Sécurité des réseaux

Sécurisation des matériels de bureau réseau

www.sharp.fr

SHARP
Be Original.

Sommaire

Introduction

Dans un monde de plus en plus connecté, il est plus essentiel que jamais de de sécuriser les informations efficacement dans l'ensemble du réseau de l'entreprise.

Chaque jour, les entreprises sont victimes d'un nombre incalculable de tentatives malveillantes destinées à voler, à modifier illégalement, à intercepter ou à diffuser des documents confidentiels, ou encore à obtenir un accès non autorisé à des réseaux privés et d'entreprise. Ce livre blanc aborde les principaux défis auxquels les entreprises sont confrontées lorsqu'elles cherchent à protéger leur infrastructure informatique, notamment leurs matériels connectés en réseau, tels que les imprimantes et les multifonctions (MFP).

Dans ce livre blanc, nous examinerons :

- **Le contexte**
  Chaque entreprise est confrontée à des défis en matière de sécurité des réseaux. Cependant, les vulnérabilités liées aux MFP et imprimantes réseau modernes sont souvent négligées. Les pirates informatiques et cybercriminels les utilisent comme porte d'entrée des organisations. Ils s'en servent pour voler les données confidentielles stockées sur leurs disques durs et autres périphériques réseau, et causent ainsi des dommages ou pertubations dans leurs activités commerciales. L'impact sur la productivité et la rentabilité peut être énorme.

- **Les problématiques**
  Le risque lié aux MFP et imprimantes non sécurisées est souvent mal compris et ignoré. Parfois, les entreprises manquent tout simplement de l'expertise et des ressources nécessaires pour s'attaquer au problème. Le manque de sensibilisation des utilisateurs engendre de mauvaises pratiques exposant les documents et données au risque d'être compromis. Les entreprises comprennent les étapes à suivre pour définir une politique d'impression sécurisée, mais ce processus peut s'avérer long et complexe.

- **Les recommandations**
  Sharp propose un ensemble de solutions matérielles et logicielles ainsi que les bonnes pratiques pouvant vous aider à créer un environnement d'impression sécurisé. Ceci, dans le but de prévenir les accès non autorisés et les attaques ciblant les périphériques connectés au réseau de votre entreprise. Le présent document vous offre des réponses spécifiques aux principaux enjeux de sécurité des données :

  - Les six étapes pour mettre en place et gérer des normes de sécurité d'impression en associant la technologie Sharp et les solutions logicielles optimisées de Sharp.
  - Des fonctionnalités et des réglages « clés en main » disponibles sur tous les périphériques réseau Sharp de la gamme actuelle : protection par mot de passe, écrasement des données, chiffrement, etc.
  - Des solutions qui vous aident à définir une politique d'impression sécurisée et à gérer vos parcs d'impression simplement et efficacement, comme le logiciel Sharp Remote Device Manager (SRDM).
  - Des fonctionnalités avancées pour MFP, comme le kit de sécurité des données (DSK).
  - Des services disponibles via les experts de Sharp : audit de sécurité, effacement des données en fin de contrat, etc.

Contexte

Au cours des dernières années, il est devenu essentiel de mettre en place un dispositif de sécurité informatique efficace. Toutefois, un domaine clé a été cruellement négligé.

La plupart des organisations soucieuses de leur sécurité ont veillé à ce que leur réseau et leurs ressources informatiques soient protégés par les toutes dernières technologies : installation de pare-feu, application de règles de mot de passe, authentification des utilisateurs, protection des données chiffrées et signées électroniquement, etc.

Les nouvelles technologies comme le cloud et le mobile ont constitué des défis supplémentaires pour les administrateurs informatiques et les responsables de la sécurité. Néanmoins, les MFP et imprimantes intelligentes modernes ont évolué pour inclure de nombreuses fonctionnalités de communication réseau et de stockage de données. En réalité, les systèmes d'impression sont devenus des ordinateurs puissants et intelligents. Selon IDC, près de 53 millions d'imprimantes et de MFP équipent bureaux et foyers d'Europe, la plupart étant connectés à un réseau. Ces systèmes d'impression constituent donc un point d'accès avec une adresse IP et sont aussi vulnérables aux attaques de programmes malveillants et de pirates informatiques que les ordinateurs ou n'importe quel autre périphérique connecté au réseau. Pour cette raison, ils nécessitent les mêmes fonctionnalités de sécurité visant à protéger les données, les communications et les informations.

Par le biais de MFP non sécurisées, les hackers peuvent avoir accès à des ports et à des protocoles non contrôlés et accéder à d'autres périphériques réseau ou encore à des informations sensibles. Les communications et les données stockées sur le disque dur ou la mémoire d'un MFP peuvent être interceptées ou envoyées sans autorisation partout dans le monde. Les périphériques réseau sont aussi vulnérables aux attaques par déni de service (« Denial of Service », ou DoS), qui ont pour but d'empêcher l'accès des ressources réseau aux utilisateurs finaux et ont un impact conséquent sur la productivité de l'entreprise. Ils peuvent également constituer une passerelle pour les attaques de hameçonnage destinées à obtenir des informations confidentielles ou à introduire des virus sur le réseau.

Cela n'est pas une exagération et il s'agit d'une menace bien réelle. Dans une récente enquête d'IDC, plus d'une personne interrogée sur quatre déclarait avoir subi une violation de sécurité informatique importante ayant nécessité des mesures correctives, et plus de 25 % de ces incidents impliquaient un matériel d'impression.[2]

Ne pas protéger ses systèmes d'impression peut avoir des conséquences dramatiques pour une entreprise. Cela peut nuire à sa réputation et à la confiance de ses clients. Une violation de sécurité a notamment pour conséquences :

- Une perte de revenus ;
- Une perte de productivité due à l'impossibilité d'accéder aux données et au réseau ;
- Perte de compétitivité due au vol d'informations ;
- Amendes pour non-conformité réglementaire ;
- Poursuites judiciaires ;
- Utilisation non autorisée des équipements et des ressources réseau.

25 % des violations de la sécurité informatique ayant nécessité des mesures correctives impliquaient un matériel d'impression.[2]

Problèmatique

Le piratage informatique et les cyberattaques sont devenus la « norme », et quels que soient le type ou la taille de votre entreprise, la menace que représentent les programmes malveillants sur vos opérations est réelle – et imminente.

Selon le bureau d'études Quocirca, et aussi surprenant que cela puisse paraître, 63 % des entreprises interrogées admettent avoir subi une ou plusieurs violation(s) de données liée(s) à l'impression[3].

Pourquoi les entreprises n'agissent-elles pas davantage pour lutter contre cette menace ?

Malheureusement, le risque potentiel est souvent négligé en raison d'un manque de compréhension des menaces auxquelles sont exposés les systèmes d'impression connectés au réseau de l'entreprise. De nombreuses entreprises disposent de moyens insuffisants ou ne possèdent pas de systèmes et d'outils permettant de sécuriser les matériels d'impression. Elles manquent souvent de personnel formé, de bonnes pratiques et de procédures de sécurité relatives à l'utilisation des périphériques réseau dans l'entreprise, etc. D'autres utilisent des matériels à des fins professionnelles alors que ceux-ci sont conçus pour un usage personnel et intègrent des fonctionnalités de sécurité limitées.

Certaines PME, notamment, n'ont mis en œuvre aucune mesure de sécurité pour les matériels d'impression et/ou n'ont jamais entrepris d'audit. Quant aux organisations de plus grande envergure, elles peuvent tout simplement manquer de ressources humaines ou d'outils de qualité nécessaires pour mesurer, contrôler et prévenir les cyberattaques sur leurs périphériques réseau et leurs technologies connectées.

De plus, les mauvaises pratiques des utilisateurs représentent souvent un défi de taille pour les administrateurs informatiques, car elles peuvent exposer l'entreprise à des problèmes de sécurité importants. Ces mauvaises pratiques incluent le fait d'imprimer de façon non sécurisée, de laisser

Près de deux tiers des entreprises ont subi une violation de données liée aux systèmes d'impression.[3]

des documents sans surveillance dans les bacs de sortie des MFP / imprimantes, d'imprimer à partir de lecteurs USB non sécurisés, d'imprimer sans chiffrement d'un point de terminaison à un autre point de terminaison, ou de stocker des documents sensibles sur le disque dur de la MFP / de l'imprimante.

Pour de nombreuses organisations, la suppression des données à la fin d'un contrat constitue aussi un véritable casse-tête. Le processus d'impression peut laisser sur le disque dur des MFP / d'imprimantes une copie des données imprimées sur le matériel. Qu'advient-il de ces données à la fin du contrat ?

Malheureusement, la mise en place d'un système de sécurité réseau ou la création d'une politique d'impression sécurisée pour détecter et prévenir tout accès non autorisé à un parc de MFP et d'imprimantes en réseau peut s'avérer complexe et chronophage. Vous devrez très probablement suivre les étapes clés suivantes :

- Evaluer et prévoir les risques potentiels de l'absence d'un système de sécurité réseau.
- Reconnaître l'existence de menaces potentielles et la manière dont elles pourraient porter préjudice à l'infrastructure réseau.

- Comprendre la nature complexe du défi auquel vous faites face, qui variera inévitablement d'une entreprise à l'autre.
- Trouver des ressources internes ou externes pour vous aider à relever ce défi.
- Identifier des outils permettant de contrôler des parcs entiers de MFP / d'imprimantes, de prévenir tout accès non autorisé à vos ressources en réseau, et de vous alerter en cas d'activités suspectes.
- Configurer et tenir à jour un système de sécurité réseau fiable englobant tous les défis auxquels votre entreprise est confrontée.

Recommandations de Sharp

Si tout cela vous a ouvert les yeux sur votre propre sécurité réseau, tant mieux ! Les risques pour votre entreprise ne doivent pas être sous-estimés, mais ne craignez rien, Sharp est à vos côtés.

Notre objectif est de vous expliquer comment mettre en œuvre facilement des mesures de sécurité pour l'utilisation de vos systèmes d'impression dans votre entreprise. Découvrez comment Sharp peut vous aider à comprendre et à renforcer vos niveaux de sécurité réseau en toute simplicité.

Passez à la protection instantanée

Selon les études réalisées par les analystes d'IDC, « Les fournisseurs de technologies de services d'impression et de gestion documentaire mettent l'accent sur la sécurité des matériels d'impression, afin d'empêcher les hackers de pénétrer les réseaux d'entreprise via les matériels d'impression ».[4] Cependant, de nombreuses entreprises négligent ou ne définissent pas encore correctement leurs « réglages de sécurité », ce qui peut les rendre vulnérables aux attaques.

Vous trouverez ci-dessous une liste des fonctionnalités et des réglages de sécurité disponibles « clés en main » sur tous les MFP et imprimantes Sharp, et qui peuvent constituer une « solution rapide ». Tou(te)s peuvent être activé(e)s et désactivé(e)s rapidement ou réglé(e)s par l'administrateur informatique pour modifier les niveaux de sécurité par défaut et fournir un niveau de protection beaucoup plus efficace en fonction de vos besoins métiers spécifiques :

- Réglages d'administration locaux : changement du mot de passe administrateur, accès à la page Web du matériels, sécurisation des opérations à distance.
- Configuration des fonctionnalités de sécurité en mode standard : contrôles des ports, réglages des protocoles, réglage SNMP MIB, filtres d'accès, SSL, S/MIME, IPSEC, IEEE802.1X, activer/désactiver les protocoles d'impression mobile, réglages de service externe, dossier public – serveur adressé au réseau (disque partagé), ID de suivi (impression des informations de suivi), réglages utilisateur, activer/désactiver les solutions de sécurité pour les utilisateurs, suppression automatique des fichiers stockés, suppression de l'intégralité de la file d'attente en cas d'erreur.
- Fonctionnalités de sécurité améliorées (en mode « sécurité standard ») : écrasement des données du disque dur (effacement des données du disque dur) après chaque copie/impression/numérisation/fax, chiffrement des données stockées, protection par mot de passe.
- Dans le même groupe, il existe plusieurs réglages avancés facultatifs. Ces réglages peuvent offrir aux administrateurs informatique un accès aux fonctionnalités de sécurité avancées nécessaires pour les organisations qui requièrent un niveau de sécurité plus élevé, telles que les organisations militaires ou gouvernementales, ou les entreprises souhaitant renforcer au maximum leur niveau de sécurité.

Six étapes simples

En envisageant la sécurité dans une perspective à plus long terme, les six étapes suivantes offrent une méthode structurée pour développer et mettre en œuvre votre propre infrastructure de sécurité réseau.

1. **Sécuriser l'accès au réseau**
   Tous les matériels connectés au réseau doivent être autant sécurisés que le point le plus vulnérable du réseau. Contrôler l'utilisation des ports et des protocoles est donc essentiel à la préservation de la sécurité du réseau. Grâce à une configuration judicieuse, les administrateurs informatique

sont capables de prévenir les activités indésirables et les attaques potentielles sur l'infrastructure. Les techniques garantissant une communication sécurisée entre chaque matériel et le réseau incluent :

- L'utilisation du filtrage IP pour limiter l'accès à des adresses IP spécifiques, ainsi que du filtrage MAC (Media Access Control). Cela permet de protéger votre réseau et vos canaux de communication en autorisant l'accès uniquement à des adresses ou des plages IP spécifiées.
- La désactivation des ports inutilisés (de sorte que seuls les ports utilisés fonctionnent) offre une couche de sécurité supplémentaire et vous donne plus de contrôle sur votre réseau, en prévenant tout accès non autorisé à l'ensemble des ressources connectées.
- La configuration des protocoles IPSec (Internet Protocol Security, pour un échange de données sécurisé et chiffré), TLS (Transport Layer Security, pour la transmission de données chiffrées) et HTTPS (Hypertext Transfer Protocol Secure, pour une communication réseau sécurisée).

2. **Sécuriser le matériel (pour protéger vos données)**
   Il existe deux manières de garantir la sécurité des données stockées sur les disques durs (HDD) de vos MFP et imprimantes :

   - Le chiffrement des données est la procédure ou la fonctionnalité qui chiffre les documents à l'aide d'un algorithme complexe de 256 bits.
   - L'écrasement des données est l'option permettant d'effacer les données présentes sur le disque dur d'un matériel. Il garantit que toutes les données déjà stockées sur le disque et toutes les images électroniques des documents imprimés sont définitivement effacées en étant écrasées jusqu'à 10 fois.

   Sharp propose un service garantissant l'effacement de toutes les données numériques stockées sur un matériel et la destruction du disque dur physique avec PV de recette faisant foi.

3. **Sécuriser l'accès des utilisateurs (par authentification et autorisation)**
   L'une des étapes les plus importantes consiste à contrôler tous les utilisateurs via l'administration de profils configurés avec des droits d'accès spécifiques. Pour cette partie, les principales actions sont les suivantes :

   - L'authentification des utilisateurs : c'est le processus par lequel les administrateurs accordent uniquement des droits d'accès aux MFP et aux imprimantes aux utilisateurs enregistrés. Les administrateurs doivent identifier les utilisateurs soit par authentification locale, en fonction de la liste des utilisateurs locaux, soit par authentification réseau, par le biais du serveur d'authentification.

   - La configuration des profils utilisateurs permet aux administrateurs d'accorder des droits d'accès aux ressources réseau de l'organisation et de contrôler leur utilisation. En fonction des informations d'identification de chaque utilisateur, ils peuvent limiter l'accès à des utilisateurs spécifiques, restreindre l'accès aux fonctions du matériels, ou interdire complètement l'accès. Les administrateurs peuvent également configurer l'accès au matériel via des badges contenant les informations d'identification de l'utilisateur.

4. **Imprimer des données confidentielles en toute sécurité**
   Les documents confidentiels ne doivent être imprimés qu'en utilisant une procédure sécurisée qui prévient tout accès et toute copie non autorisés. En règle générale, lorsqu'un travail d'impression est soumis, il est conservé sur le disque dur du matériel et n'est imprimé qu'après la saisie d'un code PIN par l'utilisateur qu'il a préalablement configuré. Une fois le document imprimé, toutes les données sont automatiquement effacées du disque dur.

5. **Contrôler l'activité du réseau**
   Lorsqu'ils sont correctement mis en œuvre, les outils de sécurité réseau peuvent offrir aux administrateurs informatique un contrôle total sur tous les matériels réseau, directement depuis leur ordinateur professionnel. Ils peuvent ainsi contrôler un parc entier de MFP

et d’imprimantes, identifier et gérer à distance la plupart des menaces de sécurité potentielles. De plus, la possibilité de cloner des profils de matériels rationalise le travail des administrateurs et offre une tranquillité d’esprit supplémentaire, car toute modification des réglages d’un matériel peut facilement se dupliquer sur l’ensemble du parc.

6. **Choisir le bon partenaire**
   De nombreuses entreprises proposent des services professionnels pour mettre en place une politique d’impression sécurisée, mais le niveau d’expertise peut varier considérablement. Sharp prend la sécurité des réseaux très au sérieux et la place au centre de tout nouveau développement de produit. En tant que fabricant, nous faisons évaluer nos équipements en conformité avec les exigences spécifiques liées à notre certification critères communs. Nos MFP embarquant le kit de sécurité des données disponible en option ont été évalués, de manière indépendante, selon les critères du JISEC (Japan’s IT Security Evaluation and Certification). Ils ont été certifiés conformes à la norme Protection Profile for Hardcopy Devices v1.0 (HCD-PP v1.0) la plus récente des critères communs, prouvant ainsi que nous pouvons aider nos clients à gérer leurs données les plus sensibles dans le monde entier.

Obtenez l'aide d'experts

Tout cela peut sembler compliqué, mais rassurez-vous, vous n'êtes pas seul. Nos experts sont là pour vous accompagner.

Sharp propose notamment plusieurs solutions, outils et services pour vérifier et analyser les éventuelles vulnérabilités de votre réseau, préparer un plan d'amélioration et concevoir différents scénarii :

- **Atelier consacré à la sécurité d'impression**
  Nous pouvons utiliser un certain nombre d'outils et de techniques afin d'aider votre organisation à comprendre les menaces de sécurité, à identifier les solutions et à élaborer un plan d'amélioration sur mesure.

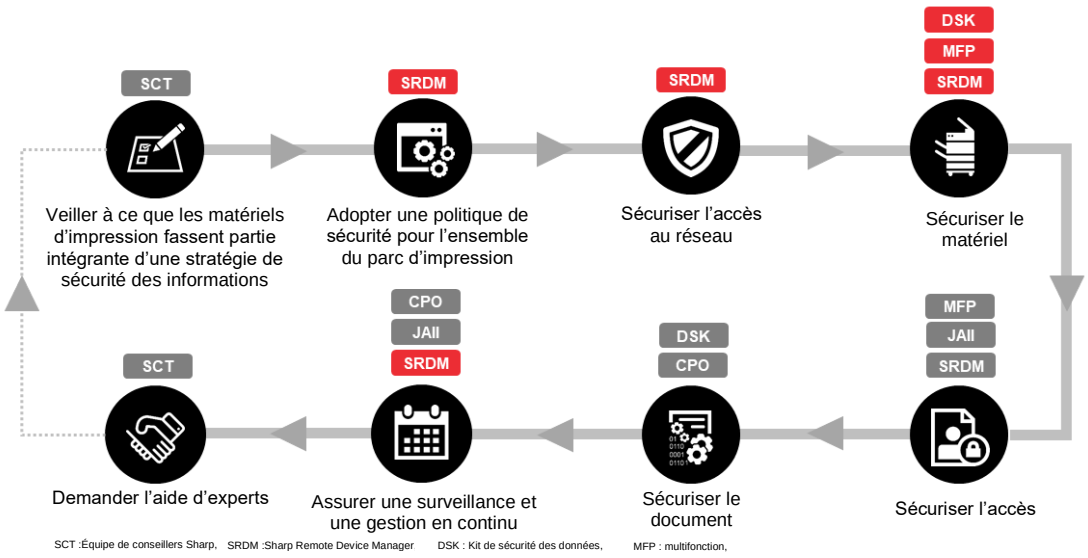
  L'audit se concentre sur tous les périphériques réseau et sur leur sécurité. Nous évaluons toutes les fonctionnalités standard et avancées disponibles pour ces matériels ainsi que les outils de détection et de prévention des menaces. Nous vérifions également si les matériels que vous utilisez dans votre entreprise sont adaptés à l'usage qui en est fait et offrent une sécurité maximale pour votre entreprise et ses utilisateurs. De plus, l'audit de sécurité d'impression décrit les « étapes ultérieures » à suivre pour élaborer une politique d'impression sécurisée et couvrir tous les aspects liés à la sécurité dans votre entreprise, notamment :

  - La sécurité des réseaux : telle présentée dans ce document ;
  - La sécurité des données : toutes les activités liées à la production de documents, telles que l'impression, la numérisation, la transmission fax et l'envoi par e-mail ;
  - La sécurité des documents : gestion des fichiers électroniques et papier utilisés au sein de votre environnement de bureau ;
  - La conformité au RGPD : conformité aux dernières réglementations de l'UE en matière de sécurité et de protection des données personnelles.

- **Pack de sécurité**
  Ce pack associe un atelier client et l'installation de Sharp Remote Device Manager (SRDM). Il inclut également la configuration et le déploiement d'un système de gestion des documents en sortie pour renforcer davantage la sécurité de votre environnement de bureau (option). Sécuriser les réseaux & sécuriser les documents imprimés ou envoyés via les matériels d'impression.

- **Sharp Remote Device Manager (SRDM)**
  Cet outil Sharp vous aide à mettre en œuvre des réglages de sécurité en quelques secondes. L'intégration de cette solution est un service proposé par Sharp avec une équipe d'experts dédiée pour vous accompagner. En fonction de vos besoins et de vos exigences, tous les paramètres de sécurité seront appliqués à votre environnement informatique afin que l'ensemble de vos systèmes d'impression Sharp soient sous contrôle.

Élaboration d'une politique de sécurité d'impression et solutions de sécurité réseau Sharp



Conclusion

Quels enseignements pouvons-nous tirer de tout ceci ? La bonne nouvelle, c'est qu'il n'y a pas que des mauvaises nouvelles !

Si les MFP et les imprimantes non sécurisés représentent une menace sérieuse (et actuellement sous-estimée) pour les entreprises, il est possible de mettre en place certaines mesures pour limiter les risques.

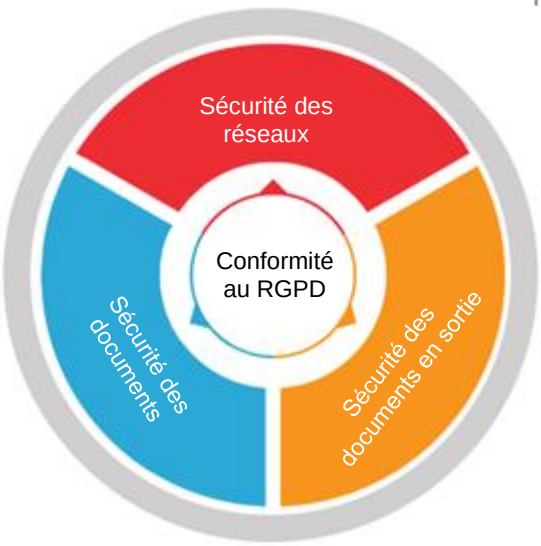
- **Votre entreprise n'est pas un cas isolé.** Chaque jour, des entreprises de toutes tailles sont la cible de violations de données, de cyberattaques, de virus et autres activités malveillantes. Le plus important est de comprendre comment votre entreprise pourrait être affectée si elle était attaquée et de vous poser la question : « Mon entreprise est-elle vraiment prête à se défendre ? ».

- **La solution n'est pas toujours simple.** Comprendre, configurer et mettre en place des mesures de sécurité appropriées peut prendre beaucoup de temps et s'accompagner de réelles difficultés de mise en œuvre. Chaque organisation étant différente, vous devez mettre en place différents outils et définir des stratégies uniques pour faire face aux menaces spécifiques auxquelles est exposée votre entreprise. Cependant, quels que soient vos besoins, Sharp peut vous proposer des solutions efficaces visant à protéger vos MFP et imprimantes.

- **Si votre entreprise n'est pas prête, essayez de comprendre le problème.** Pourquoi votre entreprise est-elle vulnérable ? Dispose-t-elle des outils et des ressources nécessaires pour définir une politique réseau et d'impression sécurisée ou pour améliorer celle en place ? Sinon, estimez-vous préférable de faire appel aux spécialistes de Sharp pour auditer vos réseaux et périphériques réseau et mettre en œuvre des outils de sécurité efficaces pour votre entreprise ?

- **Définissez vos propres objectifs de sécurité.** Afin de comprendre vos vulnérabilités potentielles et ce qu'il vous faut protéger, vous devez répondre à ces deux questions : « Où en sera mon organisation dans quelques années ? » et « Comment puis-je préparer mon entreprise à prendre les mesures nécessaires pour mettre en œuvre les stratégies et outils qui l'aideront à se prémunir contre les cyberattaques, les programmes malveillants, etc. ? ».

Infrastructure de sécurité de Sharp



- **Assurez-vous de disposer du niveau d'expertise approprié.** Si vous disposez des ressources internes requises, vous pouvez élaborer votre propre politique d'impression sécurisée. Vous pouvez également vous appuyer sur l'équipe Sharp « Professional Services » pour vous aider à créer un système de sécurité efficace et à mettre en œuvre des outils adaptés à votre type d'entreprise et à ses besoins :

  - Matériels réseau sécurisés de Sharp conformes avec les derniers certificats de sécurité ;
  - Logiciels, solutions et services de sécurité de Sharp pour élaborer une politique d'impression sécurisée : DSK, SRDM, audit de sécurité, etc.

- **Nous sommes là pour vous aider.** Avec Sharp, l'examen et la définition de votre politique d'impression sécurisée se mettront en place de manière fluide. Les experts Sharp sont là pour vous aider à évaluer votre niveau de sécurité actuel, l'examiner, et vous proposer une stratégie qui vous permettra d'élaborer une politique d'impression sécurisée efficace répondant aux besoins et aux exigences de votre organisation. Nos spécialistes vous aideront à choisir les outils et services les plus adaptés à votre entreprise :

  - Audit de sécurité de Sharp ;
  - Fonctionnalités de sécurité standard de Sharp ;
  - Outils en option (ex. : SRDM, DSK) ;
  - Pack de sécurité réseau de Sharp ;
  - Politique d'impression sécurisée.

- **Evaluez toujours la situation dans son ensemble.** Pour minimiser les failles potentielles de sécurité dans d'autres domaines de votre organisation, nous pouvons vous aider à mettre en œuvre des mesures de sécurité supplémentaires afin que vous puissiez garantir une sécurité à 360 degrés dans chacune des composantes de l'architecture IT de votre entreprise :

  - Sécurité des réseaux
  - Sécurité des données
  - 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. Rapport « Eastern and Western Europe Single-Function Printer & MFP Market Placements in the last five years » (Placements sur le marché des imprimantes monofonction et multifonctions en Europe de l'Est et en Europe de l'Ouest au cours des cinq dernières années), IDC, T4 2018
2. « IT and Print Security Survey 2015 » (Enquête 2015 sur la sécurité informatique et la sécurité d'impression), IDC, septembre 2015
3. « Printing: a false sense of security » (Impression : un faux sentiment de sécurité), Quocirca, 2013
4. « Transformative Technology in Document Security » (Technologies innovantes dans le domaine de la sécurité des documents), IDC, mai 2015

`

www.sharp.eu

SHARP

Be Original.