Université Lille 1
Sécurité des Copieurs Multi-Fonctions (MFP)
Analyse de risque
Eric CASSETTE
Avril-Mai 2016

Table des matières

1.MÉTHODE....3

2.CONTEXTE....3

3.DESCRIPTION DE LA RESSOURCE....3

4.ÉVÉNEMENTS REDOUTÉS....4

4.1.Liste des événements redoutés, sans classement....4

4.2.Evénements redoutés regroupés en grande catégories :....4

4.3.Evénements redoutés triés selon leur ordre de traitement prioritaire (tri effectué par le Groupe de Travail) :....4

5.ÉTUDE DES SCENARIOS DE MENACES....5

5.1.VULNÉRABILITÉS DÉTAILLÉES DES MPFS....5

5.1.1.Éléments de base d'un MFP....5

5.1.2.Liste des vulnérabilités associées à chaque élément de base....5

5.2.MENACES DÉTAILLÉES SUR LES MFPS....9

5.2.1.Confidentialité (menaces qui, si elles se réalisent, réduisent le niveau de)....9

5.2.2.Intégrité....9

5.2.3.Disponibilité....10

5.2.4.Possibilité d'authentification (Authenticity)....10

5.2.5.Journalisation (Accountability)....11

5.2.6.Non répudation....11

5.2.7.Qualité....12

5.3.MENACES RETENUES....12

5.3.1.Confidentialité (menaces qui, si elles se réalisent, réduisent le niveau de)....12

5.3.2.Intégrité....12

5.3.3.Disponibilité....13
5.3.4.Possibilité d'authentification (Authenticity)....13
5.3.5.Journalisation (Accountability)....13
5.3.6.Qualité....13
6.ÉTUDE DES RISQUES....14
6.1.Aucun événement redouté....14
6.2.Les données traitées par le MFP sont compromises (oubliées, volées, délivrées à la mauvaise personne, ...)....14
6.3.Un ou plusieurs, voire tous le MFP sont indisponibles trop longtemps....14
6.4.Le MFP coute trop cher à cause de consommations excessives (papier, kits d'impression, communications téléphoniques)....15
6.5.Le MFP est utilisé par rebond pour "pirater" ou bloquer d'autres ressources....15
6.6.Les impressions ou les scans sont anormaux (incomplets, non triés, ...)....15
7.MESURES DE SÉCURISATION....15
7.1.Informations provenant du groupe de travail « Sécurité des imprimantes »....16
7.2.Mesures déduites de l'étude des risques....16
7.2.1.Aucun événement redouté....16
7.2.2.Les données traitées par le MFP sont compromises (oubliées, volées, délivrées à la mauvaise personne, ...)....16
7.2.3.Un ou plusieurs, voire tous le MFP sont indisponibles trop longtemps....19
7.2.4.Le MFP coute trop cher à cause de consommations excessives (papier, kits d'impression, communications téléphoniques)....22
7.2.5.Le MFP est utilisé par rebond pour "pirater" ou bloquer d'autres ressources....22
7.3.Fusion des mesures, classement....22
7.3.1.Liste des mesures « macroscopiques » :....22
7.3.2.Liste des mesures techniques :....23

1. MÉTHODE

L'analyse de risque s'inspire en partie du plan proposé par la méthode EBIOS, ce qui permet de dérouler quasiment en parallèle les tâches suivantes :

- liste des événements redoutés
- liste des vulnérabilités (les défauts intrinsèques aux ressources)
- liste des menaces (et théoriquement, classement selon leur probabilité de réalisation)

Après avoir déroulé ces tâches, on associe leurs résultats pour déterminer et classer les mesures et recommandations de sécurisation.

Remarque : certaines tâches décrites dans la méthode EBIOS n'ont pas été traités dans cette étude :

- source des menaces (humaine, non humaine, avec plus ou moins de capacités de nuisance)
- tri des menaces selon la liste des menaces génériques EBIOS

La liste détaillée des vulnérabilités et des menaces provient d'une étude réalisée en 2013 par une agence japonaise, l'IPA (Information-technology Promotion Agency Japan)

Sources :

- EBIOS-1-GuideMethodologique-2010-01-25.pdf
  Expression des Besoins et Identification des Objectifs de Sécurité
  EBIOS
  MÉTHODE DE GESTION DES RISQUES
- EBIOS-2-BasesDeConnaissances-2010-01-25.pdf
  Expression des Besoins et Identification des Objectifs de Sécurité
  EBIOS
  BASES DE CONNAISSANCES
- 20130312report_E.pdf
  Research Report on the security of MFPs
  Information-technology Promotion Agency Japan (IPA)
  Mars 2013

2. CONTEXTE

De nombreux copieurs multi-fonctions (MPF -Multi Functions Printer-) sont installés sur l'Université ; le parc est relativement homogène grâce au marché qui a été passé avec Konica-Minolta (et qui a été renouvelé en avril 2016).

La technologie des MFPs Konica-Minolta est l'impression laser monochrome ; leur taille est imposante (environ 2 m2 d'empreinte au sol) et les destine à un usage à l'échelle d'un laboratoire, d'un service ou d'un étage de bâtiment.

Le nombre de MFPs Konica-Minolta est d'environ 160. Leur gestion administrative est centralisée (service "Reprographie) et leur installation et configuration initiale sont effectuées par un technicien de la marque.

D'autres équipements sont également en fonction sur l'Université, soit d'une autre technologie (jet d'encre, laser couleur, sublimation, "Xerox Phaser", ...), soit de capacité moindre, à usage individuel ou d'équipe. Ces matériels sont gérés localement, pas nécessairement par un informaticien.

3. DESCRIPTION DE LA RESSOURCE

Dans nos environnements, un MFP est un équipement pouvant remplir les fonctions suivantes (même si ces fonctions ne sont pas nécessairement toutes activées sur les équipements) :

- copie d'originaux papier (fonction copieur)
- impression de documents (fonction imprimante)
- numérisation d'originaux papier pour stockage local, distant, ou envoi par mail
- télécopieur

Schématiquement, un MFP est constitué des éléments suivants :

- matériel :
  - numériseur avec alimentation manuelle ou automatique (feeder)
  - bacs de stockage des supports vierges
  - système d'impression
  - système de réception et de classement des impressions
  - système de stockage temporaire (file d'attente -spool-) ou permanent, fixe ou amovible
  - interfaces de communication (téléphonie, USB, bluetooh, Wifi, Ethernet)
  - mécaniques de finition des impressions (trieuse, agrafeur, relieuse, ...)
  - autres interfaces (lecteur de carte à puce pour identification, lecteur de carte SD pour maintenance ou mise à jour du micro-logiciel)

- logiciel ("firmware") plus ou moins complexe ou système d'exploitation embarqué (souvent basé sur Linux)

Remarque : un serveur d'impression "logiciel" en exécution sur un ordinateur Windows ou Linux pourrait être considéré comme un MFP, mais on les exclut de cette étude.

4. ÉVÉNEMENTS REDOUTÉS

Une atteinte à la sécurité des MFPs pourraient amener à des situations plus ou moins perturbantes pour l'activité. Selon la terminologie EBIOS, de telles situations sont appelées des « événements redoutés ».

4.1. Liste des événements redoutés, sans classement

Un MFP est "en panne" ou détruit (trop longtemps)
Tous les MFPs d'un même modèle sont "en panne" trop longtemps
Un MFP est inaccessible
Tous les MFPs sont inaccessibles
Les impressions sont incorrectes (imprimées sur un autre MFP, absentes, manque des contenus -images par ex.-, manque des pages, attribuées à une autre personne, ...)
Les numérisations sont incorrectes
Les télécopies sont incorrectes
Un original "sensible" est oublié sur la vitre du copieur et récupéré par une personne malveillante
Une impression sensible est oubliée sur l'imprimante et récupérée par un personne malveillante
Un original sensible est envoyé par mail à un autre destinataire, voire à l'extérieur du campus
Des données sensibles stockées dans le MFP sont volées
Les partages réseaux crées pour un MFP sont accessibles à des personnes non autorisées
Des personnes extérieures au service utilisent un MFP
On reçoit des factures de consommables trop élevées

4.2. Evénements redoutés regroupés en grande catégories :

Un ou plusieurs, voire tous le MFP sont indisponibles trop longtemps
Les impressions ou les numérisations sont anormaux (incomplets, non triés, …)
Le MFP coûte trop cher à cause de consommations excessives (papier, kits d'impression, communications téléphoniques)
Le MFP est utilisé par rebond pour "pirater" ou bloquer d'autres ressources
Les données traitées par le MFP sont compromises (oubliées, volées, délivrées à la mauvaise personne, ...)

4.3. Evénements redoutés triés selon leur ordre de traitement prioritaire (tri effectué par le Groupe de Travail) :

Les données traitées par le MFP sont compromises (oubliées, volées, délivrées à la mauvaise personne, ...)
Un ou plusieurs, voire tous le MFP sont indisponibles trop longtemps
Le MFP coûte trop cher à cause de consommations excessives (papier, kits d'impression, communications téléphoniques)
Le MFP est utilisé par rebond pour "pirater" ou bloquer d'autres ressources

Les impressions ou les numérisations sont anormaux (incomplets, non triés, ...)

5. ÉTUDE DES SCENARIOS DE MENACES

« EBIOS : ce module a pour objectif d'identifier de manière systématique les modes opératoires génériques qui peuvent porter atteinte à la sécurité des informations du périmètre de l'étude : les scénarios de menaces. Les réflexions sont menées à un niveau davantage technique que fonctionnel (sur des biens supports et non plus des biens essentiels). Il permet tout d'abord de faire émerger tous les scénarios de menaces en identifiant et combinant chacune de leurs composantes : on met ainsi en évidence les différentes menaces qui pèsent sur le périmètre de l'étude, les failles exploitables pour qu'elles se réalisent (les vulnérabilités des biens supports), et les sources de menaces susceptibles de les utiliser. Il est ainsi possible d'estimer le niveau de chaque scénario de menace (sa vraisemblance)."
Remarque : il faut prendre soin de faire la différence entre vulnérabilité, menace, source des menaces.
Exemple :

- vulnérabilité :le MFP est accessible physiquement à des personnes non autorisées
- source des menaces : Source humaine interne, malveillante
- menaces (basées sur les menaces génériques EBIOS) :
  - vol de tout ou partie du MFP (MAT-PTE)
  - casse du MFP (MAT-DET)
  - débranchement électrique (MAT-DEP)
  - consultation (sans vol) d'originaux, ou d'impressions laissés sur l'imprimante (PAP-ESP)
  - vol d'originaux, ou d'impressions laissés sur l'imprimante (PAP-PTE)

5.1. VULNÉRABILITÉS DÉTAILLÉES DES MPFS

Remarque : certaines vulnérabilités ne sont pas présentes sur tous les MFPs

5.1.1. Éléments de base d'un MFP

Le document de l'IPA (20130312report_E.pdf) étudie les vulnérabilités et les menaces sur les éléments de base constituant un MFP :

- Unité principale
  - matériel (scanner, système d'impression, feeder, ...)
  - logiciel
  - licences (droits d'utilisation de telle ou telle fonction)
  - médias amovibles (pour personnels de maintenance, pour utilisateurs)
- Données nécessaires à l'exécution
  - « jobs » (données à imprimer, données scannées, mails, informations de controle)
  - paramètres de configuration
  - données d'authentification et de gestion des droits (certificats, noms, mots de passe, droits d'accés)
  - horloge interne
- Données "permanentes" et journaux
  - originaux ou impressions
  - système de stockage et autres systèmes externes (authentification, de messagerie, SMB, ...)
  - journaux d'utilisation et données de facturation
- Autres systèmes
  - éléments de communication
  - console de management
  - poste de travail utilisateur

5.1.2. Liste des vulnérabilités associées à chaque élément de base

On rappelle que ces vulnérabilités sont intrinsèques aux constituants des MFPs et indépendantes des menaces externes

5.1.2.1. Unité principale

5.1.2.1.1. Matériel (scanner, système d'impression, feeder, ...)

Le MFP est accessible physiquement à des personnes non autorisées
Les interfaces matérielles sont standards (et donc prévisibles et connues)
Les données transitant entre les différents éléments matériels ne sont pas protégées
Le MFP est sensible aux défauts électriques ou aux champs électromagnétiques
Le MPF se met en mode maintenance suite à redémarrage et séquence de touches
La clef cryptographique stockée en DRAM n'est pas protégée
Le firmware/software embarqué peut être "sorti" du MFP
Le firmware ou les paramètres de configuration sont dans des mémoires qui peuvent être physiquement remplacées
Des éléments matériels peuvent être ajoutés, supprimés, modifiés
Absence d'identification du disque interne
Les modifications matérielles ne sont pas mémorisées
Les personnels de maintenance se partagent des identifiants
Erreurs d'installation matérielles

5.1.2.1.2. Logiciel

Pas de connexion sécurisée entre console de management et MFP
Connexion possible à l'interface de débogage
Ajout de plugin non contrôle ou non authentifié
Possibilité de passer en mode privilégié ou en mode maintenance sans authentification (par exploitation de faille ou non)
Reverse-engineering aisé
Absence de journaux
Erreurs dans la MAJ du firmare
Diffusion publique de vulnérabilités
Standard cryptographiques obsolètes (SSL)

5.1.2.1.3. Licenses (droits d'utilisation de telle ou telle fonction)

Entrée de mauvaises licences possibles
Licences continuant à être utilisées après revente du MFP
Licences non supprimées en cas de revente
Licences devenant incorrectes si horloge mal réglée
License incorrecte utilisable ou non
Clef de license pouvant être devinée

5.1.2.1.4. Médias amovibles (pour personnels de maintenance, pour utilisateurs)

Absence de sensibilisation du personnel de maintenance
Pas d'indication visible d'insertion ou d'éjection de média amovible
Stockage d'informations sensibles sur supports amovibles aisément "démontable"
Stockage chiffré sur support amovible mais aisément déchiffrable

Transmission entre MFP et support amovible non protégée
Média non protégé en écriture
Possibilité d'insertion de média non autorisé
Absence d'authentification du média
Plantage ou réinitialisation à l'insertion d'un média incorrect (pour diverses raisons)

5.1.2.2. Données nécessaires à l'exécution

5.1.2.2.1. "Jobs" (données à imprimer, données scannées, mails, informations de contrôle)

Données entrant ou sortant du MFP non protégées contre l'interception
Données de spool (HDD par exemple) non sécurisées
HDD de spool pouvant être volé ou perdu (remplacement ou reprise de matériel)
Données entrant ou sortant peuvent être dupliquées ou envoyées volontairement ou non à un mauvais destinataire
Le MPF peut être surchargé
Erreurs de transmissions réseau
Certains protocoles d'impression ne requièrent pas d'authentification
Absence de validation des informations de contrôle associées à un job
Absence de logs

5.1.2.2.2. Informations de configuration

Facilité à récupérer les informations de configuration, soit localement, soit à distance
Difficultés à comprendre et configurer les paramètres du MFP
Accès à une console d'administration non vérouillée
Quantité très importante de paramètres configurables
Nombreux services ouverts par défaut
Serveur WEB d'administration sujet à déni de service en cas de surcharge du MFP
Absence de vérification de cohérence de la configuration
Serveur WEB d'administration non compatible avec certains navigateurs
Serveur WEB d'administration vulnérable

5.1.2.2.3. Données d'identification (certificats, noms, mots de passe, droits d'accés)

Mots de passe par défaut ou absence de mot de passe ou mot de passe trop simple pour les connexions en mode administrateur
Informations d'identification connues de trop de monde
Absence de protection de la clef privée du MFP
Difficultés de gestion des certificats
Horloge interne avancée (cause expiration de certificats)

5.1.2.2.4. Horloge interne

Horloge interne incorrecte pour diverses raisons
Absence de détection ou de signalement d'une anomalie de l'horloge interne
MFP en fonction trop longtemps (RAZ de compteur)

5.1.2.3. Données permanentes et journaux

5.1.2.3.1. Originaux ou impressions

MFP accessibles physiquement
Absence de sensibilisation
Mélange d'impressions de plusieurs provenances
Problèmes physiques de numérisation ou d'impression (bourrages, absences de toners, pannes mécaniques, mauvais type de papier, ...)
Identification du demandeur impossible
MFP pas assez puissant pour gérer les grands documents (taille, complexité)

5.1.2.3.2. Système de stockage et autres systèmes externes (authentification, de messagerie, SMB, ...)

Faille dans les systèmes de gestion des documents partagés
Gestion incorrecte, ou absente ou anormale des droits d'accès sur les dossiers partagés
Affichage possible des noms des documents
Médias amovibles accessibles
Mécanismes d'authentification faibles
Absence de protection du disque dur de spool
Verrouillage d'identifiant en cas de trop nombreuses tentatives infructueuses
Saturation des espaces de stockages
MFP accessible physiquement
Logs incomplets ou inexistants
Protocoles réseaux piratables

5.1.2.3.3. Journaux d'utilisation et données de facturation

Pas de logs ou logs incorrectement configurés
Accès incorrects aux logs (lecture, altération, effacement)
Pas d'analyse des logs
Saturation de logs
Timestamps inconsistants
Usage anonyme possible
Imputations des consommations incorrectes

5.1.2.4. Autres systèmes

5.1.2.4.1. Eléments de communication

Absence de protection des communications
Mauvaise configuration des protocoles de communication
Absence d'authentification mutuelle forte
MFP non fonctionnel si pas de réseau
Large visibilité du MFP sur le réseau

5.1.2.4.2. Console de management

Vulnérabilité du poste de travail de management du MFP
Confiance mutuelle trop large
Absence ou défaillance des logs
Erreurs en cas d'utilisation simultanée à partir de plusieurs consoles de management

5.1.2.4.3. Poste de travail utilisateur

Absence de driver
Faux driver
Bug dans le driver
Information d'authentification ou spool non protégés
Communications pouvant être interceptées, reroutées, bloquées, etc...

5.2. MENACES DÉTAILLÉES SUR LES MFPS

Il s'agit de faire la liste des « attaques » possibles (source de menace : humaine ou non humaine, capacités de « nuisance » : plus ou moins élevées)

5.2.1. Confidentialité (menaces qui, si elles se réalisent, réduisent le niveau de)

Interventions matérielles directement sur le MFP, permet changement de configuration (« Mode maintenance »), vol, ajout de mouchard, copie de données "circulant" ou stockées dans le MFP (HDD)
Vol du logiciel de base du MFP pour reverse-engineering et exploitation des failles du logiciel de base
Vol des licences et utilisation sur un autre MFP
Vol d'un média amovible contenant des informations de configuration ou des données sensibles
Interception des données circulant entre le MPF et un autre système (ajout d'un hub USB, écoute Wifi, Bluetooth, IP, etc...)
Récupération non autorisée d'éléments sensibles faisant partie de la configuration (noms de hosts, identifiants, adresses emails)
Vol ou divulgation involontaire d'identifiants, mots de passe admin, "IDs", clef privée du MFP
Possibilité de savoir si l'heure interne du MFP est correcte ou non
Vol d'originaux, ou d'impressions laissés sur l'imprimante
Accès à des noms ou des contenus de documents stockés dans des dossiers internes ou partagés
Accès illégitime aux logs causant divulgation d'adresses, de noms de fichiers, d'information d'accounting
Ecoute des communications réseau non chiffrées
Accès illicite aux données de configuration ou aux fonctionnalités d'une console de management
Sur poste client, vol des informations d'identification dans les données du driver ou des informations sur le MFP utilisé
Interception ou copie de données circulant entre le MFP et des systèmes externes de stockage ou de gestion de spool ou de pré-conversion ou stockées sur ces autres systèmes

5.2.2. Intégrité

Remplacement d'éléments matériels (changement du HDD, modification du firmware ou de la NVRAM, ...)
Remplacement de code dans le logiciel du MFP
Utilisation de mauvaises licences

Altération du contenu d'un média amovible contenant des données sensibles ou de configuration
Modification des données de contrôle ou du contenu d'un job (ex : les données sont imprimées ou envoyées à un autre destinataire)
Erreurs de configuration ou invalidation de certaines fonctions de sécurité ou validation de services inutiles, voire dangereux
Modification d'identifiant, modification de mots de passe admin, création d'admins "parasites"
Dysfonctionnement de fonctions dépendant de l'heure interne si celle-ci est incorrecte (logs, certificats, licences, cookies, kerberos, etc...)
Remplacement d'originaux ou d'impressions ou mélange d'impressions
Modification de documents stockés dans des dossiers internes ou partagés
Logs inutilisables car incomplets ou modifiés volontairement ou non
Modifications des informations transitant par le réseau (ex : résultats de requetes DNS)
Modification/altération des données de configuration stockées sur console de management
Modification du driver ou de la configuration du driver sur poste client
Modification des données circulant entre le MFP et des systèmes externes de stockage ou de gestion de spool ou de pré-conversion ou stockées sur ces autres systèmes

5.2.3.Disponibilité

Destruction, vol
Panne ou arrêt à cause de problèmes électriques (débranchement, coupures ou fluctuations électriques)
Suppression de tout ou partie du logiciel du MFP
Licences invalides pour diverses raisons
Vol ou perte d'un média amovible contenant des données de configuration ou indispensables au fonctionnement du MFP
Transmission ou traitement des jobs bloqués (surcharge, déni de service, problèmes réseau, ...)
Pertes des informations de configuration ou impossibilité de changer la configuration
Perte ou invalidité d'éléments d'authentification ou de certificats rendant le MFP inutilisable ou non configurable
Dysfonctionnement de fonctions dépendant de l'heure interne si celle-ci est indisponible (logs, certificats, licences, cookies, kerberos, etc...)
Impossibilité de scanner ou d'imprimer suite à pb matériels ou manque de consommable
Les services de partages de fichiers ne sont plus disponibles
Accés aux logs impossible
Erreurs de configuration réseau, pannes d'interface réseau,
Console de management indisponible
Driver non fonctionnel sur poste client
Indisponibilité par panne ou surcharge ou déni de service des systèmes externes de stockage ou de gestion de spool ou de pré-conversion

5.2.4.Possibilité d'authentification (Authenticity)

Les éléments matériels peuvent être remplacés sans autorisation ou contrôle matériel
Le logiciel du MFP peut être remplacé ou modifié sans autorisation
L'authenticité de la license ne peut être assurée (reseller, crakage de clefs)
Absence de vérification à l'insertion d'un média amovible
Poste client ou utilisateur inconnus (utilisation de protocoles sans authentification (LPR) : utilisation du MFP pour envoyer

des spams, ...)
Configuration incorrecte ou ne respectant pas la politique de sécurité
Manque de confiance dans le processus externe d'authentification s'il existe
Manque de confiance dans le serveur NTP
Non surveillance des personnes qui récupèrent des documents originaux ou des impressions sur l'imprimante
Impossibilité d'identifier qui a créé, modifié, supprimé des documents partagés
Impossibilité de savoir qui a modifié, supprimé un log
Absence d'authentification forte lors des communications réseau
Possibilité d'utiliser une console de management "non approuvée" ou de s'adresser à un MPF non approuvé
Possibilité d'installer un driver non authentifié ("signé") ou sur un poste client non autorisé
Le MPF peut communiquer avec un "faux" système externe de stockage ou de gestion de spool ou de pré-conversion

5.2.5.Journalisation (Accountability)

Impossibilité de connaître le détail des interventions de maintenance
Impossibilité de savoir pourquoi le logiciel du MFP ne fonctionne plus correctement
Impossibilité de savoir pourquoi une license est invalide
Impossibilité de savoir quand un média amovible a été utilisé
Pas de logs d'utilisation du MFP
Pas de log de mise à jour de la configuration
Pas de log de gestion des certificats et des users
Pas de log des mises à jour de l'heure
Impossibilité de savoir qui a imprimé ou copié
Impossibilité de tracer les accès aux dossiers et documents partagés
Pas de log des actions sur les logs ;-)
Pas de logs des connexions réseau
Pas d'historique des actions effectuées à partir de la console de management
Pas de log d'utilisation du MFP à partir du poste client
Pas de logs des communications ou du fonctionnement des systèmes externes de stockage ou de gestion de spool ou de pré-conversion

5.2.6.Non répudation

Impossibilité de prouver qui a effectué une maintenance matérielle
Impossibilité de prouver qui a effectué une maintenance logicielle
Impossibilité de prouver qui a modifié une licence
Impossible de prouver qu'un média amovible a été utilisé par telle ou telle personne
Les logs d'utilisation du MFP existent mais les données ne sont pas totalement fiables (possibilité de "se faire passer pour")
Pas d'authentification forte des connexions aux outils de configuration du MFP
Pas de possibilité de prouver qu'on a utilisé le bon serveur NTP
Impossibilité de prouver qui a imprimé ou copié, même si on connait son identifiant
Pas d'authentification certaine des accès aux dossiers ou fichiers partagés
Pas d'authentification certaine des actions sur les logs

Pas d'authentification certaines lors des communications réseau
Pas d'authentification certaine lors d'utilisation d'un poste console de management
Pas d'authentification certaine dans l'utilisation du driver à partir du poste client
Pas d'authentification certaine dans les communications ou le fonctionnement des systèmes externes de stockage ou de gestion de spool ou de pré-conversion

5.2.7.Qualité

Installation ou maintenance matérielle défectueuse (bypass du module de chiffrement, RAM défectueuse provoquant erreurs dans certains traitement, ...)
Installation ou maintenance logicielle défectueuse
Failles logicielles publiées mais non corrigées
Possibilité d'entrer des "fausses" clefs de licence
Défaillance d'un média amovible
La configuration désirée n'est pas enregistrée ou prise en compte par le MFP
Gestion incorrecte des mots de passe (tronqués, laissés à blanc, trop courts, etc...)
Horloge interne trop déviante
Problèmes de qualité d'impression, de copies, de finition
Contenu des dossiers ou fichier partagés incohérents suite à défaillance logicielle
Enregistrement dans les logs incorrects ou "manqués"
Mauvaise communication réseau, perte de paquets
Mauvaise qualité des outils de la console de management
Mauvaise qualité du driver sur le poste client
Mauvaise qualité des systèmes externes de stockage ou de gestion de spool ou de pré-conversion

5.3. MENACES RETENUES

« EBIOS : On ne retient que les menaces synthétiques, pertinentes, ayant une probabilité relativement importante de se produire et pouvant conduire aux événements redoutés »

5.3.1.Confidentialité (menaces qui, si elles se réalisent, réduisent le niveau de)

Interventions matérielles directement sur le MFP, permet changement de configuration ("mode maintenance"), vol, ajout de mouchard, copie de données "circulant" ou stockées dans le MFP (HDD)
Interception des données circulant entre le MPF et un autre système (ajout d'un hub USB, écoute Wifi, Bluetooth, IP, etc...)
Récupération d'éléments sensibles de la configuration (noms de hosts, identifiants, adresses emails, clef privée du MFP), soit directement sur le MFP, soit via l'interface WEB, soit sur une console de management, soit sur un poste client
Vol d'originaux, ou d'impressions laissés sur l'imprimante
Accès à des noms ou des contenus de documents stockés dans des dossiers internes ou partagés

5.3.2.Intégrité

Remplacement d'éléments matériels (changement du HDD, modification du firmware ou de la NVRAM, ...)
Erreurs de configuration ou invalidation de certaines fonctions de sécurité ou validation de services inutiles, voire dangereux
Modification d'identifiant, modification de mots de passe admin, création d'admins "parasites"

Dysfonctionnement de fonctions dépendant de l'heure interne si celle-ci est incorrecte (logs, certificats, licences, cookies, kerberos, etc...)
Remplacement d'originaux ou d'impressions ou mélange d'impressions
Modification de documents stockés dans des dossiers internes ou partagés
Modification/altération des données de configuration stockées sur console de management
Modification du driver ou de la configuration du driver sur poste client

5.3.3.Disponibilité

Destruction, vol
Problèmes électriques (débranchement, coupures ou fluctuations électriques)
Transmission ou traitement des jobs bloqués (surcharge, déni de service, problèmes réseau, ...)
Pertes des informations de configuration ou impossibilité de changer la configuration
Perte ou invalidité d'éléments d'authentification ou de certificats rendant le MFP inutilisable ou non configurable
Dysfonctionnement de fonctions dépendant de l'heure interne si celle-ci est indisponible (logs, certificats, licences, cookies, kerberos, etc...)
Impossibilité de scanner ou d'imprimer suite à pb matériels ou manque de consommable
Les services de partages de fichiers ne sont plus disponibles
Erreurs de configuration réseau, pannes d'interface réseau,
Console de management indisponible
Driver non fonctionnel sur poste client

5.3.4.Possibilité d'authentification (Authenticity)

Absence de vérification à l'insertion d'un média amovible
Poste client ou utilisateur inconnus (utilisation de protocoles sans authentification (LPR) : utilisation du MFP pour envoyer des spams, ...)
Non surveillance des personnes qui récupèrent des documents originaux ou des impressions sur l'imprimante

5.3.5.Journalisation (Accountability)

Absence d'historique des interventions de maintenance (journal des interventions)
Pas de logs fiables d'utilisation du MFP
Pas d'historique des actions effectuées à partir de la console de management

5.3.6.Qualité

Installation ou maintenance matérielle défectueuse (bypass du module de chiffrement, RAM défectueuse provoquant erreurs dans certains traitement, ...)
Installation ou maintenance logicielle défectueuse
Failles logicielles publiées mais non corrigées
Problèmes de qualité d'impression, de copies, de finition

6. ÉTUDE DES RISQUES

« EBIOS : En corrélant les événements redoutés avec les scénarios de menaces susceptibles de les engendrer, ce module permet d'identifier les seuls scénarios réellement pertinents vis-à-vis du périmètre de l'étude. Il permet en outre de les qualifier explicitement en vue de les hiérarchiser et de choisir les options de traitement adéquates."
On associe à chaque événement redouté la liste des menaces retenues

6.1. Aucun événement redouté…

Absence de vérification à l'insertion d'un média amovible

6.2. Les données traitées par le MFP sont compromises (oubliées, volées, délivrées à la mauvaise personne, …)

Interventions matérielles directement sur le MFP, permet changement de configuration ("mode maintenance"), vol, ajout de mouchard, copie de données "circulant" ou stockées dans le MFP (HDD)
Interception des données circulant entre le MPF et un autre système (ajout d'un hub USB, écoute Wifi, Bluetooth, IP, etc...)
Récupération d'éléments sensibles de la configuration (noms de hosts, identifiants, adresses emails, clef privée du MFP), soit directement sur le MFP, soit via l'interface WEB, soit sur une console de management, soit sur un poste client
Vol d'originaux, ou d'impressions laissés sur l'imprimante
Accès à des noms ou des contenus de documents stockés dans des dossiers internes ou partagés
Remplacement d'éléments matériels (changement du HDD, modification du firmware ou de la NVRAM, ...)
Erreurs de configuration ou invalidation de certaines fonctions de sécurité ou validation de services inutiles, voire dangereux
Modification d'identifiant, modification de mots de passe admin, création d'admins « parasites »
Non surveillance des personnes qui récupèrent des documents originaux ou des impressions sur l'imprimante
Failles logicielles publiées mais non corrigées
Absence d'historique des interventions de maintenance (journal des interventions)
Pas de logs fiables d'utilisation du MFP
Pas d'historique des actions effectuées à partir de la console de management

6.3. Un ou plusieurs, voire tous le MFP sont indisponibles trop longtemps

Destruction, vol
Problèmes électriques (débranchement, coupures ou fluctuations électriques)
Transmission ou traitement des jobs bloqués (surcharge, déni de service, problèmes réseau, ...)
Pertes des informations de configuration ou impossibilité de changer la configuration
Perte ou invalidité d'éléments d'authentification ou de certificats rendant le MFP inutilisable ou non configurable
Dysfonctionnement de fonctions dépendant de l'heure interne si celle-ci est indisponible (logs, certificats, licences, cookies, kerberos, etc...)
Impossibilité de scanner ou d'imprimer suite à pb matériels ou manque de consommable
Les services de partages de fichiers ne sont plus disponibles
Erreurs de configuration réseau, pannes d'interface réseau,
Console de management indisponible
Driver non fonctionnel sur poste client

Absence d'historique des interventions de maintenance (journal des interventions)
Pas d'historique des actions effectuées à partir de la console de management

6.4. Le MFP coute trop cher à cause de consommations excessives (papier, kits d'impression, communications téléphoniques)

Non surveillance des personnes qui récupèrent des documents originaux ou des impressions sur l'imprimante
Poste client ou utilisateur inconnus (utilisation de protocoles sans authentification (LPR) : utilisation du MFP pour envoyer des spams, ...)
Pas de logs fiables d'utilisation du MFP

6.5. Le MFP est utilisé par rebond pour "pirater" ou bloquer d'autres ressources

Aucune menace retenue…

6.6. Les impressions ou les scans sont anormaux (incomplets, non triés, …)

Dysfonctionnement de fonctions dépendant de l'heure interne si celle-ci est incorrecte (logs, certificats, licences, cookies, kerberos, etc...)
Remplacement d'originaux ou d'impressions ou mélange d'impressions
Modification de documents stockés dans des dossiers internes ou partagés
Modification/altération des données de configuration stockées sur console de management
Modification du driver ou de la configuration du driver sur poste client
Absence d'historique des interventions de maintenance (journal des interventions)
Pas de logs fiables d'utilisation du MFP
Pas d'historique des actions effectuées à partir de la console de management
Installation ou maintenance matérielle défectueuse (bypass du module de chiffrement, RAM défectueuse provoquant erreurs dans certains traitement, ...)
Installation ou maintenance logicielle défectueuse
Problèmes de qualité d'impression, de copies, de finition

7. MESURES DE SÉCURISATION

« EBIOS : ce module a pour objectif de déterminer les moyens de traiter les risques et de suivre leur mise en œuvre, en cohérence avec le contexte de l'étude. Les réflexions sont préférentiellement menées de manière conjointe entre les niveaux fonctionnels et techniques. Il permet de trouver un consensus sur les mesures de sécurité destinées à traiter les risques, conformément aux objectifs précédemment identifiés, d'en démontrer la bonne couverture, et enfin, d'effectuer la planification, la mise en œuvre et la validation du traitement. »

7.1. Informations provenant du groupe de travail « Sécurité des imprimantes »

Modifier systématiquement les mots de passe par défaut (avec un mot de passe complexe, remplacé si possible tous les semestres)
Toujours pour les mots de passe : attention, certains services (ie. ftp, telnet ou autres) n'ont pas la même base de mot de passe ... la pratique ci-dessus est donc à vérifier/reproduire le cas échéant
N'activer que les protocoles nécessaires (netware, Bonjour, smb, ftp, ipp, etc.)
Privilégier plutôt TCP/IP en termes de protocoles pour la communication sur le LAN
Remplacer le login "administrateur" ou "admin" par défaut avec un autre login si possible
Désactiver IPv6 si non utilisé, idem pour les interfaces USB ou Wi-Fi
Mettre en place un filtrage par le biais d'une ACL IPv4 à son réseau ou sous-réseau
Restreindre l'imprimante ou le serveur d'impression à une plage d'adresses IPv4
Restreindre les adresses de diffusion pour les mails à un domaine (ie. univ-lille1.fr)
Dans le cas d'un serveur Linux exécutant le service serveur d'impression Cups,
associer le service à un filtre fail2ban en cas d'impression non autorisée ou de tentative
d'attaque par force brute pour deviner le mot de passe administrateurs
Mettre à jour les micrologiciels des périphériques
Sauvegarder les configurations
Effectuer l'administration à distance des MFP via un protocole sécurisé, https ou ssh
Retirer et détruire le disque dur d'imprimante en cas de mise au rebut
Ne pas laisser l'historique des jobs stockés sur l'imprimante (ou définir une rotation pour la suppression)
Récupérer ses travaux après impression (surtout s'ils revêtent un critère sensible)
Activer la journalisation sur les imprimantes pour capturer l'activité des utilisateurs, les rapports d'émissions des fax, observer les changements de configuration, ... (et y jeter un oeil de temps à autre), déporter sur un serveur syslog pour analyser plus finement les comportements étranges
Bloquer l'impression via Google Print (ou sensibiliser les utilisateurs au fait que ça n'est pas une bonne pratique d'envoyer ses documents chez Google avant d'être imprimés localement)

7.2. Mesures déduites de l'étude des risques

Remarque : Quand c'est possible, on intègre les mesures proposées par le groupe de travail

7.2.1. Aucun événement redouté…

Absence de vérification à l'insertion d'un média amovible

7.2.2. Les données traitées par le MFP sont compromises (oubliées, volées, délivrées à la mauvaise personne, …)

7.2.2.1. Interventions matérielles directement sur le MFP, permet changement de configuration ("mode maintenance"), vol, ajout de mouchard, copie de données "circulant" ou stockées dans le MFP (HDD)

Ne pas laisser l'utilisateur/usager effectuer des actions de maintenance sur le MFP (arret-redémarrage, reset, changement de kit d'impression, configuration des adresses de messageries, etc...) ; dans l'absolu, même l'ajout de papier devrait être

interdit.
Installer physiquement le MFP dans un lieu à accès restreint ou pouvant être surveillé par les personnels
Effectuer régulièrement des campagnes de sensibilisation
Restreindre les adresses de diffusion pour les mails à un domaine (ie. univ-lille1.fr)

7.2.2.2. Interception des données circulant entre le MPF et un autre système (ajout d'un hub USB, écoute Wifi, Bluetooth, IP, etc...)

Ne pas laisser l'utilisateur/usager effectuer des actions de maintenance sur le MFP (arret-redémarrage, reset, changement de kit d'impression, configuration des adresses de messageries, etc...) ; dans l'absolu, même l'ajout de papier devrait être interdit.
Installer physiquement le MFP dans un lieu à accès restreint ou pouvant être surveillé par les personnels
Configurer physiquement (interfaces accessibles) et logiquement (protocoles réseau) le MFP selon le principe que tout est interdit sauf ce qui est autorisé, et vérifier que la configuration a été prise en compte et fait bien ce qu'on attend d'elle (tester et faire des contre-essais !)
Privilégier les protocoles de communication avec chiffrement pour la transmission de documents : IPP (Internet Printing Protocol) , SFTP, SMTP/STARTTLS
Effectuer régulièrement des campagnes de sensibilisation

7.2.2.3. Récupération d'éléments sensibles de la configuration (noms de hosts, identifiants, adresses emails, clef privée du MFP), soit directement sur le MFP, soit via l'interface WEB, soit sur une console de management, soit sur un poste client

Ne pas laisser l'utilisateur/usager effectuer des actions de maintenance sur le MFP (arret-redémarrage, reset, changement de kit d'impression, configuration des adresses de messageries, etc...) ; dans l'absolu, même l'ajout de papier devrait être interdit.
Installer physiquement le MFP dans un lieu à accès restreint ou pouvant être surveillé par les personnels
Effectuer régulièrement des campagnes de sensibilisation
Modifier systématiquement les mots de passe par défaut (avec un mot de passe complexe, remplacé si possible tous les semestres)
Mettre en place un filtrage par le biais d'une ACL IPv4 à son réseau ou sous-réseau
Restreindre l'imprimante ou le serveur d'impression à une plage d'adresses IPv4
Effectuer l'administration à distance des MFP via un protocole sécurisé, https ou ssh
Restreindre les adresses de diffusion pour les mails à un domaine (ie. univ-lille1.fr)

7.2.2.4. Vol d'originaux, ou d'impressions laissés sur l'imprimante

Récupérer ses travaux après impression (surtout s'ils revêtent un critère sensible)
Bloquer les impressions et ne les imprimer que sur présence locale et authentification de l'utilisateur
Ne pas laisser l'utilisateur/usager effectuer des actions de maintenance sur le MFP (arret-redémarrage, reset, changement de kit d'impression, configuration des adresses de messageries, etc...) ; dans l'absolu, même l'ajout de papier devrait être interdit.
Installer physiquement le MFP dans un lieu à accès restreint ou pouvant être surveillé par les personnels
Effectuer régulièrement des campagnes de sensibilisation

7.2.2.5. Accès à des noms ou des contenus de documents stockés dans des dossiers internes ou partagés

Ne pas laisser l'utilisateur/usager effectuer des actions de maintenance sur le MFP (arret-redémarrage, reset, changement de kit d'impression, configuration des adresses de messageries, etc...) ; dans l'absolu, même l'ajout de papier devrait être interdit.
Installer physiquement le MFP dans un lieu à accès restreint ou pouvant être surveillé par les personnels
Effectuer régulièrement des campagnes de sensibilisation
Modifier systématiquement les mots de passe par défaut (avec un mot de passe complexe, remplacé si possible tous les semestres)
Toujours pour les mots de passe : attention, certains services (ie. ftp, telnet ou autres) n'ont pas la même base de mot de passe ... la pratique ci-dessus est donc à vérifier/reproduire le cas échéant
Configurer physiquement (interfaces accessibles) et logiquement (protocoles réseau) le MFP selon le principe que tout est interdit sauf ce qui est autorisé, et vérifier que la configuration a été prise en compte et fait bien ce qu'on attend d'elle (tester et faire des contre-essais !)
Mettre en place un filtrage par le biais d'une ACL IPv4 à son réseau ou sous-réseau
Restreindre l'imprimante ou le serveur d'impression à une plage d'adresses IPv4
Restreindre les adresses de diffusion pour les mails à un domaine (ie. univ-lille1.fr)

7.2.2.6. Remplacement d'éléments matériels (changement du HDD, modification du firmware ou de la NVRAM, ...)

Ne pas laisser l'utilisateur/usager effectuer des actions de maintenance sur le MFP (arret-redémarrage, reset, changement de kit d'impression, configuration des adresses de messageries, etc...) ; dans l'absolu, même l'ajout de papier devrait être interdit.
Installer physiquement le MFP dans un lieu à accès restreint ou pouvant être surveillé par les personnels
Effectuer régulièrement des campagnes de sensibilisation

7.2.2.7. Erreurs de configuration ou invalidation de certaines fonctions de sécurité ou validation de services inutiles, voire dangereux

Configurer physiquement (interfaces accessibles) et logiquement (protocoles réseau) le MFP selon le principe que tout est interdit sauf ce qui est autorisé, et vérifier que la configuration a été prise en compte et fait bien ce qu'on attend d'elle (tester et faire des contre-essais !)
Etre présent lors de l'installation matérielle et la configuration initiale, comprendre et contrôler les paramètres de configurations entrés par le technicien qui effectue l'installation ; sinon, vérifier les paramètres de configuration avant de mettre en exploitation

7.2.2.8. Modification d'identifiant, modification de mots de passe admin, création d'admins « parasites »

Modifier systématiquement les mots de passe par défaut (avec un mot de passe complexe, remplacé si possible tous les semestres)
Toujours pour les mots de passe : attention, certains services (ie. ftp, telnet ou autres) n'ont pas la même base de mot de passe ... la pratique ci-dessus est donc à vérifier/reproduire le cas échéant
Mettre en place un filtrage par le biais d'une ACL IPv4 à son réseau ou sous-réseau
Restreindre l'imprimante ou le serveur d'impression à une plage d'adresses IPv4
Sauvegarder les configurations
Effectuer l'administration à distance des MFP via un protocole sécurisé, https ou ssh

7.2.2.9. Non surveillance des personnes qui récupèrent des documents originaux ou des impressions sur l'imprimante

Récupérer ses travaux après impression (surtout s'ils revêtent un critère sensible)
Bloquer les impressions et ne les imprimer que sur présence locale et authentification de l'utilisateur
Ne pas laisser l'utilisateur/usager effectuer des actions de maintenance sur le MFP (arret-redémarrage, reset, changement de kit d'impression, configuration des adresses de messageries, etc...) ; dans l'absolu, même l'ajout de papier devrait être interdit.
Installer physiquement le MFP dans un lieu à accès restreint ou pouvant être surveillé par les personnels
Effectuer régulièrement des campagnes de sensibilisation

7.2.2.10. Failles logicielles publiées mais non corrigées

Mettre à jour les micrologiciels des périphériques

7.2.2.11. Absence d'historique des interventions de maintenance (journal des interventions)

Activer la journalisation sur les imprimantes pour capturer l'activité des utilisateurs, les rapports d'émissions des fax, observer les changements de configuration, ... (et y jeter un oeil de temps à autre), déporter sur un serveur syslog pour analyser plus finement les comportements étranges

7.2.2.12. Pas de logs fiables d'utilisation du MFP

A

ctiver la journalisation sur les imprimantes pour capturer l'activité des utilisateurs, les rapports d'émissions des fax, observer les changements de configuration, ... (et y jeter un oeil de temps à autre), déporter sur un serveur syslog pour analyser plus finement les comportements étranges

7.2.2.13. Pas d'historique des actions effectuées à partir de la console de management

Activer la journalisation sur les imprimantes pour capturer l'activité des utilisateurs, les rapports d'émissions des fax, observer les changements de configuration, ... (et y jeter un oeil de temps à autre), déporter sur un serveur syslog pour analyser plus finement les comportements étranges

7.2.3.Un ou plusieurs, voire tous le MFP sont indisponibles trop longtemps

7.2.3.1. Destruction, vol

Ne pas laisser l'utilisateur/usager effectuer des actions de maintenance sur le MFP (arret-redémarrage, reset, changement de kit d'impression, configuration des adresses de messageries, etc...) ; dans l'absolu, même l'ajout de papier devrait être interdit.
Installer physiquement le MFP dans un lieu à accès restreint ou pouvant être surveillé par les personnels
Effectuer régulièrement des campagnes de sensibilisation

7.2.3.2. Problèmes électriques (débranchement, coupures ou fluctuations électriques)

Ne pas laisser l'utilisateur/usager effectuer des actions de maintenance sur le MFP (arret-redémarrage, reset, changement de kit d'impression, configuration des adresses de messageries, etc...) ; dans l'absolu, même l'ajout de papier devrait être

interdit.
Installer physiquement le MFP dans un lieu à accès restreint ou pouvant être surveillé par les personnels
Effectuer régulièrement des campagnes de sensibilisation
Brancher le MFP sur un réseau électrique protégé par onduleur (attention : puissance nécessaire importante)

7.2.3.3. Transmission ou traitement des jobs bloqués (surcharge, déni de service, problèmes réseau, ...)

Mettre en place un filtrage par le biais d'une ACL IPv4 à son réseau ou sous-réseau
Restreindre l'imprimante ou le serveur d'impression à une plage d'adresses IPv4
Réduire le "bruit de fond" du réseau physique (si Ethernet) en connectant le MFP sur un réseau privé

7.2.3.4. Pertes des informations de configuration ou impossibilité de changer la configuration

Modifier systématiquement des mots de passe par défaut (avec un mot de passe complexe, remplacé si possible tous les semestres)
Toujours pour les mots de passe : attention, certains services (ie. ftp, telnet ou autres) n'ont pas la même base de mot de passe ... la pratique ci-dessus est donc à vérifier/reproduire le cas échéant
Nne pas oublier les mots de passe d'administration

7.2.3.5. Perte ou invalidité d'éléments d'authentification ou de certificats rendant le MFP inutilisable ou non configurable

Modifier systématiquement les mots de passe par défaut (avec un mot de passe complexe, remplacé si possible tous les semestres)
Toujours pour les mots de passe : attention, certains services (ie. ftp, telnet ou autres) n'ont pas la même base de mot de passe ... la pratique ci-dessus est donc à vérifier/reproduire le cas échéant
Ne pas oublier les mots de passe d'administration

7.2.3.6. Dysfonctionnement de fonctions dépendant de l'heure interne si celle-ci est indisponible (logs, certificats, licences, cookies, kerberos, etc...)

Configurer le MPF pour synchroniser son heure via un serveur NTP (ntp.univ-lille1.fr)

7.2.3.7. Impossibilité de scanner ou d'imprimer suite à pb matériels ou manque de consommable

Désigner un responsable "administratif" (pour contrôle des coûts), un responsable technique (administrateur) et un référent pour les utilisateurs
Ne pas laisser l'utilisateur/usager effectuer des actions de maintenance sur le MFP (arret-redémarrage, reset, changement de kit d'impression, configuration des adresses de messageries, etc...) ; dans l'absolu, même l'ajout de papier devrait être interdit.
Installer physiquement le MFP dans un lieu à accès restreint ou pouvant être surveillé par les personnels

7.2.3.8. Les services de partages de fichiers ne sont plus disponibles

Désigner un responsable "administratif" (pour contrôle des coûts), un responsable technique (administrateur) et un référent pour les utilisateurs

Modifier systématiquement les mots de passe par défaut (avec un mot de passe complexe, remplacé si possible tous les semestres)
Toujours pour les mots de passe : attention, certains services (ie. ftp, telnet ou autres) n'ont pas la même base de mot de passe ... la pratique ci-dessus est donc à vérifier/reproduire le cas échéant

7.2.3.9. Erreurs de configuration réseau, pannes d'interface réseau,

Désigner un responsable "administratif" (pour contrôle des coûts), un responsable technique (administrateur) et un référent pour les utilisateurs
Ne pas laisser l'utilisateur/usager effectuer des actions de maintenance sur le MFP (arret-redémarrage, reset, changement de kit d'impression, configuration des adresses de messageries, etc...) ; dans l'absolu, même l'ajout de papier devrait être interdit.
Installer physiquement le MFP dans un lieu à accès restreint ou pouvant être surveillé par les personnels
Modifier systématiquement les mots de passe par défaut (avec un mot de passe complexe, remplacé si possible tous les semestres)
Toujours pour les mots de passe : attention, certains services (ie. ftp, telnet ou autres) n'ont pas la même base de mot de passe ... la pratique ci-dessus est donc à vérifier/reproduire le cas échéant

7.2.3.10. Console de management indisponible

Modifier systématiquement les mots de passe par défaut (avec un mot de passe complexe, remplacé si possible tous les semestres)
Toujours pour les mots de passe : attention, certains services (ie. ftp, telnet ou autres) n'ont pas la même base de mot de passe ... la pratique ci-dessus est donc à vérifier/reproduire le cas échéant
Ne pas oublier les mots de passe d'administration

7.2.3.11. Driver non fonctionnel sur poste client

Sur les postes clients, installer les drivers officiels, provenant du constructeur, ou validés par un gestionnaire de parc ; proposer une configuration standard de ces drivers

7.2.3.12. Absence d'historique des interventions de maintenance (journal des interventions)

Mettre à disposition du technicien de maintenance un cahier de maintenance et insister pour que ce cahier soit à jour, ou tenir à jour ce cahier soi-même
Vérifier la légitimité des personnes qui interviennent sur un MFP
Désigner un responsable "administratif" (pour contrôle des coûts), un responsable technique (administrateur) et un référent pour les utilisateurs
Ne pas laisser l'utilisateur/usager effectuer des actions de maintenance sur le MFP (arret-redémarrage, reset, changement de kit d'impression, configuration des adresses de messageries, etc...) ; dans l'absolu, même l'ajout de papier devrait être interdit.
Installer physiquement le MFP dans un lieu à accès restreint ou pouvant être surveillé par les personnels

7.2.3.13. Pas d'historique des actions effectuées à partir de la console de management

Activer la journalisation sur les imprimantes pour capturer l'activité des utilisateurs, les rapports d'émissions des fax, observer les changements de configuration, ... (et y jeter un oeil de temps à autre), déporter sur un serveur syslog pour analyser plus finement les comportements étranges

7.2.4. Le MFP coute trop cher à cause de consommations excessives (papier, kits d'impression, communications téléphoniques)

7.2.4.1. Non surveillance des personnes qui récupèrent des documents originaux ou des impressions sur l'imprimante

Installer physiquement le MFP dans un lieu à accès restreint ou pouvant être surveillé par les personnels
Bloquer les impressions et ne les imprimer que sur présence locale et authentification de l'utilisateur

7.2.4.2. Poste client ou utilisateur inconnus (utilisation de protocoles sans authentification (LPR) : utilisation du MFP pour envoyer des spams, ...)

Configurer les services du MFP pour qu'aucun accès anonyme ne puisse avoir lieu

7.2.4.3. Pas de logs fiables d'utilisation du MFP

Configurer les services du MFP pour qu'aucun accès anonyme ne puisse avoir lieu
Activer la journalisation sur les imprimantes pour capturer l'activité des utilisateurs, les rapports d'émissions des fax, observer les changements de configuration, ... (et y jeter un oeil de temps à autre), déporter sur un serveur syslog pour analyser plus finement les comportements étranges

7.2.5. Le MFP est utilisé par rebond pour "pirater" ou bloquer d'autres ressources

Aucune menace retenue...

7.3. Fusion des mesures, classement

L'ensemble des mesures sera classé en deux catégories :

- des mesures « macroscopiques », qu'on retrouve pour combattre la plupart des menaces, et qui pourraient d'ailleurs s'appliquer à d'autres ressources du système d'information que les MPFs (« objets connectés »)
- des mesures techniques ou dépendant du type de ressources

7.3.1. Liste des mesures « macroscopiques » :

Désigner un responsable « administratif » (pour contrôle des coûts), un responsable technique (administrateur) et un référent pour les utilisateurs
Ne pas laisser l'utilisateur/usager effectuer des actions de maintenance sur le MFP (arret-redémarrage, reset, changement de kit d'impression, configuration des adresses de messageries, etc...) ; dans l'absolu, même l'ajout de papier devrait être interdit.
Installer physiquement le MFP dans un lieu à accès restreint ou pouvant être surveillé par les personnels
Etre présent lors de l'installation matérielle et la configuration initiale, comprendre et contrôler les paramètres de configurations entrés par le technicien qui effectue l'installation ; sinon, vérifier les paramètres de configuration avant de mettre en exploitation
Mettre à disposition du technicien de maintenance un cahier de maintenance et insister pour que ce cahier soit à jour, ou tenir à jour ce cahier soi-même
Vérifier la légitimité des personnes qui interviennent sur un MFP
Ne pas oublier les mots de passe d'administration (séquestre des mots de passe) !
Configurer physiquement (interfaces accessibles) et logiquement (protocoles réseau) le MFP selon le principe que tout est interdit sauf ce qui est autorisé, et vérifier que la configuration a été prise en compte et fait bien ce qu'on attend d'elle

(tester et faire des contre-essais !)
Configurer les services du MFP pour qu'aucun accès anonyme ne puisse avoir lieu
Modifier systématiquement TOUS les mots de passe par défaut (avec un mot de passe complexe, renouvelé chaque année universitaire)
Effectuer l'administration à distance des MFP via un protocole sécurisé, https ou ssh
Mettre à jour les micrologiciels des MFPs
Sauvegarder les configurations
Activer la journalisation sur les imprimantes pour capturer l'activité des utilisateurs, les rapports d'émissions des fax, observer les changements de configuration, ... (et y jeter un oeil de temps à autre), déporter sur un serveur syslog pour analyser plus finement les comportements étranges
Effectuer régulièrement des campagnes de sensibilisation

7.3.2.Liste des mesures techniques :

Penser à modifier les mots de passe par défaut des services annexes (ie. ftp, telnet ou autres)
Remplacer le login "administrateur" ou "admin" par défaut avec un autre nom de login si possible
Privilégier TCP/IP en terme de protocoles pour la communication sur le LAN
Privilégier les protocoles de communication avec chiffrement pour la transmission de documents : IPP (Internet Printing Protocol) , SFTP, SMTP/STARTTLS
Désactiver IPv6 si non utilisé, idem pour les interfaces USB ou Wi-Fi
Bloquer les impressions et ne les imprimer que sur présence locale et authentification de l'utilisateur, ou récupérer ses travaux immédiatement après l'impression (surtout s'ils revêtent un critère sensible)
Retirer et détruire le disque dur du MFP en cas de mise au rebut
Brancher le MFP sur un réseau électrique protégé par onduleur (attention : puissance nécessaire importante)
Réduire le "bruit de fond" du réseau physique (si Ethernet) en connectant le MFP sur un réseau privé (évite, entre autre, saturation et blocage des interfaces Ethernet)
Mettre en place un filtrage par le biais d'une ACL IPv4 à son réseau ou sous-réseau
Restreindre l'imprimante ou le serveur d'impression à une plage d'adresses IPv4
Configurer le MPF pour synchroniser son heure via un serveur NTP (ntp.univ-lille1.fr)
Sur les postes clients, installer les drivers officiels, provenant du constructeur, ou validés par un gestionnaire de parc ; proposer une configuration standard de ces drivers
Restreindre les adresses de diffusion pour les mails à un domaine (ie. univ-lille1.fr)
Dans le cas d'un serveur Linux exécutant le service serveur d'impression Cups, associer le service à un filtre fail2ban en cas d'impression non autorisée ou de tentative d'attaque par force brute pour deviner le mot de passe administrateurs
Ne pas laisser l'historique des jobs stockés sur l'imprimante (ou définir une rotation pour la suppression)
Bloquer l'impression via Google Print (ou sensibiliser les utilisateurs au fait que ça n'est pas une bonne pratique d'envoyer ses documents chez Google avant d'être imprimés localement)