L'impression sécurisée et son rôle dans la stratégie de sécurité de l'entreprise

- Intelligence économique -

Date de mise en ligne : mardi 26 fÃ©vrier 2008

Spyworld Actu

Aujourd'hui, la plupart des entreprises sont concernées par les risques associés à l'utilisation des outils informatiques tels que les messageries électroniques ou l'Internet. Les experts en sécurité s'accordent pour recommander le suivi d'une formation spécifique des salariés, afin d'améliorer le niveau global de sécurité de l'entreprise et lui permettre d'être en conformité avec les standards européens ISO 1 7799 ou américains COBIT. Qu'il s'agisse de protéger les réseaux contre les virus ou de sensibiliser les utilisateurs à l'importance d'utiliser leur mot de passe, le succès d'une stratégie de sécurité est fortement lié à la compréhension des risques par tout un chacun.

Il est communément admis que toute stratégie de sécurité doit regrouper au minimum les cinq « piliers » suivants :

- La sécurité physique, des sites ou des voitures de fonction par exemple ;
- La sécurité des individus constituants les publics internes et externes de l'entreprise ;
- La sécurité des données concernant à la fois les données électroniques (fichiers, courriel) que papier ;
- La sécurité des systèmes réseaux qui comprend :
- la protection du système informatique et de son périmètre,
- la protection des applications logicielles (en particulier au niveau de l'architecture, de l'accès au(x) programme(s)).
- La continuité des Services Informatiques et les plans de reprise d'activité après sinistre : mesures mises en place pour s'assurer que toutes les fonctions vitales de l'entreprise soient toujours disponibles (ressources humaines, infrastructures informatique et réseaux, locaux) et récupérables, via un plan d'action, en cas de catastrophe (incendie, catastrophe naturelle, attentat, etc.).

Quels sont les risques associés au domaine de l'impression en réseau ?

Certaines entreprises ont une stratégie de sécurité qui inclut les cinq « piliers » de la sécurité mais peu d'entre elles prennent en compte les informations liées aux impressions « papier » générées par le personnel via le réseau informatique ! Nous parlerons dans ce contexte-ci de « stratégie de sécurisation de l'impression ».

Dans une entreprise, et particulièrement lors de l'utilisation d'une imprimante en réseau (c'est-à-dire partagée et physiquement accessible par plusieurs utilisateurs), un nombre important d'impressions est chaque jour oublié ou n'est pas immédiatement récupéré « sur » l'imprimante concernée, posant ainsi un problème de confidentialité important. En effet, n'importe quel collaborateur ou personne se trouvant sur le site de l'entreprise peut alors avoir accès à un document imprimé sur l'imprimante en réseau, le lire, l'emporter, le détruire ou le copier. Les risques sont multiples et d'autant plus critiques lorsqu'il s'agit de documents financiers, contractuels ou stratégiques.

La tentation de « s'emparer » d'un document laissé sur une imprimante est d'autant plus fort que les personnes ont connaissance de la classification de ces documents en tant que « public » (ouvert à tous), « confidentiel » (accès restreint à certaines personnes) ou « strictement confidentiel » (réservé à un groupe très ciblé) ; ce qui est fréquent dans les entreprises de taille moyenne et dans les grands groupes.

Quelles sont les solutions disponibles sur le marché et leurs avantages ?

Les lois sur la protection des données sont strictes et sont également valables pour les données imprimées sur les imprimantes de l'entreprise.

Il existe par exemple des solutions d'impression sécurisées permettant de stopper le document au niveau d'un serveur sécurisé qui sauvegarde temporairement le document jusqu'à ce que son propriétaire s'identifie sur l'imprimante (via par exemple un code, un badge personnel, etc.). Une fois identifié, le document peut être effectivement imprimé. Cette fonctionnalité est également viable pour les imprimantes réseaux, qu'ils s'agissent d'imprimantes traditionnelles ou d'imprimantes dites multifonctions (pouvant imprimer, scanner -reproduire- et faxer).

En ce qui concerne l'authentification des utilisateurs, tous les standards de sécurité recommandent la mise en place d'une solution robuste ne reposant pas uniquement sur des mots de passe choisis et maintenus par les utilisateurs, évitant ainsi un accès permanent aux données confidentielles. Les cartes à puces électroniques ou les mots de passe générés automatiquement toutes les minutes voire même le concept de biométrie (reconnaissance des empreintes digitales, de l'iris de l'oeil, etc.) peuvent appliquer au domaine de l'impression

Il est aussi possible de contrôler l'utilisation d'imprimantes multifonctions à travers l'accès à leurs fonctionnalités. L'entreprise peut implémenter une politique de sécurité autorisant certains utilisateurs à se servir des fonctions « scan to e-mail* » ou « scan to fax** » alors que d'autres collaborateurs ne pourront qu'imprimer ou copier des documents. Cette approche, très pragmatique, permet de contrôler le flot de documents imprimés et de définir des profils d'utilisateurs associés à chaque usage. Cette stratégie contribue conjointement à la réduction des coûts d'impression et à la mise en conformité de la politique de sécurité de l'entreprise (protection des données, lois sur les propriétés intellectuelles, etc.).

L'administration de parc, permet également d'obtenir une vue d'ensemble de l'utilisation du parc d'impression, et par là même de le sécuriser. Les solutions d'administration type WebJetadmin fournissent des rapports précis sur les données circulant sur le réseau, y compris les impressions et répondent ainsi aux exigences des standards ISO 17799 ou PCI (Payment Card Industry). Depuis une console centrale, l'administrateur créé des rapports déterminant le nombre de documents imprimés par machine, par site ou utilisateur, ...

Les solutions d'impression sécurisées offre également un contrôle des imprimantes sur le plan logistique. Par exemple, elles permettent de détecter une nouvelle imprimante sur le réseau et d'harmoniser la politique de sécurité avec le reste du parc d'imprimantes en place dans l'entreprise. Ce qui permet également de limiter les problèmes de [1]support techniques.

Comme on peut le voir la mise en oeuvre de solutions d'impression sécurisées peut finalement être rentabilisée très rapidement par à la réduction des coûts induite (en papier, toner, maintenance techniques).

Le rôle déterminant de l'impression sécurisée dans la stratégie globale de sécurité de l'entreprise

Une entreprise désireuse de se conformer au concept américain du CIA - Confidentiality, Integrity, Availability (Confidentialité, Intégrité, Disponibilité) - mais qui n'inclut pas une stratégie de « sécurisation de l'impression » prend des risques importants. La« sécurisation de l'impression » doit faire partie intégrale de sa stratégie de sécurité globale obéissant aux cinq piliers fondamentaux évoqués plus haut.

Cette stratégie permet donc à l'entreprise d'atteindre différents objectifs : réduction des coûts d'impression***,

augmentation du niveau de sécurité, amélioration notable de la productivité des employés, maintien de la confidentialité des données et donc application des lois en vigueur, et enfin diminution des coûts de support technique.

L'entreprise a désormais la possibilité de déployer des solutions techniques lui permettant de sécuriser ses données, d'administrer l'utilisation des ressources de son parc d'impression de façon proactive et de créer facilement des rapports sur les documents imprimés sur son réseau.

La stratégie de sécurité du domaine de l'impression joue donc un rôle important dans la stratégie globale de sécurité de l'entreprise.

**scan to e-mail : numériser pour créer un e-mail*

***scan to fax : numériser pour créer une télécopie*

****selon le Gartner, le coût de l'impression représente entre 1 à 3% du chiffre d'affaires des entreprises.*

Post-scriptum :

http://www.itrnews.com/articles/746...