Premiers secours en cas de piratage

Que faire en cas de cyber-attaque ?

Quand il y a un incendie, vous appelez les pompiers. Quand il y a un cambriolage, vous appelez la police. Mais que faire si vos systèmes informatiques sont touchés par une cyber-attaque ?

Rares sont encore les entreprises qui s'y préparent correctement. Alors que le risque d'une cyber-attaque est beaucoup plus important que le risque de subir un incendie. Conséquence ? Des dizaines de milliers de dollars de dommages, une perte de réputation et la perte de données précieuses.

Soyez donc toujours préparés à subir un « incendie numérique ».

PRIVAL®

Secutec

Prevent now, secure tomorrow

Préparation

Vous devez toujours prendre certaines précautions, même si elles semblent évidentes.

Un système de back-up sûr

Chacun sait qu'il est raisonnable de réaliser régulièrement des back-up de ses données. Ces derniers ne sont pourtant pas toujours réalisés correctement. Notre conseil : avec votre prestataire de services informatiques, veillez à ce que les trois points suivants soient toujours en ordre.

- Réalisez des back-up réguliers.
- Conservez les back-up en un lieu numérique ET un lieu physique.
- Testez régulièrement vos back-up.

Bonne connexion

Vous voulez pouvoir réagir rapidement en cas de cyber-attaque ? Dans ce cas, de bons fichiers logs sont indispensables. Veillez à ce que des fichiers logs des principaux composants de votre réseau soient toujours disponibles. Et veillez à ce qu'ils ne puissent pas être contaminés par le virus placé dans votre système par les hackers.

Protocole de crise

Dans une situation de crise, il est généralement trop tard pour réfléchir et agir posément. Il est dès lors recommandé d'établir un protocole de crise.
Il se compose généralement de deux parties :

- La partie 1 porte sur la gestion de l'organisation en situation de crise, également dénommée Business Continuity Plan (BCP).
- La partie 2 porte sur la communication interne et externe.

Les informations importantes doivent également être disponibles sur papier

Le piratage peut rendre inaccessibles les coordonnées enregistrées au format numérique et rendre impossible tout accès à Internet ou au réseau de l'entreprise afin de les rechercher.
Il n'est pas impossible qu'un ou plusieurs canaux de communication ne fonctionnent plus. Conservez dès lors toutes les informations importantes de votre protocole de crise sur papier. Dans ce contexte, n'oubliez surtout pas :

- les personnes qui interviennent dans l'équipe de crise ;
- les données de contact de tous les collaborateurs ;
- les données de contact des instances publiques ;
- les données de contact des clients (vous faites parfois partie d'une chaîne) ;
- les données de contact des fournisseurs (vous faites parfois partie d'une chaîne) ;
- les données de contact de votre partenaire informatique ou d'experts de la sécurité ;
- les informations disponibles sur le darkweb au sujet de votre entreprise.

Dans le cas d'une fuite de données, vous devez disposer des données de contact des instances suivantes :

- Lorsqu'une entreprise québécoise subit **une fuite de données** impliquant des **renseignements personnels**, elle doit impérativement contacter la **Commission d'accès à l'information du Québec (CAI)** (https://www.cai.gouv.qc.ca/commission-acces-information/nous-joindre).
- Si l`entreprise opère dans plusieurs provinces, veuillez aussi informer le **CPVP** (https://www.priv.gc.ca/fr/)

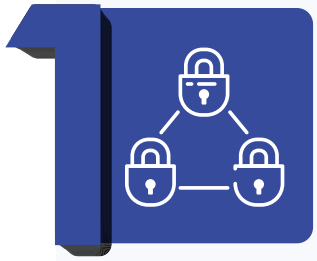
Assurance

Il existe des polices d'assurance pour vous assurer contre (une partie des) les dommages pouvant être causés par une cyber-attaque sur votre organisation et aux tiers. Il est intéressant d'examiner si une assurance (et de quel type) est nécessaire, compte tenu du fonctionnement et des risques encourus par votre organisation.

Lorsque vous avez conclu votre assurance, conservez toujours les données de votre personne de contact sur papier.

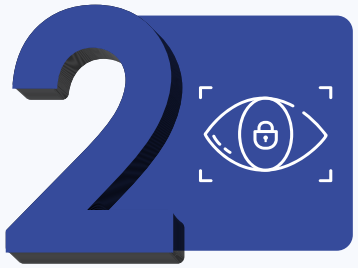
Quid si vous êtes victime d'une attaque ?

Si vos systèmes informatiques sont piratés, il est préférable de suivre une procédure standard. Parcourez les étapes énumérées ci-après avec un spécialiste informatique qui a de l'expérience des cyber-attaques et un spécialiste de la communication. Ces personnes peuvent être internes ou externes à la société.



LIMITER LA PROPAGATION

Déconnectez aussi rapidement que possible du réseau de l'entreprise les systèmes sur lesquels la présence du virus est constatée. Il est préférable de déconnecter également les systèmes épargnés pour qu'ils ne puissent pas être contaminés. N'éteignez jamais totalement l'ordinateur, car cela complique l'enquête.



ANALYSEZ LA CONTAMINATION ET L'IMPACT

Enquêtez pour savoir de quel virus il s'agit, comment il est arrivé et dans quelle mesure il s'est propagé (éventuellement aussi en externe). Une première ébauche des possibilités de réparation peut alors être réalisée sur cette base. Donnez toujours la priorité aux appareils critiques au sein de votre réseau, afin de pouvoir redémarrer rapidement.

3 ANALYSEZ LES BACK-UP

Lors de l'installation du back-up, vous devez tenir compte des éléments suivants :

- **Qualité**
  Le back-up est-il complet et contient-il toutes les informations essentielles ?
- **Âge**
  De quand date le back-up ?
  Quelle quantité d'informations avez-vous définitivement perdues lors de la réinstallation ?
- **Sécurité**
  Le back-up est-il contaminé par le virus ?
- **Temps**
  Combien de temps faudra-t-il avant que les systèmes fonctionnent de nouveau ?

Remettre en place ou recommencer ?

Après l'analyse suit une décision importante : remettons-nous le back-up en place ou réinstallons-nous tout à partir de zéro ?
Dans le protocole de crise, indiquez qui prend quelle décision, à quel moment et cherchez d'ores et déjà un fournisseur qui peut vous livrer rapidement du nouveau matériel (ou remis à neuf) sur site.

4 PAYER OU PAS ?

Si l'installation d'un back-up n'est pas possible, vous êtes face à un choix cornélien : faut-il payer la rançon pour les informations piratées ?
Plusieurs considérations importantes interviennent dans ce choix :

- À quel point êtes-vous certains de récupérer vos données quand vous aurez payé ?
- Qui décide si vous payez ?
- Quel est le montant maximum que vous acceptez de payer ?
- Qui mène les négociations avec les hackers ?
- Pour des raisons d'anonymat, le paiement est souvent demandé en crypto-monnaie (par exemple Bitcoin). Comment pouvez-vous acquérir cette monnaie et comment l'utiliser pour payer ?

5 COMMUNICATION INTERNE ET EXTERNE

La communication (interne et externe) autour d'un événement aussi important qu'un piratage doit être bien réfléchie. Il est intéressant de la définir dans le protocole de crise. Celui-ci contient des réponses aux questions suivantes notamment :

- Comment et quand informons-nous nos collaborateurs ?
- Comment procédons-nous avec les collaborateurs qui sont encore chez eux ?
- Quand informons-nous les externes impliqués (fournisseurs et clients) de la situation ?
- Est-il opportun d'informer d'autres parties prenantes internes et externes avant d'informer la presse ?
- Comment éviter que la presse ne reçoive des informations avant même que vous n'ayez communiqué avec le monde extérieur ?
- Quelles informations faut-il envoyer à la presse et à quel moment ?

Clients, fournisseurs et pouvoirs publics

Quand les données de votre entreprise sont piratées, une instance extérieure a eu accès à des informations pouvant se rapporter à des personnes et organisations externes à votre entreprise.

Cela a des conséquences sur la loi sur la protection des renseignements personnels et les documents électroniques (LPRDE). Dressez la liste des entreprises, organisations et personnes qui doivent être informées du fait que des informations les concernant ont peut-être fuité et de quelles informations il s'agit. Prenez également contact, dans les 72 heures, avec les pouvoirs publics cités précédemment.

Aide d'un spécialiste

La liste mentionnée ci-dessus donne une bonne image des nombreuses analyses, parfois complexes, qui devront être réalisées et des décisions qui doivent être prises en cas de cyber-attaque.

Il est conseillé d'impliquer un expert en sécurité expérimenté durant les premières étapes. Votre fournisseur informatique actuel ne dispose pas d'un tel expert ? Dans ce cas, veillez à trouver les données d'une entreprise spécialisée en cyber-sécurité.

Moins de stress et économie d'argent ?

C'est un cliché, mais il vaut toujours mieux prévenir que guérir.

Comment pouvons-nous réduire autant que possible les risques de cyber-attaque pour votre organisation ? Asseyons-nous autour d'une table. Nous examinerons les meilleures solutions. S'agit-il d'une formation de sensibilisation pour vos collaborateurs ? D'un audit de sécurité ? Ou d'un monitoring ?

Vous voulez vous épargner du stress et économiser de l'argent ? N'hésitez pas à prendre contact avec nous et nous examinerons ensemble ce que nous pouvons faire pour votre organisation. Vous pourrez ainsi dormir sur vos deux oreilles.

Secutec
Cybersecurity Intelligence

Secutec Canada
4000-1 Place Ville Marie
H3B4M4 Montréal
Canada
+1 438 728 84 32
info@secutec.com

PRIVAL®

Prival
9935 Rue de Châteauneuf Bureau 120
Brossard, QC J4Z 3V4 (CA)
info@prival.ca
www.prival.ca