Lutter contre la cybercriminalité en renforçant vos contrats

Les infractions commises dans l'environnement numérique sont multiples : intrusions dans un système d'information, escroquerie aux faux ordres de virement, altération du site internet, déni de service, rançongiciels, usurpation d'identité, fraudes, e-réputation et concernent autant les personnes individuelles que les entreprises et les États.

Le nombre de cyberattaques croît de manière exponentielle et les préjudices, polyformes, peuvent être très conséquents.

Si la lutte contre la cybercriminalité est avant tout une affaire technique, la cybercriminalité doit être également appréhendée en amont, de manière préventive, dans les contrats conclus entre les entreprises et leurs fournisseurs. il est également indispensable de sensibiliser le personnel sur les risques liés à l'utilisation des ordinateurs, smartphones, connexions ... mis à leur disposition par l'entreprise.

Diagnostics de l'exposition au cyber-risque de l'entreprise

Au niveau contractuel, la première étape de la protection contre la cybercriminalité consiste à tracer les liens entre l'entreprise et chacun de ses prestataires (FAI, hébergeur, développeur, maintenance etc...) pour vérifier l'existence d'un contrat et les conditions de celui-ci.

Les engagements contractuels vont être analysés également à la lumière de l'audit technique qui pourrait révéler des failles.

Les professionnels en sécurité numérique et les juristes pourront, main dans la main, apprécier la nature des menaces (techniques et juridiques) et améliorer la protection des données à haute valeur ajoutée, des données personnelles et des données sensibles, du secret des affaires, en élaborant un plan d'actions cohérent.

La cybergouvernance contractuelle : renforcer vos contrats avec vos fournisseurs

Un certain nombre de contrats sont impactés par le cyber-risque. Par exemple :

- Le contrat d'intégration : la livraison d'une nouvelle version peut contenir un malware. Les phases de tests doivent prévoir des mesures de sécurité spécifiques liées aux environnements tests et de production. Il est recommandé d'effectuer des tests sur des données fictives...
- Le contrat d'hébergement : l'hébergement de serveurs, de sites internet, d'applications, de données sensibles suppose des conditions de sécurité et des agréments[1] spécifiques.

- Le contrat Saas : toutes les données sont accessibles et hébergées par le prestataire, ce qui présente un risque élevé.

- Les contrats de TMA, de maintenance par lesquels, les prestataires livrent des patch, se connectent au SI de l'entreprise et sont donc des cibles potentielles pour une cyber-attaque.

Pour faire face à ces risques, de nouvelles exigences contractuelles doivent être insérées dans les contrats afin d'engager les prestataires (i) à respecter, notamment, les meilleurs standards de l'état de l'art, ceux-ci devant être décrits et vérifiables, (ii) à communiquer au client les résultats des tests, (iii) à appliquer les recommandations de l'ANSSI et surtout (iv) à contractualiser leurs engagements techniques.

De leur côté, les prestataires ont tout intérêt à apporter de la transparence et à favoriser la bonne compréhension réciproque des mesures techniques qui sont appliquées et leurs limites.

La cybergouvernance interne : la responsabilité digitale de l'entreprise

Les cyberattaques trouvent souvent leur origine dans une négligence interne, une erreur humaine (ex ouverture d'un mail douteux) qui aurait pu être évitée par une sensibilisation du personnel et la transmission des bons réflexes.

Outre la mise en place d'une équipe transverse, plusieurs outils juridiques sont disponibles pour « contractualiser » les mesures internes de lutte contre la cybercriminalité, dont :

- Le règlement intérieur qui permet de rendre opposable les mesures de protection définies par l'entreprise ;

- La charte d'utilisation des moyens d'information et de communication mis à la disposition des salariés : traçabilité, filtrage, synchronisation... qui doit avoir un caractère contraignant ;

- Le PSSI qui a pour fonction de décrire la politique de sécurité du SI de l'entreprise.;

- La formation des salariés, essentielle pour assurer la compréhension et le respect des mesures définies et pour responsabiliser chacun ;

- Les audits internes et les plans d'actions.

Comme pour les contrats avec les prestataires, ces documents doivent être enrichis par de nouvelles exigences spécifiques, qui complètent celles mises en place dans le cadre du RGPD, et par les bons réflexes à adopter pour contenir une cyberattaque et préserver les preuves.

Le télétravail étant un facteur d'augmentation du cyber-risque, la mise en place d'une cybergouvernance interne est particulièrement opportune.

Nos recommandations : Renforcer les contrats avec vos prestataires, compléter les bonnes pratiques internes et intégrer, si ce n'est déjà le cas, un juriste (in house ou externalisé) dans une équipe transverse.

Isabelle BOUVIER
BOUVIER AVOCATS

1 - CNIL décision 4 octobre 2021 Francetest : outre un défaut de configuration du site web, la société Francetest qui met à la disposition des pharmaciens un site web pour leur permettre de collecter les données personnelles et de les acheminer vers un système d'information national de dépistage du Covid, a confié l'hébergement des données de santé à une société qui n'était pas agréé, outre d'autres insuffisances constatées.