Sécurité des multifonctions

Auteur: Ronald Eygendaal

La tendance actuelle consiste à utiliser de plus en plus ce qu'on appelle des appareils multifonctions ou MFC. Les multifonctions sont des appareils tout-en-un qui servent à la fois d'imprimante et/ou de fax et/ou de scanner et/ou de photocopieur. Un multifonction moderne a un serveur web qui reçoit les fichiers à imprimer via un réseau et les traite avant de les imprimer. Cela permet d'intégrer le MFC directement dans un réseau et de le gérer via un navigateur Internet standard. Les utilisateurs peuvent aussi établir, par exemple, une connexion Internet Explorer avec le serveur web dans le multifonction pour accorder la priorité à des documents dans la file d'attente ou à contrôler le niveau du papier. Il est en outre possible d'établir une connexion avec un multifonction depuis un poste de travail individuel afin de pouvoir utiliser la fonctionnalité de scanner.

Si des personnes malintentionnées réussissent à accéder, via un réseau, à ce serveur web et/ou au disque dur sur lequel se trouvent les données d'impression, fax ou documents numérisés, elles peuvent faire une utilisation abusive de ces informations avec toutes les conséquences que cela suppose. Même en réfléchissant sur la lutte contre les virus, les firewalls, etc., on peut prendre conscience que les multifonctions contiennent des informations précieuses et sont un élément crucial du processus. Compte tenu de la position centrale occupée par les multifonctions dans les réseaux, il ne faut pas négliger leur protection. Des évaluations ont révélé qu'une utilisation sécurisée des multifonctions nécessite l'établissement et le maintien de directives. Qui plus est, la sécurité des multifonctions doit faire partie intégrante de la politique de protection d'une entreprise. En résumé, les mesures physiques et techniques jouent un rôle crucial dans la sécurité de multifonctions. Des propriétés telles que l'authentification, le codage, la protection des données du disque dur, des numérisations et du serveur de documents sont extrêmement importantes.

PROTECTION TECHNIQUE

Contrairement à l'imprimante personnelle, les multifonctions sont en général installés dans des couloirs ou dans des pièces communes. Les personnes malintentionnées ont une prédilection pour ce genre de pièces, parce qu'il leur est facile de subtiliser des documents imprimés sans se faire remarquer. Les multifonctions modernes ont une fonction d'accès par code PIN pour combattre de telles pratiques. Un utilisateur peut entrer un code PIN pour imprimer, se rendre à l'imprimante et imprimer les documents en question avec son code PIN.

Il est également possible d'installer un lecteur de cartes sur les multifonctions ce qui permet à l'utilisateur concerné d'imprimer à l'aide d'un pass d'accès.

Pour empêcher des personnes non autorisées d'accéder au réseau interne, une séparation logique est faite entre le réseau normal et le réseau des multifonctions. L'opération s'effectue de préférence via des V-Lan.
Comme les multifonctions ont les propriétés d'un serveur intégral, par exemple disques durs, mémoire, etc., il convient de les protéger comme un serveur.

Des manipulations non autorisées, voire des intrusions sur le réseau étant possibles, il faut limiter l'accès au réseau et aux multifonctions. Une autre mesure de sécurité consisterait à bloquer les communications FTP (File Transfer Protocol) et à ne les débloquer qu'à la réception effective d'une commande d'impression. Le protocole FTP convient aussi pour le transfert de fichiers qui peut faciliter une intrusion sur le réseau.

Pour empêcher des personnes non autorisées d'accéder via la ligne de fax d'un multifonction au réseau interne d'une entreprise, il faut séparer la fonction fax des autres circuits de l'appareil. Comme il n'y a pas de connexion entre les deux réseaux, un éventuel hacker ne peut donc pas accéder au réseau de l'entreprise via la ligne de téléphone. La seule communication possible de l'extérieur est le fax. On pourrait envisager aussi une mesure complémentaire pour n'utiliser que des lignes de téléphone unidirectionnelles. (Une ligne de téléphone unidirectionnelle ne permet d'appeler que dans un sens, par exemple uniquement des appels sortants.)

Les multifonctions ont en outre un disque dur qui contient les données d'impression, fax ou documents numérisés. De ce point de vue, les multifonctions doivent permettre de transférer des données qui restent sur le disque dur interne après utilisation. Ce transfert doit avoir lieu quand la restauration des données transférées n'est plus possible. Nashuatec appelle cette fonction Data Overwrite Security (DOS). Xerox parle de 'Image Overwrite', d'autres fournisseurs utilisent des appellations encore différentes.

Le transfert de données doit avoir lieu de préférence après l'exécution de chaque commande de copie, d'impression, et/ou de numérisation. Les données qui restent après une commande numérisation ou de fax doivent faire l'objet d'un transfert quotidien pendant la nuit.

FONCTIONNALITÉS RESTREINTES

Les multifonctions ont des fonctionnalités restreintes du point de vue de la protection. La plupart de ces appareils permettent, par exemple, de numériser un document et de l'envoyer simultanément par e-mail ou fax. Ce sont des fonctions accessibles à tous qui présentent un risque énorme de fuite d'informations confidentielles. Il est en effet très facile de faire semblant de photocopier un document et d'utiliser en même temps la fonction de numérisation avec envoi par e-mail pour envoyer des informations confidentielles à une adresse e-mail non identifiée. il s'agit donc de bien réfléchir à la protection de cette fonctionnalité. Une solution possible consisterait à n'autoriser que l'envoi à des adresses e-mail internes sur le multi-

⇨ Suite à la page 56

⇨ Suite de la page 54

fonction concerné. Ou mieux encore, utiliser l'e-mail avec un code PIN car il reste des traces de ces e-mails. La même procédure s'applique bien sûr aussi aux fax.

La réception de fax présente également des risques car les multifonctions se trouvent en général dans des salles communes. Si la secrétaire pouvait autrefois surveiller l'arrivée des messages fax et s'il existait encore une forme de protection sociale, aujourd'hui les fax arrivent sur un appareil multifonction dans une salle commune. Il est en effet facile pour des personnes non autorisées de faire disparaître des fax entrants. Il faut donc trouver des solutions à l'installation de serveurs fax. Divers fournisseurs sont en mesure de proposer de telles solutions.

Comme un multifonction moderne a un disque dur, les utilisateurs peuvent se servir de ce disque (machinalement ou non) comme support de stockage de fichiers (par exemple, pour l'archivage). Cela n'est pas souhaitable du point de vue de la sécurité.

IEEEE P2600

Les fabricants de multifonctions ne sont heureusement pas restés les bras croisés et il ont identifié le problème de la sécurité. Ils ont créé des groupes de travail spécialisés dans la sécurité auxquels Hewlett-Packard, Lexmark, Canon, Xerox, Sharp, Ricoh, IBM, Epson, Okidata, Equitrac et Oce ont participé. Ceux-ci se sont penchés sur la norme P2600 sous la supervision de l'organisme de normalisation IEEE. "IEEE P2600" aidera les fabricants, gestionnaires de systèmes et utilisateurs à assumer les nombreuses responsabilités potentielles en matière de sécurité liées aux appareils hardcopy.
La P2600 décrit toute la chaîne d'impression, c'est-à-dire l'imprimante, le transfert des données, l'autorisation et l'impression des données. La norme P2600 security printing permet aux fabricants de certifier leurs multifonctions en fonction des Critères communs. La P2600 comprend quatre niveaux de sécurité qui dépendent entre autres du mode d'authentification. À savoir: un single-factor et trois techniques d'authentification two-factor.

P2600.1 Primary PIN (or card swipe) uniquement
P2600.2 Primary PIN (or card swipe) et secondary PIN
P2600.3 Network user ID et mot de passe
P2600.4 Primary PIN (or card swipe) et mot de passe réseau

LEASING OU LOCATION

De nombreuses entreprises ont des multifonctions en leasing ou location, ce qui peut gêner la mise en œuvre de la sécurité. Elles redoutent à juste titre la fuite d'informations via le disque dur d'un multifonction. Comme déjà indiqué, toutes les données sont stockées sur le disque dur d'un multifonction. Par expérience, nous savons que la fonction d'effacement est insuffisante dans de nombreux cas. La norme Gutmann, mais aussi la norme américaine DOD 5220.22M se basent sur le transfert de certains caractères effectué 35 fois. Comme la plupart des fournisseurs ont opté pour un transfert effectué trois fois, il est donc possible de récupérer des données effacées.

D'où l'intérêt de conclure des accords solides dans le cas du leasing ou de la location. Dès que le multifonction quitte l'entreprise, le disque dur est physiquement retiré et détruit.

RISQUES DE REMPLACEMENT DE FAX

Comme déjà indiqué, les multifonctions possèdent des fonctions de fax. Il est donc logique qu'ils remplacent le fax dès de leur installation. Ce processus de remplacement peut présenter des risques de fuite d'informations, surtout en ce qui concerne des fax thermiques. Ces appareils envoient des fax «thermiquement» sur du papier A4 ordinaire. Le mécanisme d'encrage est un rouleau de carbone appelé aussi rouleau de toner qui permet d'imprimer. Le carbone est du papier noir d'un côté qui peut être imprimé via un processus thermique. Un rouleau de carbone utilisé pour des fax peut conserver ses dimensions compactes, malgré ses limitations par rapport à la technologie du jet d'encre de qualité supérieure. Sa capacité d'impression est aussi limitée et dépend de la marque et du type de fax, car le rouleau est épuisé après un certain nombre d'impressions et il faut le remplacer.

Tous les fax reçus apparaissent en image miroir sur le rouleau plein. C'est très intéressant pour les personnes malintentionnées. Si on déroule le rouleau et le place sur un rayon lumineux, on peut lire tous les fax reçus. Il est donc important de retirer et détruire les rouleaux utilisés.

Pour la sécurité des informations, il ne faut pas oublier de prévoir un processus d'élimination des rouleaux de carbone utilisés.

CONCLUSION

L'achat et le remplacement de photocopieurs, de fax et d'imprimantes par des multifonctions ont passé le facility management. Les multifonctions offrent de plus en plus de fonctionnalités IT. Des correctifs de logiciels sont même disponibles pour eux. Il est donc possible de considérer un multifonction comme un composant IT à part entière et de configurer les processus et procédures comme dans IT.

Ronald Eygendaal est Security Consultant chez Getronics PinkRoccade et il a plus de quinze ans d'expérience dans la sécurité, l'étude des fraudes et la protection des données en particulier. Il est président du groupe professionnel Protection des informations de la Vereniging Beveiligingsmanagers Nederland (VBN).

liens

http://www.governmentsecurity.org/articles/HackingMulti-FunctionalPrinters.php

http://www.scmagazineus.com/Copiers-are-also-a-compliance-issue/article/35180/