Le Cabinet ACDL Expertise vous informe :

Cyberprudence : comment sensibiliser son personnel?

Tous les salariés n'ont pas intégrés les risques induits par l'explosion de la cybercriminalité. Des cessions d'information, de formation et de communications ciblées sur les nouvelles pratiques des cybercriminels peuvent contribuer à accélérer la prise de conscience et la cyberprudence.

Plus aucune entreprise, quelle que soit sa taille, n'est à l'abri d'une attaque de cybercriminels. C'est une réalité dont tous les salariés n'ont pas encore pris conscience.

« *Pour en souligner l'importance, la question doit être portée par la direction générale* », conseille Coralie Hériter, directrice générale de l'éditeur de logiciels spécialisé dans la sécurisation des données et de l'identité numérique IDnomic. Elle doit par ailleurs être abordée d'entrée de jeu avec les nouveaux collaborateurs.

« *Lorsque l'entreprise dispose d'une charte informatique, ce qui est fortement recommandé, celle-ci doit être annexée au règlement intérieur, remise avec le livret d'accueil et signée lors de la prise de poste pour en confirmer la prise de connaissance* », poursuit Coralie Héritier.

Ce document peut d'ailleurs prévoir des sanctions disciplinaires, mais aussi rappeler les risques de poursuites judiciaires, par exemple en cas de violation des droits d'auteur.

Cyberprudence : une alerte sur les nouveaux risques

Mais au-delà de ces précautions formelles, une sensibilisation aux bonnes pratiques est indispensable. « *Celle-ci doit être pragmatique et s'appuyer sur des exemples concrets* », explique Michel Guillout, responsable informatique et qualité de Cigeco. Ce cabinet d'expertise comptable, membre de France Défi, a mis en place des sessions d'une demi-journée de formation à la sécurité informatique dans le cadre de son dispositif d'intégration des nouveaux collaborateurs.

« *Il existe de nombreux outils disponibles en ligne qui peuvent servir de support, comme les guides de bonnes pratiques proposés par l'Agence nationale de sécurité des systèmes d'information (ANSSI) ou le site Hack Academy développé notamment par le Club informatique des grandes entreprises française (CIGREF) pour alerter, sur un ton décalé, sur les cyber-risques* », remarque de son côté Coralie Héritier.

Et pour éviter que cette préoccupation passe au second plan, rien ne vaut des piqures de rappel régulières. « *Par mail ou sur l'intranet, nous rappelons régulièrement les principaux risques et les manière de s'en prémunir. Et nous envoyons des alertes lorsque de nouveaux types de pratiques frauduleuses apparaissent afin de favoriser la prudence* », indique Michel Guillout.

Des règles à définir en fonction de son activité

Principal point d'entrée des virus et autres ransomware, la gestion des messageries électroniques doit être au cœur de la cyberprudence.

Dans ce domaine, les règles doivent être claires. Les mots de passe doivent être robustes, c'est à dire comprendre des caractères alphanumériques et spéciaux. Ils doivent également être régulièrement modifiés.

« *Au sein de notre cabinet, les collaborateurs sont contraints de le faire tous les 46 jours* », indique Michel Guillout. D'autres sujets doivent aussi faire l'objet de mises en garde, comme l'obligation de passer les fichiers extérieurs à l'antivirus avant de les introduire dans le système d'information de la société ou l'interdiction d'y connecter des clés USB venues de l'extérieur.

A chaque entreprise, ensuite, de définir et de rappeler des règles en fonction de son activité et des contraintes de ses salariés.

Par Jean-Marc Engelhard, Accroche-press' pour France Défi
jeudi 20 avril 2017 08h02

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