Le Cabinet ACDL Expertise vous informe :

Cybersécurité : quatre outils pour être bien protégé

Plus les circuits d'information d'une entreprise font appel au numérique, plus son système informatique doit être sécurisé. Voici quatre outils et démarches indispensables à la cybersécurité pour se prémunir des risques d'intrusions, d'altération ou de vol de données.

• Cybersécurité : un anti-virus mis à jour

A défaut d'être totalement infaillibles, les anti-virus sont indispensables. « *Les virus mutent si vite que les outils chargés de les traquer n'ont pas toujours le temps de s'y adapter, mais ils contribuent à renforcer la sécurité* », assure Pascal Guicherd, directeur informatique du cabinet d'expertise comptable MG, membre du groupement France Défi.

Les anti-virus préinstallés sur les systèmes d'exploitation récents s'avèrent assez efficaces. Parmi les solutions payantes, Norton, Kaspersky et Bitdefender tiennent la corde.

Mais Avast est un très bon choix … gratuit ! Reste ensuite à vérifier régulièrement que ceux-ci sont activés et à jour ! A noter : pour maximiser les chances de stopper les attaques, il est conseillé d'installer des anti-virus différents sur les serveurs et les postes de travail.

• Un firewall bien paramétré

Contrôlant le trafic et filtrant les flux de données afin de protéger le système des intrusions, un firewall constitue le premier niveau de protection en matière de cybersécurité.

« *Son paramétrage, souvent complexe, doit être effectué avec soin. Si l'entreprise n'a pas prévu de permettre à ses clients d'accéder à certaines fonctionnalités internes, les accès depuis l'extérieur doivent être fermés* », souligne Pascal Guicherd.

Dans le cas inverse, les autorisations d'accès doivent être bien délimitées. Enfin, un firewall doit être protégé par un mot de passe robuste, afin d'en rendre l'accès impossible à qui souhaiterait le désactiver.

• Un anti-spam de dernière génération

La messagerie électronique, c'est le maillon faible d'un système d'information par lequel passent la majorité des infections.

« *Filtrer les e-mails avant même qu'ils arrivent sur le serveur de l'entreprise est donc essentiel. Pour cela, un anti-spam est de rigueur, et de préférence de dernière génération* », prévient Cédric Manca, directeur des centres de services sécurité de l'intégrateur Exaprobe.

« *Les plus efficaces sont ceux qui demandent une authentification lors d'un premier échange, comme MailInBlack. Ils sont infranchissables par les robots !* » explique Pascal Guicherd.

Dans ce domaine, il existe d'ailleurs des solutions externalisées, telle que Altospam, avec mises à jour automatisées. Les mails indésirables sont filtrés sans qu'il soit nécessaire d'installer un logiciel.

• Des données « sectorisées »

A l'exception de la direction, aucun salarié n'a besoin d'accéder à l'ensemble des informations de l'entreprise. « Pour réduire les risques, les entreprises peuvent sectoriser leur système d'information, en permettant aux collaborateurs de n'accéder qu'aux données dont ils ont besoin dans le cadre de leur activité », explique Cédric Manca.

Une « gestion des identités » qui s'apparente aux habilitations données à chaque intervenant dans des secteurs sensibles comme la Défense. A ne pas négliger enfin, l'obligation faite aux salariés d'adopter des mots de passe robustes.

En fonction de leur niveau de complexité, il faut entre quelques minutes et plusieurs dizaines d'années aux robots malveillants pour les « cracker » !

Par Jean-Marc Engelhard, Accroche-press' en partenariat avec Le Parisien Éco pour France Défi
lundi 24 avril 2017 00h44

Les collaborateurs du cabinet se tiennent à votre disposition pour tout renseignement complémentaire.

Votre expert-comptable : Guillaume GAHIDE 03.27.62.18.11 / ggahide@acdl.fr