MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

LETTRE CYBER en Région Grand Est

Gendarmerie nationale

GENDARMERIE

NOTRE ENGAGEMENT, VOTRE SÉCURITÉ

JANVIER 2025

LA THEMATIQUE DU MOIS:
Les entreprises et leurs prestataires de service Cyber

Le numérique est un élément incontournable dans la vie des entreprises. De l'artisan à la multinationale en passant par les PME et TPE, il est omniprésent. Mais les connaissances des uns et des autres dans ce domaine sont variables et finalement, personne (ou presque) ne peut prétendre savoir maîtriser pleinement les outils informatiques. Les sociétés ou les collectivités territoriales font donc souvent appel à un ou plusieurs prestataires de service pour gérer leur environnement numérique. Mais comment choisir son sous-traitant ? Pouvons-nous lui faire confiance ? Est-il infaillible ? Plein de questions qui méritent qu'on s'y intéresse.
Nous verrons ensemble comment choisir son prestataire et également pourquoi il est important de garder un certain contrôle sur ses activités. Nous finirons par quelques exemples et conseils.

Choisir son prestataire

Choisir son prestataire de service cyber n'est pas une mince affaire car ils sont nombreux sur le marché. Mais alors comment faire pour savoir si l'un est meilleur que l'autre ?
Le plus souvent, en fait, on ne parlera pas de meilleur mais de **plus adapté**. Comme pour n'importe quel autre prestataire, votre choix doit d'abord prendre en considération plusieurs éléments comme vos besoins, sa réputation et son expérience ou encore ses tarifs.
Dans un cadre plus spécifiquement Cyber, il est également important de bien prendre en compte la manière dont votre prestataire remplit ses obligations juridiques, que ce soit, par exemple, dans le domaine du RGPD que dans celui de l'hébergement de vos données.
Et surtout, parce que les cyber-attaques (rappelons-le encore une fois) n'arrivent pas qu'aux autres, vous devrez faire attention à la façon dont votre prestataire entend gérer les incidents cyber, en terme de temps de réponse ou de qualité de la remédiation.
Vous l'aurez compris, il n'est pas aisé de choisir un bon prestataire de service cyber. Cela requiert une vrai étude en interne pour **bien cerner vos besoins**, et une prospection sérieuse pour trouver celui qui pourra y répondre.

Gérer son prestataire

Une fois le choix du prestataire effectué, les clauses du contrat devront correspondre aux besoins que vous avez définis et surtout bien circonscris. Par exemple, si vous cherchez un prestataire pour gérer uniquement un seul des progiciels que vous utilisez, il n'est peut-être pas utile qu'il ait accès librement à l'ensemble de votre cartographie informatique. Plus que dans d'autres domaines, en matière numérique, la mission du prestataire détermine ses accès et ses restrictions.

Communiquer régulièrement avec son prestataire

Vous allez lui confier l'accès de données, souvent sensibles, mais il ne faut pas oublier que ces données restent votre propriété et que vous demeurez responsable de l'utilisation qui en est faite. Vous devez donc régulièrement vous assurer de la manière dont elles sont stockées et de ce qu'en fait votre prestataire. Une communication entre vos services est donc incontournable. Ce n'est pas une surveillance tatillonne qui doit s'instaurer, mais plutôt une manière de collaborer efficacement en ayant toujours le souci d'un traitement optimum de vos données.

Quelques exemples

Un point doit être bien compris : votre prestataire, quelque soit son sérieux et son expérience, n'est pas à l'abri lui non plus d'une cyberattaque... Ses activités doivent donc s'inscrire en pleine cohérence avec votre propre stratégie de sécurité informatique. Voici quelques exemples d'attaques souvent liées au prestataire cyber :

- le défacement de site internet : c'est une attaque qui consiste à hacker un site web de manière à modifier les pages, le plus souvent celle d'accueil. Dans la plupart des cas, le site internet est hébergé chez un prestataire de service ;
- l'attaque XSS (Cross-Site Scripting) : c'est une attaque qui exploite les vulnérabilités des applications web en injectant un code malicieux. Cette attaque vise à voler des données sensibles. Tout comme le défacement, ces applications web sont souvent hébergées chez des prestataires ;
- l'attaque sur la supply chain (chaîne d'approvisionnement) : elle vise à compromettre un tiers, comme un fournisseur de logiciel ou un prestataire, afin de cibler la victime finale.

Cette liste d'attaques est évidemment pas exhaustive.

CONCLUSION

La sélection et la gestion d'un prestataire de service en cybersécurité est finalement tout aussi complexe que de recruter un bon employé. Les conséquences d'une décision trop rapide ou mal calibrée peut avoir des conséquences lourdes et le choix d'une entreprise prestataire doit être fait avec sérieux et prudence. Ce n'est pas toujours facile et c'est pourquoi l'ANSSI a rédigé une liste des prestataires qualifiés afin de vous aider dans vos démarches.

Ce qu'il faut retenir : **Faire confiance à son prestataire n'en exclut pas le contrôle.**

+ D'INFOS

ANJ AUTORITÉ NATIONALE DES JEUX

Grand Est Cybersécurité CENTRE D'ASSISTANCE DE PROXIMITÉ 0 970 512 525

CYBER MALVEILLANCE .GOUV.FR

PHAROS PLATEFORME D'HARMONISATION, D'ANALYSE, DE RECOUPEMENT ET D'ORIENTATION DES SIGNALEMENTS

e-Enfance 3018

CNIL. PROTÉGER les données personnelles ACCOMPAGNER l'innovation PRÉSERVER les libertés individuelles

ANSSI Agence nationale de la sécurité des systèmes d'information

Région de gendarmerie du Grand Est
LA LETTRE CYBER en région Grand Est

Directeur de la publication: GCA O.KIM
Responsable éditorial: COL L. GRAU
Rédacteur: AdJ Chef STOUFFLET

Si vous souhaitez recevoir cette lettre, envoyez un mail à :
Laurent.grau@gendarmerie.interieur.gouv.fr
Sebastien.stoufflet@gendarmerie.interieur.gouv.fr

Suivez l'actualité de la gendarmerie: