7 recommandations clés pour préserver la sécurité de votre réseau informatique

Un article écrit par les experts de TELUS

Pour s'assurer de sécuriser au maximum le réseau informatique de votre entreprise, procéder par étapes est nécessaire. Voici une liste de vérification pour n'oublier aucun aspect.

1. Centraliser et simplifier

Une solution de gestion unifiée des menaces (United Threat Management, UTM) comporte trois avantages majeurs : elle permet de réduire les coûts associés à la sécurité informatique, d'assurer la compatibilité des différentes composantes de sécurité et de bien coordonner les efforts de surveillance.

Cette solution centralisée permet d'économiser non seulement de l'argent, mais aussi du temps. Il n'est pas nécessaire de consacrer plusieurs heures à la coordination des différents services de sécurité, puisqu'ils le sont déjà. Résultat : une réponse beaucoup plus rapide en cas de cyberattaque. Avec un système centralisé, il est aussi plus facile de former les employés et de s'assurer que tous comprennent le fonctionnement des réseaux.

Attention toutefois, la solution UTM doit comprendre toutes les caractéristiques nécessaires pour surveiller les activités de votre entreprise. De plus, acheter d'autres services complémentaires contredirait l'objectif de consolidation.

2. Crypter l'information

L'idéal est de crypter tous ses disques durs, pour brouiller l'information aux yeux des pirates potentiels. Cette opération est nécessaire si un disque dur est cloné, après avoir été volé par exemple, car il peut même révéler des fichiers que l'on croyait supprimés. Pour crypter les données, les utilisateurs de Windows peuvent utiliser le logiciel BitLocker, gratuit avec la version professionnelle de Windows 8 et les versions Ultimate et Entreprise de Windows 7. Les utilisateurs de Mac bénéficient automatiquement de FileVault, qui fait partie du système d'opération OS X.

Si votre entreprise fonctionne avec un nuage informatique, comme Dropbox, crypter l'information qui y est téléversée est aussi nécessaire, puisque les nuages informatiques sont devenus une cible de choix des pirates. L'entreprise SpiderOak se spécialise d'ailleurs dans les nuages informatiques cryptés. La synchronisation de pair à pair offerte par BitTorrent Sync réplique automatiquement des données sur des ordinateurs privés, en brisant l'information en une infinité de petits morceaux pour faciliter et sécuriser l'opération.

3. Sécuriser les ports d'entrée et les points de connexion

Il est primordial de sécuriser les passerelles, car elles sont responsables de la connexion entre les réseaux informatiques. L'approche la plus sécuritaire est de bloquer les menaces à la périphérie du réseau, grâce à l'inspection des paquets en profondeur (deep packet inspection). Les menaces prennent habituellement des formes anodines : courriels, échange de fichiers ou applications mobiles. Cette technologie permet d'analyser le contenu des données en paquets, afin de repérer les logiciels malveillants cachés dans ces fichiers en apparence inoffensifs.

Sécuriser les points de connexion est essentiel, étant donné la réalité du télétravail et la multiplication d'appareils mobiles. Une technologie Clean VPN analyse la sécurité des appareils extérieurs qui se connectent au réseau et peut les mettre à niveau à distance. Elle s'assure qu'une fois la connexion sécurisée, les données circulant sur le réseau sont exemptes de menaces.

4. Intégrer la redondance et le basculement (failover)

Les activités d'une entreprise ne devraient pas être compromises par un seul point de défaillance, c'est-à-dire que le système s'écroule parce qu'une composante éprouve un problème. Les coûts d'un tel risque sont énormes. L'entreprise paralysée par une perte d'accès à Internet en est un exemple classique, mais désolant puisqu'il est facile à prévenir.

Cette éventualité met en lumière l'importance de la redondance en sécurité informatique. Un deuxième équipement doit toujours être prêt à prendre le relais du premier. Le basculement (failover) redirige le service défaillant vers un deuxième appareil ou réseau de sauvegarde, afin de maintenir les activités de l'entreprise. Il est même possible de maintenir les transactions sécurisées d'une boutique en ligne en cas de problème. Ces deux caractéristiques sont habituellement intégrées dans les solutions UTM.

5. Être conforme : intégrer la conformité à la surveillance

Les entreprises doivent de nos jours respecter de nombreux protocoles de sécurité, et les vérifier un à un peut devenir fastidieux. La conformité des réseaux n'est que la base de la sécurité informatique et elle ne suffit pas à assurer une sécurisation

maximale. Pourtant, bien des entreprises négligent cette vérification, ce qui contrecarre leur stratégie globale.

Automatiser la conformité des réseaux est la solution la plus simple et la plus efficace. Elle est d'ailleurs intégrée dans la solution UTM. L'automatisation libère également du temps pour les employés de sécurité qui peuvent se concentrer sur des tâches plus importantes.

6. Sécuriser physiquement ses réseaux

Toutes ces mesures sont inutiles si on laisse la porte grande ouverte aux malfaiteurs ! En plus de s'assurer que seulement les bonnes personnes ont accès aux appareils et réseaux sensibles, installer des mots de passe complexes est obligatoire.

Il faut également pouvoir effacer à distance les données d'un appareil perdu ou volé. La conteneurisation, qui divise le contenu d'un appareil en deux, sépare plus efficacement le contenu critique qui doit rapidement être effacé. Cette mesure est mieux accueillie par les employés, qui seraient réfractaires à ce qu'on efface de leur appareil personnel leurs photos de famille pour éviter que des informations sensibles concernant la compagnie ne se retrouvent entre de mauvaises mains.

7. Se préparer aux imprévus

Devant les menaces informatiques, il ne faut pas seulement être réactif, mais proactif. En deux ans, les entreprises qui mettent en place des mesures de sécurité proactives ont été 53 % plus efficaces pour bloquer les cyberattaques, alors que celles qui demeuraient réactives se sont améliorées d'à peine 2 %, selon une étude d'Accenture et du Ponemon Institute.

Un imprévu peut être aussi banal qu'une fuite d'eau dans les bureaux ! Pour toutes les situations, l'équipe TI doit prévoir comment elle réagirait et tester son efficacité face à ces menaces, qui vont du simple hameçonnage à l'attaque par déni de service. Dans le cas où l'intégrité du réseau est compromise physiquement, un réseau privé virtuel de type SSL (secure sockets layer) offre aux employés la possibilité d'accéder au réseau de l'entreprise à distance.

Procéder à chacune de ces sept étapes permet d'assurer une sécurité optimale pour les réseaux de votre entreprise. De plus, n'oubliez pas que tous les employés de sécurité doivent être formés et conscientisés à l'importance de la sécurité informatique pour assurer le succès de l'opération…