Principes de Sécu Info – Notes

Grégoire Roumache

Septembre 2020

Table des matières

1 Quick-Wins pour RSSI

1.1 Abréviations

- DFIR = digital forensics & incident response
- AD = active directory = service centralisé d'identification et d'authentification à un réseau d'ordinateurs
- forêt AD = forêt active directory = configuration active directory contenant des domaines (ex: *example.com*), des utilisateurs, des ordinateurs, des règles de groupes
- DC = domain controller = service sur les serveurs microsoft qui répond aux demandes d'authentification de sécurité dans un domaine windows

1.2 Liste des Quick-Wins

1. **Quick-Win 1** : Supervisez les antivirus

   > Faites monitorer les instances d'antivirus sur votre parc. Quand ils plantent/s'arrêtent/sont désinstallés sur plusieurs machines en temps restreint, sonnez l'alarme.

2. **Quick Win 2** = Migrez les administrateurs dans Protected Users

   > Migrez vos administrateurs Windows dans le groupe Protected Users de l'Active Directory.

3. **Quick Win 3** = Scannez votre espace d'adresses IP

> Faites scanner vos adresses IP exposées sur Internet régulièrement, et investiguez les changements de services avant que les attaquants ne le fassent.

4. **Quick Win 4** = Développez la connaissance des applications et de leurs propriétaires

   > Listez les principales applications de votre organisation et prenez un verre/repas/café informel avec chacun de leur propriétaire plusieurs fois par an pour connaitre leurs préoccupations et projets. Bonus si vous récupérez leur GSM pour les appeler le jour où.

5. **Quick Win 5** = Activez le multi-facteur dans le cloud

   > Activez le multi-facteur d'Office 365/GSuite pour les comptes d'utilisateurs importants: services financiers, administrateurs techniques, VIP. N'attendez pas d'avoir un facteur matériel idéal: un MFA soft (même SMS) est mieux que pas.

6. **Quick-Win 6** : Supprimez `seDebugPrivilege`

   > Faites supprimer le privilege seDebugPrivilege des utilisateurs du domaine Windows. Ce privilège permet de lire la mémoire de n'importe quel processus, et de manipuler processus et taches indépendemment de leur propriétaire. Par défaut, il est donné à "Local Admin" et les seuls qui en aient besoin sont les développeurs système.

7. **Quick Win 7** = Identifiez les prestataires DFIR

   > Faites une liste des prestataires potentiels de réponse à incident et de gestion de crise. Contactez chacun pour connaître ses conditions contractuelles, tarifaires, point de contact et délais de réponse en cas d'urgence. Bonus si vous revoyez la liste tous les ans.

8. **Quick Win 8** = Déployez un outil de gestion de mot de passe

   > Faites déployer(si ce n'est déjà en place) un outil de gestion de mot de passe sur tout le parc bureautique (comme Keepass). Et préparez une campagne de "nudging" sur l'usage des mots de passe générés uniques et le stockage sécurisé.

9. **Quick Win 9** = Utilisez HaveIBeenPowned

   > Inscrire ses domaines DNS sur HaveIBeenPowned pour découvrir les mots de passe leakés avant que les attaquants ne le fassent.

10. **Quick Win 10** = Bloquez les IP suspectes sur les services exposés

    > Faites bloquer sur le pare-feu devant les services internes exposés sur Internet (webmail, portail VPN, portail RH...) les adresses IPs de sorties TOR et (si possible) des principaux VPN publics.

1.3 Questions/Réponses

1. **Quick Win 2**: le groupe Windows Protected Users est-il utilisable dans une foret AD hétérogène ? Par hétérogène, entendez ici, une foret dans laquelle on trouverait des DC de générations différentes (2008, 2012, 2016, 2003).

   > Cette feature n'existe que depuis windows server 2012, pour les serveurs plus vieux, il faut créer une forêt dédiée.

2. Quel outil peut être utilisé pour vous aider dans l'application du **Quick Win 3**, à condition d'être utilisé dans un mode de fonctionnement "raisonnable" (autrement dit, en évitant d'utiliser des options de scan trop intrusives) ?

> *nmap* peut être utilisé pour faire un scan de ports.

3. **Quick Win 4**. Qu'est-ce que le "propriétaire d'une application" dans un contexte professionnel d'entreprise ? En anglais, on utilise aussi souvent le terme "business owner".

   > Le propriétaire de l'application est la personne responsable de l'application. Elle est responsable de s'assurer que l'application atteigne les objectifs fixés et respecte les mesures de sécurité appropriées.

4. **Quick Win 5** : Vrai ou faux ? 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, ça peut démotiver le hacker et rendre son job plus difficile.

5. **Quick Win 7** : connaître le numéro des pompiers avant l'incendie... Voilà un résumé du **Quick Win 7** mais connaissez-vous le nom d'un tel prestataire en Belgique ?

   > Il y a des groupes de consultance locaux (en Belgique) et des grands groupes internationaux comme deloitte ou ernst & young.

6. **Quick Win 8** : Donnez le nom d'un gestionnaire mot de passe open source.

   > Keepass.

7. **Quick Win 9** : Testez le service HaveIBeenPowned sur une de vos adresses mail.

8. À quel **Quick Win** liez-vous cette page web ?
   https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRtCAK

   > le Quick Win 10.

2 Ransomware guide ANSSI

2.1 Abréviations

- CERT = computer emergency response team = centre belge (fédéral) pour gérer les urgences informatiques
- SAN = Storage Area Network
- NAS = Network Attached Storage
- VLAN = virtual local area network
- RETEX = retour d'expérience
- CNIL = commission nationale de l'informatique et des libertés
- DPO = délégué à la protection des données
- responsable SI = responsable du système d'information
- responsable SSI = de la sécurité du système d'information

2.2 Questions/Réponses

1. Qu'est-ce qu'une attaque de type Big Game Hunting ?

   > Ce sont des attaques menées par des groupes cybercriminels qui s'en prennent à des organisations aux moyens financiers importants ou aux activités particulièrement critiques. Les rançons peuvent atteindre jusqu'à plusieurs millions d'euros.

2. Qu'est-ce qu'une attaque indirecte (pour un secteur donné) ? Quelles peuvent-être les conséquences (préjudices) ?

   > Des attaques par rançongiciels qui ciblent des entreprises sous-traitantes ou clés du secteur.

3. Le paiement de la rançon garantit-il la récupération des données ? Faut-il la payer ?

   > Le paiement des rançons entretient cette activité criminelle et ne garantit pas à la victime la récupération de ses données.

4. Ils l'ont vécu... Quel est le secteur d'activité des entreprises/organisations qui témoignent:

   (a) CHU Rouen

   > secteur médical

   (b) M6

   > secteur des médias (radio)

   (c) Fleury Michon

   > secteur agro-alimentaire

5. Quelle est la mesure prioritaire permettant de réduire les pertes liées à l'attaque par ransomware ?

   > L'objectif principal d'un rançongiciel est d'empêcher la victime d'accéder à ses données, le plus souvent par le chiffrement de ces dernières. Devant cette menace, la réalisation de sauvegardes régulières des données apparait comme la mesure prioritaire pour réduire les pertes liées à une attaque par rançongiciel.

6. Pour mettre en œuvre le principe de défense en profondeur, on peut notamment travailler sur 2 axes techniques. Quels sont ces 2 axes (indice : ce sont aussi des intitulés de cours...) ?

   > L'application du principe de défense en profondeur sur les différents éléments du système d'information permettra de limiter le risque d'indisponibilité totale. Les 2 axes technique du principe de défense en profondeur sont:
   >
   > (a) La segmentation réseau par zones de sensibilité et d'exposition des différents éléments du système d'information.
   >
   > (b) La limitation des privilèges accordés aux utilisateurs ou encore par la maîtrise des accès à Internet.
   >
   > Point pas technique mais cité quand même:
   > Sensibiliser les utilisateurs aux risques, évaluer l'opportunité de souscrire à une assurance cyber, préparer un plan de réponse aux cyberattaques et la stratégie de communication associée.

7. Une société réalisant régulièrement des snapshots de machines virtuelles stockés dans un SAN ou sur un NAS connecté (solution orientée backup-less), peut-elle se passer d'un logiciel de sauvegarde plus traditionnel ?

   > Des sauvegardes régulières de l'ensemble des données, y compris celles présentes sur les serveurs de fichiers, d'infrastructure et d'applications métier critiques doivent être réalisées. En effet, ces sauvegardes peuvent aussi être affectées par un rançongiciel.
   >
   > Ces sauvegardes doivent être déconnectées du système d'information pour prévenir leur chiffrement. L'usage de solutions de stockage à froid, comme des disques durs externes ou des bandes magnétiques, permettent de protéger les sauvegardes d'une infection des systèmes et de conserver les données critiques à la reprise d'activité.

8. S'il s'avère impossible de patcher un poste, que peut-on mettre en œuvre pour l'utiliser tout de-même de façon sécurisée.

   En cas d'impossibilité avérée, pour des raisons métier par exemple, il s'agira de mettre en œuvre des mesures d'isolement pour les systèmes concernés.

9. Comment les CERT peuvent-ils vous aider à lutter contre les ransomwares ?

   Le CERT permet de rester informé de la découverte des vulnérabilités logicielles et matérielles des services utilisés dans votre entité et de la disponibilité des correctifs.

10. Si je crée, sur un switch 4 VLANs, (IT, RH, PROD et COMPTA) qui accèdent à Internet grâce au routeur connecté au switch, est-ce que je réalise du cloisonnement ?

    Oui parce que les appareils qui sont dans un VLAN ne peuvent pas accéder aux autres VLAN.

    Attention !
    À cause du routeur, les VLANs sont des réseaux **directement connectés**. Il faut rajouter des **ACL** (= access control list) + un **firewall** sur le routeur.

11. Pouvez-vous donner 2 fonctions assurées par une passerelle Internet sécurisée ?

    (a) Filtrer les tentatives de connexion en fonction de la catégorisation ou de la réputation des sites visités (ex: filtrer les sites douteux).

    (b) Identifier les activités anormales (ex : transmission d'un volume de données important).

12. La journalisation / supervision des journaux est une mesure de sécurité souvent mise en avant. Cependant, pour bon nombre d'entreprises, elle restera une utopie. Pourquoi ? (indice : la réponse n'est pas dans le guide... à vous de réfléchir !)

    - le coût — il faut une personne pour les lire en temps réel
    - difficulté à trier les logs — il y en a trop et tout le temps, difficile d'en tirer des informations pertinentes
    - il faut de l'expertise — pas facile d'automatiser l'analyse par exemple, il faut s'y connaître

13. Quel est le rôle d'un plan de continuité ? Idem pour le plan de reprise. Notez qu'ici, la frontière entre sécurité opérationnelle (2 IR) et gouvernance (3IR) est très fine.

    Plan de continuité informatique = permettre à l'organisation de continuer à fonctionner quand survient une altération plus ou moins sévère du système d'information.

    Plan de reprise informatique = remettre en service les systèmes d'information qui ont dysfonctionné. Il doit notamment prévoir la restauration des systèmes et des données.

14. Vrai ou faux ? "Un exercice visant à tester les plans cités ci-dessus, c'est l'affaire des geeks du service info !" Dès que l'on répond à cette question, on quitte le monde de la sécurité opérationnelle et on bascule dans celui de la gouvernance... Autant le savoir !

    - le service informatique est responsable de fournir le service informatique
    - **mais** tout le monde est concerné lors d'une reprise après une attaque
    - comme lors d'un **exercice incendie** — tout le monde doit sortir mais ce sont bien les pompiers qui éteignent l'incendie

- test de cyberattaque = couper des serveurs/services pour tester

15. Que doit contenir, en termes d'informations, le dossier main courante à alimenter durant l'incident ?

    Chaque entrée de ce document doit contenir, à minima :

    - l'heure et la date de l'action ou de l'évènement ;
    - le nom de la personne à l'origine de cette action ou ayant informé sur l'évènement ;
    - la description de l'action ou de l'évènement.

    Ce document doit permettre à tout moment de renseigner les décideurs sur l'état d'avancement des actions entreprises.

    Un peu comme un **journal de bord**.

16. Qu'est-ce que le(s) RETEX ? C'est un terme souvent utilisé sur le web, par un public francophone (p.ex. dans des podcasts français)

    RETEX = retour d'expérience

17. Considérez le scénario basique suivant : "Vous êtes responsable SI ou SSI dans une entreprise victime d'un ransomware". Dressez la liste des actions que vous allez réalisées à partir du moment où vous découvrez l'attaque.

    Attention !

    (a) isoler les équipements infectés
    (b) ouvrir une **main courante**
    (c) informer la direction, la police et l'APD (si il s'agit de données à caractère personnel)
    (d) contacter des prestataires externes si nécessaire
    (e) communiquer aux métiers affectés
    (f) s'assurer de la continuation des services essentiels de l'entreprise
    (g) restaurer les systèmes affectés à l'aide des backups

18. Pourquoi une entreprise française devrait-elle communiquer avec la CNIL en cas d'attaque de type ransomware ? Quel est l'équivalent belge à la CNIL ? Qui est le DPO, quel est, de façon résumée son rôle au sein d'une entreprise ?

    CNIL = Commission nationale de l'informatique et des libertés
    DPO = délégué à la protection des données

    - Pourquoi ? $\Longrightarrow$ obligation légale (si des données à caractère personnel sont touchées par un ransomware)
    - équivalent CNIL en Belgique = APD (= autorité de protection des données)[a]
    - rôle DPO = monsieur/madame GDPR, il veille à la bonne mise en oeuvre des mesures du GDPR au sein de l'entreprise

    [a] https://www.autoriteprotectiondonnees.be

19. Faut-il porter plainte après une attaque ? En Belgique, à qui s'adresser ? (indice : la réponse est dans le document Ransomware: Protection et prévention" du CERT.be).

> Il faut s'adresser à:
>
> - la police
> - l'APD (si il s'agit de données à caractère personnel)
> - au CERT

20. Quel est l'objectif poursuivi par le projet No More Ransom ?

> Ce projet partage des moyens de déchiffrement de certains ransomwares.

3 Que faire en cas d'attaque ?

1. Ouvrir une main courante,
2. isoler tous les équipements infectés,
3. déconnecter les entrées possibles de l'attaquant (internet) pour limiter l'attaque en cours.
4. Appeler à l'aide :
   - Police, CERT.be
   - Prestataire spécialisé, (idéalement le choisir à l'avance...),
   - Une éventuelle assurance.
5. Assurer la communication :
   - Avec la hiérarchie,
   - Avec le métier,
   - Avec l'extérieur.
6. Lancer le plan de continuité des services (passage en mode dégradé, si c'est encore possible...).
7. Prévenir l'Autorité de Protection des données (APD.be) si des DACP (Données à Caractère Personnel sont impactées). <!> au délai légal...
8. Trouver le programme malveillant (p.ex. vérifier les logs).
9. Supprimer le ransomware du système informatique infecté. Le système (OS) est intégralement réinstallé si nécessaire (dans une version à jour).
10. Corriger les vulnérabilités relatives au point d'entrée de l'attaquant.
11. Restaurer les données à l'aide d'une sauvegarde saine.

4 CVSS

- CVSS = Common Vulnerability Scoring System, is a risk assessment system, designed to convey the common attributes and severity of vulnerabilities in computer hardware and software systems
  - Standardized vulnerability scores
  - Open framework with metrics
  - Helps prioritize risk in a meaningful way
- CVSS uses three groups of metrics to assess vulnerability
  - **Base Metric Group** - characteristics that are *constant over time* and *across contexts*
  - **Temporal Metric Group** - characteristics that may *change over time*, but *not across user environments*

  - **Environmental Metric Group** - measures the aspects of a vulnerability that are *rooted in a specific organization's environment.*

- CVSS Base Metric Group criteria:
  - Attack vector
  - Attack complexity
  - Privileges required
  - User interaction
  - Scope
- Impact metric components include:
  - Confidentiality Impact
  - Integrity Impact
  - Availability Impact

5 Place de la sécu dans l'entreprise (notes tirées du schéma)

- une entreprise / une organisation / une institution – définit son identité par – des valeurs
  - ex: innovation, respect, qualité
- des valeurs – permettent de définir – une mission et une vision
  - mission = "la définition de sa raison d'être, l'aspiration suprême qu'elle tente continuellement d'atteindre"
  - vision = "l'état futur désiré"
  - la vision peut changer plus rapidement que la mission pour s'adapter au changement.
- une mission et une vision – se déclinent en – une stratégie
- une stratégie – se concrétise en – une politique
- (en fait ce sont *des stratégies* et *des politiques*)
  - stratégie = "la détermination des orientations à long terme de l'entreprise et l'adoption des actions consécutives, y compris l'allocation des ressources nécessaires à la réalisation de ces objectifs"
  - caractéristiques d'une politique:
    1. * simple et compréhensible
       * utilisable/utilisée au quotidien
    2. * aisément réalisable
       * orientée objectifs
       * vérifiable et contrôlable
    3. * durée de vie: 3-4 ans
       * de maintenance facile
- une stratégie – a comme sous-composante – la stratégie de sécurité de l'information
- la stratégie de sécurité de l'information – à laquelle correspond – une politique de sécurité informatique
- la politique de sécurité informatique – est déclinable en plusieurs documents:
  - politique de contrôle d'accès
  - politique de gestion des droits numériques
  - politique de prévention
  - politique de protection

  - ...
- ces documents – sont complétés de – procédures et documentations techniques
- ces documents – utilisent des sources d'information comme:
  - la loi
  - les bonnes pratiques
  - une analyse des risques + une méthodologie dédiée
  - une analyse des risques systematique fondee sur les retours d'experience des utilisateurs
  - toute autre source d'information jugée utile