ceis

JUIN 2019

IMPRIMANTES MULTIFONCTIONS (MFP) : CYBERSÉCURITÉ, MODE D'EMPLOI

Estelle AUGAT & Wissame ZOUGGARI, Consultantes cybersécurité, sous la direction de Vincent RIOU, Directeur associé de CEIS

Livre blanc

L'INTELLIGENCE DE LA DÉCISION

LIVRE BLANC

Les informations recueillies dans le cadre de ce Livre blanc ont été obtenues en sources ouvertes sur les différentes couches du Web ou sont issues des documentations commerciales des différents constructeurs. L'analyse a été enrichie par la réalisation de quelques entretiens individuels. Les principaux acteurs du marché (Canon, HP, Konica Minolta, Kyocera, Ricoh et Xerox) ont été contactés dans le cadre du présent Livre blanc. Nous les remercions chaleureusement pour leur collaboration. Cependant, les données recueillies et exploitées ne sauraient être présentées comme exhaustives. CEIS et ses consultants ne pourront ainsi être tenus pour responsables d'une information qui s'avérerait obsolète ou inexacte. CEIS se tient à ce titre à la disposition des constructeurs pour enrichir les prochaines éditions de ce Livre blanc.

AVANT-PROPOS

La sécurité du système d'information est désormais une priorité d'ordre stratégique des entreprises et des administrations publiques. Les entreprises savent que le risque cyber n'est plus un risque comme les autres. Elles le qualifient d'hyper-risque dans la mesure où tous les processus essentiels de l'entreprise sont désormais portés par le système d'information, alors que la menace cyber est polymorphe et en constante mutation. Les dirigeants eux-mêmes exigent une confiance renouvelée dans le niveau de sécurisation de l'activité dont ils portent la responsabilité.

Les systèmes multifonctions d'impression constituent un élément du système d'information, peu visible en tant que tel, mais de plus en plus ouvert et connecté pour répondre aux nouveaux enjeux de servicisation des solutions d'impression. La prise de conscience de l'impératif de leur sécurisation est encore à développer. Puisse cette note stratégique y participer !

Henri D'AGRAIN
Délégué général du CIGREF

TABLE DES MATIÈRES

1. CYBERSÉCURITÉ : UN ENJEU MAJEUR POUR LES ENTREPRISES DE TOUTE TAILLE

Alors que les grands groupes ont pris conscience des enjeux liés à la cybersécurité, la plupart des entreprises de taille plus modeste restent démunies face aux attaques. Même si le niveau de maturité et de préparation des grandes entreprises est hétérogène selon les secteurs, elles se donnent les moyens pour analyser les risques et mettre en place des mesures et des solutions adaptées. A l'opposé, les petites et moyennes entreprises n'ont généralement ni la culture de la cybersécurité, ni les ressources humaines et les moyens techniques pour faire face aux menaces.

Pourtant, paradoxalement, la cybersécurité est une préoccupation pour 76% des PME, ce qui est déjà en soi une évolution importante (Source : IFOP[1]). Il est donc fondamental que leurs prestataires leur apportent des solutions « clés en main » propres à renforcer leur résilience cyber.

UNE PME SUR CINQ VICTIME D'UNE CYBERATTAQUE EN 2018.

D'après une récente étude de la CPME, 42% des PME françaises déclarent avoir déjà subi une ou plusieurs attaques informatiques. L'étude menée par l'IFOP établit qu'elles seraient 21% à avoir été victimes au cours des douze derniers mois, soit une PME sur cinq victime en 2018. De plus, ces chiffres ne traduisent que les attaques détectées par les cibles. Sachant que les vols de données sensibles s'effectuent via des attaques par essence discrètes mais dévastatrices pour le business, ces chiffres ne sont pas parfaitement représentatifs de l'étendue des dégâts.

Ils illustrent bien le pillage organisé à grande échelle contre nos entreprises. Que ce soit un vol de données ou un détournement de fonds, par le biais d'un *malware*, d'un *ransomware*, d'un *phishing*, ou encore d'une arnaque au président, la cybercriminalité est subie au quotidien par un grand nombre d'entre elles.

Ce fléau touche tous les secteurs et peut avoir des conséquences sociales dramatiques. Ainsi, la société Clermont Pièces, près de Clermont-Ferrand, employant huit personnes, a déposé le bilan fin 2017 à la suite d'une attaque par rançongiciel ayant chiffré l'ensemble de ses données clients, fournisseurs et comptabilité, ainsi que son système de sauvegarde[2].

---

[1] *Étude IFOP réalisée pour le compte de Kaspersky Lab et Euler Hermes, « Les PME face aux enjeux de sécurité informatique » (novembre 2018).*

[2] *https://www.lamontagne.fr/clermont-ferrand-63000/economie/victime-d-un-piratage-informatique-la-societe-clermont-pieces-va-fermer-boutique_12561803/*

Très récemment, le pétrolier Picoty SA, dont le siège est à La Souterraine (Creuse) et les entrepôts à La Rochelle, a été victime d'attaquants réclamant 500 000 euros contre la clé de déchiffrement.

La cybercriminalité, hélas, peut rapporter gros, pour beaucoup moins de risques que la criminalité « classique ». En effet, peu d'entreprises portent encore plainte et, quand elles le font, la difficulté technique des enquêtes donne encore un sentiment de relative impunité aux attaquants. Les rançons exigées s'adaptent également à la capacité de paiement de la cible (de 300 euros pour un particulier jusqu'à 500 000 euros et plus pour de grandes entreprises) afin de semer le doute dans l'esprit des dirigeants sur l'intérêt d'un dépôt de plainte. La multiplication des victimes sur une courte période permet d'engranger des sommes importantes, tandis que les compétences techniques nécessaires aux attaques deviennent plus accessibles, avec nombres d'outils clés en main disponibles pour quelques dizaines d'euros sur les marchés noirs du Dark Web.

De plus, depuis l'entrée en vigueur du Règlement général sur la protection des données (RGPD) en mai 2018 et les sanctions financières conséquentes en cas de violation constatée, la protection des données à caractère personnel est devenue un sujet majeur pour les clients et les consommateurs.

La meilleure solution pour les entreprises est donc de rendre plus complexe le travail des attaquants, afin qu'ils reportent leurs actions vers des cibles plus accessibles.

Au-delà des nécessaires actions de sensibilisation et de prévention, il faut bien comprendre que le niveau de sécurité globale d'une entreprise est celui de son maillon le plus faible. Il est complexe et coûteux de rajouter des fonctionnalités de sécurité *a posteriori*. Il faut donc choisir des solutions sécurisées dès la conception (*« by design »*), adaptées à son niveau de risque et ce pour chaque composant de son système d'information.

« Tous connectés, tous impliqués, tous responsables » martelait Guillaume POUPARD, Directeur général de l'ANSSI lors de l'édition 2019 du Forum International de la Cybersécurité (FIC), encourageant le développement d'une culture « cybersécurité » au sein de l'ensemble des organisations et de leurs dirigeants.

Les solutions d'impression ne doivent pas échapper à cette règle, quelle que soit la taille de l'entreprise. Voyant transiter des documents très sensibles et étant intégrées au coeur du système d'information, elles sont une cible privilégiée des attaquants.

Véritables plateformes de services numériques, les systèmes de numérisation et d'impression ont subi une profonde mutation ces dernières années, accélérée par la recrudescence des attaques informatiques de toutes natures. Encore faut-il faire le bon choix dans le large panel proposé par les constructeurs.

Ce Livre blanc a pour objectif d'aider à guider les décisions des entreprises vers des solutions d'impression leur permettant d'optimiser leurs coûts d'usage sans compromis sur leur sécurité. En effet, pour le choix d'équipements aussi sensibles, la sécurité ne doit pas être une option.

2. LE MFP : BIEN PLUS QU'UNE IMPRIMANTE

2.1. Un terminal sophistiqué et connecté

Un MFP (*« Multiple Function Printer »)*, ou imprimante multifonction, se distingue d'une imprimante « classique » par l'ajout de multiples fonctionnalités, la transformant en un équipement sophistiqué, polyvalent et pleinement connecté au système d'information de l'entreprise. Appareil « tout-en-un » agissant comme une véritable plateforme centralisée de services, il combine différentes fonctionnalités (i.e. impression, numérisation, console d'administration, envoi de documents, copie et fax) et remplace l'ensemble des périphériques associés. Intégrant en propre un système d'exploitation, des disques durs, des serveurs et une connexion permanente au réseau, ces imprimantes permettent une optimisation de la gestion des flux numériques et un meilleur traitement de l'information, centré sur le document, au sein de l'entreprise.

Ainsi, Bernard DECUGIS, Président du Syndicat National des Entreprises de Solutions et Systèmes d'Information et d'Impression (SNESSII), présente le marché des systèmes d'impression comme étant « *passé du statut de périphérique à celui d'objet connecté pleinement intégré dans le système d'information de l'entreprise* ».

Véritables couteaux suisses d'une organisation, les imprimantes multifonctions sont indispensables au quotidien des professionnels, malgré une baisse naturelle de l'impression papier au profit de la numérisation. Startups, PME, ETI, multinationales, administrations, tous ont aujourd'hui recours à ce type d'équipements, comme en témoigne le chiffre impressionnant de 3,5 millions d'unités vendues en 2017 en France[3], sur le marché *Business to Business* (BtoB).

À ce jour, le marché français est dominé par quelques grands acteurs japonais (Canon, Konica Minolta, Ricoh) et américains (Xerox, HP). Les autres acteurs du domaine sont Toshiba, Sharp, Kyocera et Samsung. Tous n'ont pas le même degré de maturité ni la même antériorité par rapport à l'intégration de la sécurité dans leurs solutions et de nombreuses fonctionnalités importantes restent hélas optionnelles. Il en va donc de la responsabilité du client final d'intégrer les éléments essentiels de sécurité dans son cahier des charges afin que le critère « prix » ne soit plus le seul déterminant. Certes, la sécurité a un coût, mais quel est le coût de l'insécurité ?

[3] *Données présentées par le Syndicat National des Entreprises de Solutions et Systèmes d'Information et d'Impression.*

2.2. Une mine d'or pour les attaquants

Parce qu'ils proposent une large gamme de fonctions et de choix combinés, les MFP comportent de nombreux éléments – logiciels ou purement matériels – susceptibles de présenter des vulnérabilités. Ces équipements concentrent dans leurs disques un très grand nombre de documents sensibles ou de données personnelles (salaires, propositions commerciales, listes de fournisseurs, stratégie d'entreprise…). De plus, ils sont un excellent moyen d'accès au reste du réseau de l'entreprise.

A la différence d'autres périphériques tels que les ordinateurs ou les appareils mobiles, les risques de sécurité liés aux MFP ont souvent été sous-estimés, voire négligés par les organisations dans le cadre de l'élaboration de leur politique de sécurité. Il s'agit avant tout d'un problème de perception. Si les premiers appareils cités sont immédiatement associés au risque informatique, il n'en va pas de même pour les imprimantes.

Or, à l'instar des autres objets connectés, les MFP constituent, depuis plusieurs années déjà, un vecteur pour des cyberattaques et des cibles potentielles pour des actes de malveillance, que ce soit à des fins d'exfiltration de documents directement stockés sur ces périphériques, ou de pénétration dans le réseau interne de l'entreprise. Le volume massif de données – professionnelles ou personnelles – aujourd'hui imprimées, numérisées, enregistrées, stockées, ou transmises par ces imprimantes représente un actif vital dont la perte est susceptible de porter atteinte aux intérêts économiques fondamentaux de l'entreprise.

Illustrant la vulnérabilité de ce type d'équipements périphériques, un utilisateur de Twitter (identifié sous le pseudonyme @TheHackerGiraffe) a, en décembre 2018, pris le contrôle à distance de plus de 50 000 imprimantes lui permettant d'imprimer des tracts invitant les gens à s'abonner à une chaîne YouTube appelée PewDiePie.

Pour ce type d'attaque massive, non ciblée, une simple recherche sur Shodan couplée à l'utilisation de l'outil PRET[4] (*Printer Exploitation Toolkit*) a permis à l'attaquant d'identifier et d'exploiter des centaines de milliers d'imprimantes vulnérables connectées à Internet.

De même, en août 2018, les chercheurs de la société de cybersécurité Check Point ont fait la démonstration d'une attaque exploitant les vulnérabilités des protocoles de communication de la fonction fax d'une machine HP. Cette attaque, dénommée « *Faxploit* », ne nécessite qu'une seule donnée relative à l'entreprise – son numéro de fax – et permet l'accès à l'ensemble des ressources réseau de l'entreprise. Précisons que HP a travaillé avec Check Point afin de corriger cette vulnérabilité dans ses machines[5].

POURQUOI LES IMPRIMANTES SONT-ELLES UNE CIBLE PRIVILÉGIÉE POUR LES ATTAQUANTS ?

Elles sont plus facilement accessibles physiquement ;

Elles concentrent un grand nombre de documents sensibles ;

Elles sont généralement moins bien protégées que les autres équipements du réseau ;

Elles donnent un accès direct à un très grand nombre d'utilisateurs et souvent à l'*Active Directory* (annuaire de l'entreprise).

[4] Shodan est un moteur de recherche spécialisé dans les objets connectés à Internet qui permet de récupérer des informations sur les ports et les adresses IP des imprimantes connectées et parfois même la cartographie des imprimantes en réseau. Shodan est souvent utilisé par les attaquants pour rechercher des dispositifs mal sécurisés.
Conçu pour automatiser les attaques contre les MFP, l'outil PRET permet quant à lui de « brute-forcer » les mots de passe (tester l'ensemble des combinaisons de mots de passe possibles) sur plusieurs types de MFP.

[5] https://blog.checkpoint.com/2018/08/12/faxploit-hp-printer-fax-exploit/

Tout composant technologique possède de manière quasi-certaine une ou des vulnérabilité(s), connue(s) ou non, qui génère(nt) alors un ou des impact(s) potentiel(s) propre(s). Ces impacts peuvent être rassemblés ou combinés en 3 catégories :

Nature	Définition	Vulnérabilité appliquée au MFP
Confidentialité	Implique l'accès aux informations par les seules personnes autorisées	Le contenu de l'impression ou d'autres fichiers transitant par le MFP est intercepté par les acteurs malveillants
Intégrité	Les données doivent être intactes et non altérées de manière fortuite ou malveillante	Le contenu d'impression ou d'autres fichiers du système est modifié
Disponibilité	L'accès aux services et ressources	Les services d'impression ne sont plus disponibles pour les utilisateurs

Les cas d'usage liés à la seule confidentialité des flux d'impression de documents sont aussi pléthoriques qu'hétérogènes : billets d'avion ou de train, réservations d'hôtel, fiches de paie, documents bancaires, travaux de recherche, propositions commerciales et réponses aux appels d'offres, tableaux de bord de gestion de l'entreprise, relations contractuelles avec des soustraitants, etc. On peut ainsi les classer de la manière suivante :

- ***Informations à caractère personnel*** (au sens du RGPD, concernant aussi bien les salariés, clients, prestataires ou sous-traitants de l'entreprise) ;
- ***Informations stratégiques de l'entreprise*** (données et tableaux de bord financiers, participations et patrimoine, contrats, accords de confidentialité, etc.) ;
- ***Informations à forte valeur financière, aisément « monétisables »*** (*credentials*[6] de salariés, coordonnées bancaires, brevets, patrimoine technologique ou scientifique, etc.).

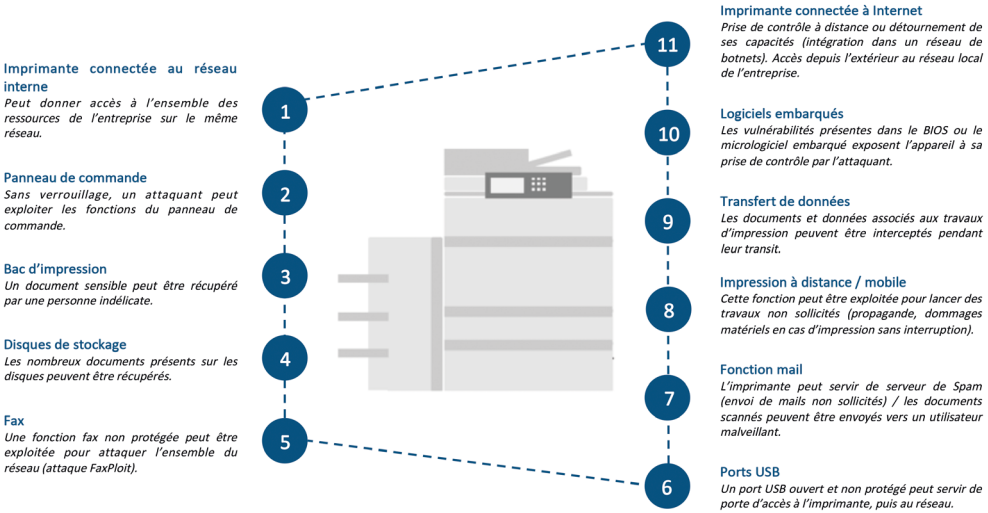
Lorsqu'une atteinte à la confidentialité des impressions est caractérisée, une fuite de données provoquera des conséquences socio-économiques différentes, plus ou moins sévères pour l'entreprise, en fonction de la nature des données et du périmètre de la fuite de données (interne ou externe).

[6] *Credential : couple identifiant / mot de passe d'un utilisateur.*

Plus globalement, les impacts provoqués par la compromission d'un MFP pourront engendrer les conséquences suivantes :

- ***Pertes d'avantages concurrentiels et érosion du chiffre d'affaires*** (divulgation de secrets industriels ou technologiques, politique de prix, etc.) ;
- ***Pertes financières*** (frais de remédiation, de réparation, de notification, de gestion de crise, etc.) ;
- ***Pertes d'exploitation*** (arrêt / perturbation de production) ;
- ***Sanctions financières*** (jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires au niveau monde en cas de manquements graves au RGPD, frais de justice, etc.) ;
- ***Atteinte à l'image de l'entreprise*** (réputation, perte de confiance).

Le schéma suivant présente une synthèse des principales vulnérabilités et risques touchant les systèmes d'impression :



3. LES VECTEURS D'ATTAQUE

3.1. Les acteurs malveillants

Pour pénétrer l'environnement IT d'une entreprise, l'attaquant va soigneusement étudier sa cible (phase de reconnaissance). À la manière d'un cambrioleur, il choisira systématiquement le point d'entrée le plus faiblement défendu, voire pas défendu du tout. Ainsi, les imprimantes connectées peuvent constituer le maillon faible de la chaîne de sécurité et représenter une cible de choix pour différents groupes d'attaquants qui peuvent se classer en quatre grandes catégories :

- ***Les Hacktivistes (contraction de « Hacker » et « Activiste ») aux motivations idéologiques.*** Ces derniers pourraient choisir de tenter de perturber le bon fonctionnement d'une entreprise identifiée comme cible en manipulant les tâches d'impression afin de faire passer un message revendicateur ;
- ***Les concurrents, aux motivations commerciales et économiques.*** Ces derniers tenteraient alors d'obtenir par tous les moyens des données leur permettant de bénéficier d'un avantage concurrentiel certain (politiques de prix, appels d'offres, marchés visés, nouveaux produits) par l'interception de tous les documents imprimés au sein de l'entreprise ;
- ***Les cybercriminels, aux motivations financières.*** Un *ransomware* se propagerait sur l'ensemble des réseaux et impacterait les systèmes d'impression, les rendant ainsi inopérants. Le *ransomware* ne viserait pas spécifiquement le MFP, qui serait ici une victime collatérale de la tentative d'extorsion ;
- ***L'employé revanchard, animé par un objectif de vengeance personnelle.*** Celui-ci chercherait à nuire au maximum à l'entreprise par la divulgation de données confidentielles ou la suppression des données informatiques essentielles de celle-ci.

Quelle que soit sa motivation, une catégorisation des attaquants peut également être faite en fonction de leur niveau d'accès au MFP :

- ***L'attaquant dispose d'un accès physique à l'imprimante.*** Il peut envoyer des fichiers malveillants directement à l'imprimante via le port USB s'il est activé. Cet attaquant peut également modifier les paramètres du MFP si le mot de passe n'est pas assez robuste ou non défini ;
- ***L'attaquant dispose d'un accès logique au réseau de l'entreprise.*** Il peut donc accéder à l'ensemble du parc informatique relié au réseau ;
- ***L'attaquant ne dispose d'aucun accès au réseau interne.*** Il peut tenter d'accéder au MFP si celui-ci est relié à Internet sans aucune protection (absence de pare-feu, mot de passe par défaut non modifié lors de l'installation…) afin de disposer d'une porte d'accès au système d'information de l'entreprise en contournant simplement les mesures de protection mises en place.

3.2. Les différents types de cyberattaques possibles

DDOS

Les attaques par déni de service (DDoS) visent à rendre indisponible le service des MFP en exploitant, par exemple, une vulnérabilité logicielle ou matérielle. Les méthodes d'attaques connues ont pour objectif de maintenir l'imprimante occupée en traitant des fichiers malveillants, de désactiver la fonctionnalité d'impression, voire d'endommager durablement le stockage.

Un type d'attaque DDoS vise le canal de transmission. La plupart des imprimantes traitant les tâches en séries, elles ne peuvent donc prendre en charge qu'un seul travail à la fois. Si ce travail n'est pas terminé, le canal d'impression est bloqué jusqu'à ce qu'un délai d'attente soit déclenché. Un attaquant peut alors lancer un nombre important d'impressions, ce qui empêche les utilisateurs légitimes d'imprimer. Toute personne pouvant accéder au port 9100/tcp peut exploiter cette vulnérabilité[7].

[7] *Exploiting network printers, Müller Jens, Vladislav Mladenov Juraj Somorovsky, Jörg Schwenk.*

NB : *Les méthodes d'attaques sont facilement accessibles sur Internet et peuvent être exécutées sans difficulté par des débutants (script-kiddies).*

Parallèlement, d'autres types d'attaques DDoS peuvent être lancés contre un MFP, non plus comme cible principale – afin de le rendre indisponible – mais comme ressource destinée à toucher une cible plus large. À l'instar d'autres objets connectés, si le MFP est mal configuré et qu'il présente des vulnérabilités, il pourrait être exploité par un *malware* pour opérer des attaques sur des sites Internet. Le *botnet* Mirai, dont l'utilisation sur des objets connectés avait permis une attaque DDoS massive fin 2016, en est l'exemple parfait. En octobre, 600 000 machines étaient ainsi infectées et contrôlées par Mirai[8] qui aurait également exploité les vulnérabilités (mots de passe faibles par défaut) des caméras IP de Hangzhou Xiongmai Technology[9] pour mener une attaque DDoS, provoquant l'interruption du réseau. En mai 2017, Persirai[10], nouveau *malware* contenant une partie du code de Mirai, contaminait à nouveau 120 000 caméras IP dans le but de mener d'autres attaques DDoS massives.

RÉINITIALISATION DES PARAMÈTRES D'USINE

En règle générale, l'accès aux MFP est basé sur les rôles. Les capacités de gestion de la sécurité des MFP sont accordées à un administrateur et l'impression, la copie et le scan de documents à un groupe d'utilisateurs. Ces mesures de sécurité peuvent être contournées si le périphérique n'est pas protégé. Le MFP peut alors facilement être réinitialisé aux paramètres d'usine et des portes dérobées peuvent être déployées par un utilisateur malveillant. Effectuer une réinitialisation à partir du panneau de commande de l'imprimante ne prend que quelques secondes et constitue donc un scénario réaliste pour les attaquants internes.

[8] *https://www.zdnet.fr/actualites/mirai-itineraire-d-un-botnet-de-l-iot-ne-des-guerres-minecraft-39856268.htm*

[9] *https://www.lemondeinformatique.fr/actualites/lire-des-cameras-ip-chinoises-a-l-origine-de-la-gigantesqueattaque-ddos-66311.html*

[10] *https://www.presse-citron.net/objets-connectes-malware-persirai-sattaque-a-120000-cameras-ip/*

MODIFICATION DES TÂCHES D'IMPRESSION

Un attaquant peut aussi tenter de modifier les tâches d'impression. Le mode opératoire de cette attaque est d'infecter un périphérique d'impression avec un logiciel malveillant qui force l'imprimante à manipuler d'autres documents pendant une impression.

Parmi les attaques modifiant les tâches d'impression, on trouve la superposition de contenus, moyen simple de modifier l'apparence des impressions :

- ***Printer Command Langage (PCL)*** a une fonction permettant de placer des macros superposées au-dessus d'un document. Cette fonctionnalité est limitée aux travaux d'impression en cours et ne peut pas être rendue permanente ;
- ***PostScript (PS)*** n'offre pas la fonctionnalité par défaut. Cependant, PS peut être programmé en redéfinissant ses opérateurs, une technique connue de l'industrie de l'impression. Avec l'opérateur *exitserver*, ces modifications peuvent être rendues permanentes – au moins jusqu'au redémarrage de l'imprimante. Lorsque de nouveaux documents légitimes sont imprimés et que cet opérateur est appelé, la version de l'attaquant est exécutée : elle peut contenir des graphiques arbitraires à superposer. Cette attaque fonctionne même si le document a été signé numériquement et vérifié par un serveur d'impression, car le document lui-même reste intact et l'étape de manipulation a lieu immédiatement avant l'impression[11].

VOL D'INFORMATIONS SENSIBLES

Le vol d'informations sensibles peut se traduire par différents types d'attaques :

- ***Vol des données contenues dans la mémoire.*** L'accès à la mémoire permet à un attaquant d'obtenir des données sensibles (mots de passe ou documents imprimés). L'accès en écriture à la mémoire peut conduire à l'exécution de code malveillant ;
- ***Vol des données de système de fichiers.*** Si l'attaquant a un accès en lecture au système de fichiers, il peut alors potentiellement récupérer des informations sensibles comme des fichiers de configuration ou des travaux d'impression stockés ;

[11] *Exploiting network printers, Müller Jens, Vladislav Mladenov Juraj Somorovsky, Jörg Schwenk.*

- ***Fuite du travail d'impression.*** Un attaquant peut réimprimer les travaux d'impression – et donc récupérer les données qui y sont contenues – en utilisant le panel de contrôle sur le serveur Web. Pour cela, il faut que les travaux d'impression soient explicitement stockés sur la mémoire ;

- ***Vol des données d'authentification.*** Au moment de la configuration d'un MFP, l'utilisateur doit définir un mot de passe pour sécuriser le périphérique[12]. En utilisant l'outil Praeda[13] (récupération des noms d'utilisateur et des adresses électroniques à partir de l'interface Web de l'imprimante) ou l'attaque *pass-back*[14] (redirection d'un MFP vers une authentification sur un système non fiable) par exemple, des utilisateurs malveillants peuvent récupérer le couple identifiant / mot de passe[15]. Ils auront, dans un premier temps, accès à l'ensemble des données et dossiers (messagerie, applications métier, serveur interne, MFP, systèmes de gestion et comptabilité, etc.) de la victime et pourront, dans un second temps, obtenir davantage d'informations d'authentification et ainsi effectuer une escalade de privilèges.

> ***NB :*** *L'attaque pass-back[16] fonctionne dans les configurations où un MFP vérifie les utilisateurs en demandant un serveur LDAP externe (le mot de passe pour accéder au serveur LDAP est stocké sur le MFP lui-même). Si le MFP autorise un attaquant à modifier l'adresse du serveur LDAP tout en conservant l'ancien mot de passe, à chaque fois que l'attaquant tente de s'authentifier auprès du MFP, le MFP transmet le mot de passe LDAP d'origine au serveur contrôlé par l'attaquant.*

---

[12] *La plupart des MFP sont déployés avec un mot de passe par défaut.*

[13] *https://github.com/percx/Praeda*

[14] *https://hackinparis.com/data/slides/2014/DeralHeilandandPeterArzamendi.pdf*

[15] *Exploiting network printers, Müller Jens, Vladislav Mladenov Juraj Somorovsky, Jörg Schwenk. / Plunder, Pillage and Print, the art of laverging multifunction printers during penetration testing, Deral Heiland, Pete Arzamendi - Rapid7.*

[16] *http://foofus.net/goons/percx/praeda/pass-back-attack.pdf*

EXÉCUTION DE CODE À DISTANCE

L'exécution de code peut être une conséquence de différents types d'attaques :

- ***Les débordements de mémoire tampon.*** Basée sur le même principe qu'un DDoS, cette attaque a pour principe d'envoyer un nombre de caractères supérieur à celui autorisé afin de saturer le MFP au niveau logiciel. Ceci va entraîner un débordement de la mémoire de stockage, provoquant ainsi le blocage du programme et de l'ensemble du système d'impression ;

- ***La mise à jour des firmwares[17].*** Cette technique vise à apporter des modifications arbitraires et persistantes aux *firmwares* de la victime en exploitant les défauts de conception couramment rencontrés sur l'ensemble des logiciels embarqués. Les attaques de *firmwares* peuvent affecter des familles entières de périphériques adhérant au même système de conception. Selon le type de *firmware* modifié, le pirate disposera d'un large panel d'actions : réinitialisation du mot de passe administrateur de l'imprimante, extraction d'images stockées dans le *firmware* du MFP puis accès à des travaux d'impression sensibles, renvoi de toutes les tâches d'impression sur Internet, ajouts de nouvelles fonctionnalités, etc. ;

- ***L'installation de logiciels personnalisés par des tiers.*** Les constructeurs[18] proposent depuis quelques années des *Software Development Kits* (SDKs) afin que leurs revendeurs et distributeurs exclusifs puissent développer des applications personnalisées pour leurs clients (logiciels spécialement dédiés à l'optimisation et à la supervision des MFP). Ces derniers ne sont donc pas édités par les constructeurs eux-mêmes. Le risque réside ici dans la propagation d'un *malware* via une mise à jour malveillante diffusée directement par les serveurs d'une entreprise tout à fait légitime, mais compromise. Cette méthode, nommée attaque sur la *supply chain,* est de plus en plus utilisée. C'est notamment cette dernière qui a été à l'origine des premières versions du *malware* NotPetya en juin 2017[19].

---

[17] *Firmware : micrologiciel, programme intégré dans le MFP.*

[18] *Chai/OXP (HP), EIP (Xerox), MEAP (Canon), ESA (Ricoh), HyPAS (Kyocera/Utax), bEST (Konica Minolta).*

[19] *https://www.zdnet.fr/actualites/cryptojacking-supply-chain-et-iot-quelles-tendances-2019-pour-la-cybersecurite-39878387.htm*

3.3. Exemples de scénarios basés sur des cas réels

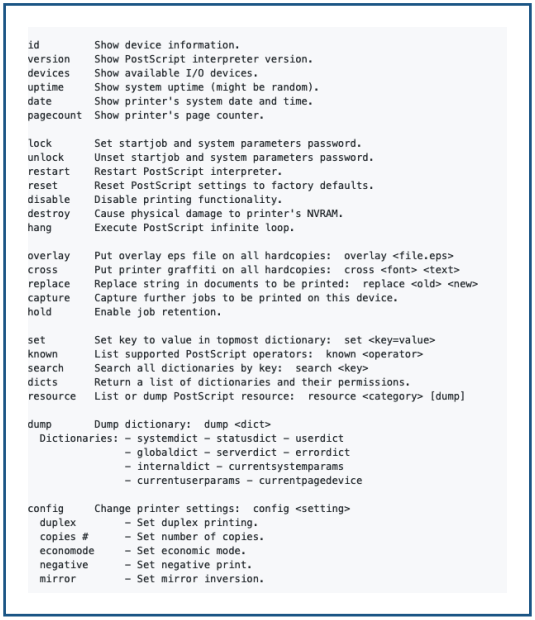
SCÉNARIO N°1 : INTRUSION DANS LE SYSTÈME D'INFORMATION DE L'ENTREPRISE VIA L'IMPRIMANTE CONNECTÉE

Un groupe de cybercriminels est mandaté par une société privée, qui elle-même agit pour les besoins d'un client très intéressé par un produit non encore breveté et développé dans un laboratoire privé. Les cybercriminels vont effectuer une reconnaissance passive du périmètre du laboratoire.

Ils se rendent compte que celui-ci dispose d'un réseau d'imprimantes connectées à Internet. Il s'agit d'une porte d'entrée pour s'introduire dans le système d'information du laboratoire. Les cybercriminels vont tout d'abord vérifier quels sont les ports ouverts et/ou les vulnérabilités exploitables. Ils utilisent des outils accessibles en source ouverte, notamment Shodan[20].

Une fois l'adresse IP de la cible détectée et grâce à l'outil PRET, ils vont pouvoir exécuter toutes les commandes listées page suivante.

[20] *MFP dont le port 9100 est ouvert : https://www.shodan.io/search?query=device%3Aprinter+port+9100*



```
id          Show device information.
version     Show PostScript interpreter version.
devices     Show available I/O devices.
uptime      Show system uptime (might be random).
date        Show printer's system date and time.
pagecount   Show printer's page counter.

lock        Set startjob and system parameters password.
unlock      Unset startjob and system parameters password.
restart     Restart PostScript interpreter.
reset       Reset PostScript settings to factory defaults.
disable     Disable printing functionality.
destroy     Cause physical damage to printer's NVRAM.
hang        Execute PostScript infinite loop.

overlay     Put overlay eps file on all hardcopies:  overlay <file.eps>
cross       Put printer graffiti on all hardcopies:  cross <font> <text>
replace     Replace string in documents to be printed:  replace <old> <new>
capture     Capture further jobs to be printed on this device.
hold        Enable job retention.

set         Set key to value in topmost dictionary:  set <key=value>
known       List supported PostScript operators:  known <operator>
search      Search all dictionaries by key:  search <key>
dicts       Return a list of dictionaries and their permissions.
resource    List or dump PostScript resource:  resource <category> [dump]

dump        Dump dictionary:  dump <dict>
  Dictionaries: - systemdict - statusdict - userdict
                - globaldict - serverdict - errordict
                - internaldict - currentsystemparams
                - currentuserparams - currentpagedevice

config      Change printer settings:  config <setting>
  duplex         - Set duplex printing.
  copies #       - Set number of copies.
  economode      - Set economic mode.
  negative       - Set negative print.
  mirror         - Set mirror inversion.
```

L’accès à certaines données de configuration de l’imprimante peut permettre aux cybercriminels de récupérer des identifiants de connexion reliés à l’imprimante. Ces données leur donnent accès à la messagerie en ligne de l’un des chercheurs, car ce dernier utilise les mêmes identifiants que pour l’imprimante. Les cybercriminels y trouvent alors des échanges de mails non chiffrés concernant le produit confidentiel. Ils vont transmettre tous les éléments, moyennant rémunération, à la société privée qui le livrera à son client.

Les effets sont dévastateurs pour le laboratoire. Les cybercriminels ont choisi de conserver leur accès au système d’information grâce à des *malwares* espions, ils récupèrent toutes les informations sensibles afin de les revendre à toute personne intéressée. Le laboratoire a perdu l’avantage concurrentiel que constituait le produit que le client de la société privée va développer plus rapidement de son côté et mettre en vente. Des pertes financières lourdes sont à prévoir, du fait du gain manqué, mais également dûes aux coûts de sécurisation du matériel informatique si le laboratoire se rend compte de l’intrusion. La médiatisation de la fuite causera un préjudice à l’image du laboratoire, dont les financements seront retirés.

SCÉNARIO N°2 : MODIFICATION DES TÂCHES D'IMPRESSION ET HACKTIVISME

Un groupuscule d'extrémistes politiques souhaite porter atteinte à la réputation d'un cabinet d'avocats qui défend un membre d'un groupe concurrent. Leur objectif est de faire sortir à l'impression des feuilles sur lesquelles sont écrits des messages outrageants envers les avocats du cabinet en question, tout en lançant des impressions à distance en continu, afin de monopoliser leur système d'impression pendant plusieurs jours.

Après avoir défini le périmètre cible en utilisant des outils accessibles en sources ouvertes comme Shodan, les attaquants vont s'équiper en logiciel et en matériel pour effectuer une attaque sur le système d'impression de l'entreprise et, grâce à l'outil PRET, exécuter des commandes visant à modifier les caractères d'impression.

L'impact sera immédiat. Les avocats ne pourront plus accéder à leurs imprimantes et ne pourront plus envoyer les documents de procédure nécessaires. Certains délais de procédure seront dépassés, les entravant dans leurs activités de défense et de conseil. Leurs clients perdront confiance et cela aura un impact contractuel. De plus, le cabinet va devoir mettre en place des mesures correctives immédiates et, à long terme, des mesures de renforcement de défense informatique qui auront un véritable coût financier.

La menace est réelle.

Les conséquences d'une attaque sont très importantes, quelle que soit la taille de l'entreprise concernée, et encore plus si elle est petite, donc plus fragile.

C'est maintenant l'heure du choix : **la sécurité de l'impression est-elle encore une option ?**

4. COMMENT CHOISIR UNE SOLUTION D'IMPRESSION SÉCURISÉE ?

4.1. Intégrer la sécurité dans les exigences contractuelles

Afin de réduire les coûts de l'infrastructure d'impression et des consommables, les entreprises et organisations signent des contrats avec des prestataires ou revendeurs spécialisés. Cependant, les exigences de sécurité intégrées aux appels d'offres sont souvent absentes ou optionnelles, car largement perçues comme un surcoût secondaire pour de nombreux clients, persuadés, dans le meilleur des cas, que les fonctions de sécurité périmétriques du réseau de l'entreprise suffiront. Or, il faut mettre en place une « défense en profondeur », en protégeant de manière systématique tout point d'accès au réseau, y compris derrière le pare-feu. Les MFP ne font pas exception.

Il en va de la responsabilité de l'entreprise d'intégrer la sécurité dans toutes les exigences d'acquisition d'un équipement connecté au réseau, *a fortiori* s'il traite des données sensibles.

Les fonctions de sécurité décrites dans ce chapitre 4 doivent donc impérativement être intégrées au juste niveau dans le cahier des charges, afin que le critère « prix » ne soit plus le seul paramètre guidant le choix d'un équipement.

De plus, l'intégration de ces fonctions de sécurité concourt à la réponse aux exigences de conformité du Règlement général sur la protection des données (RGPD) et limite donc le risque d'exposition à d'importantes amendes en cas de fuite ou vol de données personnelles du fait d'un système d'impression insuffisamment protégé, vecteur de compromission de données personnelles.

4.2. Bilan de maturité des offres actuelles

4.2.1. Introduction

Au cours de ces dernières années, des solutions techniques liées à la cybersécurité intrinsèque des MFP ont été progressivement déployées par les constructeurs en lien avec la transformation du marché et le développement d'un certain nombre de normes. Ainsi, les fabricants ont, dès le milieu des années 2000, mis l'accent sur la sécurisation des systèmes d'exploitation – généralement propriétaires – de leurs produits, selon les recommandations du standard international « *Common Criteria* » (ISO/CEI 15408).

Cette démarche, certes indispensable, est cependant loin d'être suffisante eu égard aux évolutions technologiques, au renforcement de la règlementation en matière de sécurité numérique et aux menaces cyber de plus en plus nombreuses et sophistiquées.

Parallèlement à l'élargissement des gammes de produits et l'intégration de services de plus en plus connectés, de nombreuses fonctions ou options de sécurité sont proposées par les différents fournisseurs. Au-delà des aspects marketing, une analyse comparative de certaines gammes de MFP permet de mieux comprendre la réalité de ce marché.

Nous avons retenu, dans l'analyse qui suit, les gammes de MFP professionnels sécurisés des principaux acteurs du marché intégrant des solutions de sécurité :

- **Canon :** Image RUNNER Advance
- **HP :** Gammes Pro et Entreprise
- **Konica Minolta :** Bizhub i-Series
- **Kyocera :** TASKalfa
- **Ricoh :** Gammes IM et MP
- **Xerox :** VersaLink et AltaLink

L'analyse et le recueil d'éléments sont réalisés sur la base des informations disponibles en source ouverte, complétées par quelques entretiens avec les constructeurs.

4.2.2. Les fonctions couvertes par l'ensemble des offres de MFP sécurisés

Les grands constructeurs ont tous, ces dernières années, intégré dans leurs gammes les fonctions essentielles de cybersécurité. Ces fonctions sont indispensables lors du choix d'un équipement. Certaines fonctionnalités importantes de sécurité sont néanmoins positionnées en option afin de ne pas alourdir la facture pour rester attractif dans un marché tendu par une concurrence pratiquant des prix toujours plus bas.

Il conviendra à l'acheteur averti d'y prendre garde et à l'administrateur de vérifier si ces fonctions de sécurité sont bien activées par défaut à l'installation des machines.

Fonction de sécurité	Caractéristique
1 Le chiffrement et l'intégration du disque dur au sein du MFP	L'utilisation généralisée de mécanismes de chiffrement au niveau des flux de communication, du réseau ou des disques durs permet, en cas d'interception de données par un acteur malveillant, de rendre ces dernières difficilement exploitables. Ces fonctionnalités essentielles (1 à 4) sont toutefois grandement paramétrables par les administrateurs. Il convient donc qu'ils s'assurent : ✓ Que le mot de passe d'accès par défaut a bien été changé pour un mot de passe unique et complexe ; ✓ Que la fonction de chiffrement du disque dur est bien activée (elle peut être optionnelle chez quelques constructeurs) ; ✓ Que le contenu du disque est effacé régulièrement selon une méthode suffisamment robuste, de manière automatique ; ✓ Que les données temporaires sont écrasées tâche par tâche, dès qu'elles ne sont plus nécessaires pour la tâche en cours ; ✓ Que les options de chiffrement des PDF scannés et des emails sont activées par défaut.
2 L'effacement sécurisé des fichiers[21]	
3 Le chiffrement des emails (du MFP vers l'utilisateur lors de numérisations)	
4 Le chiffrement du flux d'impression sur le réseau de l'entreprise	

[21] *Effacement sécurisé des fichiers : réécriture de patterns (patrons de conception) empêchant la réexploitabilité du support.*

5 L'authentification réseau pour accéder à la console de supervision Web	La personne souhaitant effectuer des réglages sur le MFP doit s'authentifier sur le réseau, ce qui empêche l'utilisation de la console par une personne non autorisée.
6 L'authentification physique pour l'accès aux documents imprimés	Seul un salarié se trouvant physiquement dans l'entreprise et disposant des droits nécessaires pourra accéder aux documents.
7 L'emploi de PINS et mots de passe chiffrés	Avec ce type de protection, un attaquant infiltré dans le réseau ne pourra pas récupérer l'ensemble des mots de passe. Néanmoins, l'exigence de sécurité diffère en fonction des constructeurs. Si certains utilisent seulement des mots de passe alphanumériques, d'autres vont plus loin en intégrant un mécanisme d'authentification basé sur un échange de clés. Ce dernier permet d'éviter des attaques par « brute-force » par exemple.
8 L'accès basé sur les rôles pour contrôler les fonctionnalités du panneau de commande	Afin d'assurer un niveau de sécurité avancé, les MFP permettent d'autoriser ou d'interdire l'utilisation de certaines fonctions sur l'appareil. L'administrateur peut alors contrôler ces fonctionnalités en adéquation avec les besoins des utilisateurs concernés.
9 La signature numérique des *firmwares* et *softwares*	Cette signature numérique permet de réduire le risque de falsification des *firmwares* et *softwares* en confirmant leur source, ce qui aide le MFP à différencier les *firmwares* et *softwares* authentiques des logiciels malveillants.
10 Le module de plateforme de confiance (TPM)	Aussi appelé module de plateforme sécurisée, ou *Trusted Platform Module* en anglais, TPM est un module cryptographique qui vise à améliorer la sécurité et la confidentialité du MFP. Pour cela, il génère et protège les clés de chiffrement afin de renforcer la protection des informations d'identification chiffrées et des données stockées sur le périphérique.

11 La désactivation des ports physiques	Cette protection empêche un accès direct à la machine. Si les ports physiques ne sont pas désactivés, l'utilisation de vecteurs d'attaque USB de types « BadUSB » ou « Rubber Ducky » est possible. Le code malveillant, niché dans le *firmware* de la clé, est indétectable par les solutions de sécurité classique. Cette clé USB contient un programme qui se fait passer pour un clavier auprès du système afin d'exécuter des actions. L'ensemble des frappes du script intégré sur la clé USB de l'attaquant peut être adapté à l'OS intégré dans l'imprimante pour générer des actions malveillantes, pouvant mener à la prise de contrôle du MFP.
12 Le filtrage des adresses IP par liste blanche *(« whitelisting »)*	Seul un nombre restreint d'adresses IP, correspondant uniquement à celles de l'entreprise, est autorisé à accéder au MFP.
13 Le démarrage sécurisé	Le démarrage sécurisé correspond à un démarrage sous contrôle. Le *firmware* système du MFP vérifie que le logiciel de démarrage est signé avec une clé chiffrée autorisée par une base de données contenue dans le *firmware*.
14 L'utilisation de la norme IEEE 802.1X[22] sur les réseaux étendus (WAN) et locaux (LAN)	La norme permet de sécuriser le réseau en interdisant les communications de réseau (http par exemple) avec des systèmes non autorisés, sauf pour les demandes d'authentification. Ce système empêche qu'un appareil externe accède au réseau. L'accès au réseau n'est donc possible qu'avec une authentification, un mot de passe ou un certificat approprié.
15 La désactivation des protocoles et ports réseaux	La désactivation des protocoles et ports réseaux non utilisés peut permettre de protéger le MFP de certaines attaques, comme par exemple un « brute-force » d'un protocole de transfert de fichiers (FTP) non sécurisé afin de récupérer des documents confidentiels.

[22] *Norme IEEE 802.1x : standard lié à la sécurité des réseaux informatiques, proposé en 2001 par l'Institute of Electrical and Electronics Engineers (IEEE, fournissant une couche de sécurité pour l'utilisation des réseaux câblés et sans fils en contrôlant l'accès à chacun des ports d'un équipement réseau actif (commutateur, borne Wi-Fi, etc.)).*

16	La présence d'IPsec[23]	IPsec permet d'assurer une communication privée et sécurisée sur des réseaux IP. Son objectif est double : authentifier et chiffrer les données pour assurer que le flux ne puisse être compréhensible que par le destinataire final d'une part et éviter la modification des données par des intermédiaires d'autre part.
17	L'utilisation du protocole HTTPS	Si le protocole HTTPS n'est pas disponible sur le MFP, une interception de données sensibles transmises par le biais du protocle HTTP est facilement réalisable. On appelle cette opération l'attaque de l'homme du milieu (*« man in the middle »*).
18	L'utilisation du protocole TLS 1.1 / 1.2	TLS pour *Transport Layer Security.* Il permet l'échange de données de manière sécurisée entre le client et le serveur en garantissant (1) l'authentification du serveur, (2) la confidentialité des données échangées (chiffrement) et (3) l'intégrité des données échangées. Par rapport à TLS 1.1, la version 1.2 remplace les méthodes de chiffrement (notamment MD5/SHA-1) par des méthodes plus sûres (comme SHA-256 et AES).
19	L'utilisation du protocole SMTP sécurisé	SMTPS pour *Simple Mail Transfert Protocol Secure.* Méthode de sécurisation du protocole SMTP en l'encapsulant dans le protocole TLS. Cette méthode permet de fournir une authentification des partenaires de communication ainsi que l'intégrité et la confidentialité des données échangées par courriers électroniques.
20	La version 3 du protocole SNMP	SNMP pour *Simple Network Time Protocol*. C'est un protocole de gestion de réseau. SNMP permet de gérer, superviser et diagnostiquer des problèmes réseaux et matériel à distance.

[23] *IPsec (Internet Protocol Security) : protocole défini par l'Internet Engineering Task Force (IETF) qui permet de chiffrer la communication entre l'Internet local (serveur, PC, client) et le MFP.*

4.2.3. Les fonctions de sécurité majeures partiellement adressées

Un certain nombre de mesures de sécurité que nous jugeons pourtant importantes, afin de rendre complexe le travail de l'attaquant, ne sont que partiellement adressées par les acteurs interrogés sur leurs modèles de MFP sécurisés.

Les pourcentages suivants dressent un bilan (à la date de parution de l'analyse) du nombre de constructeurs étudiés proposant ces fonctions de sécurité. Il conviendra à l'acheteur averti d'y prendre garde lors de son choix.

	Fonction de sécurité	Caractéristique	Intégration (%) par les constructeurs étudiés
1	Code PIN pour la réception et l'envoi des fax	Les fax entrants sont imprimés immédiatement par un télécopieur ou par une imprimante multi-fonction. Ils peuvent donc être vus de tous dans le bac de sortie. Pour empêcher tout accès non autorisé au fax, il est nécessaire de mettre une protection par mot de passe. Sinon, cela peut être problématique pour toute entreprise susceptible de recevoir des fax confidentiels ou sensibles.	83 %
2	Intégration de la norme fédérale américaine FIPS140 relative à la qualité des modules cryptographiques	La norme américaine FIPS140, publiée par l'Institut national des normes et de la technologie (NIST), a été établie dans le but de protéger les informations sensibles dans les systèmes informatiques et de télécommunication (y compris les systèmes vocaux). Pour cela, elle coordonne les exigences de sécurité et les normes relatives aux modules cryptographiques. Son intégration vient apporter une forme de garantie en matière de sécurité des accès, des données et du réseau.	83 %
3	Blocage des fichiers exécutables à partir d'une mémoire USB	Cette mesure permet d'empêcher l'exécution d'un code malveillant à partir d'une clé USB.	83 %
4	Mot de passe exigé après un délai d'inactivité prédéfini	Afin de protéger la session de l'utilisateur / du MFP, la plupart des modèles de MFP déconnectent l'utilisateur lorsqu'un délai d'inactivité défini par l'administrateur s'est écoulé. Si l'option n'est pas activée, cela implique l'ouverture continue de la session. Une personne malveillante peut utiliser cette faille pour récupérer des documents professionnels confidentiels.	83 %

5	Enregistrement des événements de sécurité et intégration possible dans un SIEM	La possibilité d'enregistrer l'ensemble des actions liées au MFP permet d'auditer les activités pour éviter toute utilisation non-autorisée. L'intégration des événements de sécurité du MFP au SIEM *(Security Information and Event Management)* permet de l'intégrer pleinement dans la chaine de cybersécurité de l'entreprise, dont le SOC *(Security Operations Center)*, chargé de la supervision globale de la sécurité dans les entreprises les plus matures.	83 %
6	Activation ou désactivation de la mise à jour du micrologiciel à distance	L'exécution d'une mise à jour du micrologiciel à distance est une fonction réservée aux administrateurs d'une entreprise. Si ces administrateurs maintiennent la fonction active en permanence et que les micrologiciels ne sont pas signés, un utilisateur malveillant peut prendre le contrôle du MFP à distance et récupérer par exemple les fichiers contenus dans ce périphérique. Ainsi, l'administrateur doit pouvoir désactiver cette fonction pour en maîtriser les conséquences sur la sécurité du parc.	67 %
7	Détection automatique d'intrusion au démarrage	L'absence de détection automatique d'intrusion au démarrage permet à une personne malveillante d'utiliser plusieurs types d'attaques (dont la diffusion d'un *malware* via une clé USB) afin de s'introduire dans le système. Nous constatons quelques approches divergentes chez les constructeurs, avec, comme exemples, HP qui apporte une réponse rapide avec ses MFP qui peuvent s'auto-réparer (avec les limitations de l'automatisme), tandis que Konica Minolta privilégie l'intervention humaine d'un expert afin d'assurer un suivi auprès de PME qui ne sont pas toujours dotées de profils techniques en interne. Deux approches intéressantes, qui peuvent convenir à des typologies de clients différents.	67 %
8	Mot de passe spécifique pour une utilisation en dehors des heures ouvrables	Cette configuration permet aux administrateurs de protéger les MFP par des mots de passe spécifiques interdisant l'utilisation de l'imprimante en dehors des heures ouvrables. En cas de vol d'identifiant, il est probable que l'attaquant attende le soir ou la nuit pour mener des actions frauduleuses sur le système, par souci de discrétion. Cette protection supplémentaire permet de limiter le risque par l'emploi de mots de passe spécifiques aux tranches horaires d'absence des employés.	50 %

4.2.4. Les fonctions de sécurité importantes restant à couvrir

Les fonctions de sécurité du présent tableau, trop peu couvertes, nécessitent une plus grande attention de la part des fabricants.

	Fonction de sécurité	Caractéristique	Intégration (%) par les constructeurs étudiés
1	Détection automatique d'anomalie sur le réseau (Host IPS)	La détection automatique d'anomalie sur le réseau permet de détecter des problèmes physiques ou techniques tels qu'une panne d'électricité ou des échecs de serveur de fichiers, des changements brusques causés par le trafic légitime comme la surcharge du réseau, des foules subites, ainsi que des comportements risqués illégitimes comme des attaques de déni de service (DoS) et déni de service distribué (DDoS).	33 %
2	Authentification pour l'accès au clavier physique	Le fait de ne pas exiger une authentification pour l'accès au clavier physique peut constituer une véritable faille de sécurité pour une entreprise. Un attaquant peut par exemple tenter de prendre le contrôle total de l'imprimante et donc s'introduire dans le réseau de cette dernière afin de voler des données confidentielles et/ou de diffuser des *malwares*.	33 %
3	Mot de passe complexe par défaut	L'exigence de mots de passe complexes[24] par défaut peut protéger l'utilisation des MFP au sein d'une entreprise même si cette dernière n'a pas de maturité en sécurité. Les constructeurs ne semblent pas exiger de mots de passe complexes par défaut pour les utilisateurs et transfèrent cette responsabilité aux administrateurs. C'est donc à eux d'établir une politique de sécurité qui fixe un seuil de complexité pour les mots de passe de l'ensemble des utilisateurs. Si l'administrateur n'est pas sensible aux exigences de cybersécurité, cela peut constituer un véritable risque pour l'entreprise.	0 %

[24] *L'ANSSI définit un mot de passe complexe comme comportant au moins 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux). Selon une étude réalisée par l'éditeur SplashData, parmi les mots de passe les plus utilisés en 2018 figuraient notamment « 123456 », « password », « 123456789 », « 12345678 », « sunshine » et « qwerty ».*

Sans surprise, plusieurs types d'attaques visent spécifiquement les mots de passe :

- L'attaque *pass-back* ;
- L'utilisation de l'outil PRET permettant de « brute-forcer » les mots de passe.

Afin de pallier le problème, il semblerait pertinent que la machine (et donc les constructeurs) impose un changement de mot de passe à l'installation du MFP.

4.2.5. Focus sur une solution essentielle, mais peu adressée : l'antivirus

Alors qu'on n'imagine pas un ordinateur personnel sans sa solution anti virale embarquée, on peut s'étonner de ne retrouver cette fonction que dans très peu de MFP. Fort heureusement, certains constructeurs ont noué des partenariats avec des fournisseurs d'antivirus – reconnus pour la qualité de leurs produits –, comme Xerox avec McAfee et Konica Minolta avec Bitdefender (dans leur gamme Bizhub i-Series).

Les antivirus sont intégrés directement dans le MFP dans le but d'analyser en temps réel – ou en temps défini par les administrateurs – toutes les données qui y transitent. Le logiciel va donc scanner les données (numérisées, imprimées et partagées) ainsi que les emails, les adresses IP, les logiciels, *hardwares*, etc. qui passent par le périphérique, à la recherche de *malwares*. Parallèlement, l'antivirus va procéder de la même manière pour l'interface administrateur et les connectivités locales (clé USB, NAS[25]) et réseau (SMTP, FTP, etc.), ainsi que le stockage *cloud* éventuel.

De par leurs fonctions, les antivirus viennent d'une part réduire les risques de sécurité liés aux attaques des logiciels malveillants externes – tels que les vers (« *worms* » en anglais), les virus, et aussi l'injection de code telle que le « *buffer overflow* » – et peuvent d'autre part amener de la confiance dans l'intégrité des fichiers, garantissant que le système est dans un état sécurisé et fiable.

Ces solutions permettent non seulement d'amener un niveau de protection indispensable à l'équipement lui-même, mais également de limiter les risques de propagation d'un programme malveillant à l'extérieur par le biais du MFP.

[25] *Un NAS (Network Attached Storage) est un serveur de stockage de fichiers autonome.*

En analysant le contenu des paquets, l'antivirus va plus loin que le filtrage des adresses IP par liste blanche par exemple, qui lui va uniquement contrôler le flux sans analyser le contenu. Dans un aéroport, l'antivirus pourrait être représenté par la machine scannant le contenu des bagages à main tandis que le filtrage des adresses IP par liste blanche s'apparenterait au contrôle du passeport. Ce n'est pas parce que son passeport est valable qu'une personne ne présente aucun danger. Il faut vérifier ses bagages. C'est le rôle de l'antivirus en complément des pares-feux de filtrage.

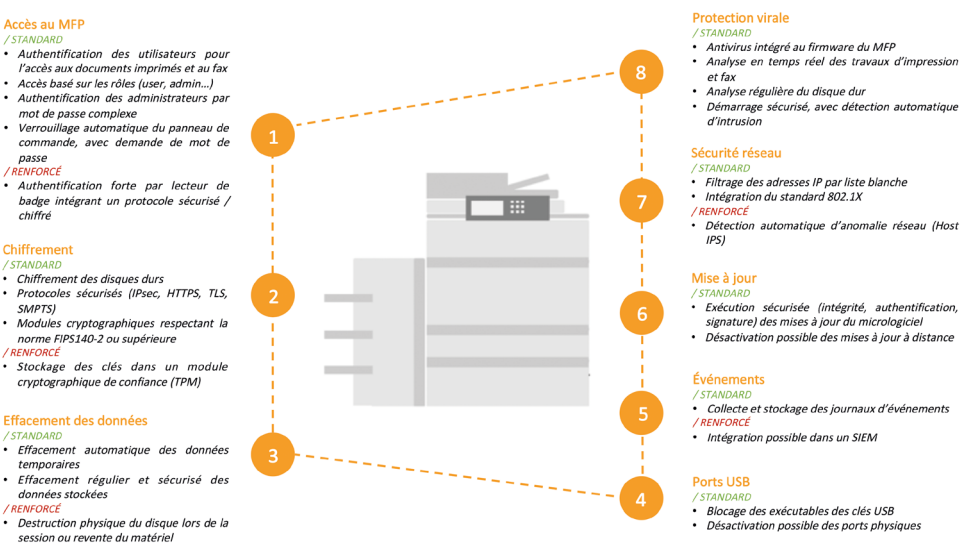
4.3. En synthèse : spécifications d'un MFP sécurisé

Le schéma suivant présente une synthèse des fonctions indispensables au choix d'un système d'impression multifonction sécurisé. Le lecteur pourra y trouver un guide utile lors de ses échanges avec les distributeurs et revendeurs de solutions.

Par souci de simplification, nous présentons deux niveaux de sécurité.

Le niveau « Standard » intègre les fonctions indispensables à toute solution en entreprise, quelle que soit sa taille, à partir du moment où celle-ci est amenée à imprimer, faxer ou scanner des documents sensibles (fichiers clients, fournisseurs, comptables, commerciaux…).

Le niveau « Renforcé » présente des spécifications qui peuvent être importantes pour des entreprises ayant un niveau de risque plus élevé ou des contraintes règlementaires spécifiques.



5. CONCLUSION

+ La cybersécurité d'une organisation est une chaîne dont la résistance repose sur celle de son maillon le plus faible. Les MFP n'y font pas exception. Ils doivent donc être pleinement intégrés dans la maîtrise opérationnelle des risques dans un contexte d'ouverture et d'interconnexion croissante du système d'information. Il est de la responsabilité des clients de prendre en compte la sécurité du MFP dans leurs critères de décision.

+ Aujourd'hui, les constructeurs ont pris conscience de l'importance d'intégrer la sécurité *by design* dans leurs produits et certains ont même noué des partenariats avec des éditeurs spécialisés. Leurs offres sont néanmoins pléthoriques, avec de nombreux modules optionnels. L'objectif de ce Livre blanc est de permettre un échange constructif entre les clients et les constructeurs ou revendeurs.

+ Certains constructeurs veulent dépasser la stricte sécurisation de leurs produits en proposant des services numériques additionnels (infogérance, conseil, intégration), y compris en matière de sécurité des systèmes d'information. Face à des clients encore peu matures sur les enjeux de cybersécurité, TPE/PME en premier lieu, ces fournisseurs positionnent leurs produits au centre de la chaîne de valeur IT globale en y apportant des services nouveaux, à forte valeur ajoutée. Cette démarche doit être encouragée car allant dans le sens de la sécurité globale du client.

+ Les organisations, en fonction de leur maturité en matière de cybersécurité, n'ont pas les mêmes besoins. Alors que la plupart des grands comptes bénéficient déjà d'un environnement piloté de cybersécurité (SOC, SIEM), les PME, généralement moins dotées en ressources humaines et techniques spécialisées, auront quant à elles un réel besoin d'accompagnement et de solutions sécurisées *by design*. C'est la proximité avec leur partenaire revendeur ou intégrateur qui fera alors la différence, par sa capacité à intégrer la sécurité dans les enjeux majeurs de l'entreprise, au-delà de la simple optimisation du coût d'exploitation du parc d'impression.

ceis

PUBLICATIONS RÉCENTES

Les Black Markets francophones. Structure et fonctionnement Janvier 2019
Fuite de données : gestion de crise, mode d'emploi Janvier 2019
Réalité immersive, Usage des réalités virtuelle et augmentée pour la Défense Octobre 2018
Blockchain, Enjeux, usages et contraintes pour la Défense Octobre 2018
Intelligence artificielle, Applications et enjeux pour les Armées Octobre 2018
A2/AD, déni d'accès et interdiction de zone – Réalité opérationnelle et limites du concept Août 2018
Soutien des forces – Transformations d'une fonction essentielle pour les Armées Août 2018
Le secteur de la santé face au risque cyber : enjeux, risques, remédiations Janvier 2018
Sécurité des grands événements sportifs Janvier 2018
Blockchain : état des lieux et perspectives Janvier 2018

CK Document imaging
by Charles Kieffer Group

Tél. +352 26 380 1 **Fax** +352 26 380 380
sales@ck-group.lu
2, rue Léon Laval - Z.A. Am Bann
L-3372 Leudelange
ck-documentimaging.lu