Fédération des Entreprises Romandes
Genève

Clusis : Ransomwares

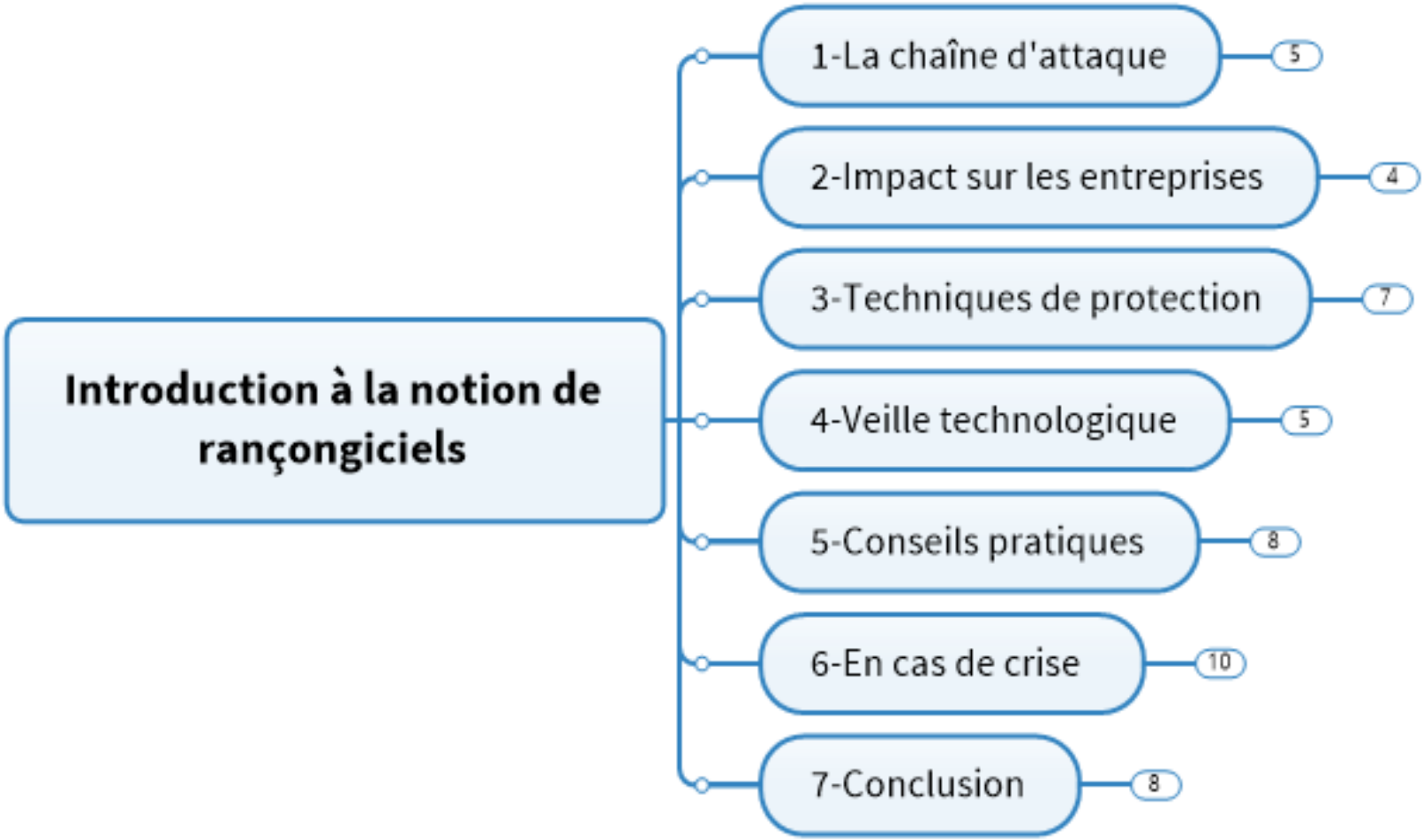
Evolutions, chaîne d'attaque, protection

Raoul Diez, Directeur, Conseil Cyber PME, FER Genève

“

La meilleur manière de résoudre un problème, est encore de l’éviter

Notions concernant les rançongiciels



Raoul Diez raoul.diez@fer-dg.ch

La chaîne d'attaque

Rançongiciels

“

Comment les rançongiciels pénètrent dans les systèmes, comment ils se propagent et comment ils sont activés pour crypter les données

La chaîne d'attaque

- **Exploits de vulnérabilités** : les attaquants utilisent des exploits pour cibler les vulnérabilités dans les systèmes informatiques.
- **Phishing** : les attaquants envoient des e-mails de phishing pour tromper les utilisateurs en leur faisant cliquer sur des liens malveillants qui téléchargent des logiciels malveillants.
- **Campagnes de diffusion massive** : les attaquants utilisent des techniques de diffusion massive pour diffuser des rançongiciels à un grand nombre de victimes en même temps.
- **Programmation malveillante** : les attaquants utilisent des techniques de programmation pour dissimuler les logiciels malveillants et les faire passer inaperçus par les systèmes de sécurité.
- **Hameçonnage** : les attaquants utilisent des sites web de hameçonnage pour tromper les utilisateurs en les incitant à entrer leurs informations confidentielles.

Impact sur les entreprises

Rançongiciels

“

Il est important de mettre l'accent sur les implications économiques, les risques pour la vie privée et les conséquences potentielles pour les entreprises et les clients

Impact sur les entreprises

- **Le coût moyen d'une cyberattaque :** dépend de plusieurs facteurs, tels que la nature de l'attaque, la taille de l'entreprise, la complexité du système informatique et le temps nécessaire pour remédier à l'incident.
- **Il peut varier de quelques milliers de francs à plusieurs millions :** https://www.letemps.ch/economie/cyberattaque-coute-centaines-milliers-francs
- **Les frais de restauration des systèmes, ne représente qu'une partie du coût total d'une cyberattaque :** Il faut également prendre en compte les coûts indirects, tels que la perte de revenus, la réputation, les coûts juridiques et de conformité.
- **En fin de compte, la meilleure façon de limiter les coûts d'une cyberattaque :** est de mettre en place des mesures de sécurité efficaces pour minimiser les risques, de former le personnel à la sécurité informatique et de disposer d'un plan de réponse aux incidents en cas d'attaque.

Techniques de protection

Rançongiciels

“

Les mesures ne garantissent pas une protection complète contre les rançongiciels, mais elles peuvent aider les entreprises à minimiser les risques et à se préparer en cas d'attaque

Techniques de protection

- **Sauvegarde régulière des données** : les entreprises peuvent effectuer des sauvegardes régulières de leurs données pour s'assurer de pouvoir les restaurer en cas d'attaque de rançon.
- **Logiciels de sécurité à jour** : les entreprises peuvent installer et maintenir à jour des logiciels de sécurité tels que des antivirus et des pare-feu pour détecter et bloquer les rançongiciels.
- **Mise en œuvre de stratégies de sécurité de réseau** : les entreprises peuvent implémenter des stratégies de sécurité de réseau, telles que la segmentation du réseau et la mise en place de pare-feu pour limiter la propagation des rançongiciels.
- **Sensibilisation du personnel** : les entreprises peuvent former leur personnel à la sécurité informatique et les sensibiliser aux techniques utilisées par les attaquants pour diffuser les rançongiciels, telles que les e-mails de phishing.
- **Mise en place de politiques de sécurité strictes** : les entreprises peuvent mettre en place des politiques de sécurité strictes pour gérer les accès aux données sensibles et limiter les privilèges d'administration.
- **Mise en œuvre de stratégies de sécurité pour les e-mails** : les entreprises peuvent implémenter des stratégies de sécurité pour les e-mails, telles que la vérification de l'authenticité des e-mails et la détection des e-mails malveillants.
- **Surveillance en temps réel du système** : les entreprises peuvent surveiller en temps réel leur système pour détecter rapidement tout comportement anormal et réagir rapidement.

Veille technologique

Rançongiciels

“

Mettre en place une veille technologique efficace pour se protéger contre les rançongiciels et les autres menaces informatiques

Veille technologique

- **Établissez une équipe dédiée à la veille technologique** : désignez un ou plusieurs responsables de la veille technologique pour surveiller les dernières menaces et mises à jour de sécurité.
- **Définissez les sources d'information** : recherchez les meilleures sources d'information pour rester informé des dernières tendances et des dernières menaces en matière de sécurité informatique.
- **Utilisez des outils de veille** : utilisez des outils de veille tels que les alertes de sécurité, les moteurs de recherche dédiés à la sécurité informatique et les abonnements aux bulletins d'alerte de sécurité pour vous tenir informé en temps réel.
- **Participez à des conférences et à des webinaires** : Sur la sécurité informatique pour rester informé des dernières tendances et des meilleures pratiques.
- **Créez des plans d'action** : en utilisant les informations recueillies, créez des plans d'action pour faire face aux menaces identifiées et mettre en œuvre des mesures de sécurité pour les prévenir.

Sites populaires pour la veille technologique

- **CERT-FR** : Centre National de la Sécurité des Systèmes d'Information (CNSSI) en France. https://www.cert.ssi.gouv.fr/
- **SANS Institute** : une organisation à but non lucratif spécialisée dans la formation et la recherche en matière de sécurité informatique https://www.sans.org/emea/
- **US-CERT** : le Centre de la cybersécurité des États-Unis https://www.cisa.gov/uscert/
- **The Hacker News** : un site d'actualités de sécurité informatique https://thehackernews.com/
- **KrebsOnSecurity** : un blog d'actualités sur la sécurité informatique dirigé par Brian Krebs https://krebsonsecurity.com/

Conseils pratiques

Rançongiciels

“

Suivre ces conseils pour renforcer la sécurité informatique et réduire les risques d'attaque de rançongiciel

Conseils pratiques

- **Sauvegardez régulièrement vos données** : assurez-vous de sauvegarder régulièrement vos données sur un disque dur externe ou dans le cloud pour pouvoir les restaurer en cas de rançongiciel.
- **Mettre à jour vos logiciels régulièrement** : les mises à jour de sécurité corrigent les faiblesses du système et peuvent aider à prévenir les attaques.
- **Attention aux e-mails suspects** : soyez vigilant envers les e-mails qui semblent suspects ou qui viennent de sources inconnues. N'ouvrez pas les pièces jointes ou les liens si vous n'êtes pas sûr de leur origine.
- **Installez un logiciel antivirus** : utilisez un logiciel antivirus fiable et mettez-le à jour régulièrement pour protéger votre ordinateur contre les rançongiciels et d'autres logiciels malveillants.
- **Évitez les réseaux publics non sécurisés** : les réseaux Wi-Fi publics peuvent être des points d'entrée pour les cyberattaques. Évitez d'utiliser des réseaux publics non sécurisés pour effectuer des transactions sensibles ou pour accéder à des informations confidentielles.
- **Configurez les pares-feux** : configurez les pares-feux pour bloquer les connexions entrantes non autorisées et renforcer la sécurité du réseau.
- **Formez les employés à la sécurité informatique** : formez régulièrement les employés à la sécurité informatique pour les sensibiliser aux risques et les aider à adopter de bonnes pratiques de sécurité.
- **Selon les autorités, en cas d'attaque de rançongiciel ne payez pas la rançon** : Car cela encourage les attaquants et peut ne pas garantir la récupération de vos données.

En cas de crise

Rançongiciels

“

En suivant ces mesures, vous pouvez minimiser les dommages causés par un rançongiciel et préparer votre entreprise pour de futurs incidents de sécurité informatique

En cas de crise

Pendant l'incident :

- **Arrêtez toutes les activités sur l'ordinateur infecté** : Pour éviter la propagation du rançongiciel à d'autres ordinateurs ou parties du réseau, arrêtez toutes les activités sur l'ordinateur infecté.
- **Déconnectez-vous du réseau** : Pour limiter la propagation du rançongiciel.
- **Contactez un expert en sécurité informatique** : Pour obtenir une assistance professionnelle et déterminer les mesures à prendre pour éliminer le rançongiciel.

En cas de crise

Après l'incident :

- **Restaurez les données à partir de sauvegardes sécurisées** : Pour récupérer les fichiers cryptés par le rançongiciel.
- **Analysez les causes de l'incident** : Pour déterminer comment le rançongiciel a pu s'infiltrer dans le système et comment éviter de futurs incidents.
- **Mettre à jour les mesures de sécurité** : Pour renforcer la défense contre les rançongiciels et d'autres menaces informatiques.
- **Informez les parties concernées** : Telles les employés, clients et partenaires, de l'incident, et de ce que vous avez fait pour le résoudre.
- **Suivez les lois et les réglementations applicables** : Telles que la LPD et le RGPD, pour garantir la conformité et éviter les poursuites judiciaires.

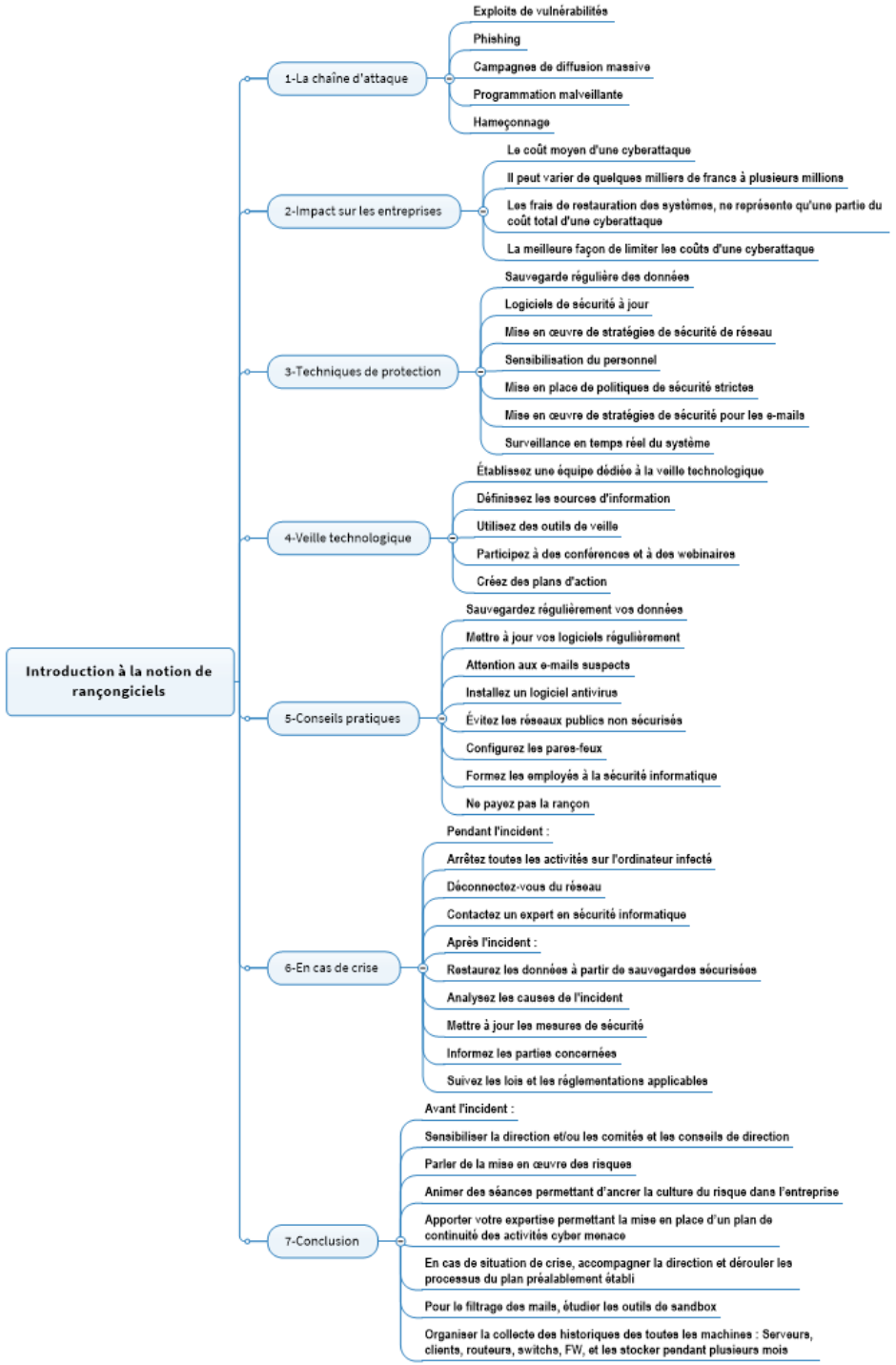
Conclusion

Rançongiciels

En conclusion

Avant l'incident :

- **Sensibiliser la direction et/ou les comités et les conseils de direction**
- **Parler de la mise en œuvre des risques**
- **Animer des séances permettant d'ancrer la culture du risque dans l'entreprise**
- **Apporter votre expertise permettant la mise en place d'un plan de continuité des activités cyber menace**
- **En cas de situation de crise, accompagner la direction et dérouler les processus du plan préalablement établi**
- **Pour le filtrage des mails, étudier les outils de sandbox**
- **Organiser la collecte des historiques des toutes les machines : Serveurs, clients, routeurs, switchs, FW, et les stocker pendant plusieurs mois**
- **Se renseigner auprès des assureurs : Cela permettant de voir s'il est possible d'assurer le risque**


Introduction à la notion de rançongiciels
1-La chaîne d'attaque
Exploits de vulnérabilités
Phishing
Campagnes de diffusion massive
Programmation malveillante
Hameçonnage
2-Impact sur les entreprises
Le coût moyen d'une cyberattaque
Il peut varier de quelques milliers de francs à plusieurs millions
Les frais de restauration des systèmes, ne représente qu'une partie du coût total d'une cyberattaque
La meilleure façon de limiter les coûts d'une cyberattaque
3-Techniques de protection
Sauvegarde régulière des données
Logiciels de sécurité à jour
Mise en œuvre de stratégies de sécurité de réseau
Sensibilisation du personnel
Mise en place de politiques de sécurité strictes
Mise en œuvre de stratégies de sécurité pour les e-mails
Surveillance en temps réel du système
4-Veille technologique
Établissez une équipe dédiée à la veille technologique
Définissez les sources d'information
Utilisez des outils de veille
Participez à des conférences et à des webinaires
Créez des plans d'action
5-Conseils pratiques
Sauvegardez régulièrement vos données
Mettre à jour vos logiciels régulièrement
Attention aux e-mails suspects
Installez un logiciel antivirus
Évitez les réseaux publics non sécurisés
Configurez les pares-feux
Formez les employés à la sécurité informatique
Ne payez pas la rançon
6-En cas de crise
Pendant l'incident :
Arrêtez toutes les activités sur l'ordinateur infecté
Déconnectez-vous du réseau
Contactez un expert en sécurité informatique
Après l'incident :
Restaurez les données à partir de sauvegardes sécurisées
Analysez les causes de l'incident
Mettre à jour les mesures de sécurité
Informez les parties concernées
Suivez les lois et les réglementations applicables
7-Conclusion
Avant l'incident :
Sensibiliser la direction et/ou les comités et les conseils de direction
Parler de la mise en œuvre des risques
Animer des séances permettant d'ancrer la culture du risque dans l'entreprise
Apporter votre expertise permettant la mise en place d'un plan de continuité des activités cyber menace
En cas de situation de crise, accompagner la direction et dérouler les processus du plan préalablement établi
Pour le filtrage des mails, étudier les outils de sandbox
Organiser la collecte des historiques des toutes les machines : Serveurs, clients, routeurs, switchs, FW, et les stocker pendant plusieurs mois

www.fer-ge.ch

98, rue de Saint-Jean
Case postale
1211 Genève 3

fer-ge@fer-ge.ch

058 715 31 11

Fédération des Entreprises Romandes
Genève