

Cyber attaque Que faire?

Vous êtes généralement vigilant et vérifiez toujours l'expéditeur des e-mails que vous recevez. Mais voilà qu'un jour, vous ou l'un de vos employés cliquez sur un lien infecté. Comment réagir dans pareille situation ? Devez-vous faire comme si de rien n'était, en continuant simplement à travailler, ou agir au plus vite pour éviter le pire ?

Voici les mesures à prendre si cette éventualité devait se produire.

que faire si...

... votre ordinateur est bloqué par un virus ou si vous avez cliqué sur un lien ou un fichier suspect ?

Coupez au plus vite votre connexion à Internet.
Déconnectez les disques durs externes ou autres périphériques connectés à l'ordinateur.
Fermez immédiatement le lien suspect, le fichier infecté ou le programme indésirable.
Prenez une photo de votre écran.
Lancez une analyse avec votre programme antivirus.

... votre compte a été piraté ?

Informez-en la compagnie qui gère votre compte (Facebook, Google, etc.).
Prévenez vos contacts quant à d'éventuels messages envoyés en votre nom.
Réfléchissez à la manière dont cela peut s'être produit (quelqu'un connaît votre mot de passe, la compagnie qui gère votre compte a elle-même été piratée, etc.).
Si vous utilisez le même mot de passe pour d'autres comptes, changez-le immédiatement !

... vos données personnelles apparaissent soudainement sur Internet ?

Informez les personnes ou autorités compétentes (votre banque, votre employeur, etc.).
Contactez le site ou le service piraté et demandez-leur quelles sont les mesures qu'ils ont prévu.
Si vous avez des questions concernant la protection de vos données, contactez la commission de la protection de la vie privée.
Gardez toutefois à l'esprit que ces données resteront publiques à jamais, et ce, quelles que soient les mesures que ces entités peuvent avoir prises.

et ensuite ?

Modifiez l'ensemble de vos mots de passe
Contactez un service de réparation informatique : ils pourront vous conseiller au mieux afin de « nettoyer » votre ordinateur.
Toutes les entreprises belges et organisations (gouvernementales) peuvent se tourner vers CERT.be pour signaler une cyber attaque ou demander des conseils en matière de sécurité informatique. Vous pouvez signaler un incident à l'adresse cert@cert.be ou au numéro de téléphone 02 790 33 33. Cette démarche est importante, car elle permet de vérifier s'il s'agit d'un incident isolé ou non.

quelles sont les informations à renseigner ?

Vos données de contact
De quel type d'incident il s'agit : une attaque DDoS, un logiciel malveillant, ... ?
Quand l'incident s'est-il déroulé ?
L'incident est-il encore en cours ?

Comment avez-vous remarqué l'incident ?

Quel en est l'impact ?

Êtes-vous déjà intervenu ? Avez-vous déjà pris des mesures ? Si oui, lesquelles ?

Disposez-vous de journaux d'activité ou d'autres données techniques ?

Qui avez-vous déjà informé ?

Qu'attendez-vous après avoir signalé l'incident ?

Si vous souhaitez déposer une plainte, veuillez contacter la police locale.

que peut faire votre courtier pour vous ?

Dès la moindre suspicion de cyber attaque, prenez directement contact avec votre courtier. Il introduira une déclaration de sinistre auprès de nos équipes spécialisées en cyber risques.

Votre cas est plus spécifique ou complexe ? Nos équipes travaillent main dans la main avec des partenaires externes disponibles 24h/24, qui évalueront avec précision le préjudice subi. Votre sinistre nécessite une intervention spécifique au niveau de la communication, IT ou légal ? La cyber attaque subie sera prise en charge à tous ces niveaux.

Sources:

https://www.axa.be/ab/FR/dossiers/cyber-protection/Pages/que-faire-en-cas-de-cyber-attaque.aspx?utm_source=quantum&utm_medium=havas&utm_campaign=tpe2018&utm_content=non-vie-article1

<https://cert.be/>

<https://www.safeonweb.be/fr>

<https://www.b-ccentre.be/wp-content/uploads/2014/05/B-CCENTRE-BSCG-FR.pdf>

Symantec