DPO Consulting
Your personal data protection officer
Bourgogne Franche-Comté

LETTRE D'INFORMATION
Juin 2021

CYBERATTAQUES : RENFORCER SA SÉCURITÉ EN FORMANT SES SALARIÉS

L'hostilité émanant du cyber espace ne cesse de croître, en attestent : les 192 signalements de ransomware relevés par l'ANSSI en 2020 (contre 54 en 2019) et l'augmentation de 400% des tentatives de phishing. Dans son rapport d'activité publié le 12 mai dernier, cybermalveillance.gouv.fr indiquait que les demandes d'assistance émanant des professionnels du public comme du privé concernent des ransomwares dans environ 20% des cas, plaçant cette menace en tête de liste en 2020.

La sécurité des systèmes d'information est désormais une préoccupation majeure. L'utilisation du numérique a depuis longtemps transformé nos façons de travailler et elle s'est encore intensifiée avec la crise sanitaire.

Cette évolution ne s'est pas faite sans que les acteurs cyber malveillants perfectionnent leurs méthodes et adaptent leurs communications au contexte actuel : faux courriels en lien avec la pandémie, faux sites Internet. À titre d'exemple, l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) recense déjà 322 nouveaux sites ajoutés à sa liste noire au cours du 1er trimestre 2021[1]. Les cybercriminels intensifient leurs activités pour exploiter les failles offertes par les mesures sanitaires, comme le recours au télétravail.

Il faut dire que leur activité est lucrative : **la cybercriminalité a coûté 1 000 milliards de dollars à l'économie mondiale au cours de l'année 2020, ce chiffre pourrait être multiplié par 6 cette année[2].**

Les cas de cyberattaques ayant contraint les victimes à mettre la clé sous la porte ne sont ni des mythes, ni des cas isolés. Les consciences s'éveillent petit à petit à force de rappeler aux PME et TPE qu'elles suscitent elles aussi l'intérêt des hackers. En effet, leur plus faible investissement en termes de temps et de budget concernant l'élaboration de process de sécurité informatique, facilite les moyens d'intrusion. Elles sont plus enclines à payer la rançon pour préserver leur activité. Elles peuvent également servir d'accès stratégique pour atteindre une cible figurant parmi leurs clients (attaque de la *supply chain*).

Les actes de cybermalveillance mettent également en lumière les enjeux liés aux fuites de données de données personnelles qui constituent un marché juteux sur le darkweb. La revente d'un dossier médical sur le marché noir peut se monnayer jusqu'à 250€[3].

Le risque pèse également sur les données confidentielles de l'entreprise qui risquent une divulgation au public par les hackers ayant pris le temps de les extraire. Ces scénarios peuvent placer les victimes dans des situations délicates (chantage, usurpation d'identité…).

Le Réglement Général sur la Protection des Données (RGPD) vient responsabiliser les organisations en matière de données personnelles et leur sécurité. Il prévoit la possibilité, pour l'autorité compétente (la CNIL), de sanctionner lourdement les manquements constatés notamment en matière de sécurité.

Un défaut de sécurisation fait donc peser de nombreuses menaces sur la tête des dirigeants : demandes de rançon, fuites de données, sanctions administratives, atteinte à la réputation et l'image de l'organisation, responsabilité pénale...

Dans ce contexte, l'obligation de formation découlant du RGPD répond à deux préoccupations majeures et intimement liées que sont la sécurité des systèmes d'information et le respect des règles relatives à la protection des données personnelles.

1 Thibault Lamy, « *Placements, crédits… attention, les sites d'arnaques se multiplient* », Capital.fr, 14 avril 2021
2 Le club des juristes, Rapport « LE DROIT PÉNAL À L'ÉPREUVE DES CYBERATTAQUES », avril 2021
3 Article de FranceTVinfo du 9 février 2021

Qu'en est-il de la formation des collaborateurs ?

L'essentiel de la sécurité de votre système d'information passera par ce qui est placé entre l'ordinateur et la chaise de bureau : vos collaborateurs.

Les incidents de sécurité informatique proviennent d'une erreur humaine dans 90% des cas[4], les salariés constituant le plus souvent le maillon faible de la chaîne relative à la sécurité informatique. Ainsi, tous les utilisateurs du système d'information de l'entreprise doivent être fortement sensibilisés aux risques et bonnes pratiques à adopter à leur échelle, en mettant l'accent sur les campagnes de phishing qui sont à l'origine de 91% de toutes les cyberattaques[5].

Cette sensibilisation en amont est largement promue par Guillaume POUPARD, directeur de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) qui déclarait déjà en 2017 *« la formation et la sensibilisation doivent être une priorité stratégique pour tous les dirigeants »*[6]. L'ANSSI publie à ce titre des guides et documents préventifs afin de les aider dans cette tâche.

Une obligation légale renforcée par le RGPD

La sécurité des données s'entend par :

- l'intégrité (la donnée est exacte),
- la disponibilité (elle est accessible),
- la confidentialité (elle n'est connue que des personnes autorisées).

La Cour de cassation a déjà eu l'occasion de se prononcer sur la condamnation des responsables d'une structure qui, **par une formation insuffisante du personnel, avait favorisé l'accès par des tiers non autorisés à des données nominatives** (*arrêt de la chambre criminelle du 30 octobre 2001, n°99-82.136).*

L'obligation de sécurité des données n'est pas une nouveauté du RGPD, elle était déjà prévue dans l'article 34 de la loi Informatique et libertés qui dispose que *« le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »*

L'article 32 du RGPD vient renforcer cette loi en imposant quant à lui de mettre en œuvre « *les mesures techniques et organisationnelles appropriées* », compte tenu de l'état des connaissances, des coûts de mise en œuvre et des caractéristiques du traitements de données.

Votre structure a nommé un Délégué à la Protection des Données (DPO) ?

C'est à lui que revient la tâche de sensibiliser et de former vos collaborateurs, comme l'indique le RGPD. En effet, son article 39 énumère les missions obligatoirement confiées au délégué à la protection des données (ou DPO) que l'organisme a désigné. Il a donc pour mission de *« contrôler le respect du présent règlement, d'autres disposition du droit de l'Union ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la* ***sensibilisation et la formation du personnel participant aux opérations de traitement****, et les audits s'y rapportant »* (article 39.1.b).

Le texte invite donc à former les collaborateurs pleinement impliqués dans les opérations de traitement de données, lesquels devront bénéficier d'une formation sur les principes du RGPD auxquels les traitements sur lesquels ils opèrent sont soumis ainsi que les évolutions législatives et réglementaires les concernant.

Cependant, pour combler entièrement l'exigence de sécurité de l'article 32 du RGPD, nous ne pouvons que vous conseiller de sensibiliser tous les collaborateurs qui utilisent le système d'information aux mesures d'hygiène informatique.

---

4 Kapersky, Livre blanc « La sensibilisation des collaborateurs à la sécurité informatique », 2019

5 Selon le cabinet de conseil Deloitte dans un article publié le 9 janvier 2020 : https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html

6 Interview accordée à Paul Molga par Guillaume Poupard, *LesEchos*, 19 octobre 2017

En l'absence de désignation d'un DPO ?

Si vous n'êtes pas dans l'obligation de nommer un DPO, il est recommandé au responsable de traitement de suppléer, lui-même ou un délégataire, à celui-ci afin de dispenser cette sensibilisation/formation et ainsi se conformer à l'article 32 du RGPD relatif à la sécurité du traitement.

Cette mission pédagogique n'est soumise à aucun formalisme imposé par le RGPD. Les dirigeants sont donc libres de choisir le moyen le plus adapté à leur organisation, les données traitées et les risques qu'elles encourent.

L'adoption d'une charte informatique peut constituer un premier niveau de sensibilisation aux questions de sécurité informatique et de protection des données personnelles. (*Nous préparons une note d'information qui lui sera consacrée dans les semaines à venir.)*

Comme évoqué précédemment, l'ANSSI publie également des guides de bonnes pratiques, d'hygiène informatique sur lesquels vous pouvez vous appuyer pour élaborer les formations qui seront dispensées à vos collaborateurs. Enfin, incitez-les à passer le MOOC *SecNumacademie* de l'ANSSI ou *L'atelier RGPD* proposé par la CNIL pour permettre aux acteurs qui sont au cœur des traitements de données personnelles d'approfondir leurs connaissances sur les principes posés par le RGPD. Cette dernière publie également sur son site internet une large documentation qui pourra vous servir.

Vous pouvez enfin faire appel à des prestataires externes de la cybersécurité ou de la protection des données personnelles. Cette option vous permet de bénéficier d'une formation dispensée par des spécialistes desdits domaines et donc d'être assuré de la qualité des interventions.

Vous pouvez retrouver nos précédentes notes d'informations sur le site internet :

- la conformité des sites web
- la responsabilité du sous-traitant avant et après le RGPD
- la prospection commerciale sur LinkedIn

DPO Consulting franchise Bourgogne Franche-Comté
SAS MCC au capital de 31 490 € - ZA les Salines - 25115 POUILLEY-LES-VIGNES
RCS Besançon 434 463 683 - TVA FR 24 434 463 683 - CRCA Besançon République 12506 20049 24447562010 78
Éric CUENOT / Président & Data Privacy Officer 06 65 91 28 76 eric.cuenot@dpo-consulting.com
Stéphanie BROGGINI / Data Privacy Officer 07 55 58 02 80 stephanie.broggini@dpo-consulting.com