La sécurité du réseau informatique de l'entreprise

Comme un grain de sable qui enraye une machine, le moindre virus peut avoir un impact majeur sur l'activité de votre PME. Raccordé en permanence à Internet, votre réseau doit être blindé contre les différentes attaques informatiques.

Le ciel peut vous tomber sur la tête du jour au lendemain, dès la première heure. Sans raison apparente, un virus vient de pénétrer votre réseau informatique. Dans de nombreux cas, il s'agit d'un ransomware (ou rançongiciel). Caché généralement dans la pièce jointe d'un email, ce code malveillant peut en quelques secondes « chiffrer » (ou crypter) tous vos dossiers.

Si vous avez mis en place une politique de sauvegarde cohérente, votre activité ne sera pas longtemps paralysée. Sinon, c'est la catastrophe. Fin septembre 2017, une petite entreprise du Puy-de-Dôme a été contrainte de mettre la clé sous la porte après ce type de piratage.

La sécurité du réseau informatique de l'entreprise : les mesures élémentaires à mettre en place

- **Première mesure : la sécurité physique**
  Trop souvent négligée, elle est pourtant essentielle ! **La pièce où sont installés les serveurs et l'équipement réseau doit être fermée à clé.** Son accès doit être réservé à quelques personnes dûment identifiées. Cette précaution qui ne coûte presque rien permet d'éviter des actes malveillants ou involontaires au cœur de l'entreprise, qui pourraient entraîner un effacement ou une fuite des données ou provoquer un dysfonctionnement de l'infrastructure.

- **Deuxième mesure : cloisonner son réseau**
  Après avoir déterminé les composants critiques (équipements, serveurs, postes de travail d'utilisateurs sensibles, etc.), il est nécessaire de cloisonner son réseau. Dans la Marine, si un bateau est touché il ne coule pas, car sa coque est divisée en parties indépendantes. Cela doit être la même chose pour un réseau informatique ; **si une partie est infectée, l'ensemble ne doit pas être contaminé** sous peine de bloquer toute l'activité.

- **Troisième mesure : sécuriser le Wi-Fi**
  Les accès sans fil de type Wi-Fi doivent utiliser un chiffrement en l'état de l'art (WPA2 pour « Wi-Fi Protected Access 2 » ou WPA2-PSK avec un mot de passe complexe). Il convient aussi de modifier le SSID (nom du réseau Wi-Fi fourni). Si un accès sans fil est disponible pour les personnes extérieures (techniciens pour la maintenance, stagiaires...), il doit être séparé du réseau interne et avoir un accès temporaire. Les clés d'accès au Wi-Fi doivent être « fortes » (comporter différentes lettres en minuscules et majuscules, des chiffres et des signes) et être changées tous les six mois par exemple.

- **Quatrième mesure : tenir un inventaire de ses équipements**
  Il est indispensable de tenir à jour la **liste précise de tous les équipements informatiques qui peuvent se connecter au réseau** (ordinateurs personnels, imprimantes, photocopieurs, etc.). Cet inventaire doit également indiquer les utilisateurs classés par droits d'accès (répertoires, applications, dossiers dans le Cloud, etc.) de façon graduée.

- **Cinquième mesure : filtrer les accès à son réseau**
  Cet objectif peut être atteint grâce à des **pare-feux dits de « nouvelle génération ».** Qu'il soit matériel ou logiciel, ce firewall intègre des capacités traditionnelles (filtrage de paquets, blocage d'URL…). Mais il peut également détecter et stopper de nombreuses attaques sophistiquées en analysant des applications et des protocoles de communication. À la différence des pare-feux de première génération, ceux-ci intègrent en effet des éléments de contexte supplémentaires (comme des bases de réputation des sites ou d'adresses IP malsaines) afin d'améliorer les processus de prise de décision. Il s'agit notamment d'identifier précisément les détails du trafic Web afin de bloquer les flux illégitimes et l'exploitation de vulnérabilités.

Ce qu'il ne faut pas faire

- **Ne jamais laisser les mots de passe par défaut**
  Même un appareil aussi anodin qu'une imprimante connectée ou une caméra de vidéosurveillance peut être utilisé pour pénétrer un réseau informatique. Dès que ces équipements sont installés, il est donc indispensable de modifier le mot de passe par défaut (que l'on peut trouver facilement sur internet pour chaque marque !) par un autre plus complexe et connu seulement de quelques personnes dans l'entreprise.

- **Ne pas se soucier des accès à distance**
  Qu'il s'agisse du télétravail, de la téléassistance ou de la téléadministration, cette connexion peut être à l'origine volontaire ou involontaire d'une infection de votre réseau informatique. Il **est donc recommandé d'installer un VPN**. Un « Virtual Private Network » ou « Réseau Privé Virtuel » désigne un accès sécurisé entre deux appareils ou plus. C'est en quelque sorte un tunnel réservé aux véhicules identifiés et autorisés. Il doit être mis en place pour le télétravail et les connexions à distance (cadres à l'étranger, télémaintenance…). L'accès à un VPN doit être sécurisé par l'utilisation de carte à puce ou d'un boîtier générateur de mots de passe à usage unique.

Pour aller plus loin

- **Protégez-vous contre le « phreaking »**
  Non sécurisé, votre réseau téléphonique peut vous coûter très cher. Surtout si vous êtes victime d'un **« phreaking »**, **un piratage de votre serveur téléphonique.**
  Fin août 2014, à l'issue d'un week-end, une entreprise implantée en région Rhône-Alpes constate que son serveur téléphonique a été piraté. Plusieurs centaines d'appels ont été émis essentiellement à destination de l'Afrique. Le préjudice est estimé à environ 12 000 € HT.

- **Pour limiter les risques :**
  - Verrouillez les lignes sortantes durant les périodes d'inactivité de l'entreprise (nuits, week-ends, jours fériés, vacances…).
  - Changer périodiquement les clés sécurisées d'accès au modem du serveur téléphonique et les mots de passe des comptes de messagerie vocale des salariés.

Pour vous accompagner dans la protection de vos postes de travail, découvrez l'offre Generali Protection Numérique
https://www.generali.fr/professionnel/assurance-cyber-risques/

Generali IARD. Société anonyme au capital de 94 630 300 euros. Entreprise régie par le Code des assurances - 552 062 663 RCS Paris
Siège social : 2 rue Pillet-Will - 75009 Paris

Informations non contractuelles à caractère publicitaire données à titre purement indicatif et dans un but pédagogique. La compagnie ne saurait être tenue responsable d'un préjudice d'aucune nature lié aux informations fournies. La contractualisation éventuelle avec le partenaire nommé ci-dessus se fait sous votre seule et unique responsabilité et ne saurait engager la responsabilité des sociétés Generali en France. Le choix de contractualiser ou pas avec ce partenaire relève de la gestion de votre entreprise et est sans incidence sur vos contrats d'assurance Generali qui demeure tiers à vos relations.

GAMP0002FC8A - Mars 2018