Sécurité des documents sortants.

Protéger les documents imprimés et numérisés

www.sharp.fr

SHARP
Be Original.

Sommaire

Introduction

La nécessité de protéger les documents qui sont générés physiquement ou électroniquement à partir des MFP et des imprimantes est un aspect souvent négligé de la sécurité de l'information.

Sharp définit la sécurité des documents sortants comme la sécurité liée aux sorties papier et aux documents scannés générés à partir de systèmes d'impression. Cette catégorie inclut tous les documents imprimés et les images électroniques des informations en transit entre un ordinateur et un matériel d'impression (y compris l'impression via des serveurs d'impression dédiés), la numérisation (y compris la numérisation vers un dossier, la numérisation vers un e-mail, la numérisation vers le Cloud, la numérisation vers un disque dur) et le fax.

Le présent livre blanc se décompose comme suit :

- **Le contexte**
  Ce chapitre décrit pourquoi la gestion des documents sortants est un aspect souvent négligé de la sécurité de l'information. Ce chapitre souligne également les vulnérabilités potentielles dont tout administrateur informatique doit avoir conscience, parmi lesquelles :

  - Le nombre croissant d'organisations qui consolident leurs parcs de MFP/d'imprimantes ,
  - Le nombre croissant d'utilisateurs connectés, qui doivent tous être identifiés et gérés ;
  - Le nombre croissant de documents qui sont générés et qu'il est nécessaire de contrôler ;
  - L'absence d'outils permettant de suivre l'ensemble des tâches effectuées sur un matériel d'impression et la création de rapports d'analyses.

- **La problématique**
  Ce chapitre s'intéresse aux défis en matière de gestion des documents sortants auxquels peuvent être confrontés les responsables informatiques, les utilisateurs finaux et la direction des entreprises. Ces défis comprennent la gestion des accès utilisateurs, le suivi de l'activité des utilisateurs, l'établissement de rapports d'activité, l'accès à l'impression depuis des périphériques mobiles, la numérisation des documents vers des destinations multiples et la transmission de documents par fax à l'extérieur de l'organisation.

  Ce chapitre fournit également quelques données de recherches qui montrent la complexité de ce sujet et l'étendue des problématiques.

- **La solution**
  Ce chapitre présente comment la gamme de produits Sharp (solutions logicielles) ainsi que des bonnes pratiques qui peuvent vous aider à créer un environnement sécurisé et empêcher tout accès non autorisé aux systèmes d'impression, ainsi qu'aux documents (y compris les images électroniques de documents), copies, fax, numérisations et impressions qu'ils produisent et qu'ils stockent.

Ce chapitre décrit comment Sharp peut vous accompagner en vous aidant à :

- Choisir la solution adaptée pour répondre à vos besoins et mettre en place les fondations solides de votre politique d'impression sécurisée : une solution de gestion des matériels d'impression permettant de contrôler l'accès, appliquer des règles d'impression, limiter les fonctionnalités accessibles et garantir un suivi et un enregistrement précis de tous les documents qui sont générés.

Contexte

Lorsque les entreprises recensent les risques en matière de sécurité des données, elles ne considèrent que rarement, voire jamais, les MFP et les imprimantes réseau comme une faille protentielle – et encore moins les documents imprimés.

D'après le cabinet d'études Quocirca, 60 % des organisations ont été confrontées à au moins une violation des données liée à des habitudes d'utilisation des matériels d'impression non sécurisées. La menace est réelle aussi bien pour les petites entreprises que pour les grandes[1]. Cependant, même si vous déployez des solutions visant à protéger vos données contre les pirates informatiques ou les cybercriminels, cela ne suffit pas toujours.

Certaines des violations les plus courantes sont aussi simples que la récupération d'un document imprimé par la mauvaise personne. Si des documents sensibles sont oubliés au niveau d'un système d'impression pendant trop longtemps, n'importe qui peut les récupérer et utiliser les informations à son profit.

56 % des entreprises ne prennent pas en considération les imprimantes dans leur politique de sécurité des périphériques.[2]

Si vous réfléchissez du point de vue d'un « voleur » potentiel, le bac de sortie est de loin la cible la plus facile si vous voulez voler des informations confidentielles. Par conséquent, un défi souvent sous-estimé pour les administrateurs informatiques est de s'assurer que les documents imprimés ne sont pas laissés sans surveillance sur un matériel d'impression non sécurisé, où ils pourraient tomber dans de mauvaises mains.

Toutefois, chaque organisation moderne qui souhaite garantir la sécurité des documents sortants est confrontée chaque jour à des défis plus nombreux, pour un certain nombre de raisons :

1. **Des parcs de matériels de plus en plus importants**
   Le nombre d'organisations qui consolident leur parc de MFP et d'imprimantes est en augmentation, et les entreprises recherchent l'unification et la standardisation. Ceci fait apparaître un certain nombre de défis en raison du manque d'outils permettant de contrôler les MFP et les imprimantes :

   - Fonctionnalités accessibles ;
   - Données sortantes ;
   - Sécurité réseau.

2. **Nombre d'utilisateurs connectés (en réseau)**
   Dans certaines organisations, le nombre d'employés peut être élevé, et atteindre des centaines d'utilisateurs, qui effectuent des impressions sur une dizaine jusqu'à plus d'une centaine de matériels. À cela s'ajoute le nombre croissant de règlementations relatives à la sécurité, telles que le RGPD, et les défis peuvent être considérables en ce qui concerne les aspects suivants :

   - Authentification utilisateur ;
   - Gestion des comptes utilisateurs (y compris le contrôle du nombre d'utilisateurs connectés) ;
   - Intégration des utilisateurs aux systèmes bureautiques existants ;

- Les limitations relatives à la façon dont les organisations peuvent gérer les données à caractère personnel dans leurs systèmes, telles que la suppression des données des utilisateurs qui en feraient la demande à des fins de conformité au RGPD.

3. **Nombre important de documents sortants à contrôler**
   Le nombre sans cesse croissant d'utilisateurs et le nombre moyen de pages imprimées par utilisateur signifient qu'un nombre important de documents sortants doivent être contrôlés :

   - Documents copiés ;
   - Documents imprimés ;
   - Documents numérisés ;
   - Documents transmis par fax ;
   - Documents imprimés via des smartphones et des tablettes (impression mobile / Bring Your Own Device (BYOD) – « Apportez votre équipement personnel de communication » - français).

4. **Absence d'outils de contrôle**
   De façon générale, il existe un manque d'utilisation d'outils capables de suivre de façon précise tous les documents sortants et d'établir des rapports d'analyses.

Problématique

La sécurité des documents sortants devrait être considérée comme l'une des préoccupations principales de toute entreprise moderne qui utilise des MFP et des imprimantes.

Fournir les bons outils

Les analystes soulignent la nécessité de mettre en œuvre des outils et des mesures permettant de gérer de multiples fichiers imprimés, sur de multiples matériels d'impression, au profit de multiples utilisateurs.

Sécuriser l'accès aux documents sortants

Le défi pour chaque administrateur informatique consiste à savoir comment gérer plusieurs comptes et utilisateurs enregistrés dans le réseau de l'entreprise. Plus le nombre d'utilisateurs est élevé, plus la charge de travail de l'administrateur informatique est importante. Il complique également le processus de gestion des utilisateurs ainsi que l'ensemble des activités des utilisateurs liées aux documents sortants, telles que la copie, l'impression, la numérisation et la transmission par fax. Le défi est donc de savoir comment gérer efficacement la sécurité des documents sortants.

Certaines des solutions les plus connues, telles que les codes PIN, l'identifiaction par identifiant/mot de passe, les badges sont des méthodes efficaces pour protéger les documents sortants. Elles peuvent toutefois représenter un véritable cauchemar pour l'administrateur informatique si elles sont mal mises en œuvre et/ou mal gérées. Cela est d'autant plus vrai que de nombreux administrateurs informatique cherchent également à connecter les matériels à des systèmes existants, tels que des comptes utilisateurs Microsoft.

Nombre important de documents et impressions laissées sans surveillance

Les documents sortants sont des documents papier traditionnels qui sont imprimés ou copiés sur les matériels, des documents électroniques transmis aux MFP/imprimantes par le biais du réseau d'entreprise, ou encore qui sont envoyés à l'aide des fonctions de numérisation et de fax.

De nouvelles règlementations, telles que le RGPD, ont également fait apparaître un ensemble de questions sur la façon de protéger les impressions laissées sans surveillance, et la mesure dans laquelle les informations personnelles qu'elles contiennent sont réellement sécurisées.

Comprendre les risques

Afin de protéger efficacement les données, il est important de bien comprendre les risques que présentent les différents usages :

- **Copie**
  Méthode la plus populaire de partage des documents dans les années 1980 et 1990, la copie a de nos jours été supplantée par l'impression. Pour autant, la copie demeure un domaine clé à contrôler via les systèmes d'impression, particulièrement pour les documents sensibles.

- **Impression**
  De nos jours, l'impression est évidemment une méthode très courante de transmission des documents d'entreprise. Toutefois, il existe de nombreux risques lorsque l'impression n'est pas contrôlée ou n'est pas régie de façon centralisée. Ces risques comprennent :

  - Accès non sécurisé et non contrôlé aux systèmes d'impression, ainsi qu'aux fonctionnalités et données qu'ils contiennent, par exemple : données du disque dur ;
  - Accès libre aux documents imprimés qui permet à tous les employés/utilisateurs (et même les visiteurs, éventuellement) d'accéder à des documents laissés sans surveillance ;
  - Une incapacité à suivre les activités des utilisateurs et à les consigner dans des

rapports, c'est-à-dire qui a imprimé quoi pendant une période définie ;
- Une incapacité à suivre et à empêcher les violations des données utilisateur, ce qui pourrait donner lieu à des amendes/dépenses importantes liées à des règlementations strictes en matière de sécurité, par exemple le RGPD ;
- Une incapacité à suivre les utilisateurs itinérants et l'impression depuis des périphériques mobiles, tels que des smartphones et des tablettes.

- **Numérisation**
  La numérisation peut complexifier le processus de sécurité, car les documents peuvent être numérisés non seulement vers des dossiers réseau et des e-mails, mais aussi vers des systèmes externes basés sur le Cloud. Il existe également les risques suivants :

  - Numérisation de documents d'entreprise sensibles vers des destinations externes, c'est-à-dire numérisation vers des adresses de messagerie électronique personnelles plutôt que professionnelles ;
  - Numérisation vers divers dossiers, autres que les dossiers réseau ou dossiers personnels d'entreprise, sans approbation de l'administrateur informatique ;
  - Numérisation sans indexation, ce qui pourrait causer de graves problèmes pour la recherche et l'audit des documents numérisés et l'audit de l'activité liée à la numérisation (documents numérisés et destinations de numérisation).

- **Télécopie**
  À l'instar de la numérisation, la transmission par fax pourrait représenter un maillon faible potentiel de la stratégie de sécurité des documents sortants de l'entreprise. Quelle que soit la méthode de transmission - transmission par fax analogique ou envoi de fax par messagerie électronique – les documents faxés sont exposés au même niveau de violations de sécurité que les documents numérisés.

- **Impression mobile – Bring Your Own Device (BYOD) (Apportez votre équipement personnel de communication)**
  La mobilité est considérée par de nombreux cabinets d'études comme l'un des piliers de l'impression dans le futur. Elle confronte toutefois l'entreprise à des défis, qui portent sur la façon d'intégrer les solutions d'impression mobile dans une organisation ou sur la façon de suivre et de gérer de façon précise les activités des utilisateurs itinérants. En outre, la façon dont une stratégie d'impression mobile s'intègre dans la stratégie globale de l'organisation soulève des questions importantes. Malheureusement, de nombreuses entreprises ne reconnaissent pas que la mobilité des employés est une tendance forte ou une véritable nécessité pour l'entreprise. Dès lors, la nécessité d'une sécurité des documents en sortie est souvent négligée dans ce domaine.

- **Suivi et reporting**
  Il existe un réel problème de sécurisation des différents canaux de création de documents au sein des entreprises, mais aussi la façon dont elles suivent et enregistrent l'ensemble documents sortants.

  Il est important que le rapport d'audit soit également précis et sécurisé :

  - Qui bénéficie d'un accès ?
  - Les données sont-elles exactes ?
  - Peuvent-elles être supprimées ?
  - Qui gère le système ?

Recommandations

Il est essentiel de comprendre que la sécurité des documents sortants ne constitue qu'un des nombreux aspects de la sécurité, qui peuvent varier d'une organisation à une autre.

Certaines entreprises peuvent décider que leurs mesures de sécurité réseau seront suffisantes si elles sont prises au sérieux et mises en œuvre avec soin. Toutefois, à mesure que leur activité croît, le nombre de documents générés augmente lui-aussi, de même que les défis associés en matière de sécurité.

Cela exige une approche plus étendue de la sécurité dans laquelle non seulement le réseau est sécurisé, mais aussi tous les documents sortants et informations connexes qui sont générés et partagés à l'extérieur de l'organisation.

En d'autres termes, il est essentiel de sécuriser le réseau et les périphériques connectés. La sécurité des documents sortants constitue une mesure logique d'amélioration de votre sécurité réseau, non seulement dans les grandes entreprises, mais aussi dans les PME en forte croissance.

Utiliser des solutions de gestion documentaire (telles que l'une des solutions de gestion des impressions optimisée ou de numérisation optimisée de Sharp) vous aidera à :
-sécuriser l'ensemble des documents sortants
-intégrer vos matériels aux systèmes existants (c'est-à-dire Windows)
-déployer rapidement une politique d'impression et de numérisation sécurisée.

Le contrôle constitue le facteur le plus important dans la sécurité des documents sortants, car vous pouvez mesurer puis sécuriser tout ce que vous contrôlez. Nos systèmes vous offrent un contrôle total sur chaque information ou document sortant : copie, impression, numérisation et fax.

Grâce à son intégration transparente à votre parc d'impression existant, la gestion des documents en sortie vous permet d'économiser un temps précieux. Par exemple, importer tous les utilisateurs par le biais d'un protocole LDAP (Lightweight Directory Access Protocol) est simple et rapide. Vous pouvez ajouter, identifier et intégrer tous les utilisateurs dans le système en quelques secondes. En outre, tous les identifiants utilisateur sont transférés à l'aide du protocole TLS (Transport Layer Security) afin de réduire les risques d'interception.

Toutefois, les véritables atouts d'un système de gestion documentaire, sont les fonctionnalités avancées qui facilitent considérablement la vie de des administrateurs et des utilisateurs :

- **Authentification utilisateur**
  Pour contrôler l'accès à un matériel d'impression, l'authentification utilisateur est la première mesure à mettre en place ainsi que l'une des plus importantes. Des solutions offrent plusieurs façons d'identifier l'utilisateur et de lui accorder l'accès aux matériels connectés. De nos jours, la méthode la plus rapide et la plus populaire est l'identification par badge. Ces derniers stockent l'ensemble des informations à caractère personnel, et l'authentification s'effectue à l'aide d'un lecteur de badges installé sur le matériel. Les administrateurs informatique ont également la possibilité d'utiliser un certain nombre de méthodes d'authentification alternatives, telles que les codes PIN, les ouvertures de session avec saisie d'un identifiant et mot de passe, ainsi que les lecteurs biométriques.

  Il est également possible d'utiliser les badges existants que vous utilisez peut-être déjà dans votre entreprise pour l'accès aux locaux, à certains services ou à des salles protégées. Il existe de nombreux standards de badges et de lecteurs de badges qui utilisent différentes fréquences et méthodes de communication. Nous vous invitons donc à contacter nos consultants en solutions, qui vous aideront à choisir le système adapté à votre entreprise.

- **Sécuriser la file d'attente d'impression**
  Lorsque l'impression d'un document est initiée via un ordinateur selon la méthode habituelle, la communication entre le pilote de l'ordinateur et la gestion des documents sortants commence. Seuls les utilisateurs enregistrés peuvent imprimer sur le système et ils peuvent le faire uniquement depuis les matériels autorisés qui ont été configurés à l'aide du logiciel nécessaire. L'utilisateur transmet la tâche au serveur de gestion des documents sortants et, lorsqu'il se connecte au matériel (à l'aide d'un badge, d'un code PIN ou après ouverture de session avec la saisie d'un identifiant et d'un mot de passe), le système l'identifie comme un utilisateur enregistré ayant l'autorisation d'imprimer.

- **Rétention d'impression**
  Disposer d'une file d'attente sécurisée et d'une mise en attente des tâches sur un serveur offre un autre bénéfice important : celui de vous permettre de profiter de la fonctionnalité de rétention d'impression (également appelée impression suivie) depuis n'importe quel matériel connecté. L'utilisateur final peut donc imprimer depuis n'importe quel matériel – situé dans un autre service, à un autre étage ou même dans un autre bâtiment (s'il se trouve sur le même réseau) – ou depuis tout emplacement où le système de gestion des documents sortants est installé.

84 % des organisations désignent la sécurité comme leur priorité numéro un jusqu'en 2025, et l'expertise en matière de sécurité constituera le principal critère de sélection des fournisseurs pour 58 % des organisations.[3]

La rétention d'impression signifie également moins de périodes d'indisponibilité des systèmes d'impression pour votre entreprise. Lorsque l'un des matériels d'impression est en panne ou en cours de maintenance, il vous suffit de vous rendre au matériel disponible le plus proche pour libérer vos travaux d'impression.

- **Suppression automatique des tâches**
  Un défi supplémentaire pour les administrateurs informatique est le grand nombre de documents qui sont stockés temporairement, dans l'attente de leur sortie ou de leur indexation. Grâce à une fonction de suppression automatique des tâches, les administrateurs informatiques peuvent définir une politique de conservation des documents. Par exemple, si un document a été imprimé à 8h00 et n'a pas été sorti sur l'appareil dans un délai de 24 heures, il sera automatiquement supprimé de la file d'attente du serveur. Cette fonctionnalité est entièrement configurable et dépend des besoins de chaque organisation.

- **Élimination des impressions en double**
  Un autre avantage offert par la mise en œuvre de solutions de gestion des documents sortants est l'élimination des impressions en double. Après authentification et ouverture de session sur le matériel de leur choix, les utilisateurs peuvent visualiser la liste complète des fichiers soumis. Ils peuvent facilement voir si un document a été envoyé plusieurs fois et décider lesquels imprimer et lesquels supprimer. De plus, les utilisateurs peuvent décider d'imprimer et de supprimer un document de la file d'attente, ou de l'imprimer et le conserver le document dans la file d'attente pour une prochaine réimpression.

- **Numérisation, transmission par fax et copie sécurisées**
  La gestion des documents sortants vous permet de contrôler l'ensemble des fonctionnalités offertes par le matériel. Les opérations de copie, de numérisation et de transmission par fax sont contrôlées via le même accès utilisateur au matériel, et chacune de ces opérations peut être suivie en conséquence. En outre :

  - Pour communiquer de façon sécurisée, les matériels Sharp utilisent le protocole TLS pour SMTP et le chiffrement d'e-mails

S/MIME afin de garantir des communications par e-mail sécurisées.
- Le composant d'interface réseau LAN du contrôleur du MFP est totalement isolé de la ligne téléphonique RTC du fax. Ceci empêche les attaquants potentiels d'avoir accès aux systèmes internes du MFP ou au réseau local.

- **Suivi et reporting**
  Pour de nombreuses organisations, le suivi et le reporting sont les critères les plus importants. Avec un système de gestion des documents sortants, toutes les activités sont suivies. Que vous réalisiez une impression, une numérisation, une copie ou une transmission par fax, toutes vos tâches seront enregistrées dans le système. Des rapports détaillés peuvent être générés en fonction de votre compte personnel, du service ou d'un compte client pour la refacturation.

- **Suppression des données utilisateurs conformément au RGPD**
  L'Article 17 du RGPD fournit des instructions détaillées sur la gestion des informations personnelles. Ceci inclut « le droit d'obtenir, du responsable du traitement, l'effacement, dans les meilleurs délais, de données à caractère personnel de la personne concernée, et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais ». Grâce au système de gestion documentaire de Sharp, ce n'est pas un problème. Ce système vous permet de supprimer toutes les données utilisateurs et de vous conformer à ces règlementations particulièrement strictes. Même lorsque les données utilisateurs ont été supprimées, les administrateurs informatiques peuvent toujours utiliser certaines statistiques et informations relatives aux impressions pour générer des rapports d'utilisation.

- **Impression mobile**
  Il s'agit d'un concept très simple : les utilisateurs peuvent imprimer à l'aide de leur smartphone ou de leur tablette - BYOD (Apportez votre équipement personnel de communication). Les administrateurs informatique peuvent décider quelle application est la plus adaptée pour leur organisation. Les impressions issues de l'application mobile optimisée de Sharp, grâce à sa configuration simple et rapide, peuvent être suivie via la gestion des documents sortants, de sorte que tous les documents imprimés à partir d'un périphérique mobile sont enregistrés dans le système et peuvent être utilisés pour les statistiques et l'élaboration de rapports.

Développer une politique de sécurité encore plus solide

La sécurité des documents sortants joue un rôle très important dans la définition, la création et la mise en œuvre de votre propre politique d'impression sécurisée :

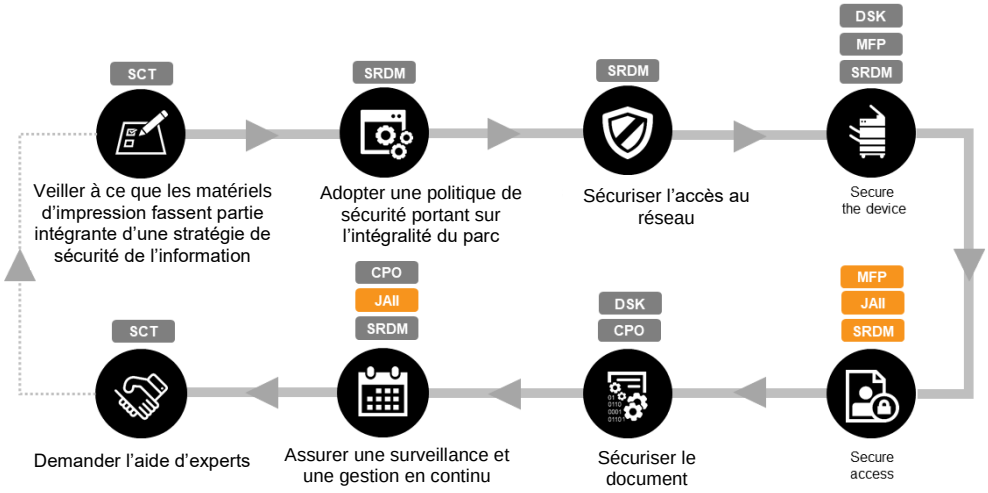
- Les solutions de gestion documentaire optimisées de Sharp sont extrêmement utiles lors de l'application d'une telle politique, principalement car elles contribuent aux étapes de « sécurisation de l'accès » et de « suivi et gestion continus ».

- Ajouter d'autres produits de notre portefeuille, tels que les MFP de Sharp, le kit de sécurité des données (DSK), Sharp Remote Device Manager (SRDM) et Cloud Portal Office (CPO) vous aide à créer un système de sécurité unique, fiable et simple à administrer, qui fonctionne parfaitement, tant pour votre équipe informatique que pour votre entreprise.

Par conséquent, pour mettre en place les niveaux de sécurité les plus poussés, les entreprises devraient travailler avec des fournisseurs qui peuvent non seulement apporter des bénéfices tangibles dans le domaine de la gestion documentaire, mais qui sont également des intégrateurs expérimentés et reconnus.

Sharp possède de nombreuses années d'expérience dans la fabrication de MFP/imprimantes sécurisés, la conception de solutions de gestion documentaire et la mise en œuvre de solutions complexes. Nous sommes donc dans une position idéale pour conseiller et orienter nos clients sur tous les aspects relatifs à la sécurité, y compris les politiques de sécurité d'impression et de sécurité des documents sortants.

Élaboration d’une politique d’impression sécurisée et solutions de gestion documentaire de Sharp



SCT – Équipe de consultants Sharp, **SRDM** – Sharp Remote Device Manager, **DSK** – Kit de sécurité des données, **MFP** – Imprimante multifonctions, **JAII** – Job Accounting II, **CPO** – Cloud Portal Office

Conclusion

Une nouvelle réalité à prendre en compte pour les entreprises est l'exposition potentielle à un risque de vol, des données imprimées, copiées, numérisées ou faxées par un utilisateur.

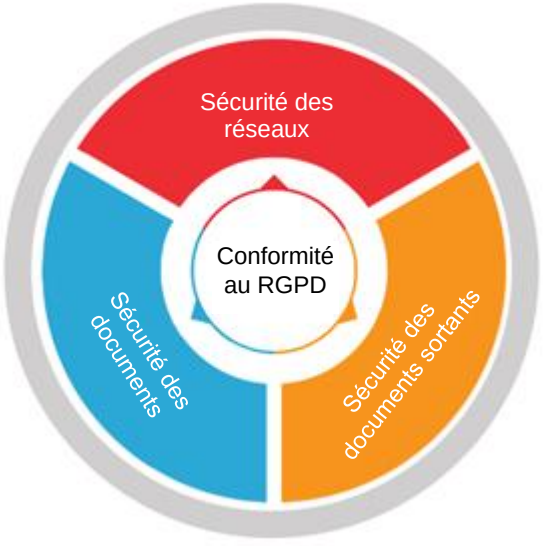
Les entreprises doivent prendre davantage conscience des risques existants à laisser sans protection des copies physiques ou électroniques de documents sensibles. Les enjeux clés sont les suivants :

- La sécurité des documents sortants est essentielle pour toute entreprise moderne, quelle que soit sa taille. Le nombre croissant de documents générés par les entreprises fait naître des défis importants en matière de contrôle de l'environnement informatique. Plus particulièrement, ces défis incluent la gestion du nombre croissant d'utilisateurs, le poids croissant des fichiers, la quantité d'informations partagées, les surcharges réseau et le parc d'imprimantes.

- Un système de gestion des documents sortants vous confère une flexibilité maximale en termes de configuration. Les administrateurs informatiques peuvent non seulement restreindre l'accès à des groupes fermés d'utilisateurs, mais aussi suivre l'ensemble de leur activité sur le MFP, y compris la copie, l'impression, la numérisation et la transmission par fax.

- Sharp est conscient de l'importance que revêt la sécurité dans l'entreprise moderne. Elle offre ainsi une approche à 360 degrés unique de cette question, de la sécurité réseau (qui couvre tous les réseaux d'entreprise et tous les périphériques connectés), à la sécurité des documents sortants décrite dans ce livre blanc, en passant par la sécurité des documents, qui traite de tous les aspects de la sécurité liée aux documents.

Infrastructure de sécurité de Sharp



- Cette approche exhaustive de la sécurité permet à Sharp de vous accompagner dans votre démarche de mise en conformité aux dernières règlementations en matière de sécurité, y compris le Règlement Général sur la Protection des Données (RGPD).

Pour éviter des vulnérabilités potentielles au sein de votre organisation, nous vous invitons à découvrir comment mettre en place d'autres mesures de sécurité en matière de :

- Sécurité des réseaux ;
- Sécurité des documents ;
- Conformité au RGPD.

Pour plus d'informations sur l'ensemble de nos solutions de sécurité, consultez nos autres livres blancs ou la section « Sécurité des informations » de notre site Web : https://www.sharp.fr/cps/rde/xchg/fr/hs.xsl/-/html/information-security.htm

N'hésitez pas à prendre contact avec l'équipe d'experts Sharp pour plus d'informations.

Références

1. « Print 2025: Print Security in the IoT Era » (Print 2025 : La sécurité de l'impression à l'ère de l'IoT), Quocirca, 2018
2. « Annual Global IT Security Benchmark Tracking Study » (Étude annuelle de référence et de suivi sur la sécurité informatique à l'échelle internationale), Ponemon Institute, mars 2015
3. « Print 2025: The future of print in the digital workplace » (L'avenir de l'impression dans l'environnement de travail numérique), Quocirca, 2018

`

www.sharp.fr

SHARP
Be Original.