5 conseils pour protéger son entreprise d’une cyberattaque

Petite, grande ou moyenne entreprise, vous êtes inévitablement exposée aux cyberattaques ainsi qu’aux conséquences désastreuses qu’une telle attaque peut engendrer.

Par ailleurs, avec l’entrée en vigueur du nouveau règlement européen relatif à la protection de la vie privée, à partir du mois de mai 2018, si votre entreprise récolte des données à caractère personnel et que celles-ci font l’objet d’un vol, d’une fuite ou d’une perte, il conviendra de notifier ce vol, cette fuite, ou cette perte endéans un délai de 72h à l’autorité de contrôle et aux personnes concernées.

Il va de soi que dans cette hypothèse,, votre entreprise devra être réactive en cas de cyberattaque. Les cybercriminels ont compris la valeur des données d’une entreprise. Ils multiplient les « ransomware » afin de gagner facilement de l’argent. Il s’agit alors pour eux de crypter des fichiers importants de votre entreprise, pour ensuite les décrypter, contre paiement d’une rançon.

Il est dès lors essentiel de faire le point sur les moyens dont votre entreprise dispose pour mieux se protéger.

1. Informer

La prévention par l’information au sein de l’entreprise est extrêmement importante.

Il est essentiel d’informer les travailleurs et éventuels sous-traitants quant aux risques, aux comportements à adopter, aux procédures à suivre, ainsi qu’à la nécessité de réaliser régulièrement des mises à jour de logiciels. L’importance de cette information s’étend non seulement à la protection de la base de données de votre entreprise mais également à la valeur

du savoir-faire de celle-ci.

Vos travailleurs et sous-traitants sont en effet en première ligne pour prévenir les problèmes et agir le plus rapidement possible.

L'information des travailleurs et des sous-traitants peut se réaliser au mieux par le biais d'un règlement de travail, mais également grâce à une charte de travail, un courriel régulièrement adressé, ou encore un simple rappel.

Lorsqu'un règlement de travail est disponible, il doit être lié au contrat de travail de chaque travailleur de l'entreprise.

2. Sécuriser

Il est essentiel de sécuriser les systèmes, bases de données, et réseaux informatiques de votre entreprise.

Sécuriser, c'est d'abord et avant tout prévoir des moyens d'accès aux données/systèmes/réseaux (identifiant et mot de passe), et les changer régulièrement.
C'est aussi prévoir des anti-virus adaptés à vos systèmes, éventuellement des firewalls, et mettre en place des logiciels permettant de surveiller l'intégrité de votre système d'exploitation, de votre site web ou de vos données et de contrôler l'altération de leur intégrité.
Vous pouvez également demander à votre responsable informatique de mettre en place des techniques permettant l'accès dynamique à vos outils informatiques, des techniques de chiffrement (des données ou des supports), ou encore des techniques de conservation de données.

N'hésitez pas à mettre en place ces systèmes de sécurité sur tous les supports, en ce compris les supports de données amovibles (par exemple les disques durs externes ou les clés USB, les téléphones portables et le matériel privé des travailleurs).

3. Actualiser

Les mises à jour peuvent se faire manuellement ou de manière automatique. Il vous faut vérifier la procédure à suivre et le faire vous-même si aucune mise à jour automatique n'est prévue.

Qu'il s'agisse d'améliorer les fonctionnalités du logiciel ou d'en intégrer de nouvelles, il faut savoir que les mises à jour peuvent corriger des vulnérabilités et/ou des bugs dangereux pour vos programmes. Prendre le temps de réaliser les mises à jour de sécurité leur permet dès lors d'être plus sécurisés et stables.
En outre, certains virus envoyés par les responsables de cyber-attaques s'appuient sur des failles de programmes – dues au fait qu'ils n'ont pas été mis à jour – pour intégrer le système dans son entièreté.

En conséquence, il faut assurer la mise à jour et, notamment : le système informatique de votre entreprise, les anti-virus et les firewalls, les navigateurs, etc.

4. Limiter

Tous les travailleurs n'ont pas besoin d'avoir accès à l'ensemble des données de votre entreprise. Si un travailleur réalise ses tâches à partir de la base de données client, il y a peu de chance qu'il doive avoir également accès en permanence au business plan ou à toutes les licences de marques que possède l'entreprise par exemple.
Dans ce cadre, plus vous limiterez les accès, plus vous protégerez les informations. N'hésitez dès lors pas à distiller l'accès à l'information en fonction du besoin réel de chaque département ou travailleur.

En outre, en cas de perte de données, ou du moyen d'accès informatique, il convient d'avoir prévu une procédure permettant de bloquer totalement l'accès aux informations les plus sensibles ou à la base de données, et ce à distance. De

nombreux systèmes informatiques le permettent, 24h/24 et 7j/7.

Il s’agit également d’un excellent moyen d’assurer la sécurité et la confidentialité des données.

5. Transférer

Enfin, il ne faut pas oublier de transférer les données importantes ou de les enregistrer quotidiennement et automatiquement sur un serveur sécurisé ou dans le cloud (de manière dématérialisée).

Cela s’avère indispensable, d’une part afin de pouvoir récupérer les données et de continuer à travailler en cas de cyberattaque, et d’autre part afin de leur donner une protection plus importante.
Au vu de la multiplicité des cyber-attaques, de nombreux fournisseurs informatiques se sont par ailleurs spécialisés dans le domaine.

Conclusion

Informer – Sécuriser – Actualiser – Limiter – Transférer.

5 mots pour 5 actions à réaliser au plus vite au sein de votre entreprise et – ainsi – protéger au mieux votre réseau, vos programmes, et vos données.

Frédéric Dechamps & Caroline Lambilot – Avocats au Barreau de Bruxelles