Votre SLSP (organisation) est victime d'une cyberattaque : quelles actions mener prioritairement pour limiter les dégâts ?

Webinaire – 14/06/2022

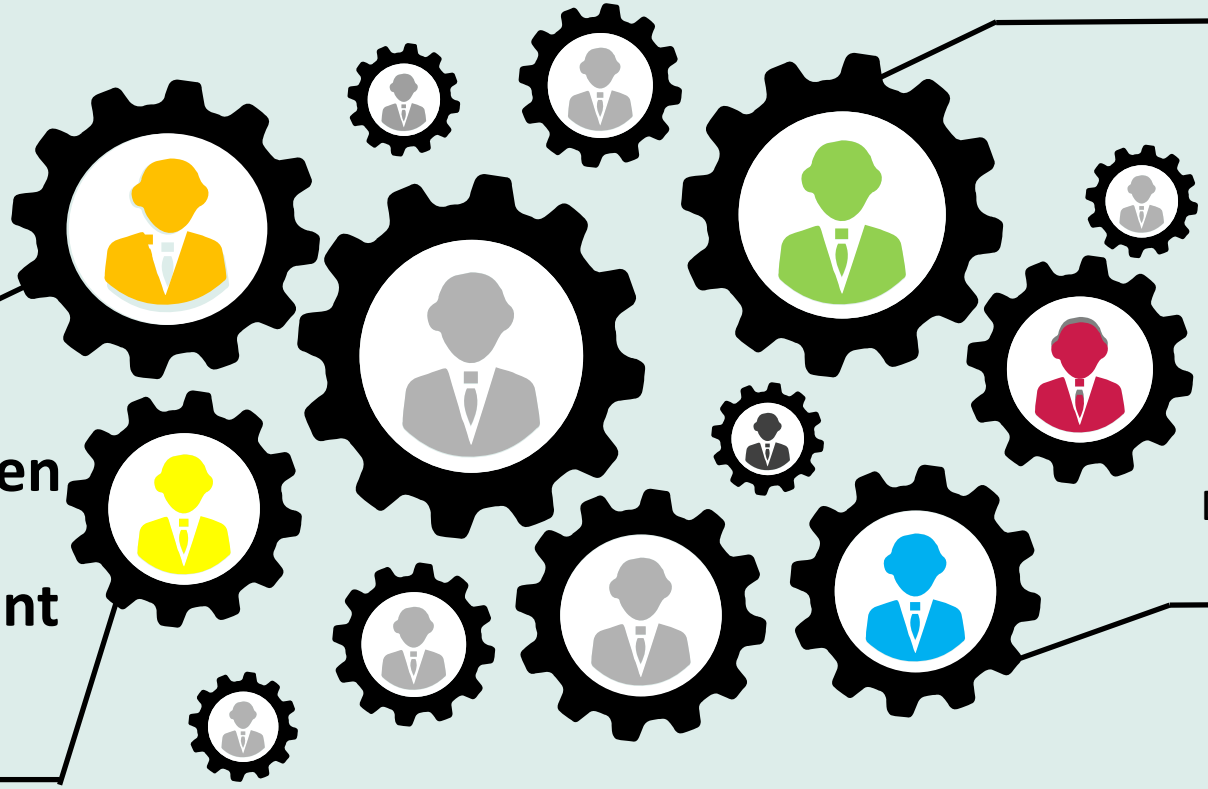
Union des Villes et Communes de Wallonie asbl

Wallonie

Nos invités

Abdel Wissam
DPD
SWL

Nathan Faes
Network & security engineer
Shinka IT



Éric Cortisse
Directeur informatique
SWL

Valentin Drouven
Account manager

Maxime Braibant
Technicien réseau
Shinka IT

Menu de la séance

01 En cas de cyberattaque : que faut-il faire prioritairement ?

02 Retour d'expérience de la SWL : quels enseignements tirer de la récente cyberattaque de la SWL ?

01 02

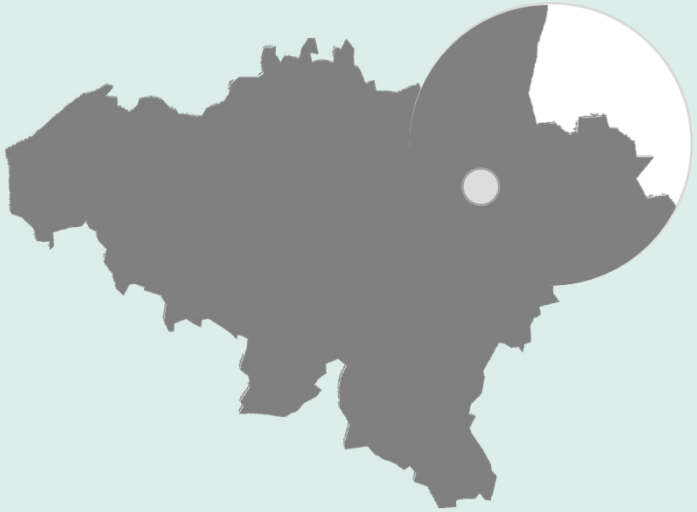
En cas de cyberattaque : que faut-il faire prioritairement ?

Nathan Faes
Network & security engineer
Valentin Drouven
Account manager
Maxime Braibant
Technicien réseau

SHINKA IT

SHINKA

- Bureau à Beaufays (Liège - Belgium)



- Depuis 2011
- 30 personnes

- Expert Réseau certifié
- Expert Sécurité certifié

- Accompagnement des organismes publics et privés dans la mise en place de solutions informatiques sur mesure.

Mise en contexte - Statistiques

+31% d'attaques entre 2020 et 2021[1]

200 Le nombre d'attaques qu'une société subit, en moyenne, par an.
2323 Le nombre de gouvernements, écoles et établissements de soins de santé victimes de ransomware en 2021

10,5 trillions Le coût total du cybercrime prédit pour 2025[2]
200 000 Le cout moyen pour une société affectée par une attaque

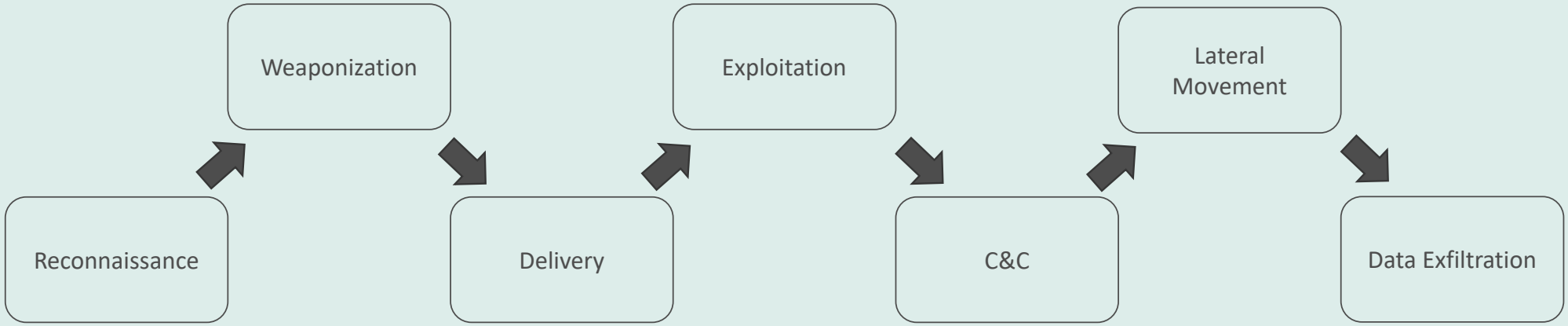
287 Le nombre de jours, en moyenne, pour une équipe de sécurité pour identifier et maitriser une violation de données[3]

36% des attaques proviennent du **Phishing**[4]
90% des attaques démarrent par une propagation d'emails de phishing[5]

[1] State of Cybersecurity Resilience 2021 Report
[2] Cisco/Cybersecurity Ventures "2022 Cybersecurity Almanac."
[3] Cost of a Data Breach 2021 – IBM Report
[4] 2021 Data Breach Investigations – Verizon Report
[5] Etude Trend Micro

Mise en contexte – Kill Chain

Kill Chain – L'anatomie d'une attaque



Les préventions bien connues (Best Practices)

- Segmentation de l'infrastructure
  - Réseau (VLAN, Routage, …)
  - Système (Privilèges, rôles, droits d'accès)
- Outils de sécurité dédiés (firewall, antispam, …)
- Backups
- Mises à jour / Patchs
- Accès VPN restreints
- Documentation

Les préventions bien connues (Best Practices)

La segmentation réseau et système

- Problèmes des réseaux non segmentés (réseau plat)
  - Broadcast / Multicast
  - Propagation du trafic malveillant à l'ensemble du réseau
  - Communications ouvertes
  - Impact de performances
  - Ex : imprimantes dans le même réseau que le serveurs
- Privilèges et rôles
  - Une gestion quotidienne est nécessaire pour gérer les droits
  - Régulièrement revoir ces droits/accès
- Point commun régulier pour ces problèmes : L'historique de l'infrastructure

Les préventions bien connues (Best Practices)

Backup 3,2,1

- **3** copies des données
- Sur **2** médias différents
- **1** copie en dehors du site
- Exemple : Les données sur le support de la production en cours + Backup sur un second média + Backup sur un support off site dans une stratégie de Disaster Recovery (A exécuter moins fréquemment).

Cold backup

- Backup qui est hors ligne et qui n'est pas disponible pour des updates (mises à jour des données, suppression, …) qui pourraient être erronées ou accidentelles.

Rétention

- 1J, 7J, 30J, …

Pas de Backup = Risque de faillite

Les préventions bien connues (Best Practices)

Sécurité – Ce qu'on retrouve habituellement dans les infrastructures ;

- Firewall en place ? Oui
- Firewall bien géré et bien implémenté ? Pas toujours
  - Règles trop permissives par gain de temps
  - Règles historiques => Maintenances régulières
  - Gestion des accès inter-vlans (entre les différents réseaux)
- AntiSpam en place ? Oui
- Sensibilisation des utilisateurs face aux emails frauduleux (ou autre) ? Non
- VPN en place ? Oui
- MFA (Multi-Factor Authentication) implémenté ? Non
- Publication d'application / site web
  - DMZ implémentée ? Oui
  - Reverse Proxy implémenté ? Non

Les préventions bien connues (Best Practices)

Mises à jour / Patches

Il est essentiel d'effectuer les mises à jour, d'installer les patches et d'effectuer les différents upgrades de vos solutions

- Corrige des vulnérabilités
- Implique un redémarrage/coupure
- Certains systèmes sont trop anciens et ne peuvent plus être mis à jour
  - => ISOLATION !!!
  - Ex : Chaines de production avec des programmes développés sur Windows XP

Les préventions bien connues (Best Practices)

Documentation

- Souvent pauvre ou incomplète
- Permet pourtant de faire évoluer le réseau de manière optimale
- Rapidement s'y retrouver en cas d'attaques =>
  - **Surtout** pour les intervenants externes qui seront ou pourraient être appelés en cas d'attaque

Gestion des assets

- Connaitre son parc

Attaque – Le jour d'après – Ne pas

Précipitation = Erreurs !

Les action à **ne pas** faire ;

- **Ne pas** éteindre les machines
  - La clé de chiffrement peut être en RAM (mémoire effacée lors d'un redémarrage)
- **Ne pas** payer
  - Vous pouvez n'avoir aucun retour de l'attaquant
  - Le déchiffreur peut ne pas fonctionner ou ne fonctionner que partiellement
  - L'attaquant découvre que son attaque a eu un impact important
  - On peut vous faire payer plusieurs fois
  - Veeam Rapport 2022 : 32% des sociétés qui ont payé n'ont jamais récupéré leurs données
- **Ne pas** supprimer de fichiers
  - On peut penser que des fichiers chiffrés ne seront plus utilisables mais il arrive qu'ils puissent être déchiffrés dans le futur
- **Ne pas** se connecter avec des comptes avec trop de privilèges
  - Création de comptes temporaires avec les droits strictement nécessaires
  - Eviter une escalade de privilèges de l'attaquant lui donnant encore plus d'accès
- **Ne pas** communiquer en externe tant que les informations ne sont pas précises

Attaque – Le jour d'après – TODO

ISOLER

- Isoler le réseau pour :
  - Eviter toute propagation au sein de l'infrastructure
  - Eviter que les données soient envoyées à l'attaquant
- Isoler le réseau en :
  - Coupant tous les ports « access » sur les switches (admin shutdown)
  - Bloquant le WiFi
  - Bloquant les accès au niveau du firewall (internes et externes)

Attaque – Le jour d'après – TODO

COMMUNICATION

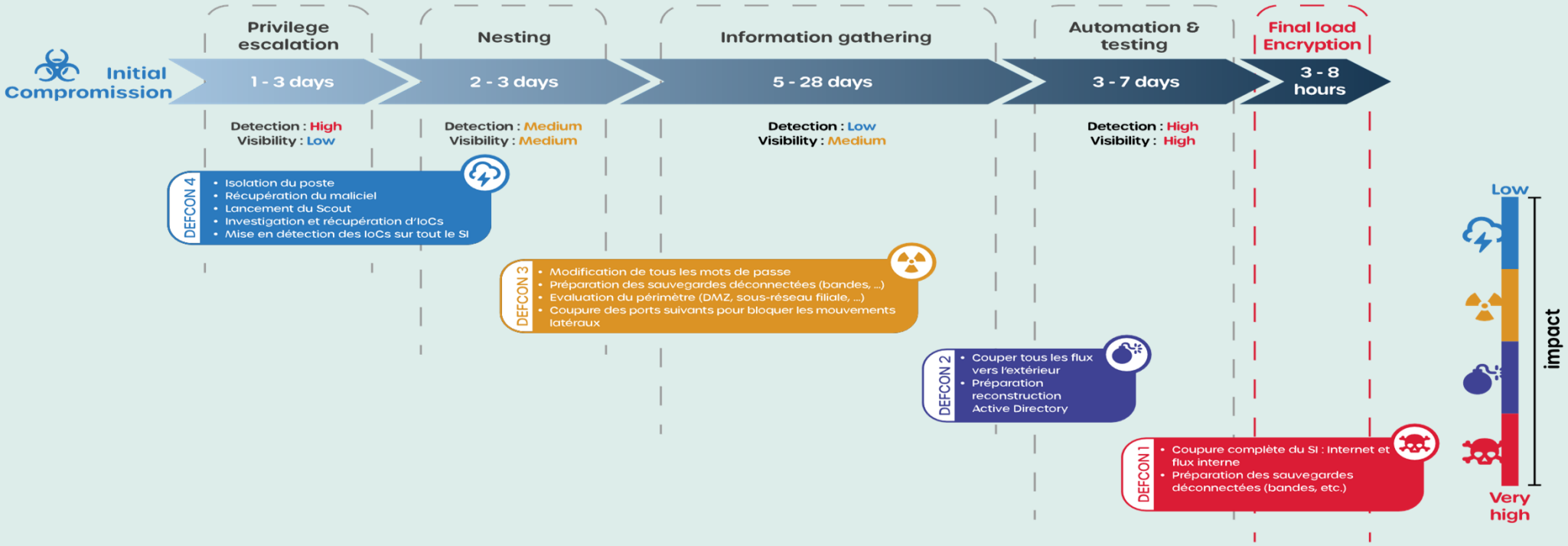
- Communication interne :
  - Avertir les utilisateurs afin qu'ils adaptent leur comportement (procédure de crise, accès restreints, …)
- Communication externe :
  - Même si l'entreprise a une obligation légale de communiquer publiquement sur l'incident – en particulier en cas de fuite de données – il n'est pas judicieux de le faire sans avoir des informations complètes, notamment sur la nature exacte des données qui ont pu être exfiltrées.
  - Une fois les informations précises récoltées, communiquer à la CCB (Cybersécurité Belgique) la nature de l'attaque. Cet organisme propose différents canaux de communication sécurisés pour l'échange d'informations.
- Faire appel à (au moins) une société spécialisée dans la gestion de ce type d'attaque
  - Notamment pour retracer tous les éléments et tenter d'identifier la source (quand c'est possible)
- Faire appel à votre assurance (CyberRisk)

Attaque – Le jour d'après – TODO

TECHNIQUEMENT

- Identifier les machines infectées
  - La Kill Chain peut être utilisée quand les premières informations commencent à être identifiées pour tenter de remonter les différentes étapes de l'attaque et analyser son impact
  - Consultation des logs => Il est important de posséder des solutions verbeuses en logs ou d'avoir un système tierce recevant l'ensemble des logs (Syslog, SIEM, …)
- Identifier le ransomware
  - https://id-ransomware.malwarehunterteam.com/
  - https://www.nomoreransom.org/
- Restaurer les backups
- Déconnecter TOUTES les sessions
  - Création de comptes système dédiés et restreints
- Changer TOUS les mots de passe
  - + Revoir la stratégie de mots de passes (Nombre de caractères par exemple)

Timeline d'une attaque & Defcon



Attaque – Et ensuite ?

- Mise en place du MFA sur tous les services externes
  - Multi-Factor Authentication
  - Limitation du risque lié au seul mot de passe qui peut être volé ou trop faible
- Solutions de sécurité avancées (Sandboxing, EDR, Reverse Proxy, …)
  - Sandbox : Emulation de fichiers + Analyse URL
    - Vérification des clés de registre
    - Exécution de macros dans des documents Word, Excel, …
    - Utilisation des ressources
    - Création / suppression de processus systèmes
    - Catégorisation des URL
    - …
  - EDR : Pas uniquement basé sur des signatures mais analyse comportementale
  - RP : Sécurité sur les publications d'application / sites web
- Réouverture **progressive** des différents services et points réseaux

Attaque – Et ensuite ?

Audits de sécurité / Pentests

- Externe
- Interne
- Social Engineering
- Sensibilisation des utilisateurs
  - Selon l'indice relatif à la veille stratégique en matière de sécurité d'IBM, **l'erreur humaine est impliquée dans plus de 90 % des incidents de sécurité.**

Conclusion

Le risque 0 n'existe pas

Mais avec des best practices en place **et bien implémentées**, on peut considérablement limiter les dégâts.

Il faut s'entourer d'experts IT

Vos équipes internes peuvent être très compétentes, elles ne pourront jamais couvrir l'ensemble des prérequis (avant et après une attaque)

L'humain :

- n°1 des cibles des attaques
- n°1 des attaques réussies

⇒ SENSIBILISATION de TOUS les utilisateurs

Merci pour votre attention !

sales@shinka.be - 04 228 22 50

Q/R

01 02

Retour d’expérience : quels enseignements tirer de la récente cyberattaque de la SWL ?

Abdel Wissam
DPD

Éric Cortisse
Directeur informatique

SWL

Sommaire

- Scénario de l’attaque
- Quelle réaction à chaud ?
- Quel impact ?
- Comment relancer l’activité ?
- Que mettre en place ?
- Et avec le recul ?
- Quels retours d’expérience ?

Scénario de l'attaque

- Cause probable: accès initial (serveurs pas à jour pour des raisons fonctionnelles)
- Mouvements latéraux non mitigés.
- Escalade de privilèges.
- Compromission du domaine.
- Désactivation de toutes les protections (AV, …).
- Processus d'encryption.
- Perte des preuves.
- Demande de rançon.

Quelle réaction à chaud ?

- On a coupé tous les flux entrant et sortant du système;
- On est resté lucide;
- On a communiqué vers tous les collaborateurs et les partenaires;
- Dès les premières minutes on s'est entouré de spécialistes;
- On a communiqué vers l'APD;
- On a essayé de récolter des preuves;
- On a déposé plainte.

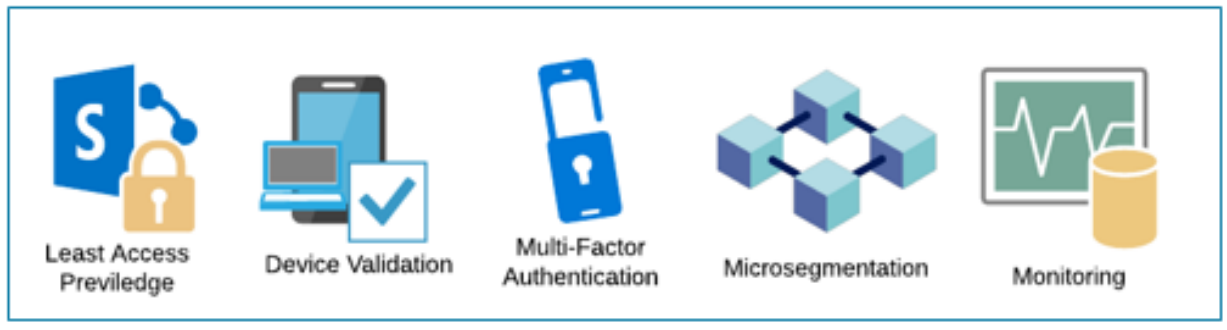
Quel impact ?

- Etendue de l’attaque
- Vérification des systèmes toujours opérationnels
- Estimation de la durée de reprise partielle des systèmes essentiels

Comment relancer l'activité ?

- Plan de reprise d'activité
- Ce plan doit être défini au préalable!
- Priorisation des actions
- La sécurité de l'infrastructure
- Procédures techniques et organisationnelles

Que mettre en place ?



- Principes fondamentaux
  - Accès strictement nécessaires
  - Validation de chaque équipement
  - Fournir au moins 2 pièces d'identité
  - Division du réseau
  - Monitoring continu (Détection des anomalies -> réaction)

Et avec le recul ?

- Couper tous les flux entrant et sortant du système;
- Rester lucide;
- Activer le PRA (DRP)
- S'entourer dès les premières minutes de spécialistes;
- Communiquer vers tous les partenaires et collaborateurs;
- Communiquer vers l'APD
- Récolter des preuves (si possible)

Quels retours d'expérience ?

- Mise à jour du PRA
- Mise en place d'une procédure de communication de crise
- Rédaction d'une feuille de route « Sécurité IT » plus stricte
  - ➢ Réduire le risque
  - ➢ Réduire l'impact

Cyberattaque : le jour d’après

Gestion d’une violation des données personnelles

Plan

- Constats
- Gestion de la violation des données
- Processus de gestion des incidents
- Les erreurs !
- Principes
- Comprendre les attaques
- Comprendre son système d’information
- Prévention
- Sécurité
- Procédures de gestion des violations de données
- Points importants à souligner

Constats

- L'attaque a eu lieu à une heure tardive → difficulté de réunir rapidement la cellule de crise
- Mise hors service de serveurs (inaccessibilité à la messagerie et difficulté de travailler en équipe)→ ralentit la réactivité pour mettre en place les étapes pour relancer les systèmes IT

Gestion de la violation des données

- Contact avec l'APD : notification, demande d'avis, suivi
- Evaluation de l'impact : estimation du risque
- Contact avec les partenaires (BCED, SLSP, sous-traitants, presse)

- Accompagnement par un consultant externe / Expert
  - Conseille sur la meilleure réponse à apporter face aux exigences de l'APD
  - Vision extérieure et systémique de l'entreprise

Gestion de la violation des données

- Rendre obligatoire le principe « Privacy By Design » : protection dès la conception pour les tous projets

- Amélioration de la campagne de sensibilisation
  - Folder « bonnes pratiques » (mensuel) disponible sur l'extranet
  - Encourager le personnel à suivre des formations
  - Bientôt : exercices de simulation phishing (en projet)

Processus de gestion des incidents

- La gestion d'un incident de sécurité de l'information nécessite une réactivité organisationnelle et technique immédiate

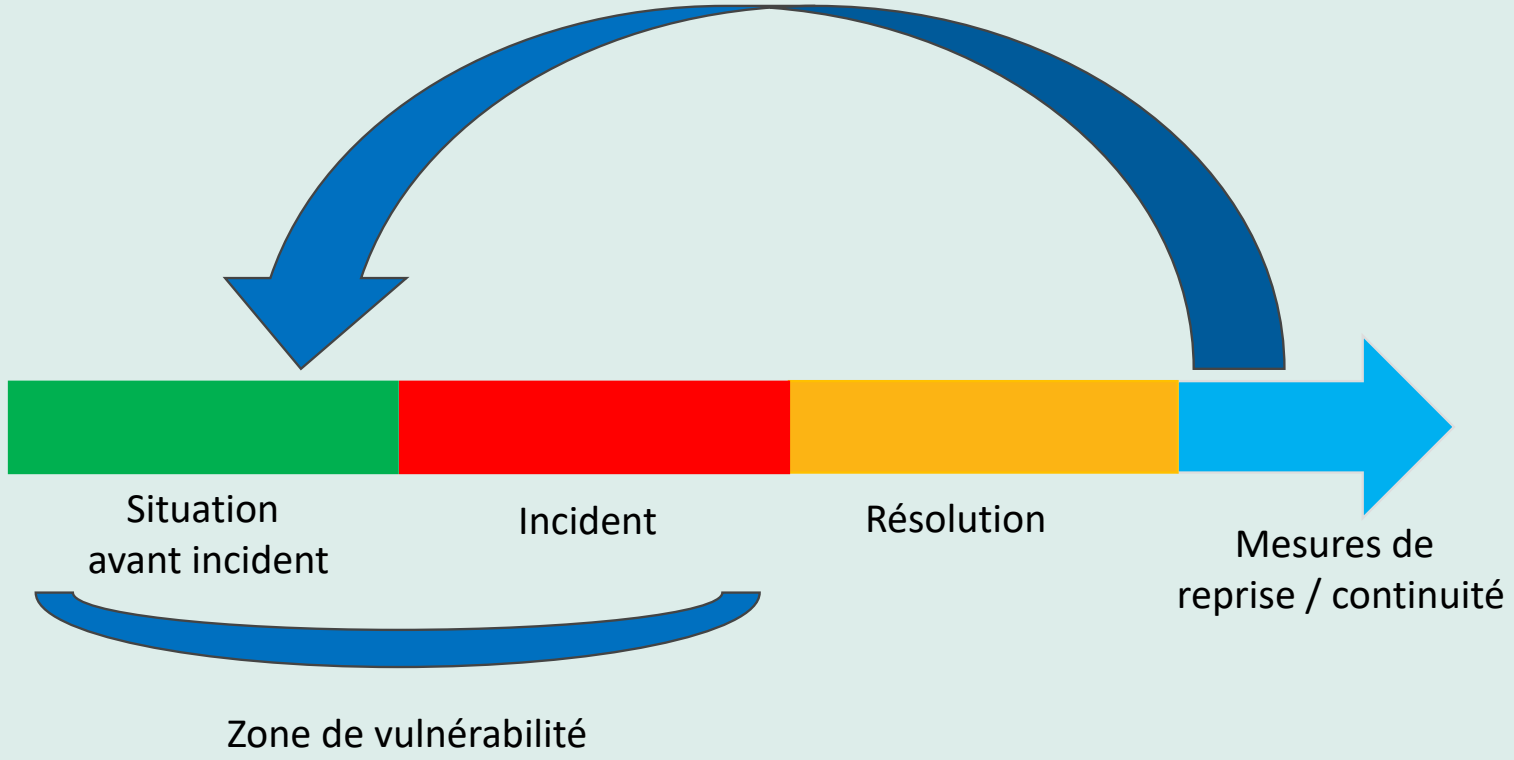
  → La gestion d'une telle crise ne peut pas s'improviser

  → Conditionnée par la mise en place d'une planification structurée en amont

Les erreurs !

- Essayer de tout faire par vous-même
- Ne pas disposer de processus documenté de gestion des incidents
- Ne pas communiquer
- Agir de manière impulsive : ne pas prendre assez de temps pour réfléchir (pas de collecte de preuves / destruction de preuves)
- Tourner en rond : prendre trop de temps pour réagir

Les erreurs !


Situation
avant incident
Incident
Résolution
Mesures de
reprise / continuité
Zone de vulnérabilité

Principes

- N’attendez pas que l’incendie se déclare → Mettre des moyens :
- Assurer une veille technologique
- Préparer une équipe dédiée (interne et externe)
- Définir des procédures de résolution d’incidents
- Définir des procédures de communication de crise (interne et externe)

Comprendre les attaques

- Les attaquants utilisent quelques astuces courantes
- Attaque à la main : difficile à arrêter
  - l'attaquant s'adapte au fur et à mesure, ne suit pas un schéma prévisible
  - prend beaucoup de temps à déployer

  → Avoir un mécanisme préventif : contrôle efficace (fréquence et volume des activités)
- Les attaques de ransomwares : opportunistes et aveugles
  - l'attaquant s'appuie sur une automatisation (pièces jointes piégées envoyées à un grand nombre de victimes potentielles par e-mail)
  - rapide, facile à déployer, pas d'expertise spéciale

  → Avoir un mécanisme réactif : détection d'intrusion , alerte

Comprendre son système d'information

- Maitriser son système d'information :
  → Vue globale sur les différents composants
  → inventaire de l'actif informationnel
- Prendre en compte la sécurité dès la conception
  → repenser à la vulnérabilité des systèmes
- Comprendre où se situe votre vulnérabilité vous assurera de ne pas tomber dans le même piège
- Liste des vulnérabilités disponibles
  https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Prévention

- Renforcer les moyens de prévention → Sensibilisation du personnel
  - Organiser des sessions de formation régulières pour les employés
  - Mettre en place des procédures de signalement et de collecte des preuves (faciles et efficaces)
- Organisation opérationnelle
  - Définir les rôles et responsabilités des parties prenantes
  - *Constitution une cellule de crise en cas de sinistre (équipe d'investigation, équipe de communication)*
  - Définir plan d'action
- Planifier des exercices de simulation
- Auditer régulièrement le mécanisme mis en place (Test + approbation)

Sécurité

- Mettre en œuvre les mesures de sécurité régies par l'article 32 du RGPD

  → fonction des moyens (capacités techniques, coût, risque résiduel)
- Pseudonymisation des archives
- Cryptage des données personnelles
- Capacité de restaurer les données en cas d'incident
- Audit régulier des mesures

Procédures de gestion des violations de données

- Déterminer si la violation concerne effectivement des données à caractère personnel (Cellule d'investigation)
- Analyser l'ampleur de la violation de données (Contexte, impact, gravité) → risque pour les droits et libertés des personnes physiques
- Procédure de contact avec l'APD
- Procédure de notification
- Formulaire spécifique
- Personnes de référence (assurer le suivi des interactions avec l'APD, la communication)

Points importants à souligner

- Réactivité tant des équipes techniques que de la direction → élément clé pour réduire l'impact sur la société
- Cellule de crise : doit se mettre en place dans les heures qui suivent l'attaque (informer par le biais d'un communiqué)
- Réponse technique : moins facile à mettre en place, (indisponibilité - black-out complet de plusieurs heures/jours)
- Pour se faire aider : soyez transparent → annoncer sans tarder que vous avez été victime de piratage
- Communiquer / Informer : autorités, usagers, services tiers, partenaires, le personnel

En conclusion et…
pour aller plus loin

Nos webinaires en replay : nouvelles technologies
https://www.uvcw.be/formations/webinaires

Espace "E-gov, TIC et simplification administrative" - Site UVCW
https://www.uvcw.be/e-gov/accueil

Votre espace eCampus
Procédure de connexion :
https://vimeo.com/518713611/f3c95176c9