Zoom sur la sécurité des données
Le MFP* au coeur du RGPD**

Sharp partenaire de votre transformation digitale

www.sharp.fr

SHARP
Be Original.

*MFP : multifonction
**RGPD : Règlement Européen sur la Protection des Données

La sécurité au coeur des préoccupations de Sharp

Sharp reconnu comme l'un des plus grands innovateurs en matière de sécurité des données

Pionnier de la sécurité relative à la gestion électronique des documents

Sharp a reçu la première homologation Critères Communs (Common Criteria Norme ISO 15408) en 2001 pour un MFP.

Le kit de sécurité de Sharp est le premier à avoir obtenu la certification EAL 4.

De plus, nous venons d'obtenir sur notre gamme couleur de dernière génération, la première certification Hard Copy Device Protection Profile (HCD-PP) v1.0 délivrée pour des systèmes multifonctions sur le marché. Ce standard de sécurité remplace la norme IEE P2600.2.

Sharp propose des solutions qui répondent aux besoins quotidiens de ses clients

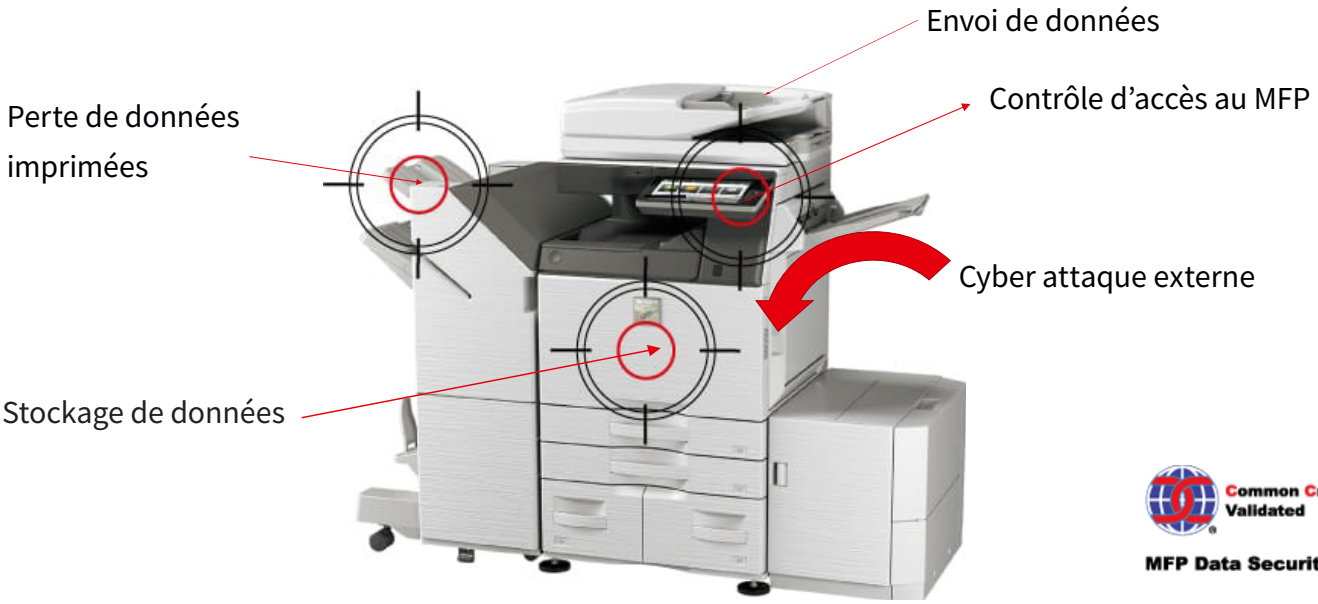
Sharp comprend les objectifs et les enjeux de ses clients et les intègre dès la conception de ses produits :

En effet, Sharp a développé une gamme de MFP intégrant des fonctionnalités de sécurité avancées qui lui permettent d'offrir un niveau de sécurité inégalé. En outre, il existe un large éventail de solutions de gestion du parc administables à distance pour optimiser la productivité mais également la protection des données transitant sur les MFP.

Sharp prend très au sérieux son engagement envers la sécurité informatique de ses clients. Sharp a été le premier fabricant de MFP à recevoir la certification Critères Communs en 2001.

Le MFP au coeur de l'entreprise : "une faille potentielle"

Un système d'impression non sécurisé peut rendre une organisation vulnérable, d'une part parce qu'il est un point d'entrée pour un hacker, d'autre part parce que les documents imprimés et scannés eux-mêmes peuvent être une source de violation de la confidentialité des données.



Common Criteria Validated

MFP Data Security Kit

Les MFP font partie intégrante des processus de management des documents au sein des entreprises, ils peuvent donc constituer «une faille » dans la sécurité du réseau et des informations qui y transitent.

Les entreprises engagent des montants importants pour la protection de leurs données numériques contre les menaces, mais négligent souvent l'un des dispositifs les plus intégrés utilisés aujourd'hui : le multifonction.
Les MFP permettent de copier, imprimer, scanner ou faxer des informations qui peuvent se révéler confidentielles et doivent donc être sécurisées. L'entrée en vigueur de la nouvelle réglementation relative à la protection des données personnelles (RGPD) va exiger des entreprises une protection accrue des données relatives à leurs clients et leurs employés qu'elles possèdent.

Les données qui transitent sur les MFP peuvent être soumises à différents types de menaces :

- Menace physique des données

Les MFP sont souvent situés dans des espaces communs et accessibles à tous, y compris des personnes extérieures à l'entreprise.
Des informations confidentielles peuvent être copiées ou faxées sans autorisation.

- Menace de sécurité réseau

Les données stockées sur un disque dur ou dans la mémoire d'un MFP peuvent être compromises, altérées ou volées si l'accès au réseau n'est pas correctement sécurisé contre les utilisateurs non autorisés.

Les données peuvent également être interceptées lors d'un transfert sur le réseau ou sur Internet, si des mesures de sécurité avancées ne sont pas mises en œuvre.

Des pirates peuvent obtenir des informations confidentielles grâce au « phishing » (tentative d'hameçonnage) , en introduisant un virus sur le réseau ou en détournant un MFP pour lancer une attaque ciblant l'infrastructure interne. La sécurisation du MFP l'empêche d'être utilisé dans le cadre d'une cyber-attaque avancée.

- Des menaces qui engagent l'entreprise

Les entreprises sont légalement responsables de la sécurité des données qu'elle détiennent, où qu'elles se trouvent, y compris dans les dossiers des employés, informations sur les clients, les données de comptes, les informations commerciales etc

Conscient du fait que la gestion sécurisée de l'entreprise et des données en sa possession sont des points clé du succès de ses clients, Sharp a développé une gamme complète de fonctionnalités de sécurité. Celles-ci ont pour but d'aider à protéger les informations et documents d'éventuelles menaces externes ou internes, tout en offrant à ses clients les garanties de conformité avec les exigences légales.

Des solutions Sharp pour garantir la sécurité des données

L'offre de sécurité Sharp

Les MFP sont le point de passage de tous types de documents. Ils peuvent y être copiés, imprimés, numérisés, faxés, envoyés par mail ou stockés sur une clé USB en quelques secondes. Sharp offre en standard de nombreuses fonctionnalités permettant de sécuriser les matériels et les données qui y transitent.

Sharp offre en standard toute une série de fonctionnalités de sécurité sur ses MFP

- l'effacement « intelligent » et paramétrable des données stockées sur le disque dur*1
- la connexion sécurisée et cryptée au réseau, filtrage de l'adresse IP/Mac et contrôle des ports de connexion
- la compatibilité S/MIME : cryptage des scans to email à l'aide de clés informatiques sécurisées ainsi que la signature certifiée du mail
- la compatibilité du Wifi avec les dernières normes (WEP, WPA/WPA2-PSK…) pour sécuriser l'utilisation des périphériques mobiles
- le contrôle de l'utilisation du MFP et rapports d'activités incluant les changements de paramétrages
- la rétention et libération d'impression sécurisée afin d'éviter la perte de documents imprimés
- l'authentification et l'accès au MFP sécurisés

Sharp est reconnu comme l'un des plus grands innovateurs en termes de sécurité et de protection des données.

La grande expérience de Sharp dans la sécurité relative à la gestion électronique des documents nous pousse à développer des solutions toujours plus adaptées aux attentes des clients.
Sharp se veut aujourd'hui être un partenaire de choix dans la transformation digitale de ses clients en apportant toute son expertise au travers de solutions permettant également de s'adapter aux contraintes réglementaires.

En standard ou avec l'option Kit de sécurité Sharp, les MFP Sharp peuvent offrir jusqu'à 4 niveaux de sécurité :

Les modes de sécurité :

1 - Le mode standard offre des fonctionnalités basiques par défaut et disponible sur tous les matériels Sharp.
2 - Le mode sécurité standard, disponible en standard et sur activation, offre un premier niveau de sécurité.
3 - Le mode Kit de sécurité, en option, assure une haute protection des MFPs et des données qui y transitent.
4 - Le mode Kit de sécurité avancé : package complet de toutes les fonctionnalités de sécurité disponibles.*1

*1 pour les matériels équipés en standard ou en option du HDD

Sharp accompagne et propose aux entreprises une multitude de solutions leur permettant d'atteindre les niveaux de sécurité souhaités

Des solutions complémentaires pour garantir la sécurité des données de l'entreprise : le Kit de Sécurité des Données (DSK : Data security Kit)

Le Kit de sécurité des données est la première solution de ce type à obtenir une certification EAL 4. (Common Criterias)

Le DSK protège et contrôle les principaux systèmes et sous-systèmes du MFP (impression, copie, tâches de numérisation et de télécopie, paramètres réseau, composants de mémoire et interfaces utilisateur locales).

La norme de cryptage avancée (AES – algorithme 256 bits) est appliquée à toutes les données du disque dur, SSD, RAM ou mémoire Flash, aidant à prévenir les attaques. Le DSK élimine également les données résiduelles en les écrasant jusqu'à dix fois avec une série de valeurs aléatoires - soit automatiquement à la mise sous tension, soit, automatiquement après chaque impression, copie, fax ou numérisation, ou encore, à la demande de l'utilisateur, selon le paramétrage défini par l'administrateur.

En complément des fonctionnalités de sécurité présentes en standard, le kit optionnel de sécurité offre un très haut niveau de sécurité et de protection des données stockées dans le MFP et notamment :

- Le nettoyage complet de la mémoire après l'utilisation des fonctionnalités de copie, numérisation et impression.

- L'effacement du journal des travaux réalisés.

- La possibilité de l'effacement complet du carnet d'adresses avant restitution du matériel.

- L'interdiction de la fonction « Document filing » ou possibilité de stocker dans le disque dur du MFP.

- La protection contre la copie non-autorisée par impression d'un filigrane invisible empêchant la copie et le scan.

- L'auto diagnostic de l'intégrité du firmware du MFP au démarrage

Signature électronique du firmware.

Le kit de sécurité de Sharp est le premier à avoir obtenu la certification EAL 4

Garantir la conformité avec les normes en vigueur

Aider nos clients dans la conformité avec la loi

L'adoption du Réglement Européen sur la protection des données le 25/05/2018 doit permettre à l'UE de s'adapter aux nouvelles réalités du numérique, fournissant une réglementation de protection des données personnelles collectées et stockées par les entreprises. Toutes les entreprises devront se conformer au RGPD à compter du 25 mai 2018. C'est à dire qu'elles devront garantir la sécurité de toutes les données personnelles de leurs clients et collaborateurs, collectées, utilisées, et stockées. Elles seront également dans l'obligation de consentir aux personnes physiques l'accès, la modification et l'effacement des données personnelles les concernant. En cas de non-respect du texte de loi, les entreprises contrevenantes encourront des amendes pouvant aller jusqu'à 4% du CA annuel ou 20 millions d'euros. Il est donc essentiel de mettre en place toutes les actions permettant de se conformer au RGPD. Sharp accompagne ses clients en mettant à leur disposition des solutions visant à sécuriser l'architecture d'impression autour du MFP.

En quoi les MFP sont-ils concernés ?

Le RGPD concerne les données stockées en ligne mais aussi physiquement. Les données copiées, numérisées, faxées et imprimées sur un MFP peuvent faire l'objet de violation, tout comme les données contenues sur les disques durs des matériels. Les MFPs étant l'un des principaux points d'entrée et de sortie des documents et informations, il est indispensable d'assurer la sécurité des données transitant sur les matériels. Il convient donc de garantir une protection optimale des données sur l'ensemble de la gamme Sharp.

Il y a plusieurs actions relatives à la sécurité autour du MFP, qui, en parallèle d'un plan global mis en place par le client, favoriseront la conformité au RGPD :

- l'authentification sur le MFP et la libération sécurisée par mot de passe des tâches d'impression.
- le cryptage des données transitant depuis ou vers le MFP, à l'aide de clés publiques ou de clés privées plus sécurisées.
- le reporting des connexions et des activités des utilisateurs permettant de contrôler l'accès aux données présentes physiquement ou numériquement sur le MFP.
- la configuration sécurisée des MFP minimisant les risques d'accès non autorisés aux fichiers stockés sur le disque dur, de piratage et d'accès non autorisés aux périphériques installés sur le réseau.
- la certification de l'effacement total et sécurisé des données stockées sur le disque dur des MFP lors de leur reprise.
- l'installation d'imprimantes et de multifonctions ayant la certification Common Criterias Norme ISO15408.

Les équipes commerciales se tiennent à votre disposition pour vous présenter l'offre de complète de sécurité de Sharp

General Data Protection Regulation*

GDPR =RGPD*

L'entrée en vigueur de la nouvelle réglementation sur la protection des données en mai prochain prouve que la sécurité des données n'a jamais été aussi importante pour les entreprises européennes.