Comment sécuriser votre système d'impression en trois étapes

Longtemps sous-estimée, la sécurisation d'un système d'impression d'entreprise doit être pleinement prise en compte afin de limiter le risque de fuite d'informations sensibles. Voici les principales précautions à prendre.

Le multifonction a longtemps été l'angle mort des politiques de cybersécurité. Connecté au réseau de l'entreprise, il représente, pourtant, un point d'entrée potentiel à son système d'information au même titre qu'un poste de travail. Il convient, donc, de le considérer comme un actif IT à part entière et lui garantir le niveau de protection associé.

Un multifonction étant traditionnellement accessible en libre-service, l'entreprise doit, par ailleurs, s'assurer que le collaborateur s'est dûment authentifié et qu'il possède les droits pour imprimer, copier ou numériser. Enfin, la dématérialisation des documents avec l'essor du cloud printing et des systèmes de Gestion Electronique de Documents (GED) présente de nouveaux risques auxquels il faut sensibiliser les collaborateurs. Découvrons trois enjeux de la sécurité documentaire à ne pas négliger.

LE MULTIFONCTION, UN PÉRIPHÉRIQUE IT À PROTÉGER

En 2024, un système de reproduction professionnel ne se limite plus à la seule impression de documents. Un multifonction propose des fonctions avancées de numérisation et de copie multiformat.

> **Le multifonction a longtemps été l'angle mort des politiques de cybersécurité.**

Longtemps perçu comme un simple équipement bureautique, il s'apparente, aujourd'hui, à un véritable ordinateur avec un disque dur, un processeur, de la mémoire et un système d'exploitation propriétaire.

Cet appareil communicant évolué dispose de sa propre capacité de stockage tout en étant connecté au réseau d'entreprise.

Le périphérique s'apparente à un véritable ordinateur avec un disque dur, un processeur, de la mémoire et un système d'exploitation propriétaire.

Vecteur d'attaques dites par rebond, un multifonction peut constituer pour des cybercriminels une clé d'entrée du système d'information d'une société. Il offre, aussi, aux hackers une mine d'informations sensibles à dérober comme un fichier clients ou un contrat commercial envoyé par un collaborateur pour être imprimé. Retranché derrière le pare-feu de l'entreprise, un multifonction doit bénéficier de la même protection qu'un poste de travail.

De fait, il est loin le temps où la perception du risque se limitait aux documents laissés en vrac à côté du multifonctions et potentiellement confidentiels. Cela ne présente, aujourd'hui que la partie émergée de l'iceberg. Avec la fonction scanner, un collaborateur malveillant peut potentiellement envoyer des documents sensibles hors de l'entreprise en utilisant une adresse mail générique.

La prise de conscience évolue toutefois. Depuis une dizaine d'années, ce n'est plus uniquement le responsable des services généraux qui prend en charge ce type d'équipement mais aussi le DSI, voire le RSSI, sur le volet gestion des risques cyber, dans les grandes entreprises privées ou les grandes administrations.

ENCADRER LE CIRCUIT DE GESTION DOCUMENTAIRE

La circulation des documents dans le cloud doit être maitrisée. Pour limiter le « shadow IT » et le recours à des solutions de contournement, comme les versions gratuites et grand public de systèmes de partage en ligne, une entreprise doit mettre à la disposition de ses salariés un environnement de partage documentaire sécurisé.

Une solution de gestion électronique de documents (GED) gère l'ensemble du cycle de vie du document, de sa création à son archivage ou sa suppression après une période définie. Elle centralise les documents d'une organisation, facilite leur diffusion, contrôle les accès et les droits, garantit la traçabilité des opérations. Plus de fichiers en vrac dans de multiples bases, le collaborateur est assuré de travailler sur la dernière version en date du document.

LA RÈGLE DES 3 A POUR UNE SÉCURITÉ OPTIMALE

Une politique de sécurité du circuit documentaire repose classiquement sur la règle des 3 A pour Authentification, Autorisation et Accounting (Traçabilité). La première étape consiste à s'assurer que le collaborateur souhaitant numériser un document ou lancer une impression est habilité à le faire et qu'il est physiquement présent dans les locaux de l'entreprise.

Depuis son terminal professionnel, dûment identifié, il envoie le travail d'impression qui est d'abord stocké dans un serveur interne ou dans le cloud. Pour libérer l'impression, l'utilisateur s'authentifie directement depuis le multifonction via un badge – le cas le plus courant -, un code PIN ou un mot de passe.

Cette impression sécurisée réduit le risque de fuite de données, potentiellement lourde de conséquences en termes de préjudices financiers, d'attentes à la réputation ou de non-respect du cadre règlementaire (RGPD).

Elle met fin aux documents laissés dans les bacs de sortie avec le risque qu'ils soient lus ou récupérés par des personnes non autorisées. Un phénomène qui n'a rien d'anodin. Selon l'agence de la transition énergétique (Ademe), « *les impressions oubliées sur l'imprimante ou jetées sans être lues représentent 400 millions d'euros chaque année.* »

Une politique de sécurité du circuit documentaire repose classiquement sur la règle des 3 A pour Authentification, Autorisation et Accounting.

Il ne suffit toutefois pas de mettre un outil à la disposition des salariés pour qu'il soit utilisé. Pour favoriser l'adhésion, un groupe d'utilisateurs participe à la définition du projet. La mise en production se fait progressivement en commençant par les services clés, comme la direction générale et la DAF, puis en élargissement le périmètre à d'autres entités.

Enfin, le déploiement doit être suivi d'un programme de conduite du changement. Les collaborateurs seront sensibilisés sur les bonnes pratiques en matière de diffusion et de partage de l'information mais aussi sur les risques associés et les procédures à respecter en cas de fuite de données.

Cette impression sécurisée répond aux contraintes du télétravail. Depuis son domicile, le collaborateur lance une impression qui sera libérée une fois qu'il se rendra au bureau. Il est possible de limiter la durée de rétention, à 72 heures par exemple, estimant qu'au-delà, l'impression n'était vraisemblablement pas si nécessaire que cela. Une entreprise peut également définir des droits d'accès par groupes d'utilisateurs. Les managers ou les membres de la direction marketing bénéficieront, par exemple, de droits étendus.

Le troisième A, c'est l'acccouting, c'est-à-dire la traçabilité des opérations. Qui a imprimé, scanné ou copié quoi ? L'authentification par badge ou par mot de passe assure cette traçabilité. Il est également possible d'exiger que le collaborateur utilise son adresse mail professionnelle pour émettre un scan. Sur le plan réglementaire, cette politique de traçabilité répond aux opérations d'audit et de contrôle dans le cadre de la norme ISO 27001 sur la sécurité des systèmes d'information.

Le recours au « cloud printing » réduit les risques d'interception des documents sensibles. Non seulement le cloud d'un fournisseur de solutions de gestion documentaire offre une sécurisation potentiellement accrue par rapport aux serveurs d'une entreprise mais les communications sont également chiffrées.

La circulation des documents dans le cloud doit être maitrisée.

Concernant le risque de vol d'informations stockées sur le disque dur, chaque périphérique possède une clé de chiffrement unique contenue dans une puce, elle-même dédiée à la carte mère. En cas de vol du disque dur, le chiffrement rend, par ailleurs, les données qu'il contient inexploitables.

Si le matériel connaît une seconde vie, les procédures de reconditionnement prévoient l'effacement de certaines données. Un document contractuel attestera de la bonne destruction des données.