Synthèse
Principe de sécurité informatique

Deuxième Bloc
Sécurité des systèmes
Année académique 2020-2021

Rédigé par Sénéchal Julien

23 Décembre 2020

1 Liste des actions à entreprendre suite à la découverte d'un RansomWare

1. Ouvrir une main courante (toute action doit y être noté)
2. Isoler tous les équipements infectés du réseau
3. Déconnecter les entrées possibles de l'attaquant pour limiter l'attaque en cours (Donc surtout Internet)
4. Appeler à l'aide les services prévu à cet effet :
   - ➤ Police, CERT.BE
   - ➤ Prestataire spécialisé (il est mieux de l'avoir choisi en amont)
   - ➤ Une éventuelle Assurance
5. Assurer la communication avec :
   - ➤ La hiérarchie
   - ➤ le métier
   - ➤ l'extérieur
6. Lancer le plan de continuité des services (redondance, pasage en mode dégradé si possible)
7. Si des données à caractères personnel ont été touché, prévenir l'Autorité de Protection des données (APD.be) (Attention au délai légal)
8. Trouver le programme malveillant (ex : Vérifier les logs)
9. Supprimer le RansomWares du système informatique infecté
10. Réinstaller l'OS si nécessaire (dans une version à jour)
11. Corriger les vulnérabilités du point d'entrée de l'attaquant
12. Restaurer les données grâce a un back-up sain

2 Les ransomwares

- Big Game Huntig
  - ➤ Attaques par ransomwares qui portent sur des victimes au moyens financiers importants. (trad : La chasse au gros)
- Attaque indirecte
  - ➤ Cibler des entreprises sous-traitantes ou clé du secteur dans le but de déstabiliser le secteur ce qui engendre un impact que le secteur.
  - ➤ Conséquences :
    - — Arrêt de production
    - — Chute du chiffre d'affaire
    - — Risques judiciaire (RGPD)
    - — Réputation
    - — Perte de confiance des clients
    - — Rupture ou dégradation de l'activité chez la victime donc impoacts sur ceux qui sont liés à l'activité
- Payer la rançon ?
  - ➤ Auncune garantie de récupérer ses données
  - ➤ Si ça fonctionne, ça retarde le problème et ne grantit pas la protection contre une seconde attaque
- Comment réduire les pertes en cas d'attaque par ransomware ?
  - ➤ Backup régulier (idéalement hors-ligne)
  - ➤ Maintien en condition de la sécurité par des correctifs
  - ➤ Mise à jour des signatures antivirus
  - ➤ Mettre en oeuvre une politique de filtrage sur les postes de travail
  - ➤ Désactiver les droits administrateur pour les utilisateurs

    - ➤ Segmentation du réseau
    - ➤ Limitation des privilèges accordés aux utilisateurs
    - ➤ Maîtrise des accès a internet
    - ➤ Sensibilisation aux risques
- 2 axes techniques pour s'en défendre
    - ➤ sécurité des réseaux (segmentation, limitation des privilèges)
    - ➤ sécurité des OS
- Besoin d'un backup même si des snapchots de machine virtuelles sont stockés sur un SAN ou NAS (Backup-less)
    - ➤ L'usage de solutions de stockage à froid permet de protéger les sauvegardes d'une infection des systèmes et de conserver les données critiques à la reprise d'activité
    - ➤ Conseillé de garder ses données à plusieurs endroits et de les maintenir à jour
- Si on ne peut pas patcher un poste, on doit prendre des mesures d'isolement
- Rôle des CERT dans la lutte contre les ransomwares
    - ➤ Assurent une veille permanente qui permet de rester informé de la découverte (des failles, type d'attaque, etc...)
    - ➤ Donnent des conseils en cas d'accident
    - ➤ Observent et analysent les problèmes de sécu en ligne et en informe l'audience
- Fonctions assurées par une passerelle Internet sécurisé
    - ➤ Filtrer les tentatives de connexion en fonction de la catégorisation ou de la réputation des sites que vos collaborateurs tentent de visiter
    - ➤ Identifier les activités anormales
- Problème de la journalisation
    - ➤ Se fait en temps réel, donc difficile de tout vérifier et de s'en rendre compte au moment opportun
    - ➤ Son but est de permettre de découvrir un problème mais pas de le prévenir
- Rôle d'un plan de continuité
    - ➤ Permet de fonctionner quand survient une altération plus ou moins sévère du système d'information
- Personnes concerné par un exercice de prévention :
    - ➤ TOUT LE MONDE doit savoir protéger ses informations
- Contenu d'une main courant
    - ➤ heure, date, action
    - ➤ nom de la personne qui fait l'action
    - ➤ description de l'action
- RETEX
    - ➤ Retour d'expérience
- Porter plainte contre X au CERT et à la police lors d'une attaque par RansomWare
- No More Ransom
    - ➤ Recensement des moyens de déchiffrement applicables à un grand nombre de rançonlogiciels

3 Quick-Wins

1. Supervisez les antivirus
2. Migrez les administrateurs dans Protected Users
3. Scannez votre espace d'adresses IP
4. Développez la connaissance des applications et leurs propriétaires
5. Activez le multi-facteur dans le cloud
6. Supprimez *seDebugPrivilege* (privilège permettant de lire la mémoire de n'importe quel processus)
7. Identifiez les prestataires DFIR (digital forensics & incident response)
8. Déployez un outil de gestion de mot de passe
9. Utilisez HaveIBeenPowned
10. Bloquez les IP suspectes sur les services exposés

4 Questions sur les Quick-Wins

- Le groupe Windows Protected Users est-il utilisable dans une foret AD hétérogène ?
  - ➤ Non si l'OS est trop vieux car cette fonctionnaité n'existe que depuis la version Windows Server 2012. Pour les serveurs plus vieux, il faut une forêt dédié
- Quel outil peut être utilisé pour vous aider à scanner votre espace d'adresses IP ?
  - ➤ nmap (scan de port)
- Qu'est-ce que le propriétaire d'une application dans un contexte professionnel d'entreprise ? (business owner)
  - ➤ Personne responsable de l'application
- L'activation d'un second facteur d'authentification, même si ce dernier n'est pas techniquement parfait, ce sera toujours mieux qu'un seul facteur d'authentification ?
  - ➤ Vrai car toujours plus de travail pour attaquer le système et peur donc démotiver le hacker. Ca peut aussi être utilisé le temps d'en trouver un meilleur
- Connaître le nom des "pompiers" de l'informatique en cas "d'incendie" pour ainsi dire (prestataire DFIR - figital forensics & incident response)
  - ➤ Nviso
  - ➤ PWC
  - ➤ KPGM
  - ➤ Deloitee
  - ➤ Ernst & Young
- Gestionnaire de mot de passe open source
  - ➤ KeePass
  - ➤ BitWarden
- Utilité de HaveIBeenPowned
  - ➤ Savoir si des informations liées à votre adresse mail ont fuité (mot de passe, nom, etc..)

5 CVE-CVSS

Ce chapitre est exclusivement le travail de Florian Nicolas, merci à lui !

- Définition
  - ➤ C'est un système de score permettant de mesurer l'exposition au danger d'une vulnérabilité
- CVSS utilise trois groupe de métriques pour évaluer une vulnérabilité :
  - ➤ Groupe de métrique de base
    - — Représente les caractèristiques d'une vulnérabilité qui est invariable dans le temps
  - ➤ Groupe de métrique temporaire
    - — Mesure les caractèristiques de la vulnérabilité qui peut changer mais pas en dehors de l'environnement de l'utilisateur
  - ➤ Groupe de métrique environnementale
    - — Mesure les aspect de la vulnérabilité qui sont spécifiques à l'environnement de l'organisation

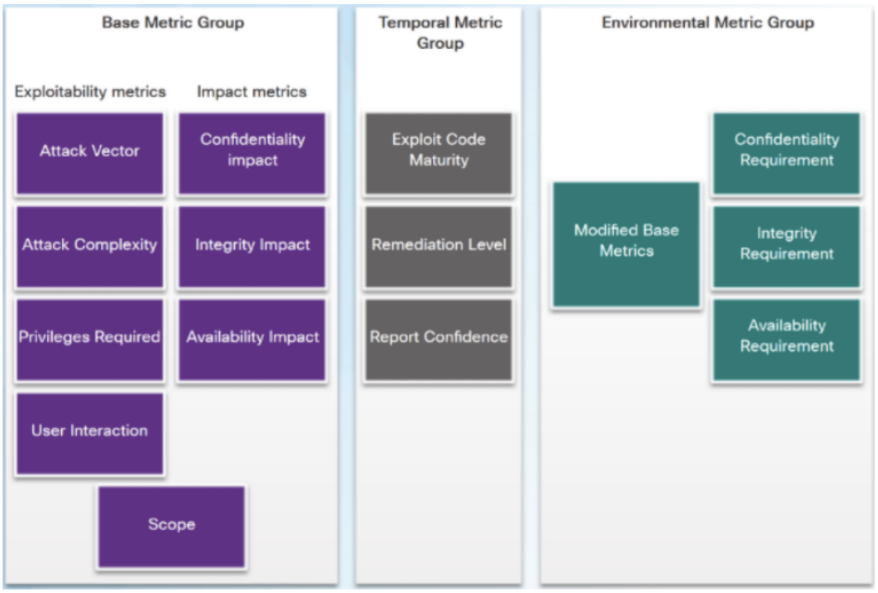

FIGURE 1 – Groupes Métriques

- CVSS Base metric group
  - ➤ Inclus
    - — Vecteur d'attaque
    - — Complexité de l'attaque
    - — Privilèges requis
    - — Interaction de l'utilisateur
    - — Objectif
  - ➤ Inclus les impacts sur :
    - — la confidentialité
    - — l'intégrité
    - — la disponibilité
- CVSS v3.0 calculator
  - ➤ Similaire à un questionnaire où chaque choix sont faits pour décrire la vulnérabilité rencontrée pour un groupe métrique
  - ➤ Le score de la vulnérabilité sera généré
- CVSS reports
  - ➤ Manière dont une vulnérabilité est mesurée :

Rating	CVSS Score
None	0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

FIGURE 2 – Groupes Métriques

6 Place de la sécurité dans l'entreprise

- Une entreprise définit son identité par des **valeurs**
  - ➤ Exemples : Innovation, qualité, intégrité, satisfaction client, etc... (Mots à choisir avec soin)
- Les valeurs permettent de définir la **mission** et la **vision** de l'entreprise
  - ➤ Mission : définition de sa raison d'être
  - ➤ Vision : l'état futur désiré
- La mission et la vision se déclienent en **stratégie(s)**
  - ➤ Stratégie : La détermination des orientations à long terme de l'entreprise et l'adoption des actions y compris l'allocation des ressources nécessaire à la réalisation de ces objectifs
- La/Les stratégie(s) se concrétise en **politique(s)**
  - ➤ Nécessite
    - — de former pour utiliser cette politique
    - — de sensibiliser le personnel
  - ➤ Caractéristiques
    - — Simple et compréhensible
    - — Facilement réalisable
    - — Vérifiable et contrôlable
    - — Durée de vie : 3-4 ans
- Une des stratégie de l'entreprise est la stratégie de sécurité de l'information
- Découle de cette stratégie la **polittique de securite informatique**
  - ➤ Déclinable en plusieurs documents
    - — Politique de contrôle d'accès
    - — Politique de gestion des droits numériques
    - — Politique de prévention
    - — Politique de protection
    - — etc...
  - ➤ Chaque focument est composé d'une partie sur :
    - — Les bonnes pratiques
    - — Une analyse des risques + une methodologie dediee
    - — La loi
    - — Une analyse des risques systematiqueent fondee sur les retours d'experience des utilisateurs (Single point of contact)
    - — Toute autre source d'information jugée utile
  - ➤ Chaque document est complété par des procédures et documentations techniques