

Spécial sécurité

La lettre d'information grands comptes de Brother France

Édito

L'impression, maillon incontournable de la sécurité



S'il est bien un sujet qui ne fait plus débat, c'est celui sur l'importance d'une politique de sécurité rigoureuse au sein des entreprises. Mais combien d'entre elles intègrent dans leur dispositif la sécurité des impressions ? Et pourtant...

Tous secteurs confondus, la sécurité informatique fait figure de priorité absolue pour toutes les grandes entreprises : confidentialité des données, intégrité et disponibilité des informations conditionnent non seulement la bonne marche des organisations au quotidien, mais aussi le maintien de leur avantage concurrentiel sur des marchés toujours plus globaux et réactifs. Entre les menaces de type viral, les tentatives d'intrusion plus ou moins malveillantes et les risques liés à des utilisateurs peu scrupuleux ou insuffisamment sensibilisés, le danger est en effet bien réel et permanent.

Tout naturellement, la sécurité constitue donc un enjeu majeur pour Brother, tant au niveau de la conception de nos produits que dans les pratiques que nous préconisons pour leur utilisation. Présentes dans toutes les grandes entreprises, les solutions d'impression Brother permettent ainsi de soutenir efficacement les politiques de sécurité mises en œuvre. Par exemple, l'utilisation systématique de mémoires volatiles dans nos imprimantes, en

lieu et place de disques durs potentiellement «bavards», réduit considérablement les risques de détournements d'information. Car on a encore trop tendance à l'oublier : l'imprimante est un élément du système d'information à part entière. Et les meilleurs dispositifs de sécurité verront leur efficacité compromise si leur périmètre d'action



MFC 8860DN

n'intègre pas ces périphériques, qu'il s'agisse d'imprimantes ou de multifonctions. Bien sûr, la première des sécurités, c'est la proximité ! Mais si les solutions Brother ont toujours été pensées pour des utilisations au plus près des utilisateurs, seule une politique d'impression et de configuration rigoureuse permettra à l'entreprise de maîtriser réellement ses informations stratégiques.

Bonne lecture

Andreas Gerber,

Président Directeur Général

Printemps 2006

Sommaire

En bref

Toutes les actus et les infos utiles : nettoyage, piratage, maintenance... Sécurisez vos imprimantes !

page 2

Dossier

Imprimantes : le risque négligé. Mettez l'impression au cœur de votre politique de sécurité

page 2

Glossaire

Tous les termes clés : adresse IP, FTP, SMB, VLAN...

page 3

Focus

Assurez la sécurité physique de vos documents en sensibilisant les utilisateurs

page 3

Avis d'expert

Les imprimantes : le pain béni des pirates !
Frédéric Charpentier, consultant sécurité pour le cabinet de conseil en informatique XMCO Partners

page 4

En bref

L'imprimante : un vrai serveur

Oubliez qu'il s'agit d'une imprimante. Le boîtier qui trône dans la salle de copie dispose d'un processeur, d'une bonne quantité de mémoire vive, parfois d'un disque dur et de nombreux services réseaux (SMB, FTP, serveur web pour l'administration...). Autant de ressources à sécuriser afin d'éviter qu'elles ne soient détournées.

Disques durs : le grand nettoyage

Votre imprimante retourne chez le fournisseur ? Si elle dispose d'un disque dur, pensez à le nettoyer. À condition bien sûr que l'équipement dispose d'une fonction de formatage sécurisé. À défaut, détruisez le disque car des traces des informations stockées sur les disques durs peuvent être récupérées très longtemps après avoir été effacées. Mais la meilleure sécurité demeure toutefois d'éviter les imprimantes dotés d'un disque dur, au profit de modèles mieux sécurisés dotés de mémoires flash volatiles pour le stockage des documents à imprimer.



Ne facilitez pas la vie aux pirates

Lorsqu'un pirate explore le réseau à la recherche d'une cible facile, il sera probablement plus attiré par une imprimante dont le nom est «direction_generale» que par celle nommée «brothers_001». Évitez de donner des noms évocateurs à vos imprimantes.

Soignez la maintenance !

Inutile d'hyper sécuriser votre périphérique d'impression vis à vis du réseau si la maintenance est assurée par n'importe qui ! Confiez la maintenance à un prestataire agréé et formé à de telles opérations en sites sensibles. Il aura probablement déjà mis en place des procédures de contrôle lors du recrutement des ses techniciens (antécédents, qualifications...). Cela afin d'éviter le «coup du plombier»...

Analyse

Imprimantes : le risque négligé

S'attacher à la sécurité du réseau et des serveurs, c'est bien. Mettre l'impression au cœur de sa politique de sécurité c'est encore mieux ! Car les imprimantes, copieurs, fax et autres multifonctions sont désormais ultra-connectés. Ils font partie intégrante du système d'information de l'entreprise et voient passer tous ses secrets. Un fait bien connu des pirates !

Pour les moyens généraux des entreprises, l'imprimante n'est qu'un élément de l'inventaire parmi d'autres. Pour l'équipe informatique, elle n'est souvent qu'un périphérique sans grand intérêt. Pour les pirates, en revanche, il s'agit d'une cible privilégiée car la qualité des informations qui y transitent rend l'attaque d'une imprimante particulièrement rentable. En effet, ce sont souvent les versions finalisées des documents qui sont imprimées. Et, surtout, les imprimantes sont rarement surveillées. Souvent gérées par les moyens généraux, mais connectées au réseau informatique, elles sont placées de facto dans un no man's land organisationnel. Chaque entité estime que c'est à l'autre de s'en occuper, ce qui laisse le champ libre aux personnes mal intentionnées.

Tout ceci n'est pas une vue de l'esprit. Les consultants en sécurité, par exemple, ne se privent jamais d'aller explorer les imprimantes connectées au réseau lors d'un test d'intrusion. Mal sécurisée, la file des documents en attente révèle souvent des informations confidentielles. Plan de licenciement en préparation, salaires des cadres dirigeants et propositions commerciales secrètes sont autant d'exemples vécus. Aucun de ces documents confidentiels n'aurait pu être intercepté sur les ordinateurs ou le réseau de l'entreprise, trop bien protégés.

Des solutions rarement mises en œuvre

L'absence de sécurité des imprimantes n'est toutefois pas imputable à un manque d'outils, mais bien souvent à une prise de conscience tardive des responsables de la sécurité. Car, bien qu'elles ne soient pas activées par défaut,



des fonctions de sécurité efficaces sont désormais intégrées aux équipements. Il est, par exemple, possible de contrôler qui peut accéder à quelle imprimante, à l'aide de mots de passe ou de méthodes d'authentification bien connues des responsables de la sécurité. Hélas, ces restrictions sont rarement mises en œuvre... De même, les techniciens du réseau découvrent souvent avec étonnement qu'ils peuvent isoler l'imprimante au même titre que n'importe quel ordinateur, ou serveur, sur le réseau. Celle-ci n'accepte alors les connexions qu'à partir de certaines adresses IP identifiées : uniquement les postes

des utilisateurs du département, par exemple. Pour plus de sécurité, ce contrôle peut être doublé d'un filtrage d'adresses MAC, qui permet d'identifier un poste de travail à l'aide d'un code inscrit en usine dans sa carte réseau.

Du Wi-Fi sécurisé

Lorsqu'elles sont compatibles Wi-Fi, les imprimantes peuvent également chiffrer intégralement

les flux d'impression à l'aide du protocole WPA, le standard en la matière. Grâce à WPA, l'imprimante et le poste de travail sont authentifiés - à l'aide d'une clé partagée et l'ensemble du trafic est protégé. Mais encore faut-il activer cette fonctionnalité ! Vis-à-vis du réseau, enfin, les équipes informatiques savent rarement évaluer les besoins et les limites des imprimantes auxquelles il est possible de se connecter depuis l'extérieur via un modem ; pour la maintenance, par exemple. Il convient alors de s'assurer que, depuis un accès modem, aucun «pont» ne

puisse être établi vers le réseau informatique local. Les imprimantes, enfin, n'ont pas nécessairement besoin d'être accessibles par l'ensemble de l'entreprise : un bon plan de segmentation du réseau - à l'aide de VLAN, par exemple - permet d'isoler chaque équipement sur la branche à laquelle il est destiné. Entre isolation réseau, filtrage et contrôle d'accès, le secret de la sécurité consiste finalement à considérer les imprimantes comme des citoyennes du réseau à part entière, au même titre que les serveurs, et sensibiliser les équipes informatiques comme les utilisateurs !



Glossaire

Adresse IP (Internet Protocol)

Le protocole IP permet aux ordinateurs d'un réseau de communiquer entre eux. Une adresse numérique unique, l'adresse IP, est attribuée à chaque machine connectée à Internet.

Adresse MAC (Medium Access Control)

Identifiant physique qui permet d'identifier de façon unique une machine sur un réseau local.

Code PIN (Personal Identity Number)

Suite de quatre chiffres ou plus permettant d'authentifier l'utilisateur d'un système.

FTP (File Transfert Protocol)

Protocole de transfert de fichiers avec identification et correction des erreurs dans les données transmises. Il permet d'envoyer (upload) et de recevoir (download) des fichiers.

Protocole WPA (Wi-Fi Protected Access)

Protocole de cryptage visant à protéger les réseaux sans fil. A été mis en place pour remplacer le protocole WEP (Wired Equivalent Privacy)

défaillant. Rend impossible la découverte des clés en assurant, plusieurs fois par seconde, le changement automatique des clés de cryptage entre les points d'accès et les postes sans fil.

Serveur d'authentification

Connecté au serveur d'accès, le serveur d'authentification renvoie les droits associés en fonction des informations d'identification fournies et valide l'identité de l'utilisateur.

SMB (Server Message Block)

Protocole utilisé pour interfacier les partages et les authentifications Microsoft. Utilise deux modes d'identification et deux modes d'envoi des mots de passe, crypté ou non.

VLAN (Virtual Local Area Network)

Réseau local virtuel dont la segmentation dépend d'une configuration logique sur laquelle on peut agir. Permet d'accroître la mobilité des utilisateurs, d'assouplir les conditions de diffusion des informations et de renforcer la sécurité.

Focus

Assurez la sécurité physique

La sécurité des documents dépasse le cadre du seul réseau informatique. La sensibilisation des collaborateurs et quelques bonnes habitudes peuvent renforcer la sécurité des documents au même titre que les meilleurs outils informatiques. Au-delà de la sécurité informatique, la perte d'un document papier ou sa lecture par un personnel non habilité représentent un risque souvent ignoré par les entreprises. Pour limiter l'occurrence de ce risque, il est nécessaire de sensibiliser les utilisateurs à ne pas laisser, par exemple, des impressions dans les bacs. Il peut également s'avérer utile d'inclure la manipulation des documents papiers dans la charte informatique de

l'entreprise en spécifiant qu'il est interdit de sortir ces derniers des locaux. Le flou habituel existant entre la politique de sécurité informatique et les règles de gestion de l'information sur d'autres supports est souvent à l'origine de pertes d'information pourtant simples à éviter. Sur le plan technique, une solution courante consiste à empêcher l'impression à distance de documents confidentiels : l'utilisateur doit être présent physiquement pour déclencher l'impression et parfois même s'authentifier à l'aide d'un code PIN. Par ailleurs, l'entreprise devrait prendre soin d'isoler physiquement les copieurs (par étage, par département...) et, si possible, de contrôler l'accès à la salle technique.



Avis d'expert



Frédéric Charpentier
Consultant sécurité

2002 : Ingénieur diplômé de l'école Polytech-Nantes.

2002 : Consultant Sécurité pour la société Trustvision.

2005 : Consultant Sécurité, responsable de l'offre «tests d'intrusion» au sein de Xmco Partners.

SPÉCIALITÉ : Tests d'intrusion des applications web de type e- business, banques et brokers en ligne.

Les imprimantes sont le pain béni des pirates !

Frédéric Charpentier est consultant sécurité pour le cabinet de conseil en informatique XMCO Partners. Il réalise couramment des tests d'intrusion pour le compte d'entreprises très diverses. Mais toutes ont des imprimantes à exploiter...

Pourquoi parle-t-on peu de la sécurité des imprimantes ?

Parce que cela n'intéresse personne dans l'entreprise ! Très souvent, les imprimantes sont configurées au minimum : lorsqu'on arrive à la faire fonctionner et que du papier en sort, plus personne n'y touche. Mais après tout comment pourrait-il en être autrement ? De nombreuses entreprises commencent tout juste à parler de gestion des droits efficaces sur les serveurs, alors leurs imprimantes sont encore très loin dans la liste des priorités sécuritaires.

Pourtant, le copieur est une cible tentante...

L'imprimante est une cible d'autant plus tentante qu'elle est facile à identifier. Par exemple, les équipes de la direction n'aiment pas lire à l'écran et ont tendance à tout imprimer. Ainsi pour un pirate il sera plus rentable de repérer l'imprimante de la direction générale ou des ressources humaines, que de s'attaquer à leurs PC, qui sont généralement mieux protégés. Et c'est un problème bien réel : durant un test d'intrusion nous avons ainsi pu récupérer un plan de licenciement qui était stocké dans la file d'attente de l'imprimante. Nous n'aurions jamais pu l'obtenir sur les PC de la direction.

Concrètement, où se situent les failles les plus courantes ?

Lors de nos tests d'intrusion, il nous arrive le plus souvent de récupérer des documents dans la file d'attente via des partages Netbios. Mais même si les accès au disque dur (lorsqu'il y en a un, ndlr) sont contrôlés, les entreprises devraient aussi se méfier des périphériques que l'on peut brancher directement sur l'imprimante. Si un collaborateur se connecte afin de transférer des documents à imprimer, on pourra parfois explorer aussi le contenu du support à travers le partage Netbios. Il s'agit là d'une erreur de configuration courante pour les imprimantes qui permettent ce type de connexion. D'ailleurs, d'une manière générale, le vrai problème est très souvent la mauvaise configuration de l'imprimante !

Faut-il une grande expertise pour «pirater» une imprimante ?

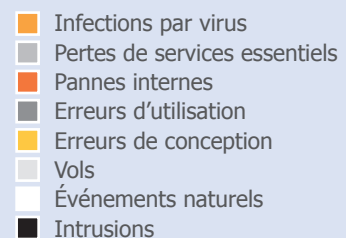
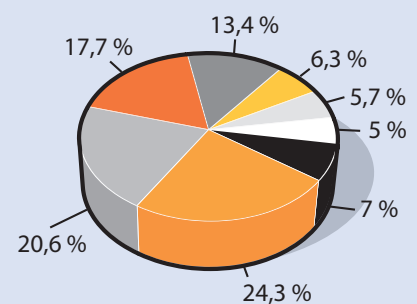
Non. Les entreprises sont souvent impressionnées lorsqu'on leur montre la faiblesse de leurs copieurs. Mais elles ont généralement tendance à minimiser l'incident par la suite, et donc sa portée. Leur excuse la plus courante est que personne chez eux n'aurait pu réaliser un tel piratage. Or c'est entièrement faux. Ce

n'est pas très compliqué et un utilisateur un peu curieux et un peu avancé peut tout à fait tomber dessus par hasard.

Les solutions sont-elles uniquement techniques ?

Non. Il faut idéalement mettre en place une charte de gestion des imprimantes et des documents imprimés au sein de l'entreprise, à la fois pour des raisons de sécurité, mais aussi pour des questions d'économies.

Évaluation de la sinistralité informatique



source : CLUSIF