Sécurisation de votre système d'impression

Livre blanc

PaperCut Software – Mai 2017

Sommaire

1.0

Sommaire
1.0 Introduction
1.1 Modèle de sécurisation de l'impression
Sécurisation de l'infrastructure d'impression
Sécurisation des flux d'impression
Sécurisation des sorties imprimées
1.2 Gestion des impressions
2.0 Sécurisation de l'infrastructure d'impression
2.1 Authentification des utilisateurs
2.2 Sécurisation du serveur d'impression
Files d'impression
2.3 Sécurisation des périphériques
Réseau
Sécurisation des connexions
Sécurisation des emplacements physiques
Accès aux périphériques
Double authentification
Firmware
2.4 Sécurisation des solutions de gestion de l'impression
Maintenance d'un système d'impression sécurisé
3.0 Sécurisation des flux d'impression
3.1 Politique d'impression
3.2 Libération d'impression sécurisée
3.3 Empêcher la libération sur une imprimante en mode erreur
3.4 Délai d'expiration d'une tâche d'impression
3.5 Responsabilisation de l'utilisateur
3.6 Confidentialité des impressions
4.0 Sécurisation des sorties imprimées

4.1 Journaux et rapports sur les activités d'impression

Activités système

Activités utilisateur

Génération de rapports

4.2 Filigrane et signatures numériques

4.3 Archivage électronique des documents imprimés

5.0 Récapitulatif

CheckList d'évaluation de la sécurité des impressions

Auteurs :

Contributeur :

1.0 Introduction

Souvent négligée par l'industrie de la sécurité IT, l'importance de la sécurité des systèmes d'impression est maintenant reconnue. En matière de politique de sécurité des informations, l'adoption d'un ensemble de mesures protégeant le système d'impression fait désormais partie des bonnes pratiques.

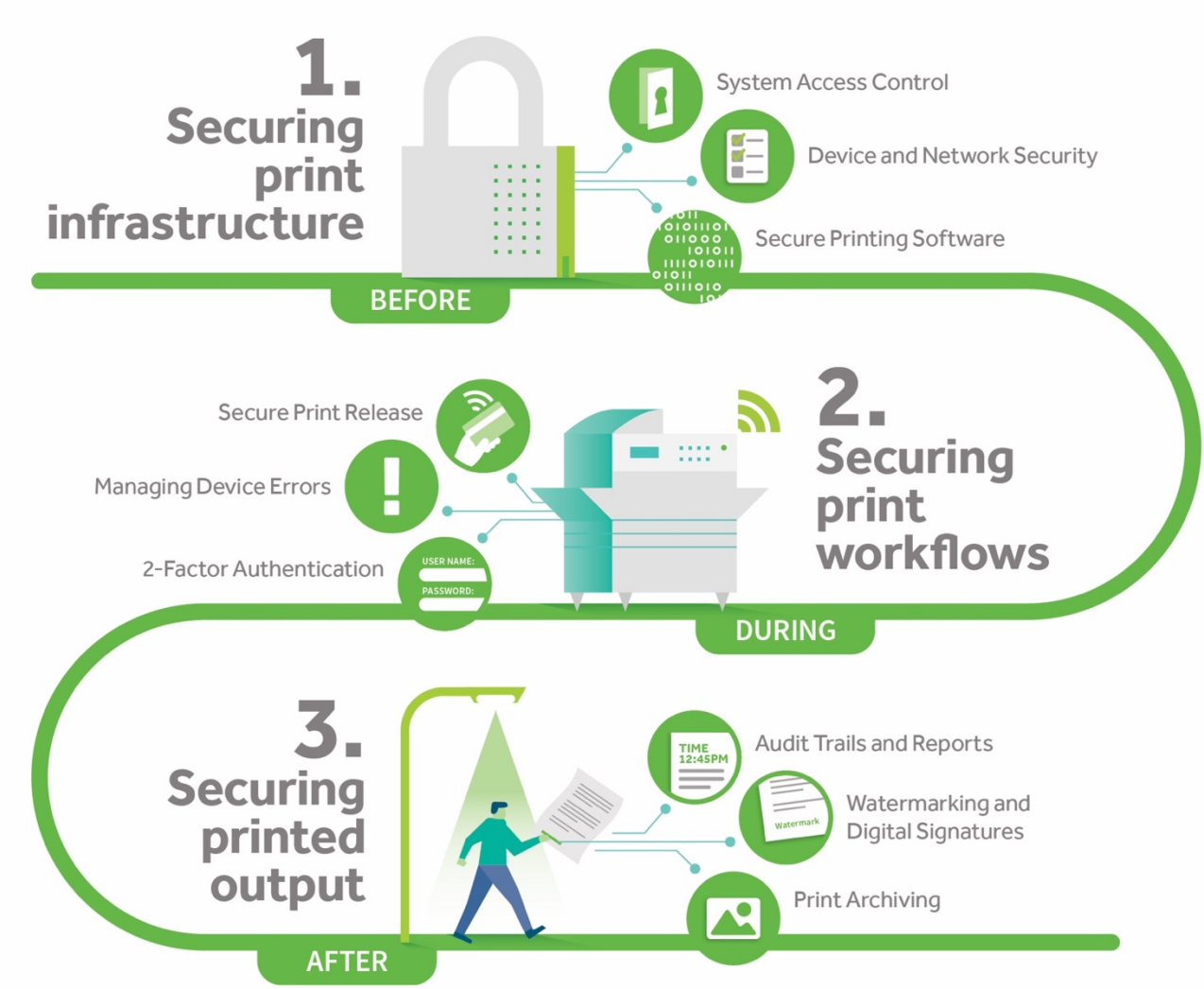
Cette tendance a été mise en évidence par le nombre croissant d'attaques de sécurité liées aux imprimantes rapportées par la presse. Selon le rapport Quocirca [1] de 2017, plus de 80% des entreprises sont préoccupées par la perte de données liées aux imprimantes, et 61% d'entre elles déclarent avoir subi des pertes au cours de l'année passée.

Les systèmes d'impression sont complexes et couvrent différents types de périphériques, réseaux et systèmes d'exploitation. Néanmoins, ils réalisent des fonctions stratégiques pour l'entreprise et traitent des informations confidentielles et des données sensibles. La surface d'attaque ainsi composée constitue une cible privilégiée pour les pirates et les attaques par déni de service. En conséquence, les audits de sécurité et les tests de pénétration désignent souvent le système d'impression comme le maillon faible de l'entreprise ou de l'organisation. Il faut aussi prendre en considération que le risque d'attaques de sécurité et de fuites de données peut venir tant de l'intérieur que de l'extérieur de l'entreprise.

Heureusement, des mesures de sécurité sont désormais disponibles pour vos systèmes d'impression. Comme toute bonne pratique, l'approche présentée dans ce document couvre différents niveaux, et traite de tous les aspects du flux d'impression.

[1] "Print in the digital age" Louella Fernandes, Quocirca 2017

1.1 Modèle de sécurisation de l'impression



Notre modèle de sécurisation de l'impression couvre toutes les phases du cycle de vie de l'impression :

Sécurisation de l'infrastructure d'impression

De nombreuses mesures doivent être prises avant l'impression de chaque document. Tous les éléments de l'infrastructure d'impression doivent être sécurisés, y compris les stations de travail, les appareils mobiles, les serveurs et les réseaux.

Sécurisation des flux d'impression

La sécurisation de votre infrastructure d'impression contre les attaques n'empêche pas la vulnérabilité de vos flux d'impression. Nous vous recommandons de mettre en place des flux d'impression sécurisés. Nos méthodes éprouvées peuvent s'avérer être extrêmement payantes.

Sécurisation des sorties imprimées

Comment préserver la sécurité d'un document une fois celui-ci imprimé ? Diverses technologies comme l'impression en filigrane et les journaux d'audit d'impression permettent d'assurer la traçabilité et encouragent des comportements responsables de la part des utilisateurs.

1.2 Gestion des impressions

Un logiciel de gestion d'impression est souvent utilisé pour procurer les fonctions de traçabilité et de sécurité décrites dans ce document. Par exemple, la fonctionnalité de libération d'impression sécurisée est essentielle pour tout système de gestion des impressions. Les solutions PaperCut NG et PaperCut MF prennent en charge toutes les mesures de sécurité mentionnées dans ce document.

2.0 Sécurisation de l'infrastructure d'impression

Lorsque l'on souhaite sécuriser un système d'impression de bout-en-bout, il est important de commencer par l'infrastructure qui supporte les processus d'impression.Cela englobe le réseau et les périphériques qui supportent la tâche d'impression à partir du moment où l'utilisateur clique sur "Imprimer" pour obtenir un document imprimé.

2.1 Authentification des utilisateurs

En matière de sécurité, la capacité à identifier l'utilisateur final de façon unique et précise est au cœur de toute bonne pratique. Les ordinateurs de bureau obligent les utilisateurs à s'authentifier via une multitude de comptes (Active Directory, eDirectory, LDAP, Open Directory) gérés de façon centralisée. Ainsi, il est possible d'attribuer des tâches à ces utilisateurs et de contrôler leur accès aux divers périphériques.

L'identification des utilisateurs se complique lorsque ceux-ci impriment depuis leur mobile ou un périphérique personnel (BYOD), d'autant que ces derniers ne requièrent pas d'authentification de l'utilisateur pour l'accès à l'impression.

Des solutions telles que PaperCut Mobility Print comblent ce manque en garantissant que les tâches d'impression sont correctement authentifiées avant d'être acceptées par un serveur d'impression.

2.2 Sécurisation du serveur d'impression

La plupart des organisations dédient un ordinateur spécifique qui joue le rôle de serveur d'impression. Ce dernier centralise les impressions et met les ressources d'impression à disposition des utilisateurs. La sécurité de ce serveur est primordiale pour assurer sa disponibilité et sa fiabilité mais aussi pour réduire les risques d'attaques.

Concernant le système d'exploitation, des mises à jour et des correctifs doivent être appliqués pour corriger les vulnérabilités connues. Vous devez mettre à jour régulièrement les définitions de virus sur vos serveurs d'impression ainsi que les pilotes d'imprimantes. La mise à jour de ces derniers doit intervenir dans le cadre d'une maintenance régulière.

L'emplacement logique du serveur sur le réseau est important si vous souhaitez réduire la surface d'attaque et les risques d'attaques. Les serveurs d'impression doivent être situés dans le réseau interne et être protégés d'internet et de la DMZ par un parefeu. Les adresses IP sur le réseau interne doivent être inaccessibles depuis un réseau externe.

Files d'impression

La restriction des droits d'accès aux files d'attentes partagées fait partie des tâches souvent négligées. Les droits sur les files partagées doivent être configurés de façon à garantir que les utilisateurs ne seront pas capables de prendre le contrôle des tâches d'impression des autres utilisateurs ou de modifier les paramètres de la file d'attente. Ainsi, un utilisateur ne doit pas être capable de suspendre une file d'attente ou de supprimer la tâche d'impression d'un autre utilisateur.

Il convient aussi de noter que tous les protocoles d'impression ne requièrent pas volontairement l'authentification. A titre d'exemple, le protocole LPR accepte les tâches d'impression sur le port 515 depuis n'importe quel client, et contourne ainsi les droits d'accès habituels. Certains scénarios requièrent l'utilisation du protocole LPR et dans ce cas, nous recommandons d'ajouter des contrôles supplémentaires pour restreindre l'accès au port LPR aux seuls clients autorisés. Une autre stratégie consiste à mettre en place la libération d'impression sécurisée dans la file d'attente LPR.

Le chiffrement des données d'impression permet aussi d'ajouter une couche de sécurité à vos tâches d'impression. Vous pouvez implémenter facilement cette fonctionnalité en activant un chiffrement au niveau du système d'exploitation du disque dur utilisé pour stocker les files d'attente. En cas d'accès non autorisé au disque dur, vous évitez ainsi une fuite des données sensibles.

Pour finir, l'accès à certaines imprimantes peut être restreint à certains utilisateurs. Le Principe du moindre privilège recommande que l'accès à un périphérique (file d'attente d'un serveur) ne doit être accordé à un utilisateur que s'il en a explicitement besoin. Ainsi, vous pouvez restreindre l'accès à une imprimante utilisant du papier à en-tête aux seuls utilisateurs concernés pour éviter une utilisation abusive du papier à en-tête.

2.3 Sécurisation des périphériques

Les périphériques multifonctions (MFD) et les imprimantes multifonctions (MFP) sont non seulement extrêmement puissants mais aussi très vulnérables aux utilisations abusives et aux attaques. Pour protéger vos imprimantes et périphériques MFD des menaces de sécurité, des mesures spécifiques doivent être appliquées.

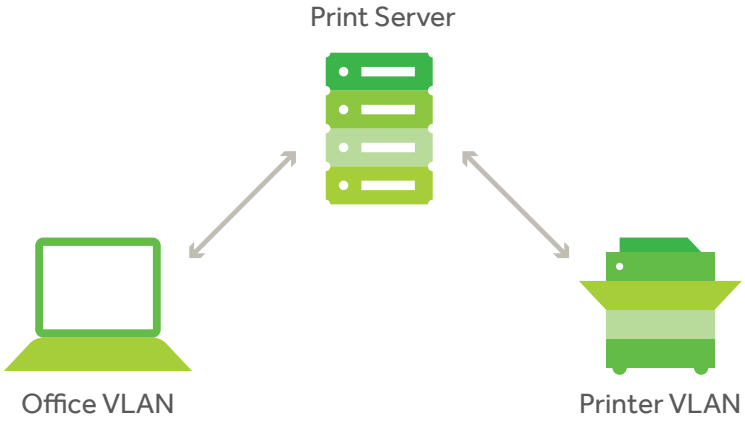
Réseau

Les MFD ont souvent besoin d'accéder au réseau de votre entreprise pour réaliser des fonctions telles que la recherche au sein de l'annuaire des utilisateurs (comme Active Directory), les services d'envoi d'emails, etc. Assurez-vous d'utiliser un compte de service ayant le niveau d'accès approprié. L'utilisation d'un compte de niveau utilisateur peut vous rendre vulnérable dans la mesure où ce type de compte est la cible préférée des hackers.

Dans une perspective comparable à la sécurisation du serveur d'impression, l'emplacement du réseau logique du MFD et du MFP doit être pris en compte afin de réduire la surface d'attaque. Votre imprimante doit-elle vraiment être accessible depuis internet, ou depuis certains de vos sites ?

Réciproquement, votre imprimante a-t-elle besoin d'accéder à internet ou au reste de votre réseau ? Limiter la routabilité du trafic réseau depuis le sous-réseau d'une imprimante peut réduire de façon significative l'impact d'un périphérique infecté.

Nous recommandons d'utiliser le serveur d'impression comme une passerelle vers les autres périphériques d'impression. Utilisez un VLAN ou un sous-réseau pour assurer que le seul périphérique pouvant voir les imprimantes est le serveur d'impression. Cela garantit, qu'en tant qu'administrateur système, vous contrôlez l'accès au périphérique via votre serveur. Cela s'obtient également en utilisant des listes de contrôle d'accès (ACL) pour les permissions de niveau compte, le filtrage d'IP pour empêcher l'accès depuis certains intervalles IP ou d'autres méthodes bloquant un accès direct aux imprimantes.



Sécurisation des connexions

Lorsque cela est possible, les périphériques doivent être configurés pour utiliser des connexions réseau chiffrées et sécurisées (par exemple, via HTTPS), et plus particulièrement lors de la transmission de données sensibles comme les documents et les mots de passe. Même si PaperCut NG/MF permet de se connecter en HTTP et HTTPS, le protocole HSTS (HTTP Strict Transport Security) est disponible pour s'assurer que l'accès est autorisé uniquement via une connexion HTTPS.

En aucun cas les mots de passe ne doivent être transmis en clair dans une connexion réseau. Configurez votre réseau de façon à utiliser les derniers protocoles TLS pris en charge par vos périphériques. Des protocoles plus anciens comme SSL v3 et des algorithmes de chiffrement tels que RC4, sont réputés pour être vulnérables et ne sont pas préconisés.

Pour éviter des attaques telles que les attaques de l'homme du milieu (ou attaques de l'intercepteur autrement appelé MITM), les connexions SSL doivent s'assurer de l'existence de certificats valides pour identifier l'hôte d'authentification (par exemple, l'hôte exécutant PaperCut MF). Même si l'on considère que l'attaque de l'homme du milieu est un risque faible, un certificat généré automatiquement peut être utilisé. Vous bénéficierez ainsi des avantages du protocole SSL tels que le chiffrement.

La connaissance approfondie de vos périphériques est un facteur essentiel. Les fabricants MFD proposent toujours plus d'options de connectivité comme le Bluetooth, le Wi-Fi Direct, ou l'impression NFC. Sans conteste ces fonctionnalités constituent un plus pour l'utilisateur. Toutefois, elles augmentent la complexité de la sécurité et étendent la surface d'attaque. Vous devez acquérir une connaissance approfondie des capacités de vos périphériques et des risques auxquels vous vous exposez.

Sécurisation des emplacements physiques

L'emplacement physique d'une imprimante est tout aussi important que son emplacement logique. La productivité de l'impression peut être affectée si les imprimantes sont constamment exposées à des endommagements physiques du fait de leur emplacement dans des zones publiques non sécurisées.

La réduction des brèches de sécurité peut être obtenue en limitant l'accès aux imprimantes aux seuls utilisateurs autorisés.Les imprimantes situées dans des campus universitaires ou des milieux scolaires sont particulièrement vulnérables du fait de leur utilisation par une population étudiante. Voici quelques mesures de sécurité supplémentaires recommandées :

- Sécurisation de l'emplacement de l'imprimante au sein des locaux de façon à éviter le vol
- Désactivation des ports d'entrée pour éviter une impression depuis un port USB ou un accès direct au disque sur de l'imprimante
- Protection de la connexion réseau. Ainsi, certains sites ont même recours à de la colle super-glue pour sécuriser les câbles réseau
- Verrouillage des bacs papier

Accès aux périphériques

Les MFD modernes et les imprimantes peuvent être considérés comme des serveurs IoT (Internet of Things) et sont vulnérables aux attaques IoT. Les équipements récents intègrent tous un ensemble complet de protocoles et de services, lesquels ne seront jamais utilisés par votre organisation. Nous recommandons donc aux propriétaires de ces périphériques de désactiver les protocoles et les services inutilisés pour réduire la surface d'attaque.

Les mots de passe de l'administrateur doivent être régulièrement modifiés et il est nécessaire d'utiliser des mots de passe sécurisés pour la configuration des machines (comme l'adresse IP) afin d'éviter qu'elles ne soient modifiées par les utilisateurs ou par du code malveillant sur le réseau. Les mots de passe constructeur (aussi appelés mots de passe usine) sont généralement connus des pirates, ce qui fait que les périphériques concernés sont vulnérables aux attaques.

De nombreux périphériques permettent aux tâches d'impression d'être stockées sur un disque dur interne ou sur la mémoire interne à des fins de réimpression. Si cette fonctionnalité est utilisée, des politiques claires doivent être adoptées en vue de s'assurer que seuls des documents publics sont stockés ou que les documents sont correctement protégés par mot de passe. Dans de nombreux cas, il est recommandé de désactiver cette

fonctionnalité. D'autre part, si vous ne souhaitez pas stocker les tâches pour une future utilisation, la plupart des MFD disposent d'une fonctionnalité d'écrasement des données. Cela permet aux données d'impression d'être écrasées ou effacées, soit immédiatement, à la demande ou à intervalles programmés.

De nombreux MFD modernes disposent d'une fonctionnalité qui permet de chiffrer toutes les partitions du disque dur susceptibles de contenir des données clients avec une technologie de chiffrement AES (Advanced Encryption Standard). Vous devez vous assurer que cette fonctionnalité est activée.

Certains fabricants MFD livrent ces fonctionnalités (impression des tâches d'impression, écrasement des données et chiffrement des données) via des kits de sécurité des données pouvant être achetés séparément. Pour disposer de telles fonctionnalités, vous devez vous assurer que vous achetez et installez le kit de sécurité approprié.

Double authentification

Les MFD ainsi que certaines imprimantes intègrent l'authentification utilisateur sur le périphérique via un badge, un numéro d'ID ou d'autres méthodes. C'est une mesure de protection essentielle pour empêcher un accès non autorisé au périphérique.

La double authentification fournit une couche de sécurité supplémentaire en demandant des informations d'authentification additionnelles à l'utilisateur. PaperCut MF, par exemple, fournit un code PIN qui sera saisi comme deuxième facteur d'authentification d'un utilisateur après la saisie d'un numéro d'ID ou un balayage de carte d'accès.

Firmware

Les fabricants d'imprimantes sont de plus en soucieux de la sécurité et effectuent des mises à jour des firmwares (microprogrammes) pour corriger les problèmes de sécurité signalés sur leurs appareils. Il est nécessaire de procéder à des mises à jour régulières des firmwares pour garantir que vos appareils bénéficient des derniers correctifs développés par leurs fabricants.

La technologie de chiffrement utilisée sur les MFD varie et ne suit pas toujours les meilleures pratiques. Toutefois, l'industrie est de plus en plus consciente des enjeux liés à la sécurité et la nécessité de maintenir à jour les firmwares des MFD est désormais essentielle. Elle permet de garantir que vos MFD utilisent les chiffrements les plus récents pour un périphérique donné.

Les anciens chiffrements tels que RC4 sont exposés aux brèches de sécurité. Par défaut et souci de compatibilité, PaperCut MF est configuré pour prendre en charge une large gamme de chiffrements. PaperCut est livré avec une version récente de l'environnement JRE (Java SE Runtime Environment), ce dernier intègre les derniers correctifs de sécurité d'Oracle. Lorsque PaperCut se connecte à un périphérique, les deux communiquent et choisissent le chiffrement le plus sécurisé mutuellement supporté.

2.4 Sécurisation des solutions de gestion de l'impression

Quel que soit le logiciel utilisé pour gérer et contrôler l'impression (nous recommandons bien sûr d'utiliser PaperCut NG ou PaperCut MF), il est nécessaire de tenir compte de certaines considérations et recommandations.

Les informations sensibles doivent être sécurisées lors de leur transmission aux différents composants de l'application. Vérifiez que les protocoles tels que HTTPS sont bien pris en charge lors de l'accès à l'interface d'administration et lors des communications entre les applications incorporées et les serveurs.

Les données stockées doivent aussi être prises en compte. Votre entreprise vous permet-elle d'utiliser et de sécuriser en toute liberté la base de données de votre choix et de gérer les sauvegardes ?

Les solutions PaperCut NG et PaperCut MF ont été développées dans une optique de sécurité. Forts de leur expérience dans le secteur de l'éducation et suite aux nombreuses attaques d'étudiants en tout point du globe, nos logiciels ont subi des batteries de tests de sécurité et nous avons renforcé leur sécurité au fil des ans.

PaperCut reste empreint d'une culture de la sécurité et les processus de notre entreprise intègrent des pratiques de sécurité proactives et réactives. Nous effectuons régulièrement des révisions des composants tierces parties intégrés à nos produits afin de détecter les vulnérabilités de sécurité. Tous les rapports de sécurité que nous recevons sont immédiatement étudiés par l'équipe PaperCut en charge de la sécurité. Des ripostes et solutions de contournement sont rapidement mises en place et des correctifs sont implémentés et publiés dans les jours qui suivent.

Nous vous recommandons de configurer tout logiciel d'impression introduit dans vos processus avec des paramètres d'identification de sécurité élevés.

PaperCut NG/MF et certaines solutions d'impression soucieuses de la sécurité préconisent d'appliquer des mesures visant à renforcer la sécurité :

- **Isolement ou séparation des processus** — le logiciel de gestion d'impression doit être exécuté dans des processus distincts du noyau du système d'exploitation. Ces processus doivent être exécutés avec des privilèges utilisateur minimum. Ainsi, il faut éviter d'exécuter de longues tâches en tant qu'utilisateur root ou administrateur.
- **API sécurisées** — les API publiques doivent avoir plusieurs couches de sécurité. PaperCut utilise des tokens d'authentification couplés avec un filtrage des adresses IP pour garantir que les appels API sont correctement authentifiés et proviennent d'une source de confiance.
- **Signature du code** — les programmes d'installation et tout code exécuté doivent être signés par leur éditeur pour garantir que le code que vous exécutez n'a pas été modifié et provient directement de cet éditeur.
- **Mise en sandbox** — s'il existe un risque minime d'infection, notre solution a été conçue pour anticiper les menaces et limiter les dommages. En faisant appel à des VM ou à des techniques de séparation des processus, la mise en sandbox permet d'ajouter des couches de sécurité afin qu'un composant infecté ne contamine pas l'ensemble du système.
- **Pages web sécurisées** — les pages web intègrent des protections contre les attaques par injection SQL, la falsification de requêtes intersites (Cross-Site forgery) et les attaques XSS (Cross-Site Scripting).
- **Services d'annuaire** — les services d'annuaire tels que AD, LDAP, etc. doivent être utilisés pour authentifier les utilisateurs plutôt que de stocker les mots de passe dans le système de gestion des impressions. Si des utilisateurs sont définis à l'extérieur d'un service d'annuaire (comme dans le cas des comptes d'impression invités), le mot de passe doit être chiffré de façon sécurisée. PaperCut NG/MF utilise la technologie Bcrypt dans ce but.
- **Mode Fail-Closed (fermeture en cas d'échec)** — la fermeture de l'accès en cas d'échec de connexion compte parmi les mesures de sécurité recommandées (par exemple si une connexion réseau à un serveur d'authentification échoue depuis un MFD). Avec le mode "fail-open", une simple action comme le retrait d'un câble réseau

peut rendre un périphérique vulnérable aux attaques. Le concept "fail-closed" est un principe de base de PaperCut NG/ MF et est présent dans toutes les situations nécessitant une impression sécurisée.

Maintenance d'un système d'impression sécurisé

Il est important d'avoir conscience de l'aspect stratégique de votre infrastructure pour la réussite de votre entreprise et d'appliquer les meilleures pratiques IT pour vos systèmes d'impression, y compris votre système de gestion d'impression. Voici quelques-unes des meilleures pratiques en la matière :

- Effectuer régulièrement des audits de sécurité pour détecter les vulnérabilités liées à l'impression.
- Sauvegarder régulièrement les bases de données de votre logiciel de gestion d'impression.
- Effectuer la maintenance de votre logiciel de gestion d'impression et appliquer les correctifs.
- Adopter un plan de récupération des données en cas de désastre.

3.0 Sécurisation des flux d'impression

Renforcer votre infrastructure contre les attaques n’est pas suffisant. En effet, vous restez exposé via vos flux d'impression. Nous pouvons vous aider en vous proposant différents flux d'impression faciles à mettre en œuvre et très efficaces.

3.1 Politique d'impression

Quelle politique d'impression adopter pour votre entreprise ? Faut-il autoriser les impressions en dehors des heures normales de bureau ? Limiter les droits de certains utilisateurs ? Une fois que vous avez une idée claire de ce que vous voulez, vous pouvez vous concentrer sur la mise en place d'une politique d’impression et de l'application de règles associées dans l'entreprise.

Le lycée du Bois Fleuri voudrait permettre à ses élèves d'imprimer gratuitement des documents, mais à deux conditions : n'autoriser l'impression que de certains documents et uniquement pendant les heures de cours. La façon la plus simple de mettre cette décision en pratique est que les professeurs acceptent (ou refusent) les demandes d'impression de chaque élève. Grâce aux politiques d'impression de PaperCut NG/MF, le lycée peut instaurer l'utilisation d'un code d'approbation que chaque professeur délivrera pour l’ensemble des tâches.

Mettre en place une politique d'impression dans une entreprise peut prendre plusieurs formes. Imprimer une brochure reprenant les grandes lignes de cette politique et la distribuer largement est une démarche qui peut s'avérer utile, mais ne garantit pas que tous les employés et visiteurs la respecte. Une application comme PaperCut NG/MF permet à une entreprise d'appliquer automatiquement la politique d'impression et les règles d'une entreprise, au moyen de pratiques intégrées et adaptables.

Exemple de politique d'impression :

Le lycée du Bois Fleuri voudrait permettre à ses élèves d'imprimer gratuitement des documents, mais à deux conditions : n'autoriser l'impression que de certains documents et uniquement pendant les heures de cours. La façon la plus simple de mettre cette décision en pratique est que les professeurs acceptent (ou refusent) les demandes d'impression de chaque élève. Grâce aux politiques d'impression de PaperCut NG/MF, le lycée peut instaurer l'utilisation d'un code d'approbation que chaque professeur délivrera pour l'ensemble des tâches.

3.2 Libération d'impression sécurisée

Dans un environnement d'impression standard, les travaux sont envoyés directement à l'imprimante pour une impression immédiate. En général, une grande partie de ces impressions sont inutiles et restent oubliées dans le bac de l'imprimante ou finissent à la corbeille. Toute sortie imprimée qui n'est pas récupérée immédiatement présente un risque pour la sécurité, s'il s'agit notamment d'un document confidentiel ou sensible.

La libération d'impression sécurisée est une solution simple qui place les travaux en attente jusqu'à ce que l'utilisateur les authentifie et les libère sur l'imprimante. Soit l'utilisateur sélectionne manuellement le fichier à libérer, soit il déclenche automatiquement son envoi à l'imprimante après authentification. Les documents sensibles ne resteront plus exposés sur l'imprimante !

La libération d'impression sécurisée, également appelée « numérisation vers boîte aux lettres », est une fonctionnalité très intéressante à prendre en considération lorsque vous concevez vos flux d'impression. Elle permet en effet à l'auteur du document de n'envoyer ce dernier à imprimer que lorsqu'il se trouve physiquement devant le MFD ou l'imprimante. La plupart des MFD prennent en charge cette fonctionnalité. Toutefois, pour permettre une expérience utilisateur globale sur l'ensemble de votre parc de périphériques, nous recommandons une solution de gestion des impressions telle que PaperCut NG ou PaperCut MF.

PaperCut NG et PaperCut MF proposent également l'impression Find-Me. Il s'agit d'une solution d'impression nomade qui permet aux utilisateurs d'envoyer leurs travaux vers une file d'attente unique. Tous les travaux d'impression sont ensuite expédiés vers l'imprimante sur laquelle l'utilisateur s'identifie, par exemple au moyen d'un badge.

Exemple de libération d'impression :

Stéphanie Morand du cabinet d'avocats Morand et Royer souhaite imprimer un contrat confidentiel. Une fois l'impression lancée, une collègue s'arrête pour discuter, empêchant la jeune femme de se rendre tout de suite à l'imprimante. Avec la libération d'impression sécurisée, Stéphanie a l'esprit tranquille car elle sait que le document ne sera imprimé que lorsqu'elle libèrera le document directement sur l'imprimante.

3.3 Empêcher la libération sur une imprimante en mode erreur

La libération d'impression sécurisée constitue un atout essentiel dans un environnement d'impression sécurisé. Mais que se passe-t-il lorsque les travaux sont libérés sur une imprimante qui se trouve en mode erreur ? Supposons, par exemple, que vous deviez faire face à un bourrage papier ou à un manque de toner ? Que se passerait-il si une fois l'erreur corrigée, les travaux s'imprimaient automatiquement en l'absence de tout utilisateur autorisé ? Il ne faut pas que l'impression se lance automatiquement une fois que la panne de l'imprimante est résolue, et que l'utilisateur n'est plus à proximité.

Avec PaperCut NG/MF, il est possible d'empêcher la libération des travaux lorsqu'une imprimante se trouve en mode erreur. Une fois l'erreur résolue, l'utilisateur doit libérer une nouvelle fois la tâche d'impression, ce qui lui

redonne le contrôle sur le moment où il veut imprimer et élimine 'éventualité de fuite de données sensibles.

3.4 Délai d'expiration d'une tâche d'impression

L'oubli des documents imprimés dans le bac de l'imprimante n'est pas le seul moyen pour un tiers d'avoir accès à des données sensibles. Les fichiers spool stockés sur le serveur d'impression avant d'être libérés peuvent eux aussi être récupérés et consultés par des individus malintentionnés. Si les mesures détaillées dans la section « L'infrastructure d'impression » permettent de lutter contre de telles pratiques, il est néanmoins important que les travaux d'impression soient automatiquement supprimés de la file d'attente après un certain délai. Vous réduisez ainsi la charge sur le serveur d'impression, et économisez du papier et du toner en éliminant les travaux d'impression devenus inutiles.

Exemple d'imprimante en mode erreur :

Stéphanie se trouve maintenant devant l'imprimante et a libéré sa tâche d'impression. Mais alors que la tâche d'impression précédente est en cours d'impression, l'imprimante tombe soudain en panne de toner. Stéphanie contacte son assistante pour qu'elle change la cartouche, mais n'a pas le temps d'attendre la fin de l'opération. Après environ une heure, elle retourne à l'imprimante pour essayer de libérer à nouveau sa tâche d'impression, mais, à sa grande consternation, elle trouve son document imprimé dans le bac papier, la cartouche d'encre ayant été remplacée. Un système de gestion sécurisé des impressions peut éviter cette situation de se produire en empêchant la libération des travaux d'impression sur une imprimante en mode erreur.

Une solution telle que PaperCut NG/MF vous permet de définir la durée pendant laquelle une tâche d'impression reste en file d'attente avant sa suppression automatique.

3.5 Responsabilisation de l'utilisateur

Il suffit de savoir que ce que vous imprimez risque de faire l'objet d'un suivi et d'une surveillance pour vous empêcher d'envoyer à l'imprimante toute

une thèse sur les qualités respectives des héros de votre série préférée, Star Trek, en incluant les 55 pages en couleur des schémas complets du Starship Enterprise !

Certains programmes d'audit du système d'exploitation permettent cette surveillance (cf. Observateur d'événements Windows), mais il s'agit souvent d'un processus manuel, chronophage et sujet à erreur. PaperCut NG/MF vous permet de gérer cet audit de façon centralisée pour tous les périphériques et les utilisateurs.

Avec PaperCut NG/MF, vous pouvez gérer l'activité d'impression d'un utilisateur sous différentes formes. Vous pouvez simplement lui communiquer son historique d'impression, ou limiter par un quota son volume d'impressions et l'inviter à faire une demande avec justification s'il veut dépasser ce quota et imprimer davantage.

3.6 Confidentialité des impressions

Les commérages vont toujours bon train dans les entreprises. Personne n'a envie de voir des semaines de travail en cachette tomber à l'eau parce que le document intitulé « Prime surprise des employés.docs » est découvert dans une file d'attente d'impression ! Pensez à cacher vos données sensibles, dès que vous le pouvez.

Vous pouvez certes mettre en place une configuration complexe de protocoles LPD/LPR, mais Papercut NG/MF vous permet de masquer les noms de document aussi bien au niveau de la file d'attente que sur l'ensemble du serveur d'impression. Vos primes surprises pour les employés resteront une surprise !

4.0 Sécurisation des sorties imprimées

Il n'est jamais facile de protéger des données, d'autant plus quand elles sont sous une forme imprimée ! Cependant, de nombreuses technologies et bonnes pratiques peuvent nettement améliorer la traçabilité et la sécurité des documents imprimés et éviter leur vol.

Les utilisateurs étant les premiers responsables de leurs documents imprimés, c'est sur leur comportement qu'il faut jouer pour sécuriser ces derniers. Par exemple, il y a peu de chance qu'un formulaire de politique d'entreprise caché au fond d'un tiroir empêche un dossier médical confidentiel de traîner sur une table à la cafétéria de l'hôpital. En revanche, si ce dossier contenait une signature numérique permettant de remonter facilement jusqu'à son propriétaire, celui-ci ferait un peu plus attention à son document et l'oublierait moins facilement dans un lieu public.

Les meilleures pratiques en matière de sécurité documentaire consistent à conjuguer plusieurs mesures complémentaires, à savoir :

- Journaux et rapports sur les activités d'impression
- Filigrane et signatures numériques
- Archivage électronique des documents imprimés

4.1 Journaux et rapports sur les activités d'impression

Un système d'impression sécurisé doit conserver un historique exhaustif de tous les travaux d'impression, comprenant diverses informations : auteur de l'impression, nom du document, ordinateur ayant lancé l'impression, périphérique de sortie, horodatage de l'impression.

L'existence de ce type d'historique renforce la responsabilisation et la traçabilité, et encourage les utilisateurs à faire preuve d'intégrité.

Avec PaperCut NG/MF, ces informations détaillées sont conservées dans des journaux et des archives. Et vous disposez d'un grand choix de rapports d'audit détaillant toutes les transactions ayant eu lieu dans le système.

Activités système

PaperCut conserve les informations détaillées des activités système dans les journaux suivants :

- Journaux d'audit — ils répertorient toutes les opérations liées aux comptes des utilisateurs, en indiquant la date, les détails et l'utilisateur ayant effectué l'opération.
- Journal d'application — PaperCut NG/MF conserve l'historique complet des événements système (par ex., erreurs, notifications, alertes, nouvelles imprimantes ou périphériques).

Activités utilisateur

At the user level, PaperCut NG/MF provides the following logs to track user activity:

- Journal des travaux — il répertorie tous les travaux d'impression, de copie, de fax et de numérisation, avec les informations sur l'utilisateur, la date et les détails de chaque tâche.
- Journal des transactions — il enregistre toutes les transactions financières, notamment les frais d'impression et les transactions de solde de compte.

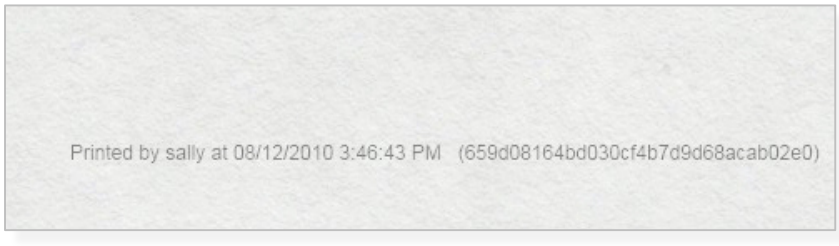
Génération de rapports

Des rapports peuvent être planifiés régulièrement pour alerter les administrateurs en cas de comportement d'impression inhabituel ou en violation de la politique d'impression de l'entreprise.

PaperCut NG/MF propose une large gamme de rapports détaillés pouvant être générés à la demande ou envoyés automatiquement par mail à la hiérarchie, à un rythme quotidien, hebdomadaire ou mensuel.

4.2 Filigrane et signatures numériques

La technologie du filigrane ajoute du texte à une page imprimée au moment de l'impression. Un filigrane peut contenir certaines informations, par exemple l'auteur du document, la date de l'impression et l'imprimante utilisée. Il peut ainsi rappeler aux utilisateurs que la source d'un document peut être identifiée et qu'il est facile de remonter jusqu'à eux.



Une signature numérique est un code numérique généré de façon unique à partir de différents attributs de la tâche d'impression, comme l'heure d'impression, le nom de l'utilisateur, le nom de l'imprimante et celui du document, qui sont combinés à l'aide d'une clé secrète. L'application d'une signature numérique sous forme de filigrane permet de retrouver facilement l'origine d'un document imprimé dans une entrée spécifique du journal d'audit d'impression.

Pour une traçabilité et une sécurité totales des documents imprimés, les meilleures pratiques consistent à combiner filigrane, signatures numériques et un journal des impressions exhaustif.

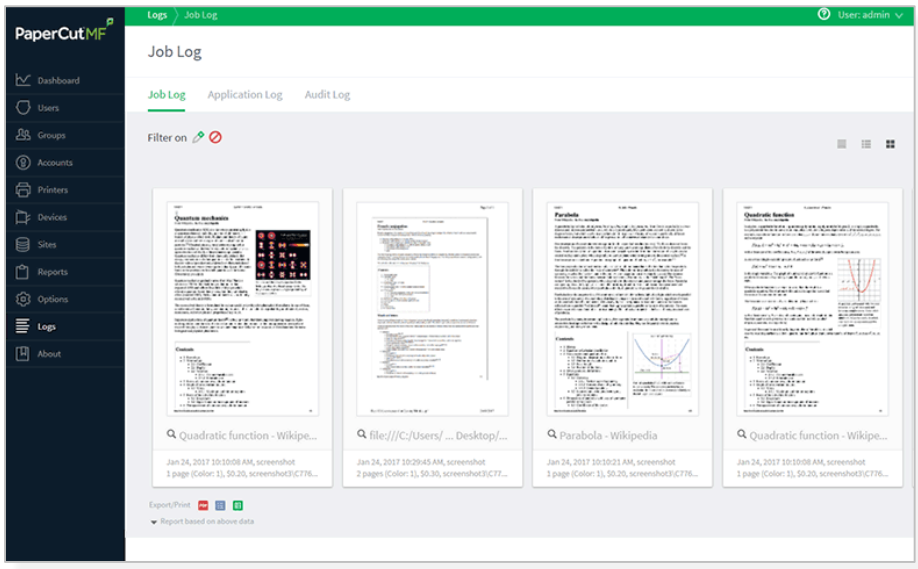
PaperCut NG/MF renforce la sécurité des documents en fournissant ces trois fonctionnalités, fonctionnant deux par deux : le filigrane et les signatures numériques, et un journal d'impression exhaustif où les recherches sont possibles par signature numérique.

Exemple d'utilisation de filigrane :

Damien Royer du cabinet d'avocats Morand et Royer a travaillé sur un dossier de divorce de personnes connues, et a été horrifié quand il a découvert que des éléments du règlement proposé entre les deux parties ont été divulgués dans la presse. Le magazine en cause lui a fourni le document source et comme le cabinet d'avocats utilise la fonctionnalité de filigrane avec signature électronique de PaperCut, qui imprime automatiquement une clé secrète sur tous les documents, Damien peut retrouver quand et où le document a été imprimé, et surtout, par qui.

4.3 Archivage électronique des documents imprimés

Respecter les obligations en matière de conservation de documents (cf. norme HIPAA) n'est pas chose facile pour de nombreuses entreprises. La gestion d'archives imprimées demande à la fois de l'argent et du temps. L'archivage électronique automatique de toutes les impressions est une solution séduisante.



La possibilité d'archiver électroniquement des documents imprimés ajoute également une autre couche de sécurité. Avec l'archivage électronique, le journal des impressions est doté d'une image du document imprimé, ce qui permet une traçabilité totale. Par exemple, il est très facile d'identifier l'auteur d'un document au contenu compromettant ou choquant à partir d'une archive, puisque les journaux d'impression incluent le contenu de la sortie imprimée.

La fonction Print Archiving (Archivage descimpressions) de PaperCut NG/MF permet aux administrateurs approuvés de parcourir et étudier le contenu des activités d'impression au sein de leur environnement. En plus des puissantes fonctionnalités de suivi et de génération de rapports intégrées à PaperCut NG/MF, cette solution dote les administrateurs système d'un large panel de fonctions d'audit, comme :

- Stockage des historiques de tout le contenu imprimé.
- Affichage des anciens travaux d'impression dans un navigateur Web.
- Contrôle d'accès affiné au contenu archivé.

- Téléchargement du fichier spool d'origine pour une ré-impression avec une fidélité à 100 %.
- Activation ou désactivation de l'archivage pour une sélection d'imprimantes et d'utilisateurs.

Exemple d'archivage :

Alors que Stéphanie se trouvait devant l'imprimante, elle a remarqué qu'une image plutôt choquante avait été imprimée, mais elle ne savait pas par qui. Grâce à l'archivage électronique, l'administrateur système peut remonter jusqu'à son auteur. Il peut afficher une image de chaque tâche d'impression pour identifier celle qu'il recherche, et il peut ensuite retrouver l'auteur responsable de l'impression choquante sur le lieu de travail.

.

5.0 Récapitulatif

Il existe des méthodes pratiques et éprouvées pour sécuriser votre système d'impression. Nous recommandons une stratégie de sécurité à plusieurs niveaux qui réponde aux vulnérabilités avant, pendant et après l'impression de chaque document.

Sécuriser votre infrastructure d'impression au moyen d'une configuration de réseau défensive, de files d'attente sécurisées et d'un accès protégé aux périphériques contribuera à vous garantir un système d'impression robuste avant même l'impression de la première tâche.

Sécuriser vos flux d'impression via une politique d'impression et la libération sécurisée des impressions, et savoir gérer les travaux libérés sur une imprimante en mode erreur constituent des techniques efficaces et très répandues en complément des solutions clés en main.

Sécuriser vos sorties imprimées en combinant les journaux des activités d'impression, la technologie par filigrane avec des signatures numériques, et l'archivage électronique, incitera l'utilisateur à se comporter correctement et à se responsabiliser sur ses impressions.

Une solution de gestion d'impression globale, telle que PaperCut NG et PaperCut MF, aidera les entreprises à se doter d'un système d'impression sécurisé en leur permettant d'instaurer un grand nombre de ces bonnes pratiques sans se ruiner. Il ne faut évidemment pas oublier de protéger le logiciel de gestion d'impression par des identifiants de sécurité forts.

Vous pouvez trouver des informations complémentaires plus à jour directement sur le site Web de PaperCut à l'adresse :

http://www.papercut.com/kb/Main/Security

Veuillez contacter l'assistance de PaperCut ou votre revendeur PaperCut local pour toute question spécifique à laquelle ce livre blanc ou la documentation en ligne ne répond pas.

Avec nos remerciements

Auteurs :

Chris Dance (CEO, PaperCut Software)
Geoff Smith (Head of Development, PaperCut Software)
Anthony Nicola (Head of Support, PaperCut Software)
Damien White (Global Technical Services Manager, PaperCut Software)

Contributeur :

Mark Hart (ACDI – Director of Business Development / National Accounts)

Diffusé dans les pays Francophones par :

Bluemega Document & Print Services (Authorized Solution Center PaperCut MF)