ASSURER LA PÉRENNITÉ

Dans ce numéro

L'avenir de la sécurité des données et des documents : ce que vous devez savoir aujourd'hui pour planifier pour demain

Dans le présent numéro, nous examinerons les tendances 2013 en matière de sécurité des entreprises et, à la lumière de ces tendances, nous verrons comment les entreprises peuvent se protéger contre les brèches de données.

Année après année, le bureau traditionnel continue à évoluer, et il en va de même pour les questions de sécurité des entreprises. En ce début d'année, il est temps d'examiner certaines des plus récentes prédictions sur les tendances en matière de sécurité des entreprises pour 2013. Dans ce numéro, vous trouverez des suggestions sur la façon de mieux protéger vos renseignements confidentiels et votre réputation.

Tendance nº 1 : il y aura une hausse de la cybercriminalité

Piratage, hameçonnage, vers, logiciels malveillants, réseaux de zombies, virus, cyberharcèlement, vols d'identité... Les crimes informatiques sont là pour rester et continueront à être un « secteur en croissance » en 2013 et au-delà. Si une entreprise est victime de l'un de ces crimes, elle peut non seulement subir des pertes financières, mais son image de marque peut aussi être ternie, la confiance des consommateurs à son endroit peut s'amoindrir et elle peut être tenue responsable d'une fuite de données. En 2013, nous pourrions voir une hausse du piratage de grande envergure des entreprises et des organismes gouvernementaux, ainsi que des mutations des logiciels espions et malveillants ciblant les téléphones intelligents et les tablettes électroniques.

ASSURER
LA PÉRENNITÉ

En raison du rythme effréné de l'évolution de la technologie, les entreprises renouvellent constamment leur matériel et leur équipement informatiques, et recyclent, vendent, donnent ou jettent simplement le matériel qu'elles considèrent désuet. À cause de cette tendance, l'élimination adéquate du matériel vieillissant et obsolète est devenue un sujet de préoccupation nationale et mondiale. Lorsque le matériel informatique n'est pas éliminé adéquatement et que les renseignements confidentiels de l'entreprise et de ses clients sont exposés à une possible restauration, la réputation de l'entreprise est mise en péril, les profits de l'entreprise sont menacés et, inévitablement, les spécialistes des TI risquent d'être congédiés.

Les entreprises et les gestionnaires des TI doivent savoir qu'en effaçant, reformatant, supprimant ou démagnétisant les disques durs et les clés USB, ils ne font pas disparaître l'information à tout jamais. Dans les faits, les données de l'entreprise peuvent toujours être restaurées. La destruction sécurisée du matériel ou du support informatique demeure le seul moyen totalement sûr d'effacer l'information. La meilleure façon de s'assurer que personne ne puisse restaurer les données confidentielles et avoir ainsi accès aux renseignements privés des clients et de l'entreprise consiste à détruire physiquement tous les supports électroniques désuets en les écrasant. Ainsi, le matériel, comme les disques durs, les clés USB et les mémoires de photocopieurs, est complètement inutilisable et ne peut pas être réparé.

Tendance nº 2 : la sécurité de l'informatique en nuage reste à prouver

Comme de plus en plus d'entreprises transfèrent leurs données privées dans le nuage, des problèmes de sécurité peuvent survenir, notamment à l'égard de la confidentialité et de la sécurité des données.

En ce qui concerne la confidentialité des données, de nombreux pays ont des lois précises indiquant que les données sur les citoyens doivent être détenues à l'intérieur du pays. Avec l'informatique en nuage, ces données peuvent être conservées n'importe où, et il se peut que le client n'ait pas la moindre idée de l'endroit (au sens géographique) où elles se trouvent réellement.

ASSURER
LA PÉRENNITÉ

Sur le plan de la sécurité, les entreprises sont, à juste titre, préoccupées par les risques associés à l'hébergement des données commerciales dans le nuage. Lorsqu'on cède le contrôle de la sécurité des données à une tierce partie, il peut être difficile de s'assurer que les données sont gérées adéquatement. Il peut également être ardu de vraiment savoir qui a accès aux serveurs et si les données électroniques obsolètes de son entreprise sont convenablement détruites. Il est primordial de ne pas ignorer les pratiques et les politiques de gestion des risques de l'entreprise lorsque l'on fait affaire avec des fournisseurs tiers en ce qui a trait au stockage en nuage et à la gestion de bases de données.

Selon une récente étude du Ponemon Institute, seulement le tiers des dirigeants des secteurs des TI et de la conformité qui ont été sondés pensent que les environnements d'infrastructures en nuage sont aussi sûrs que les centres de données « sur les lieux ». Avant de considérer l'informatique en nuage, les dirigeants d'entreprises et les gestionnaires informatiques doivent poser des questions sans complaisance. En outre, il est préférable qu'ils obtiennent une évaluation de la sécurité par un tiers neutre avant de s'engager envers un fournisseur de services informatiques en nuage.

Tendance nº 3 : un nombre grandissant d'employés mobiles signifie une augmentation des menaces pour la sécurité

Grâce aux nouvelles technologies, les employés ont la possibilité d'habiter pratiquement n'importe où. En fait, selon une récente étude de l'IDC, on estime que le nombre de travailleurs mobiles dans le monde atteindra 1,19 milliard en 2013, soit 34,9 % de la main d'œuvre.

Malheureusement pour les spécialistes des TI, une augmentation du nombre de travailleurs mobiles signifie une hausse des menaces pour la sécurité. Bien que les appareils comme les téléphones intelligents et les tablettes électroniques permettent aux employés d'avoir accès à l'information lorsqu'ils sont à l'extérieur du bureau, ces appareils portatifs sont plus vulnérables aux virus et, pire encore, ils peuvent tomber entre de mauvaises mains pendant les déplacements des employés, exposant ainsi l'entreprise à un risque de brèche de données électroniques. En outre, le concept de bureau sans papier (mobile ou non) ne correspond pas à la réalité du monde du travail. Les travailleurs mobiles continuent à imprimer des documents confidentiels et ils ne respectent pas nécessairement les politiques de l'entreprise sur la destruction sécurisée des documents lorsqu'ils n'ont plus besoin de ceux-ci, exposant une fois de plus l'entreprise à un risque de brèche.

ASSURER
LA PÉRENNITÉ

Comme la tendance des bureaux mobiles continue de s'accentuer, les entreprises doivent mettre à jour et adapter leurs politiques sur la sécurité et la destruction des documents papier et des données électroniques.

En ce qui a trait aux pratiques exemplaires, nous vous proposons ici quelques protocoles sur la sécurité électronique et en ligne ainsi que sur la sécurité des documents papier.

Pour protéger vos employés mobiles contre une brèche de données électroniques, adoptez les pratiques suivantes :

- Veillez à ce qu'on vérifie régulièrement si les ordinateurs portables sont infectés par des virus et équipez-les des toutes dernières technologies offrant des niveaux de sécurisation optimaux;
- Veillez à ce que les politiques sur l'utilisation acceptable soient appliquées en bloquant l'accès au contenu inapproprié et aux sites Web à risque et en empêchant le téléchargement excessif;
- Protégez les échanges électroniques, notamment par courriel, cybercommunication et messagerie instantanée;
- Sécurisez les interactions, peu importe si les employés accèdent aux ressources de l'entreprise à partir de points d'accès Wi-Fi, de leur résidence ou de tout autre endroit;
- Veillez à ce que les appareils portables obsolètes (ordinateurs portables, téléphones intelligents et tablettes électroniques) soient éliminés adéquatement afin que l'information confidentielle qu'ils

ASSURER
LA PÉRENNITÉ

contiennent ne puisse pas être restaurée. L'effacement des disques durs n'élimine pas les données. Il a été démontré que la destruction physique des disques durs est le seul moyen totalement sûr de détruire les données qu'ils contiennent.

Pour éviter que vos employés mobiles ne facilitent, intentionnellement ou non, l'accès à l'information confidentielle se trouvant sur des documents papier, adoptez les pratiques suivantes :

- Instaurez une politique de déchiquetage intégral. Cela signifie que tous les documents qui ne sont plus nécessaires doivent être complètement détruits, et ce, de façon régulière;
- Formez vos employés en ce qui a trait à vos politiques de sécurité. La mise en place de politiques et de procédures est une chose, mais il est aussi important que tous vos employés connaissent les procédures de destruction de l'information et qu'ils soient formés régulièrement;
- Continuez à évaluer les risques de brèche de données de votre entreprise. Effectuez périodiquement une vérification de la sécurité de l'information sur les habitudes et les pratiques de vos employés mobiles en ce qui concerne l'entreposage et la destruction de l'information;
- Engagez un fournisseur fiable et bien informé qui vous aidera à vous conformer aux lois pertinentes, aux exigences en matière de formation, etc. Permettez à vos employés mobiles de profiter des services de ce fournisseur. Il est préférable de faire affaire avec un fournisseur qui vous remet un certificat de destruction une fois le déchiquetage effectué.

En mettant en place ces mesures et en révisant régulièrement leurs politiques sur la sécurité, les organisations ayant des employés mobiles peuvent se protéger contre les répercussions importantes et à long terme d'une brèche de données. Si le personnel ignore que des politiques et des procédures sont en place, des erreurs pourraient être commises, et celles-ci pourraient être fatales pour l'avenir de l'entreprise.

À propos de Shred-it

Shred-it, chef de file mondial parmi les entreprises spécialisées en sécurité de l'information, offre des services de destruction de documents qui garantissent la sécurité et l'intégrité des renseignements confidentiels de ses clients. L'entreprise compte 140 succursales dans 16 pays et offre ses services à plus de 150 000 entreprises mondiales, nationales et régionales, dont les plus grandes agences de renseignement et de sécurité du monde, plus de 500 services de police, 1 500 hôpitaux, 8 500 succursales bancaires et 1 200 universités et collèges.