SHARP

Be Original.

Sécurisez simplement et efficacement votre infrastructure d'impression.

Index

Introduction

Les systèmes d'impression font partie des meubles dans la plupart des entreprises.

Magali Moreau,
Responsable Marketing
& Communication chez
Sharp Business Systems
France

Les MFP que nous utilisons au quotidien semblent ne pas avoir beaucoup changé au cours des dix ou vingt dernières années. Cependant, comme le savent les DSI, les MFP ont évolué pour devenir des systèmes informatiques sophistiqués, connectés au réseau de l'entreprise et à Internet.

Même si neuf employés sur dix en Europe ne considèrent pas que les imprimantes et les MFP puissent constituer une faille de sécurité, ces derniers n'en restent pas moins des cibles pour les hackers au même titre qu'un ordinateur portable ou fixe. Ils doivent être protégés par le biais d'une technologie sécurisée et associés à des usages validés.

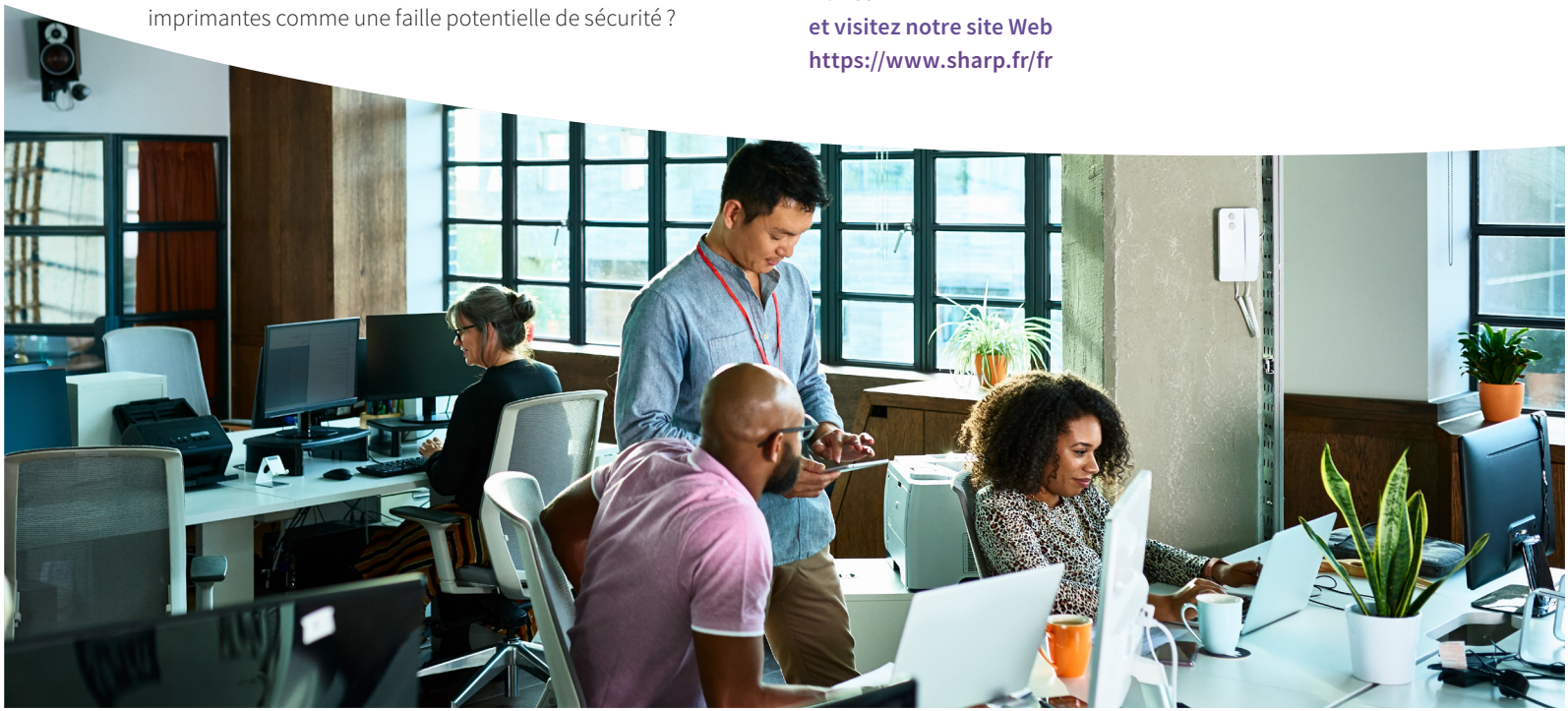
En tant que fabricant de systèmes d'impression, la sécurité est au cœur de notre stratégie de développement de produits. Nous nous assurons que nos produits et nos services simplifient la vie des utilisateurs et les rendent plus productifs, tout en leur garantissant un fonctionnement hautement sécurisé.

Nous avons analysé les habitudes d'utilisation des multifonctions par les employés.
Les personnes extérieures à notre secteur considèrent-elles les imprimantes comme une faille potentielle de sécurité ?

Nous avons interrogé plus de 5 500 employés de bureau de petites et moyennes entreprises (PME) en Europe, et avons découvert que près de la moitié des personnes interrogées ne savait même pas qu'il était possible de pirater un système d'impression.

Notre étude a également mis en évidence des lacunes évidentes en termes de formation et de conseil dans le domaine de la sécurité des systèmes d'impression. Nous souhaitons apporter une solution à ces manques en publiant des conseils techniques et des livres blancs sur notre site Web, ainsi que ce guide créé par Jens Müller, un « hackeur éthique ». Ce guide aborde les comportements relatifs à l'impression en Europe et fournit des conseils de sécurité simples à suivre dans les PME. Nous espérons que vous trouverez dans ce guide des éléments pertinents pour l'optimisation de votre politique de sécurité. Nous vous invitons à partager vos idées ou expériences sur les grandes questions liées à la sécurité des données sur notre page linkedIn.

Contactez-nous sur LinkedIn
https://fr.linkedin.com/company/sharp-business-systems-france
et visitez notre site Web
https://www.sharp.fr/fr



Votre réseau est-il sécurisé ?

Saviez-vous que les PME sont moins susceptibles que les grands groupes d'installer des fonctionnalités de sécurité sur leurs systèmes d'impression ?

Dans les entreprises de moins de 49 employés, 62 % des personnes déclarent que tout le monde peut utiliser leur imprimante ou MFP. Ce nombre chute à 43 % dans les entreprises de 151 à 250 employés.

Le fait de ne pas contrôler l'accès aux systèmes d'impression présente de nombreux risques tels que le chargement (volontaire ou involontaire) d'un programme malveillant, ou la fuite de données confidentielles due à des impressions laissées sans surveillance sur le matériel.

Chiffres clés de l'étude

10 %

Seuls 10 % des employés identifient les imprimantes ou les MFP comme failles de sécurité potentielles sur leur lieu de travail.

21 %

21 % des employés déclarent n'avoir connaissance d'aucun processus de sécurité en place pour les imprimantes ou les MFP au sein de leur entreprise.

25 %

25 % des employés déclarent avoir trouvé des informations personnelles ou confidentielles qui ne leur étaient pas destinées sur le matériel d'impression.

28 %

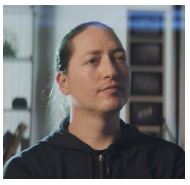
28 % des employés déclarent avoir déjà utilisé un matériel d'impression de l'entreprise pour imprimer un document personnel créé chez eux, en dehors du périmètre de sécurité de l'entreprise.

14 %

14 % des employés déclarent avoir déjà utilisé leur imprimante de bureau pour imprimer un document téléchargé malgré un avertissement de sécurité, exposant ainsi le réseau de l'entreprise à une menace potentielle.

L'étude a été réalisée par Censuswide pour le compte de Sharp. 5 514 employés de bureau d'entreprises de 10 à 250 employés ont été interrogés dans sept pays européens (Royaume-Uni, Allemagne, France, Italie, Pays-Bas, Suède et Pologne).

L’avis d’un expert



Jens Müller
Hackeur éthique

Jens Müller, hackeur éthique, explore les résultats de l’étude de Sharp et fait l’analyse des risques potentiels que représentent les systèmes d’impression pour la sécurité des données dans les PME.

L’étude de Sharp a révélé que neuf employés sur dix en Europe ne considèrent pas que leur imprimante ou leur MFP puisse constituer une faille potentielle dans la sécurité de leur organisation. Après tout, qui voudrait pirater l’imprimante ou le MFP d’une entreprise ? et pourquoi les cibler ?

Premièrement, les systèmes d’impression sont partout. Toutes les entreprises en possèdent, ils sont connectés au réseau et peuvent être facilement ciblés par les hackers lorsqu’ils ne sont pas sécurisés.

Deuxièmement, les matériels d’impression peuvent contenir de précieuses informations, ce qui en fait des cibles privilégiées. Les entreprises doivent se demander quelle valeur peut être accordée aux informations imprimées et numérisées. À l’heure où le Règlement Général sur la Protection des Données (RGPD) impose aux entreprises de protéger les données personnelles qu’elles détiennent, une défaillance de la sécurité des systèmes d’impression peut coûter très cher aux entreprises.

Il y a généralement deux types de hackers : les jeunes novices qui veulent s’amuser et tester leurs compétences par curiosité, et les profils malintentionnées qui pratiquent l’espionnage industriel. Bien que nous ne connaissions pas encore l’étendue du problème de sécurité posé par les matériels d’impression, nous savons toutefois que des dizaines de milliers de systèmes d’impression sont accessibles aisément par les hackers.

Ce serait une erreur de penser que les imprimantes et les MFP constituent uniquement un risque pour les grandes entreprises. En effet, les PME sont tout aussi vulnérables. La violation de données peut toucher tous types de structures. Une PME peut traiter autant de données sensibles qu’une grande entreprise. Néanmoins, il a été constaté dans le cadre de l’étude Sharp que les PME disposent de moins de moyens et de ressources que les grandes entreprises pour gérer la cybersécurité.

Il est important de sensibiliser les utilisateurs à cette problématique. De la même manière que les entreprises forment les utilisateurs sur des menaces de sécurité importantes telle que l’hameçonnage, elles doivent également comprendre les failles de sécurité potentielles représentées par des systèmes d’impression non sécurisés. Les entreprises doivent apprendre à limiter les risques de violation de données. Il a été constaté que 40 % des employés en Europe n’ont jamais reçu de formation ou de conseils en matière de sécurité des impressions.

Quels sont les risques liés aux systèmes d’impression non sécurisés ? Les imprimantes et les MFP peuvent non seulement donner accès à des documents sensibles, qu’ils soient imprimés, scannés ou faxés, mais il y a également un risque que ces équipements soient exploités pour infiltrer le réseau d’une entreprise ou effectuer des attaques par déni de service distribuées (DDoS). C’est ce qui s’est produit en 2016 avec le botnet Mirai, qui a infecté des appareils dans le monde entier, et qui est responsable de la plus grande attaque DDoS de l’histoire. Les hackers cherchent toujours le maillon le plus faible, qui peut tout à fait être un système d’impression.

Nous savons que plus de la moitié (52 %) des employés déclarent qu'aucune authentification n'est requise pour utiliser les fonctions de leur imprimante ou MFP. Par ailleurs, les matériels les plus anciens peuvent être davantage vulnérables dans la mesure où les fonctionnalités de sécurité ne sont pas à jour, de la même manière que les vieux matériels Windows sont plus souvent la cible des virus et des cyberattaques.
La vulnérabilité des logiciels obsolètes a très largement été pointée du doigt lors de l'attaque WannaCry de mai 2017, et les systèmes d'impression ne sont pas épargnés par ce type de risques.

Comment les PME peuvent-elles prévenir les risques liés à la vulnérabilité des systèmes d'impression ? En l'occurrence, il est plus difficile de se défendre que d'attaquer. Les hackers ont juste à trouver un moyen d'entrer, tandis que le responsable informatique (ou toute personne responsable de l'informatique dans l'entreprise) doit envisager toutes les failles potentielles.
La sécurité engendre des coûts de gestion récurrents qui tirent la rentabilité des PME vers le bas, ce qui explique probablement pourquoi ce n'est pas leur première préoccupation. Il est également difficile d'investir en priorité dans des équipements neufs alors que le matériel actuel est opérationnel et remplit correctement sa fonction principale (à savoir imprimer ou numériser des documents).

Et cela ne concerne pas seulement l'impression. Le scanner peut également représenter une faille, et les documents numérisés peuvent facilement être récupérés par un hacker. Les PME doivent envisager de crypter les documents PDF et s'assurer que les documents numérisés envoyés par e-mail depuis le MFP sont sécurisés.

La sécurité des données numériques est bien sûr une préoccupation, mais les PME ne doivent jamais sous-estimer la menace pesant sur les informations papier.
Par le passé, des personnes malintentionnées ont déjà trouvé des informations sensibles dans les ordures. Il peut être facile d'accéder à toute impression laissée sur le matériel, souvent situé dans des zones ouvertes et communes à plusieurs services.

Bien que la tâche puisse paraître difficile, assurer la sécurité des systèmes d'impression est plus facile que vous ne le pensez. Il existe des moyens simples de limiter les risques, et la plupart d'entre eux ne nécessitent aucun investissement, si ce n'est votre temps. Nous avons ennoncés les conseils de Jens Müller destinés aux administrateurs informatiques et à toutes les personnes responsables des technologies bureautiques.

Conseils de sécurité pour les systèmes d'impression

Ces conseils sont valables pour tout système d'impression connecté au réseau de votre entreprise. Certains s'appliquent aux paramètres que vous pouvez modifier vous-même en tant qu'administrateur, d'autres nécessitent l'intervention d'un expert.

Changez les mots de passe par défaut

Ne laissez pas des hackers prendre le contrôle de votre système d'impression. Choisissez un mot de passe complexe pour la page d'administration immédiatement après avoir installé votre matériel. Les systèmes d'impression sont généralement déployés avec un mot de passe par défaut très souvent connu des hackers. C'est pourquoi les administrateurs informatiques doivent impérativement définir un mot de passe pour chacun des matériels d'impression de votre espace de travail.

Authentification utilisateur

Assurez-vous que votre MFP accepte uniquement les travaux d'impression soumis par les collaborateurs autorisés à utiliser le matériel. Configurez-le de façon à ce que les utilisateurs soient obligés de s'authentifier avant de pouvoir imprimer un document. L'authentification utilisateur peut être activée via la plateforme d'administration du système d'impression. Dans le cadre de votre stratégie de sécurité, vous devez impérativement restreindre l'accès aux seuls utilisateurs approuvés et ainsi empêcher les impressions non autorisées et les attaques malveillantes.

Configurez un accès contrôlé et sécurisé

Assurez-vous que l'accès au matériel d'impression est sécurisé pour que seuls les utilisateurs autorisés puissent utiliser les fonctionnalités du matériel.
N'accordez pas non plus aux visiteurs un accès temporaire à vos systèmes d'impression. Si les visiteurs ont besoin d'effectuer des impressions, fournissez-leur un appareil qui n'est pas connecté au réseau de votre organisation.

Désactivez les fonctionnalités d'impression inutilisées

Utilisez uniquement ce dont vous avez réellement besoin. Désactivez tous les autres services réseau et services d'impressions locaux afin de réduire autant que possible le risque d'attaque. Après avoir identifié les protocoles que vous utilisez réellement dans votre installation, désactivez tous les services inutiles. Par exemple, si vous utilisez le protocole IPP, vous n'avez pas besoin de laisser le port 9100 associé au service d'impression Raw ouvert. Si vous imprimez uniquement via le réseau local, il n'est pas nécessaire d'activer les fonctionnalités de points d'accès WiFi/AirPrint du matériel d'impression.

Sécurité réseau

Internet peut présenter des risques. Assurez-vous que vos systèmes d'impression ne sont pas directement reliés à l'Internet public afin d'éviter les impressions parasites lancées par des personnes externes à l'entreprise . Vous limiterez ainsi les risques d'attaques plus pointues. Ce conseil peut paraître évident, mais en ce moment même, des dizaines de milliers d'imprimantes sont directement accessibles sur des adresses IP routées publiquement. Vous pouvez renforcer la sécurité de votre réseau interne en utilisant le filtrage des adresses IP ou MAC afin de n'accorder l'accès aux matériels qu'aux seuls postes de travail autorisés.

Sécurité physique

Il peut être plus simple pour un intrus d'accéder physiquement aux imprimantes et aux MFP que d'accéder aux serveurs ou aux postes de travail, et il ne faut que quelques secondes pour lancer un travail d'impression malveillant à partir d'une clé USB. Pour contrer ce type d'attaques, contrôlez l'accès par authentification ou désactivez tous les ports physiques afin d'éviter toute impression non autorisée via les ports USB (en façade et à l'arrière), le port parallèle, le NFC ou le Bluetooth.

Ne placez pas les systèmes d'impression à proximité de lieux publics, assurez-vous que la maintenance des matériels est effectuée uniquement par le personnel autorisé, et formez vos employés à approcher les personnes suspectes ou inconnues.

Ne laissez pas de documents confidentiels sur le matériel. Activez la fonction de libération d'impression sécurisée (également appelée « rétention impression » ou tout simplement « impression sécurisée ») qui nécessite un mot de passe ou un badge d'identification pour libérer un document.

Mises à jour du firmware

Au cours de ces dix dernières années, les systèmes d'impression, qui n'étaient que des machines dotées d'électronique, ont évolué et sont devenues de véritables systèmes informatiques autonomes. Il est donc essentiel de les traiter comme tout autre équipement de votre système informatique : assurez-vous de toujours installer les derniers correctifs de sécurité ainsi que les dernières mises à jour du firmware.

La version la plus récente est toujours la plus stable et la plus sécurisée. Elle garantit que votre matériel utilise les dernières fonctionnalités de sécurité et les derniers systèmes de protection en date. Planifiez un rendez-vous régulier à une date fixe pour déployer les mises à jour du firmware ou installez-les dès qu'elles sont disponibles.

Contrôle des tâches effectuées

Que se passe-t-il en cas de violation de sécurité ou d'activité suspecte détectée au sein du réseau de votre organisation ? Les journaux des travaux effectués peuvent être utiles pour garder une trace numérique des tentatives d'intrusion telles que des travaux d'impression malveillants (n'oubliez pas d'activer l'authentification utilisateur).

L'administrateur informatique peut également activer les notifications par e-mail afin d'être informés en cas de problème critique et de violation de sécurité.

Les matériels d'impression en fin de vie

Ne vous contentez pas de vous séparer de vos matériels d'impression en fin de vie. Des hackers peuvent en effet mettre la main sur ces matériels et accéder aux informations stockées sur le disque dur ou la mémoire non volatile (NVRAM). Si le matériel a été intégré au réseau de l'organisation, il peut contenir des informations sensibles. Lors de la mise hors service, veillez à bien effacer les données contenues dans la mémoire et les disques durs. Si le matériel doit être renvoyé au fournisseur, assurez-vous que toutes les informations confidentielles sont écrasées avant que le matériel ne quitte vos locaux.

Cryptage des données

Vos données sont précieuses. Lorsque le cryptage n'est pas activé, chaque document imprimé sur un système d'impression réseau est transmis en clair, permettant ainsi à toute personne « d'intercepter » les travaux d'impression. Les administrateurs informatiques ont généralement deux possibilités pour activer la protection des données en transit : TLS/SSL (Transport Layer Encryption) et IPSec, offrant le cryptage de l'ensemble du trafic réseau.

Si vous avez besoin d'envoyer des fichiers confidentiels vers des domaines non sécurisés, utilisez le protocole S/MIME pour crypter les e-mails de bout en bout ou utilisez le cryptage des documents PDF avec un mot de passe complexe. Afin de protéger les documents stockés sur le matériel d'impression, activez la fonctionnalité de cryptage du disque dur.

Glossaire

Authentification
Identification unique, généralement réalisée en utilisant deux informations, comme un nom d'utilisateur et un mot de passe.

Ports
Les ports sont utilisés par les matériels connectés en réseau (ordinateurs, serveurs, imprimantes, etc.) pour communiquer entre eux (p. ex., un poste de travail connecté à une imprimante). Les ports ouverts non protégés et les services peuvent être utilisés comme vecteurs d'attaque pour charger un programme malveillant, par exemple.

Protocoles
Un protocole réseau est un ensemble de règles et de formats permettant aux systèmes informatiques d'échanger des informations. Dans le contexte d'un réseau, par exemple, TCP/IP et TLS/SSL sont des protocoles.

Transport Layer Security (TLS/SSL)
Technologie qui crypte les données lorsqu'elles sont transportées ou transférées d'un appareil à un autre afin d'éviter tout espionnage. TLS/SSL est couramment utilisé pour les sites Web, mais peut également être utilisé pour protéger d'autres services.

Internet Printing Protocol (IPP)
Protocole d'impression réseau permettant de gérer les fonctionnalités d'authentification et la gestion des files d'attente des travaux d'impression. IPP est pris en charge et activé par défaut sur la plupart des imprimantes et MFP modernes.

Adresses IP
Chaque appareil connecté à Internet doit disposer d'un numéro unique (adresse IP) pour se connecter à d'autres appareils. Il existe actuellement deux types d'adresses IP : IPv4 et une version plus récente appelée IPv6.

IPSec (Internet Protocol Security)
Une suite de protocoles visant à sécuriser les communications du protocole Internet (IP) sur la couche réseau. IPsec inclut également des protocoles pour mettre en place des clés de cryptage.

S/MIME (Secure/Multipurpose Internet Mail Extensions)
Un ensemble de spécifications pour sécuriser les e-mails. Le protocole S/MIME (Secure/Multipurpose Internet Mail Extensions) repose sur la norme MIME qui est très largement utilisée pour renforcer la sécurité à l'aide du cryptage et des signatures numériques.

Adresses MAC
L'adresse MAC (Media Access Control) d'un appareil est un identifiant unique attribué à une carte réseau. Cela signifie qu'un appareil connecté au réseau peut être identifié distinctement par son adresse MAC.

Filtrage par adresses IP ou MAC
Les adresses IP et MAC sont des numéros uniques utilisés pour identifier les appareils sur Internet (IP) ou sur un réseau local (MAC). Le filtrage permet de comparer les adresses IP et MAC à une liste d'adresses approuvées avant d'autoriser les appareils à se connecter à votre réseau.

Services réseau
Les services réseau facilitent le fonctionnement d'un réseau. Ils sont généralement fournis par un serveur (qui peut exécuter un ou plusieurs service(s), défini en fonction des protocoles réseau utilisés. Ces services incluent par exemple le système de noms de domaines (DNS), le protocole de configuration dynamique des hôtes (DHCP) et le protocole de voix sur IP (VoIP).

Liste Blanche
Une liste blanche est une liste exclusive de personnes, d'entités, d'applications ou de processus bénéficiant d'autorisations ou de droits d'accès spéciaux. Concrètement, cela peut être une liste des membres du personnel et de leurs droits d'accès aux bâtiments, au réseau et aux ordinateurs. En termes informatiques, une liste blanche peut définir les applications et les processus pouvant accéder aux données stockées dans des endroits sécurisés.

DoS/DDoS
Une attaque par déni de service (« Denial of Service », ou DoS) est une attaque qui bloque ou perturbe le fonctionnement d'un appareil ou d'un réseau. Une attaque par déni de service distribué (« Distributed Denial of Service », ou DDoS) est une attaque DoS qui utilise plusieurs systèmes d'attaque afin d'amplifier le trafic réseau, ce qui peut perturber voire totalement paralyser les systèmes ou réseaux ciblés.

Hameçonnage
L'hameçonnage est une pratique frauduleuse consistant à envoyer des e-mails en se faisant passer pour une entreprise réputée afin d'inciter le destinataire à révéler des informations personnelles.

Attaque par usurpation
Une attaque par usurpation est une attaque au cours de laquelle une personne usurpe l'identité d'un autre appareil ou d'un autre utilisateur sur le réseau pour lancer des attaques contre les hôtes du réseau, voler des données, répandre des programmes malveillants ou contourner les restrictions d'accès.

Attaque par interception
Une attaque par interception est une attaque où le hacker se place entre deux parties qui pensent être connectées directement et communiquer en privé. Le hacker peut intercepter les échanges et peut également altérer la communication entre les parties.

Programme malveillant
Un programme malveillant peut être décrit comme un logiciel indésirable qui s'installe sur votre système sans votre consentement. Il peut se fixer à un code fiable et se propager ; il peut se cacher dans des applications ou se répliquer sur Internet.

Fonctionnalités de sécurité de Sharp

Sharp fournit une suite de fonctionnalités de sécurité intégrées afin d'aider les entreprises à protéger leurs informations et leurs documents contre une multitude de menaces.

Les dernières gammes de MFP A4* et A3** de Sharp sont les plus sécurisées de la marque à ce jour. Sharp offre une approche globale et unique de la sécurité, en vous proposant les outils nécessaires pour contrôler et gérer la sécurisation de votre politique d'impression. Protégez ainsi vos informations confidentielles, qu'elles soient imprimées, copiées, numérisées, faxées, stockées ou partagées sur le réseau.

De la sécurité des réseaux, qui couvre tous les réseaux d'entreprise et tous les périphériques connectés, à la sécurité des matériels d'impression eux mêmes pour contrôler et suivre les accès, en passant par la sécurité des documents, qu'il s'agisse de documents physiques ou numériques, Sharp a une solution simple à vous proposer.

Pour plus d'informations, visitez notre site internet et téléchargez les livres blancs :

- La sécurité des réseaux
- La sécurité des documents
- La sécurité des documents sortants
- Conformité-RGDP

Cette approche globale de la sécurité permet à Sharp de vous accompagner dans votre démarche de mise en conformité aux dernières réglementations de sécurité, notamment le Règlement Général sur la Protection des Données (RGPD).

Contactez-nous sans plus attendre pour plus de détails sur les exigences règlementaires relatives à la sécurité de vos données.
https://www.sharp.fr/cps/rde/xchg/fr/hs.xsl/-/html/solutions-documentaires-contacter.htm

* modèles A4, MXC303W, MXC304W, MXB356W, MXB456W
** modèles A3 : MX6071, MX6051, MX5071, MX5051, MX4071, MX4061, MX4051, MX3571, MX3561, MX3551, MX3071, MX3061, MX3051, MX2651. MXM6071, MXM5071, MXM4071, MXM4051, MXM3571, MXM3551, MXM3071, MXM3051, MXM2651.

www.sharp.fr

SHARP

Be Original.