CYBERCRIMINALITE

Les bons réflexes

Quels sont les risques ?

Faux ordres de virement

Intrusion dans la boite mail d'un ou plusieurs collaborateur(s) (phishing).

Interception de factures et modification des coordonnées bancaires .

Envoi de faux ordre de virement à l'interne (faux patron).

Ransomware

Intrusion dans le système informatique par une faille de sécurité (vulnérabilités de configuration, logicielles ou humaines).

Cryptolockage voire exfiltration des données.

Demande de rançon.

Fuite de données

Intrusion dans le système informatique par une faille de sécurité.

Exfiltration des données clients (nom d'utilisateur, mot de passe, numéro de téléphone, email, etc.) voire diffusion des informations en ligne.

DDoS

Tentative de faire tomber volontairement un serveur pour le rendre inaccessible (site internet par exemple).

Possible demande de rançon pour faire stopper l'attaque, pertes financières dues à l'indisponibilité de mon shop en ligne.

Les auteurs peuvent être motivés par des raisons idéologiques, commerciales ou politiques.

Comment me prémunir en posant les bonnes questions ?

Mon infrastructure

Où se trouvent quelles machines ? Sont-elles à jour et protégées ?

Procédez à l'inventaire du parc informatique.

Qui a accès à quoi ? Est-ce utile que tout le réseau informatique soit accessible à tous ?

Procédez à un relevé des droits d'accès de vos collaborateurs.

Des sauvegardes informatiques sont-elles réalisées régulièrement ?

Effectuez des sauvegardes régulières sur un serveur externe non connecté à votre infrastructure informatique. En cas d'attaque par cryptolockage sur votre système, elles ne seront ainsi pas affectées.

La double authentification est-elle activée (mes collaborateurs doivent-ils confirmer par SMS ou via une application pour acéder aux données de l'entreprise ?

Si la réponse est non, il faut le faire !

Puis-je accéder aux sites suspects ? Depuis ma boîte mail ? Mon téléphone ? En déplacement ?

Mettez en place des restrictions pour vous préserver des tentatives d'intrusion par des liens dangereux qui permettraient l'accès à vos données par une personne mal intentionnée.

Ai-je effectué un test de de sécurité de mon infrastructure récemment ?

L'infrastructure informatique et les applications utilisées évoluent constamment. Engagez des entreprises de sécurité externes pour tester régulièrement votre infrastructure.

En cas de problème, est-ce que je sauvegarde suffisamment d'informations utiles à la police pour enquêter ?

Les données de type adresses IP, horodatage, port source, user-agent, etc. faciliteront le travail d'investigation.

Mon personnel

Suis-je compromis ?

Des informations (mot de passe par exemple) sont compromis par des vols de données. Un contrôle doit être fait régulièrement et peut être réalisé automatiquement (www.haveibeenpwned.com).

Mes collaborateurs changent-ils régulièrement leurs mots de passe ?

Assurez-vous que votre personnel change de mot de passe régulièrement.

Mon personnel est-il formé contre la fraude en ligne ?

Organisez des sessions de formation afin de préparer votre personnel à des tentatives de fraudes (phishing, faux ordres de virement, demande d'informations sensibles et financières, etc.).

Un collaborateur / partenaire commercial m'indique un changement de coordonnées bancaires, est-ce normal ?

Prenez contact avec le collaborateur ou l'entreprise par téléphone afin de vérifier qu'il s'agit d'une requête légitime. N'utilisez pas le numéro de téléphone présent sur l'email mais le contact habituel !

Restez conscient que le risque zéro n'existe pas.
Soyez attentif à tous les points de ce document pour diminuer au maximum le risque de compromission de vos données ou de votre infrastructure.
La prévention reste la meilleure arme pour diminuer au maximum le risque.

S'il est trop tard...

Vous avez payé une facture falsifiée

- Effectuez une demande de retour de fonds à votre banque et contactez la police.
- Procédez à une analyse complète de votre système informatique afin de déterminer où et comment s'est déroulée l'intrusion.

Vos données sont cryptolockées

- Séparez tous les systèmes du réseau et désactivez le réseau sans fil.
- Ne payez pas ! Contactez la police.
- Effectuez une analyse complète de votre système informatique afin de déterminer les circonstances de l'intrusion à l'aide d'une société spécialisée.
- Préservez les traces informatiques.
- Contrôlez si un outil de décryptage existe gratuitement en ligne :
  - http://www.nomoreransom.org/crypto-sheriff.php
  - https://www.emsisoft.com/ransomware-decryption-tools/
  - https://noransom.kaspersky.com/

Vous constatez un risque interne

- Contactez la police.
- Pour plus de conseils, rendez-vous sur :

www.vbs.admin.ch/fr/securite/recherche-renseignements/espionnage-economique.html

Vous avez subi une fuite de données (data leaking)

- Déterminez comment les auteurs ont accédé au système, à quelles données ils ont eu accès et préservez les traces informatiques.
- Contactez la police.
- Remédiez immédiatement aux failles de sécurité.
- Si des données personnelles ont été compromises, avertissez les usagers rapidement.

Votre système est surchargé en raison d'un DDoS

- Contactez le GovCert / SOC cantonal et la police.
- Préservez les traces informatiques.

Pour plus de détails, rendez-vous sur :

https://www.ncsc.admin.ch/ncsc/fr/home.html https://www.skppsc.ch/fr/

https://votrepolice.ch/cybercriminalite-cat/

CONTACT
www.votrepolice.ch
021 644 44 44

canton de vaud
Police cantonale vaudoise
Police de sûreté