Réagir à une cyberattaque

C. Geffcken
DI – OCSIN – DST – SI

18 octobre 2022

REPUBLIQUE ET CANTON DE GENEVE

Département des infrastructures
Office cantonal des systèmes d'information et du numérique
Service de la sécurité de l'information et de la protection des données

Sommaire

À propos des cyberattaques

1

Définition

- Selon le «Robert», une cyberattaque est «un acte de piratage informatique sur Internet» (Le Robert)
  - → Piratage ?
    - En fait, tout type d'attaque malveillante dans le but de nuire, d'extorquer de l'argent ou de détruire la réputation d'une personne physique ou morale
  - → Informatique ?
    - Parfois, mais pas toujours. L'«ingénierie sociale» est un moyen simple et très puissant d'obtenir subrepticement des informations cachées et des accès indus
  - → Sur Internet ?
    - En général. Mais cela se fait aussi par les personnes, les téléphones, les SMS, les messageries instantanées, les fax, et même simplement sur papier (p.ex. courrier)
- L'informatique n'est qu'un moyen parmi d'autres
- Internet n'est qu'un vecteur de transmission parmi d'autres

À propos des cyberattaques

Typologie

- De nos jours, de plus en plus de cyberattaques ne sont plus ciblées
- Chaque personne ou entité est donc une victime potentielle
  - → Attaques opportunistes
    - Si l'attaquant découvre une faille, alors il l'exploite
  - → Attaques indépendantes de la taille de l'entreprise
    - Les petites PME sont souvent celles qui sont le moins protégées
  - → Attaques indépendantes de la fortune de la victime
    - «Les petits ruisseaux font de grandes rivières»

À propos des cyberattaques

Méthodologie

3

- Il existe de multiples méthodes d'attaques
  - → Déni de service, maliciel, rançongiciel, phishing, arnaque au président, défacement, trolling, etc…
- Dans la plupart des cas, une cyberattaque combine plusieurs méthodes pour être plus efficace
- Les méthodes changent en fonction des buts de l'attaquant
  - → Gagner de l'argent, nuire à l'entité, faire le buzz, s'amuser, etc…

À propos des cyberattaques

4

Par conséquent…

- Nous sommes toutes et tous des victimes potentielles
- Il est donc nécessaire
  - → d'en être conscient
  - → de s'y préparer
  - → d'avoir des défenses «de base» en place
  - → de savoir comment réagir
- C'est le sujet de cet exposé !

Avant une cyberattaque…

Avant une cyberattaque…

1

Préparation

- Être prêt est crucial pour «survivre» à une cyberattaque
- La capacité de résistance à une cyberattaque dépend d'au moins 4 axes
  - → L'axe organisationnel
  - → L'axe humain
  - → L'axe technique
  - → L'axe informationnel
- Chaque entité, quelle que soit sa taille, doit les mettre en œuvre en fonction de ses buts et de ses moyens

Avant une cyberattaque…

2

Axe organisationnel, première partie

- Une cyberattaque est une crise pour l'entité, comme le serait par exemple un incendie
  - → Quelle que soit la taille de l'entité, quelqu'un doit être nommé pour piloter les actions éventuelles en cas de cyberattaque
    - Directeur, responsable IT, Responsable de la sécurité des systèmes d'information (RSSI), etc.
  - → Créez si possible une «cellule de crise» (activable dans tous les cas, pas seulement pour une cyberattaque)
  - → Préparez comment communiquer en cas de crise
- Réfléchissez et débattez en interne (direction, juridique, finances, etc.) de la ligne de conduite à suivre en cas de rançongiciel
  - → En principe, on ne doit jamais payer de rançon !

Avant une cyberattaque…

3

Axe organisationnel, deuxième partie

- Identifiez aussi:
  - → Quelles sont les ressources critiques (humaines et techniques) de l'entité
  - → Quelles procédures existent déjà pour préserver ces ressources
  - → Les personnes et entreprises qui pourraient vous aider et vous conseiller en cas de crise, et ayez leur coordonnées
- Assurez-vous d'avoir une **copie papier** de ces éléments
- Évaluez le rapport coût-bénéfice d'une cyberassurance
  - → Portez une grande attention aux conditions nécessaires pour que l'assurance soit activée, et surtout aux prérequis et aux exclusions

Avant une cyberattaque…

4

Axe humain

- La «cible» la plus simple d'une cyberattaque est un membre du personnel
- *Tout* le personnel doit être sensibilisé à la sécurité de l'information
  - → «Examinez attentivement l'expéditeur du message», «Le sujet est-il vraisemblable ?», «En cas de doute, ne cliquez ***jamais*** sur une pièce jointe»
  - → «Le DG ne téléphonerait jamais pour demander un versement urgent de 10'000.- au Groland»
  - → «`abc123`, `HopSuisse!` ou `JeanDupont15` ne sont pas des mots de passe acceptables»
  - → «Privilégiez la sécurité à tout autre considération»
- *Tout* le personnel doit être responsabilisé quant aux conséquences potentielles pour l'entité
  - → Finances, image de marque, poursuites légales, interruption des prestations, temps nécessaire aux équipes, etc.
- Le personnel critique (au moins la direction, l'IT et les unités primordiales pour l'entité) doit être formé pour savoir comment agir et réagir en cas d'attaque

Avant une cyberattaque…

5

Axe technique, première partie

- Mettez en œuvre une «politique de mots de passe» qui soit robuste et efficace
  - → Longueur, durée de validité, complexité, jeux de caractères, unicité, etc.
  - → Assurez-vous que le personnel connaisse les bonnes pratiques à ce sujet
- Utilisez un antivirus récent et à jour
- Assurez-vous que tous les systèmes
  - → sont «patchés» correctement et régulièrement
  - → sont redémarrés régulièrement, surtout après les patches
  - → ont une «source de temps» commune, unique et correcte
- Assurez-vous que les messages d'alertes générés par vos systèmes sont reçus, lus et compris par leur(s) destinataire(s)

Avant une cyberattaque…

6

Axe technique, seconde partie

- Procédez régulièrement à des sauvegardes (‘backups’)
  - → Assurez-vous que
    - le plan de sauvegarde s’exécute régulièrement
    - toutes les sauvegardes nécessaires sont faites
    - chaque sauvegarde s’est achevée avec succès
    - vous pouvez restaurer ces données. En clair, *testez vos sauvegardes*
  - → Evitez de tout miser sur des sauvegardes «en ligne»
    - Gardez une sauvegarde récente sur un support physique que vous avez à disposition en cas de besoin
- Assurez-vous qu’au moins deux personnes connaissent les mots de passe critiques
  - → Mais limitez ce nombre au maximum ! Idéalement, au plus deux personnes
- S’il y a lieu
  - → Réfléchissez comment obtenir du matériel de secours et du support

Avant une cyberattaque…

Axe informationnel

- Vous êtes responsable …
  - → des données qui vous ont été mises à disposition par vos clients ou administrés
  - → des données de vos collaborateurs
  - → des données de votre entité
  - → et bien sûr, de vos propres données
- Donc, pour ces données, assurez-vous …
  - → qu'elles sont correctement classifiées (p.ex. «interne», «confidentiel», …)
  - → que leur accès est réglementé
  - → que vous savez «où» elles se trouvent
  - → qu'elles sont sauvegardées

Pendant une cyberattaque…

En premier lieu… Restez calme !

Conseils de base

- En cas d'attaque avérée, il est important de rester calme, de se concentrer sur les actions à mener, et d'assurer la pérennité de l'entité
- Demandez de l'aide aux personnes et entreprises que vous avez identifiées
- Si vous les avez préparés, récupérez
  - → les procédures à appliquer
  - → le concept de communication

Actions à effectuer

Liste non exhaustive; ordre variable

1

- Activez la cellule de crise
- Déconnectez du réseau toutes les machines impactées, mais ne les éteignez pas !
- Récoltez toutes les informations disponibles
  - → Heure exacte, actions effectuées par les personnes sur les machines concernées, logiciels employés, comportement des systèmes, etc.

Actions à effectuer

2

Liste non exhaustive; ordre variable

- Informez le 'National Cyber Security Center' à Berne
  - → https://www.ncsc.admin.ch/ncsc/fr/home.html
  - → Informer le NCSC deviendra prochainement obligatoire pour les cas graves
- Si l'attaque est grave,
  - → informez la police
  - → déposez plainte
- Si l'attaque a permis de capturer des données personnelles, informez le préposé fédéral ou cantonal, suivant le cas de l'entité

Actions à effectuer

3

Liste non exhaustive; ordre variable

- Laissez faire les experts
  - → Les spécialistes des autorités ou des entreprises mandatées, notamment
- Évitez d'improviser.

  Appliquez les procédures que vous avez mises en place au préalable
- Communiquez
  - → Aux membres de l'entité
  - → Aux autorités habilitées
  - → Éventuellement aux médias, si cela s'avère nécessaire
- Une bonne communication, bien préparée, évite bien des déboires

Actions à ne pas faire

- Arrêter les systèmes impactés
  - → Cela pourrait entraîner la perte des éléments d'investigation ou de preuve
- Réinstaller spontanément les systèmes impactés, ou restaurer spontanément une sauvegarde
  - → Cela entraînera la perte des éléments d'investigation ou de preuve
- Garder le secret
  - → L'attaquant sait, et il communiquera à votre place s'il le juge utile

Cas du rançongiciel

- ***Faut-il payer la rançon ?***
  - → Toutes les autorités et les entreprises recommandent clairement de **ne pas payer** de rançon, dans tous les cas
  - → Si l'entité est préparée, ça ne posera aucun problème
  - → Si ce n'est pas le cas, alors la question peut devenir existentielle pour l'entité…

Après une cyberattaque…

Actions à prendre

Liste non exhaustive

1

1. Assurez-vous que la crise est ***vraiment*** terminée
   - → L'attaque s'est arrêtée ou n'est plus possible
   - → Les systèmes sont à nouveau opérationnels, les données sont restaurées, et les mots de passe réinitialisés (chaque mot de passe doit être changé)
   - → Les experts éventuellement mandatés vous le confirment
2. Annoncez la fin de la crise au personnel
3. Faites une analyse *post-mortem*
   - → Renseignez par écrit ce qu'il s'est passé, et les actions effectuées

Actions à prendre

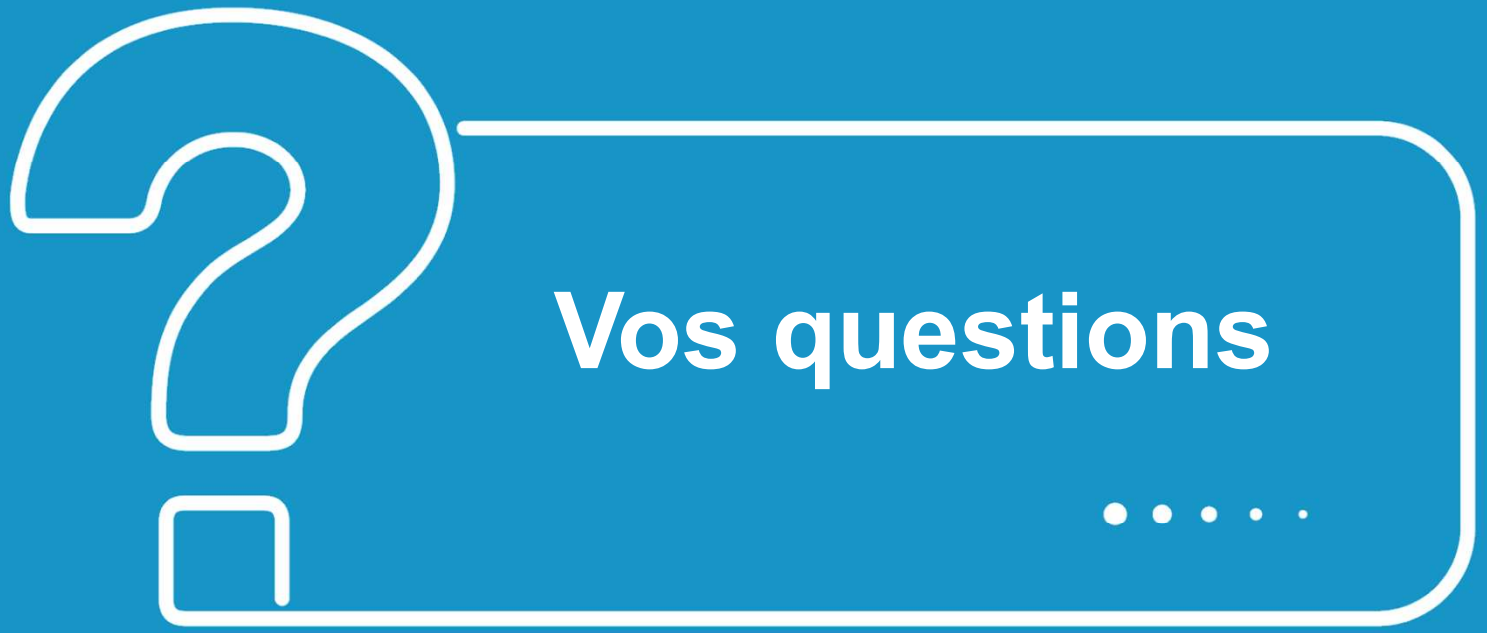
Liste non exhaustive

2

4. Désactivez la cellule de crise
5. Capitalisez sur les leçons apprises, et améliorez ce qui peut l'être
6. Vérifiez la résilience de vos systèmes informatiques
   - → Mandatez une société pour un test de sécurité

Conclusion

- La préparation est la clé
  - → Celle-ci doit être adaptée à la situation
- Il ne faut pas hésiter à demander de l'aide
- Il faut réagir vite, mais sans précipitation, tout en gardant son calme
- Si cela arrive, il faut en tirer les leçons pour que ça ne se reproduise plus
- Il faut se tenir au courant, pour bénéficier des expériences (parfois malheureuses) de ses pairs


Vos questions

Merci de votre attention !

Christian Geffcken

Christian.Geffcken@etat.ge.ch

REPUBLIQUE
ET CANTON
DE GENEVE

Département des infrastructures
Office cantonal des systèmes d'information et du numérique
Service de la sécurité de l'information et de la protection des données