brother
at your side

Conseils de sécurité Brother

Avril 2016

LES DANGERS CACHÉS DE VOTRE IMPRIMANTE ET CE QUE VOUS POUVEZ FAIRE POUR LES CONTRER

Les environnements d'impression et de numérisation en entreprise deviennent toujours plus polyvalents et performants. Mais ces progrès vont de pair avec une hausse des risques de sécurité. Et rares sont les entreprises qui s'en prémunissent.

De nos jours, les mesures de sécurité sont omniprésentes au travail. Les entreprises utilisent de nombreux outils pour se protéger. Ceux-ci vont des badges ou clés d'accès aux logiciels de sécurité réseau pour la protection des données.

Mais il reste un domaine où beaucoup d'entreprises ont encore de possibles failles de sécurité: dans la façon dont les périphériques tels que les imprimantes ou les scanners sont raccordés au réseau par ailleurs sécurisé.

En 2015, Brother a interrogé plus de 2 500 PME sur les défis auxquels elles font face. 75 % d'entre elles ont déclaré que la sécurité des données était une préoccupation importante dans leur entreprise et 59 % ont indiqué que la sécurité des données jouait un rôle central dans la prise de décisions relatives à la gestion des impressions et des documents.

Ces préoccupations augmentent avec l'accroissement des problèmes de sécurité dans toutes les branches. Une étude de Quocirca, également réalisée en 2015 auprès de 200 entreprises, a montré pour la première fois que la sécurité figurait au premier rang des priorités. En effet, 75 % des entreprises interrogées ont indiqué que la sécurité était un sujet important ou très important (note moyenne de 4,01 sur 5). Au total, 74 % des entreprises utilisent des solutions d'impression sécurisées ou prévoient d'en employer dans l'avenir.

Quels sont réellement les dangers?

Il existe essentiellement quatre possibilités pour les imprimantes et scanners réseau de représenter un risque pour une entreprise.

1. **TRANSMISSION INVOLONTAIRE DE DONNÉES CONFIDENTIELLES LORS DE L'IMPRESSION**
2. **TRANSMISSION INVOLONTAIRE DE DONNÉES CONFIDENTIELLES LORS DE LA NUMÉRISATION**
3. **ACCÈS RÉSEAU NON AUTORISÉS DU FAIT D'UNE SÉCURITÉ INSUFFISANTE**
4. **ACCÈS PHYSIQUE D'UTILISATEURS NON AUTORISÉS À DES APPAREILS NON SÉCURISÉS**

Afin d'aider les entreprises à supprimer ces menaces qui pèsent couramment sur la sécurité, Brother a réuni les risques spécifiques que les administrateurs système devraient connaître et les technologies qui permettent d'atteindre une meilleure protection et donc une meilleure sécurité.

1. TRANSMISSION INVOLONTAIRE DE DONNÉES CONFIDENTIELLES LORS DE L'IMPRESSION

Quels sont les dangers?

Peu importe l'efficacité des règles de sécurité de votre entreprise, si quelqu'un peut s'approcher d'une imprimante et emporter tout simplement les pages qui n'ont pas encore été récupérées, vos données sont en danger.

En général, nous ne travaillons pas juste à côté de l'imprimante que nous utilisons. Il y a donc toujours un risque que les impressions (parfois des documents strictement confidentiels) que nous n'avons pas encore récupérées soient accessibles à des tiers.

Que peuvent faire les entreprises pour s'en prémunir?

Le seul moyen vraiment efficace de résoudre ce problème est de repousser l'impression jusqu'à ce que l'utilisateur autorisé se trouve près de l'appareil. Pour ce faire, le mieux est d'utiliser un mot de passe ou un lecteur de cartes sécurisé. Selon la taille et les exigences de l'entreprise, Brother recommande différentes solutions. L'une des possibilités est la fonction **Secure Print**. Elle convient surtout à ceux qui n'impriment qu'occasionnellement des documents confidentiels. Avec Secure Print, les utilisateurs peuvent repousser l'impression jusqu'à ce qu'ils se trouvent près de l'imprimante. Ainsi, lorsque vous devez imprimer un document confidentiel, vous attribuez un mot de passe à cette commande d'impression au moment de l'envoyer à l'imprimante. Si vous imprimez régulièrement des documents confidentiels, nous vous recommandons la fonction **Active Directory Secure Print**. Celle-ci limite d'une manière générale l'accès à toutes les fonctions de l'imprimante et en verrouille l'accès à toutes les personnes non autorisées. Pour déverrouiller l'imprimante et récupérer leurs impressions, les utilisateurs doivent s'identifier avec leur nom d'utilisateur et leur mot de passe Windows® Active Directory. Dans les deux cas, la commande d'impression est mise en attente dans la mémoire interne de l'imprimante jusqu'à ce que l'utilisateur la récupère.

Pour pouvoir utiliser Active Directory Secure Print, une entreprise doit déjà utiliser Microsoft® Active Directory. Si ce n'est pas le cas, Brother propose aussi une solution d'impression sécurisée sur des serveurs à bases de données LDAP. Elle fonctionne comme Active Directory Secure Print, à la différence que la communication transite par un serveur LDAP.

Pour renforcer encore la sécurité des fonctions Active Directory Secure Print ou LDAP Secure Print, il est possible de mettre en place une limitation temporaire pour la mise en attente des commandes d'impression dans la mémoire de l'appareil. Ainsi, les documents confidentiels ne restent pas indéfiniment dans l'appareil.

Pour les entreprises dans lesquelles chaque utilisateur a des besoins différents en matière d'impression de données confidentielles, l'approche réseau est assurément une meilleure solution. Par exemple, la fonction PrintSmart Secure Pro de Brother enregistre les documents sur un serveur central plutôt que sur l'appareil. Cela signifie que l'utilisateur peut récupérer ses documents sur n'importe quelle imprimante raccordée au serveur PrintSmart à l'aide de son mot de passe ou en s'identifiant avec une carte NFC. De plus, les administrateurs système peuvent ainsi surveiller de plus près l'utilisation.

Mais malgré toutes ces mesures, il reste un maillon faible: il suffit d'un bon logiciel pour intercepter vos données lors de leur envoi à l'imprimante. Pour vous en prémunir, les appareils Brother incluent Transport Layer Security (TLS) et Secure Socket Layer (SSL), le chiffrement utilisé par les sites d'e-commerce pour protéger les informations de paiement des clients. Ainsi, vos documents peuvent être chiffrés en 256 bits pour la transmission.

2. TRANSMISSION INVOLONTAIRE DE DONNÉES CONFIDENTIELLES LORS DE LA NUMÉRISATION

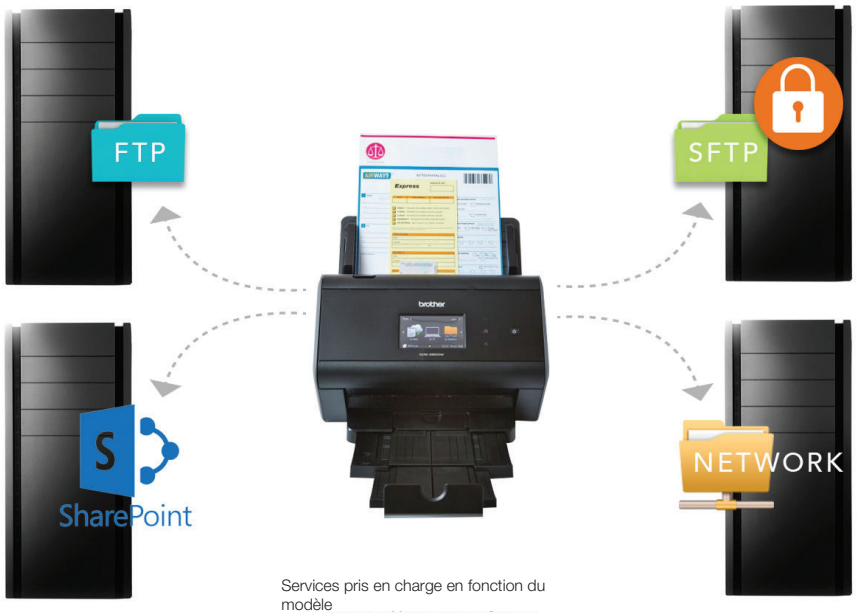
Quels sont les dangers?

Même si votre imprimante est sécurisée, un autre risque pour la sécurité guette à deux pas de là. En effet, les utilisateurs disposent de différents moyens pour enregistrer ou partager les documents numérisés. Le partage de documents numérisés par e-mail ou par Internet présente un grand risque pour les données confidentielles, car il suffit d'une petite erreur dans les documents pour qu'ils tombent entre de mauvaises mains. Et le pire, c'est que le document peut être copié et multiplié à l'infini.

Que peuvent faire les entreprises pour s'en prémunir?

La solution la plus simple consiste à transformer vos documents numérisés en **PDF protégés** par mot de passe. Les scanners individuels ou multifonction de Brother peuvent protéger tout nouveau fichier PDF avec un code à quatre caractères afin que personne ne puisse les ouvrir sans y être autorisé.

De nombreux scanners individuels ou multifonction Brother permettent aussi de **numériser vers un serveur SFTP**. Le protocole réseau Secure File Transfer Protocol assure la sécurité et la confidentialité du flux de données. Le contrôle plus étroit de l'accès aux serveurs SFTP permet même aux entreprises de rendre l'ensemble du réseau plus sûr en fermant complètement une passerelle de et vers leur système.



Services pris en charge en fonction du modèle

3. ACCÈS RÉSEAU NON AUTORISÉS DU FAIT D'UNE SÉCURITÉ INSUFFISANTE

Quels sont les dangers?

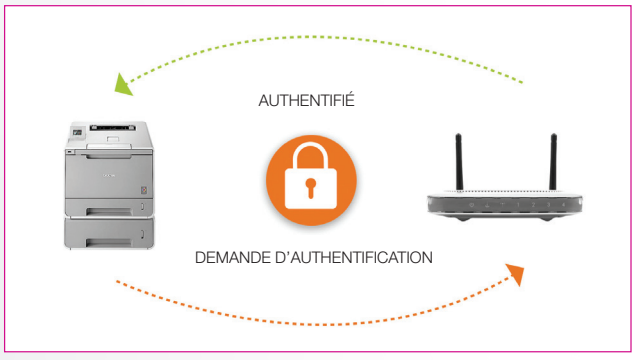
Il est courant que les tablettes et les ordinateurs portables exigent des certificats, des noms d'utilisateur et des mots de passe pour se connecter à un réseau sécurisé. Mais pour les imprimantes, ce n'est que rarement le cas, même si leur raccordement au réseau représente un danger tout aussi important pour la sécurité de l'ensemble du réseau.

Que peuvent faire les entreprises pour s'en prémunir?

Menaces externes

Les appareils Brother incluent différentes méthodes de chiffrement et offrent donc plusieurs possibilités pour améliorer la sécurité et combler les failles de sécurité.

802.1x: les appareils Brother sont tous conformes à la très exigeante norme de sécurité IEEE 802.1x, qu'ils soient connectés en filaire ou sans fil à un réseau d'entreprise.



IPsec: plusieurs appareils Brother peuvent se raccorder rapidement, facilement et à faible coût à des environnements sécurisés internes et externes grâce à IPsec. IPsec est déjà intégré à ces appareils, pas besoin donc d'installer d'intergiciel ou de logiciel tiers pour le raccordement.

SNMPv3: les appareils Brother respectent des règles de sécurité réseau strictes et comprennent donc toutes les instructions des versions SNMP chiffrées 1, 2 et 3 (MD5 et SHA1), y compris pour l'installation à distance et la maintenance courante.

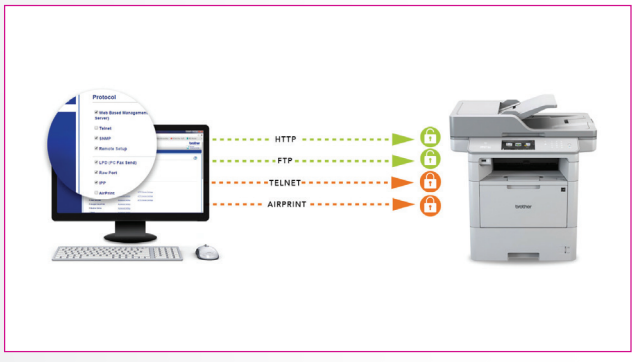
Même si les entreprises utilisent leurs propres outils pour administrer centralement leur parc d'imprimantes plutôt que le programme BRAdmin de Brother, les imprimantes Brother s'intègrent facilement et rapidement à leur réseau sécurisé.

Menaces internes

Le chiffrement protège efficacement contre les dangers externes. Mais si des collaborateurs internes peuvent utiliser des imprimantes réseau par accès distant, les réseaux peuvent devenir vulnérables. Pour éviter tous ces problèmes, les imprimantes Brother prennent en charge les **serveurs Web intégrés protégés par mot de passe**, qui interrompent la connexion au bout de cinq minutes d'inactivité.

Ils prennent également en charge le **blocage d'IP**, qui permet d'empêcher l'accès à l'appareil via le réseau. Dans cet exemple, l'imprimante n'autorise que les utilisateurs avec les adresses IP suivantes à se connecter: 10.45.12.1, 12.45.12.45, 10.45.12.46 et 10.45.12.47.

La **surveillance des protocoles** est moins restrictive et permet de bloquer les protocoles non indispensables sans verrouiller complètement l'accès à tout (par exemple FTP ou SMTP). L'exemple ci-dessous montre comment un collaborateur informatique a bloqué les fonctions suivantes: Telnet, AirPrint, proxy et serveur FTP.



4. ACCÈS PHYSIQUE D'UTILISATEURS NON AUTORISÉS À DES APPAREILS NON SÉCURISÉS

Quels sont les dangers?

Même avec toutes ces fonctions de renforcement de la sécurité, il reste possible de s'approcher d'une imprimante et d'y interroger les données. Sauf si elle se trouve dans un local fermé et sécurisé. Pour les petites et moyennes entreprises avec une infrastructure informatique restreinte, la sécurisation physique est particulièrement importante.

Dans l'enquête menée par Brother en 2015, deux tiers des décisionnaires ont déclaré que la sécurité des données jouait un rôle central dans la prise de décisions relatives à la gestion des impressions et des documents. Ils se sont notamment montrés préoccupés par la façon dont l'imprimante conservait les documents.

Que peuvent faire les entreprises pour s'en prémunir?

Pour ces entreprises, Brother propose toute une série de fonctions de sécurité permettant d'éviter que des personnes non autorisées ne manipulent les appareils.

Setting Lock fait exactement ce que vous en attendez. Cette fonction limite l'accès aux réglages de l'appareil via le panneau de commande. Cette solution est idéale pour les entreprises qui ne veulent pas limiter les fonctionnalités, mais s'assurer que les utilisateurs non autorisés ne peuvent pas modifier les réglages.

La fonction **Secure Function Lock** va un peu plus loin en empêchant l'accès aux réglages de l'appareil et à certaines fonctions. L'administrateur système peut décider qui peut faire quoi sur quel appareil en attribuant des codes personnels ou des cartes d'accès NFC. Il peut par exemple définir qui peut faxer et numériser, ou fixer des limites mensuelles.

La capture d'écran ci-dessous montre la page de configuration de la fonction Secure Function Lock du serveur Web intégré de l'appareil. On voit sur la première ligne «Mode public» que toutes les fonctions sont bloquées pour les utilisateurs non autorisés. L'utilisateur 1 dispose d'un accès illimité à toutes les fonctions (deuxième ligne). L'utilisateur 2 ne peut pas envoyer ni recevoir de fax et peut imprimer dans la limite de 100 pages. Cette limite peut être modifiée ou supprimée manuellement par un administrateur système ou être supprimée automatiquement au bout d'un certain temps.

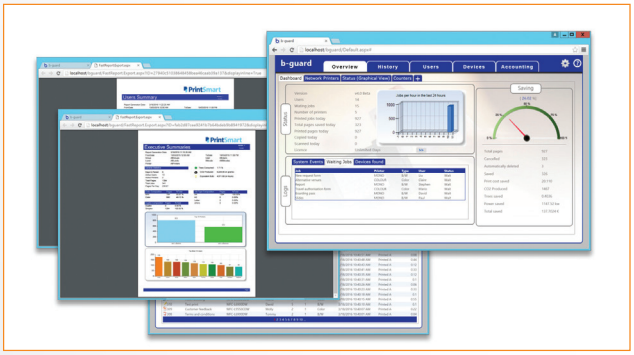
Dans les entreprises où plusieurs utilisateurs utilisent les mêmes imprimantes ou qui sont obligées de placer les imprimantes dans des lieux accessibles à tous, il peut s'avérer difficile d'éviter les abus sans affecter l'utilisation normale. Mais l'authentification via Brother Active Directory ou LDAP permet aux collaborateurs d'accéder facilement aux imprimantes à l'aide de leurs identifiants réseau actuels.

Le pack complet

Pour les entreprises qui souhaitent maîtriser leur sécurité et savoir précisément comment leurs appareils sont utilisés, Brother propose avec **PrintSmart Secure Pro** une solution logicielle innovante et abordable pour renforcer la sécurité, accroître l'efficacité, rendre les coûts d'impression transparents et réduire le gaspillage de papier. Une interface utilisateur simple fournit aux administrateurs système une meilleure vue d'ensemble ainsi que toutes les informations nécessaires à l'utilisation des imprimantes dans leur entreprise. Ils peuvent ainsi surveiller et piloter les activités et par là même suivre, contrôler et réduire les coûts d'impression.

De plus, les imprimantes Brother s'intègrent facilement aux solutions tierces de gestion des impressions. **Brother Solutions Interface (BSI)** est une plateforme ouverte de développement d'interface qui permet à des tiers de développer leurs propres solutions pour les appareils Brother.

Les entreprises peuvent donc adapter précisément l'interface utilisateur à leurs besoins.



Recommandations

Le danger que représentent les imprimantes et les scanners pour la sécurité des données et des réseaux doit assurément être pris au sérieux dans toutes les branches. Pour l'instant, il n'existe pas de solution universelle. Les administrateurs système doivent choisir la solution la mieux adaptée en fonction des risques, de leur infrastructure et de l'état actuel de la sécurité. Si une entreprise peut confirmer les trois points suivants:

1. **les appareils ont été sécurisés,**
2. **les données sont protégées lors de la transmission et après l'impression,**
3. **le réseau est protégé contre les accès non autorisés,**

il y a tout lieu de penser que ses imprimantes et scanners sont bien armés contre les éventuels problèmes de sécurité.

[1]Source: Brother SMB Research, menée par B2B International auprès de 2 502 entreprises au Royaume-Uni, en France, en Allemagne et aux États-Unis

[2]Source: Quocirca Managed Print Services Landscape, 2015. Enquête auprès de 200 entreprises de plus de 1 000 employés au Royaume-Uni, en France, en Allemagne et aux États-Unis