes de control de l'IT sont une partie très importante de l'exécution de l'acte Sarbanes-Oxley. La vertu de cette loi est dans les mains le la direction de l'entreprise pour garantir, juger et surveiller l'efficacité du contrôle interne des informations financières. Sur le marché il y a des systèmes IT lesquelles sont spécialisés sur ces conditions. Le software FFM n'est pas un système de contrôle IT mais n'as pas de effets mauvaise ou dangereuse sur des autres systèmes de control.

Pour d'autres informations sur l'acte Sarbanes-Oxley veuillez voir le site
<http://thecaq.aicpa.org/Resources/Sarbanes+Oxley/>

L'exécution de la loi sur les actes Gramm-Leach-Bliley (GLBA) n'est pas altérée par les applications software de FFM.

L'utilisation des applications software de FFM n'est pas du tout une infraction pour les départements participants (Covered Entities) à l'acte sur Gramm-Leach-Bliley (GLBA). En effet les applications software de FFM ne gardent pas des informations sur le contenu des ordres d'impression. Veut dire qu'il n'y a aucune possibilité d'en garder et transmettre ou avoir accès sur des informations financières, même si ces informations ont été imprimées ou transmis autrement à des imprimantes surveillées par des applications software de FFM.

Pour d'autres informations sur l'acte Gramm-Leach-Bliley veuillez voir le site
<http://thecaq.aicpa.org/Resources/Sarbanes+Oxley/>

L'exécution de la loi sur le management de sécurité des informations de l'état (Federal Information Security Management Act-FISMA) n'est pas altérée par les applications software de FFM.

Les applications software de FFM ne sont pas faites pour les utiliser dans un système de contrôle pour l'exécution du FISMA et ils en n'auront pas des effets sur ces contrôles. L'utilisation des applications software de FFM n'est pas du tout une infraction pour les départements participants (Covered Entities) au management de sécurité des informations de l'état (FISMA).

En effet les applications software de FFM ne gardent pas des informations sur le contenu des ordres d'impression. Veut dire qu'il n'y a aucune possibilité d'en garder et transmettre ou avoir accès sur des informations avec des risques hautes même si ces informations ont été imprimés ou transmis autrement à des imprimantes surveillées par des applications software de FFM.

Pour d'autres informations sur les produits de FFM veuillez contacter René Faigle SA
Téléphone 044 308 43 43 ou visitez notre site www.faigle.ch