brother
at your side

LES ENTREPRISES FACE AUX ENJEUX DE LA **SÉCURITÉ DES DONNÉES**

Édito

La dématérialisation croissante des documents ne signifie pas la disparition en entreprise des périphériques d'impression. Et si la sécurité s'est beaucoup concentrée ces dernières années sur la protection des données disponibles sur le système d'information, notamment au travers des projets de déploiement du chiffrement, elle ne peut négliger la sécurité des impressions.

L'Agence Européenne chargée de la Sécurité des Réseaux et de l'Information (ENISA) a d'ailleurs tenu récemment à rappeler aux entreprises les enjeux de sécurité en ce domaine. Bien souvent, des disques durs mis au rebus et des documents papiers comportant des informations sensibles, finissent à la portée de n'importe qui.

Les risques sont en effet multiples, comme le souligne le rapport de l'ENISA. Le vol d'un document peut par exemple porter atteinte à la réputation de l'entreprise. L'agence européenne note également que les configurations d'accès administratifs tels que Telnet, SNMP, FTP et HTTP sont ouverts à la plupart des imprimantes. Ils permettent entre autres aux pirates d'utiliser les appareils d'impression pour pénétrer le réseau, en changer la configuration, récupérer les impressions, les relancer, etc.

Une politique de sécurité globale, tournée vers un contrôle des flux de personnes et informatiques, tout aussi efficace soit-elle, nécessite de s'accompagner de mesures préventives concernant la gestion des données. Brother, spécialiste de l'impression, du partage de l'information et du document, propose de découvrir les solutions intégrées à ses périphériques.

Sommaire

DERRIÈRE LES PÉRIPHÉRIQUES D'IMPRESSION SE CACHENT DES FAILLES DE SÉCURITÉ

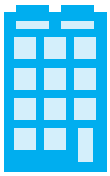
Grâce à des fonctionnalités de plus en plus performantes et polyvalentes, les imprimantes multifonctions prennent davantage d'importance au sein des entreprises. Ce phénomène nécessite de faire preuve de vigilance quant à l'apparition de risques liés à la sécurité des données.

Aujourd'hui, les mesures de sécurité sont au cœur des préoccupations des entreprises. Soucieuses de protéger leurs données, elles s'équipent désormais de systèmes de sécurité adéquats.

L'un des domaines qui présente souvent des faiblesses en matière de sécurité est la connexion des équipements informatiques tels que des multifonctions à un réseau pourtant sécurisé.

2500 PME* intérogées sur leurs préocupations liées à leur activité

Pour 200 ENTREPRISES**



75% d'entre elles ont répondu que la sécurité des données était un **enjeu crucial**

Pour la 1ère fois, la sécurité est considérée comme leur **1ère préoccupation**

59% pensent que la sécurité des données **influence leurs décisions** en matière de gestion des impressions et des documents

74% ont mis en place ou prévoient de **mettre en place des solutions** d'impression sécurisées

Quels sont les risques auxquels les entreprises sont confrontées ?

Les périphériques connectés en réseau sont particulièrement exposés et doivent donc être protégés afin d'éviter toute perte de données. L'utilisation de ces périphériques peut présenter de multiples risques pour les entreprises :

- **Divulguer des informations confidentielles imprimées**
- **Divulguer des informations confidentielles numérisées**
- **Être confronté à des intrusions réseau en raison d'une sécurité défaillante**
- **Permettre à des utilisateurs non autorisés d'accéder aux solutions d'impression**

Brother apporte des solutions adaptées afin d'accompagner les TPE/PME et grandes entreprises à supprimer ces risques.

*Dans une enquête menée en 2015
**Selon une étude Quocirca 2015

DES INFORMATIONS CONFIDENTIELLES **IMPRIMÉES** À LA PORTÉE DE TOUS

Quels sont les risques ?

Quelle que soit la politique de sécurité de votre entreprise, si tout le monde a accès à une imprimante et peut récupérer tous types d'impression, vos données courent effectivement un risque. Nous sommes rarement assis à côté de l'imprimante que nous utilisons. Il existe donc toujours un risque que les impressions potentiellement très confidentielles, soient à la portée de n'importe qui.

Que peuvent faire les entreprises pour se protéger ?

La seule manière de combattre efficacement ce problème consiste à retarder l'impression jusqu'à ce que l'utilisateur autorisé se trouve physiquement à côté de l'imprimante et puisse récupérer ses documents. Pour cela, la meilleure solution est d'utiliser un code PIN ou un lecteur de badge sécurisé. Brother recommande ainsi plusieurs solutions selon la taille et les besoins de chaque entreprise :

La première est **Secure Print**, une solution conçue avant tout pour les utilisateurs qui n'impriment des documents confidentiels qu'occasionnellement. Secure Print permet aux utilisateurs de retarder l'impression jusqu'à ce qu'ils se trouvent physiquement à côté de l'imprimante : un code PIN est attribué à cette tâche dans le pilote.

Si l'impression de documents confidentiels est plus fréquente pour un utilisateur, une solution telle qu'**Active Directory Secure** Print sera plus efficace. Cette solution limite complètement l'accès aux fonctions de l'imprimante en bloquant les personnes non autorisées. Pour déverrouiller l'imprimante et récupérer le document, l'utilisateur doit s'identifier avec son nom d'utilisateur et son mot de passe Windows® Active Directory.*

Dans certains environnements, les besoins d'impressions confidentielles varient entre les différents utilisateurs. Ils vont donc privilégier une approche plutôt basée sur le réseau, qui se révèle être certainement plus adaptée. Une solution telle que **PrintSmart Secure Pro** de Brother conserve les documents sur un serveur central plutôt que sur le périphérique. L'utilisateur peut ainsi récupérer ses documents à partir de n'importe quel périphérique du bâtiment connectée au serveur PrintSmart Secure Pro en utilisant une authentification PIN ou, le cas échéant, par carte NFC.

*Pour utiliser Active Directory Secure Print, l'entreprise doit au préalable utiliser Microsoft® Active Directory.

DES INFORMATIONS CONFIDENTIELLES **NUMÉRISÉES** À LA PORTÉE DE TOUS

Bien que les mesures de sécurité des imprimantes puissent être optimales, un risque existe pour les documents numérisés. Une fois un document confidentiel numérisé, l'utilisateur peut le conserver ou le partager de différentes manières. Choisir le partage par e-mail ou sur le web peut s'avérer être risqué. Le nombre de copies effectuées à la suite d'un envoi constitue une variable inconnue.

La solution la plus simple consiste à convertir un document numérisé en un Secure PDF protégé par code PIN. **Les scanners et multifonctions Brother sécurisent immédiatement un fichier PDF avec un code PIN** à quatre chiffres, de manière à ce que personne ne puisse le consulter sans y être autorisé.

Il est également possible d'utiliser de nombreux scanners et multifonctions Brother pour numériser vers SFTP et HTTPS*. **Le Secure File Transfer Protocol** établit un flux de données privé et sécurisé. En contrôlant de plus près l'accès aux serveurs SFTP, les entreprises peuvent contribuer à rendre leur réseau plus sûr en fermant complètement une passerelle vers et depuis leur système.

Derrière l'intégralité de ces solutions professionnelles subsiste malgré tout un inconvénient : par le biais de logiciels malveillants, il demeure possible d'intercepter les données pendant qu'elles sont envoyées aux solutions d'impression et aux scanners. Pour assurer une protection contre ce type d'intrusion, **les imprimantes et scanners Brother sont dotés du cryptage Transport Layer Security (TLS) et Secure Socket Layer (SSL)**, des technologies utilisées en e-commerce pour protéger les données bancaires. Les fichiers les plus confidentiels peuvent ainsi être cryptés jusqu'à 256 bits au cours de leur transmission via/dans le réseau.

Pour les entreprises qui n'ont pas recours à ce système, Brother prend également en charge l'impression vers **des serveurs de données utilisateurs LDAP.** Cette solution fonctionne de la même manière qu'Active Directory Secure Print, mais communique avec un serveur LDAP. Pour instaurer un niveau de sécurité supplémentaire, les administrateurs peuvent définir un délai limite de conservation des tâches d'impression non collectées dans la mémoire de l'imprimante. Ainsi, les documents confidentiels ne restent pas conservés dans les périphériques.

*Périphériques à configurer

INTRUSIONS RÉSEAU EN RAISON D'UNE SÉCURITÉ DÉFAILLANTE

L'utilisation de certificats, de noms d'utilisateurs et de mots de passe lors de la connexion de tablettes ou d'ordinateurs portables à un réseau sécurisé est chose courante. En revanche, pour ce qui est de la connexion à des périphériques d'impression, il en est tout autre. En effet, il est important de souligner que ces périphériques présentent également des risques pour la sécurité du réseau dans son ensemble.

Que peuvent faire les entreprises pour se protéger face aux :

MENACES EXTERNES

Les imprimantes et multifonctions présentent plusieurs types de chiffrements cryptés. Brother en propose plusieurs afin d'améliorer la sécurité et d'éviter les fuites :

1 - 802.1x : tous les périphériques Brother, qu'ils soient connectés par câble ou intégrés dans une infrastructure sans fil, respectent les normes de sécurité extrêmement élevées établies par l'IEEE dans le cadre des règles 802.1x.

2 - IPsec : plusieurs périphériques peuvent être connectés directement à des environnements sécurisés internes ou externes grâce à IPsec. IPsec étant intégré dans les solutions d'impression Brother, il n'est pas nécessaire d'installer un plug-in ou de recourir à une solution logicielle tierce pour intégrer les solutions d'impression au réseau.

3 - SNMPv3 : Conçues pour respecter des politiques de sécurité réseau strictes, les solutions d'impression Brother comprennent toutes les instructions fournies en chiffrement SNMP, versions 1, 2 et 3 (MD5 et SHA1), et ce même durant les opérations de configuration à distance et de routines de maintenance.

MENACES INTERNES

Le cryptage comme expliqué précédemment, permet de protéger les données contre les menaces externes. Toutefois, le réseau reste vulnérable si les membres du personnel accèdent à distance aux imprimantes connectées au réseau. Pour éviter tout problème de ce type, les périphériques d'impression Brother prennent en charge les Password Protected Embedded Web Servers, qui s'éteignent après une période d'inactivité de cinq minutes.

Ils prennent également en charge le IP Blocking, qui empêche tout accès au périphérique depuis le réseau. Et pour cause, ces derniers n'acceptent que les connexions des utilisateurs employant les adresses IP suivantes : 10.45.12.1, 12.45.12.45, 10.45.12.46 et 10.45.12.47.

Une solution moins restrictive se trouve en Protocol Control. Elle permet aux administrateurs de désactiver les protocoles non nécessaires.

ACCÈS D'UTILISATEURS NON AUTORISÉS AUX SOLUTIONS D'IMPRESSION

Quels sont les risques ?

À moins que les imprimantes ne soient installées dans des salles sécurisées, il est toujours possible que quelqu'un puisse récupérer les documents imprimés ; et ce quelles que soient les mesures de sécurité mises en place. Il est de fait crucial, de disposer d'une méthode pour sécuriser les petites et moyennes entreprises ne disposant pas ou ayant une petite infrastructure informatique.

2/3
des décideurs IT*

ont déclaré que la sécurité des informations **influence leurs décisions** en matière de gestion des impressions des documents

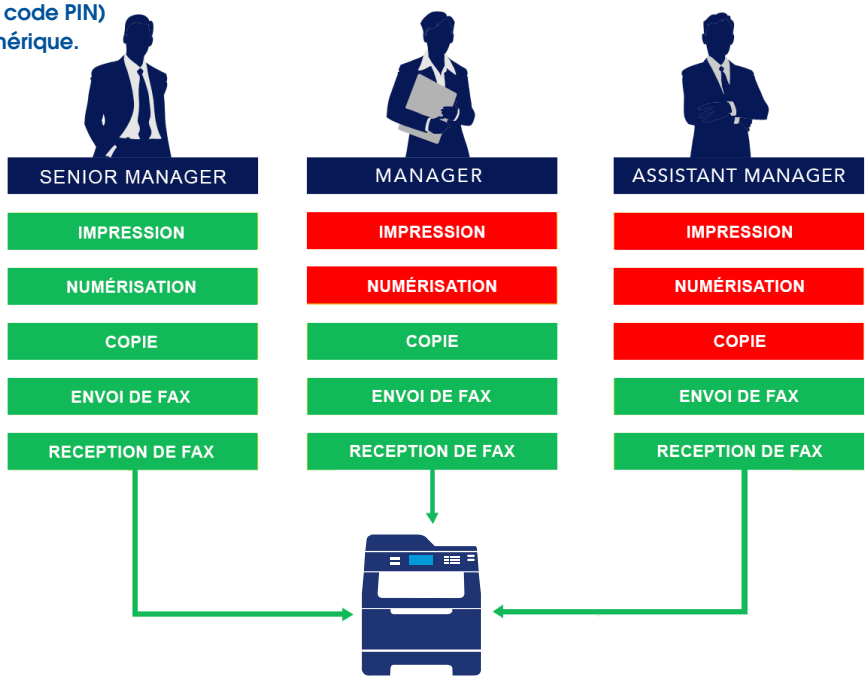
Que peuvent faire les entreprises pour se protéger ?

Brother propose à ces structures, un éventail de solutions sécurisées qui préviennent toute intervention de personnes non autorisées :

1 - Setting Lock permet de limiter l'accès aux paramètres de l'appareil par le biais du panneau de contrôle. C'est la solution idéale pour les entreprises qui ne souhaitent pas limiter la manière dont les utilisateurs emploient les fonctionnalités mais veulent parallèlement s'assurer qu'aucun d'entre eux, non autorisé ne puisse modifier les paramètres.

2 - Secure Function Lock va plus loin encore, en bloquant l'accès aux paramètres de l'appareil mais aussi à certaines fonctions. Les administrateurs peuvent ainsi décider du niveau d'autorisation de chaque utilisateur pour chaque périphérique, en déterminant par exemple lesquels d'entre eux peuvent faxer et numériser ou en mettant en place des quotas mensuels par le biais de codes PIN uniques ou de badges NFC.

Les paramétrages de Secure Function Lock (verrouillage sécurisé avec code PIN) du serveur web intégré du périphérique.



Certaines fonctions sont bloquées ou limitées pour les utilisateurs non autorisés. Le senior manager peut imprimer, numériser, copier et faxer à volonté, tandis que la manager ne peut ni imprimer ni numériser et que l'assistant manager peut seulement envoyer ou recevoir des fax.

*Dans une étude menée par Brother en 2015

En plus de bloquer une fonction, il est également possible d'en limiter l'utilisation. Par exemple, au lieu de bloquer complètement l'accès de la manager à l'impression, il est possible de limiter le nombre de pages qu'elle peut imprimer chaque mois. Ce quota peut être ajusté et remis à zéro manuellement par un administrateur ou se remettre à zéro automatiquement à intervalles réguliers.

3 - Par ailleurs, lorsque plusieurs utilisateurs d'une même structure partagent des imprimantes ou que des périphériques doivent être placés dans un lieu public, il peut s'avérer difficile de contrôler les abus sans perturber l'utilisation de ces derniers. Cependant, avec l'authentification Brother Active Directory ou LDAP, le personnel peut facilement utiliser ses identifiants réseau existants pour accéder aux imprimantes en cas de besoin.

Une solution globale ?

Pour les entreprises qui souhaitent contrôler leur sécurité et mieux connaître les coûts liés à l'utilisation de leurs imprimantes, Brother propose **PrintSmart Secure Pro, une solution logicielle innovante et abordable qui améliore la sécurité, l'efficacité et la visibilité des coûts d'impression et réduit le gaspillage de papier,** contribuant ainsi à protéger l'environnement. L'interface utilisateur ergonomique offre davantage de visibilité aux administrateurs en leur présentant l'intégralité des informations liées à l'utilisation des multifonctions dans leur entreprise, leur permettant ainsi de contrôler, de maîtriser et de réduire leurs coûts d'impression. Avec **l'Interface Solutions Brother (BSI) incluse dans la gamme, la personnalisation et la modularité sont possibles.** La plateforme BSI permet aux développeurs tiers de **créer des solutions intégrées** avec des périphériques Brother. Des interfaces utilisateur « sur-mesure » peuvent être imaginées pour aider les clients à améliorer le flux de travail et la sécurité. Grâce à leur interface ouverte, les solutions d'impression Brother peuvent également s'intégrer dans des solutions de gestion de l'impression tierces.

Ainsi, les entreprises ne sont pas limitées par une approche préétablie mais peuvent adapter l'interface utilisateur comme elles le souhaitent.

Recommandations Brother

Il ne fait aucun doute que de nombreuses entreprises, tous secteurs confondus, ont besoin de prendre davantage en considération les risques liés à la sécurité des données et des réseaux via les multifonctions et scanners.
Il revient aux administrateurs IT de sélectionner les solutions appropriées en fonction des risques, des infrastructures et des systèmes de sécurité déjà en place dans chaque société.

Une entreprise peut avoir toute confiance en la sécurisation de ses systèmes d'impression et de numérisation si elle peut s'assurer :

- **de sécuriser ses périphériques,**
- **de protéger ses données avant et après l'impression,**
- **et de protéger son réseau contre d'éventuelles intrusions.**

elle peut avoir toute confiance en la sécurisation de ses systèmes d'impression et de numérisation.

brother
at your side

OmniJoin
LA WEBCONFÉRENCE PAR BROTHER

(1) Sources : Brother SMB Research conduite par B2B international sur 2502 Entreprises au Royaumes unis, en France, Allemagne et aux Etats Unis.
(2) Sources : Quocirca Managed Print Services Landscape. 2015., menée auprès de 200 organisation de plus de 1000 employés aux Royaume-Unis, en France , en Allemagne et aux Etats Unis.