Université de Lille 1 SCIENCES ET TECHNOLOGIES

Sécurité des Imprimantes-Copieurs Multifonctions (MFP)

Groupe de travail « Sécurisation des imprimantes »*

RECOMMANDATIONS

octobre 2016

QUOI ?

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 m^2 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.

QUEL RISQUE ?

Comme tout équipement informatique connecté à un réseau, les MFPs sont susceptibles de tomber en panne ou d'être « piratés » localement ou à distance. Ces événements sont plus ou moins perturbants pour l'activité et pour la confidentialité et l'intégrité des données traitées par les MFPs (données = impression, numérisation, fax, carnet d'adresses , etc.)

Le groupe de travail « Sécurisation des imprimantes »
a déterminé et classé par ordre d'importance ces situations « anormales » :

- **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 anormales (incomplètes, non triées, ...)**

QUE FAIRE ?

Pour éviter de se trouver dans une des situations « anormales » listées ci-dessus, il est recommandé d'agir **préventivement** en suivant les recommandations listées ci-dessous. Pour établir cette liste, le groupe de travail « Sécurisation des imprimantes » s'est basé sur sa propre expérience, complétée par une analyse de risque exhaustive (disponible sur demande).

L'ensemble des recommandations est classé en deux catégories :

1. **RECOMMANDATIONS « 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 »)
2. **RECOMMANDATIONS TECHNIQUES**, ou dépendant du type de ressources

! **Remarque importante |** Les recommandations ne dépendent pas d'une marque ou d'un type particulier de MFP. Il vous reste donc à les adapter aux matériels que vous gérez...

** : en 2016, le groupe de travail « Sécurisation des imprimantes » était constitué de Cyrille Allet, Eric Cassette, Loik Desmons (étudiant), Caroline Domont, Julien Iguchi-Cartigny, Arnaud Lagache, Mickael Masquelin, Thomas Olivier, Franck Plouvier, Anthony Raingeval (étudiant) et Julien Wachowiak (étudiant). Nous les remercions pour leur participation.*

1 - RECOMMANDATIONS « 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
- ☐ **Être 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)
- ☐ **Administrer** 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

2 - RECOMMANDATIONS 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)