CNAM Bretagne, Cybersécurité SEC101, eduf@ction
Notes de cours éditées le 8 avril 2020

Stratégies de cyberdéfense

Eric DUPUIS[1,2]*

Résumé
Ce document donne les grands supports d'une stratégie de cyberdéfense d'entreprise.
Il fait partie du cours introductif aux fondamentaux de la sécurité des systèmes d'information vue sous deux prismes quelques fois opposés dans la littérature : la gouvernance et la gestion opérationnelle de la sécurité. Le cours est constitué d'un ensemble de notes de synthèse indépendantes compilées en un document final unique.
Ce document ne constitue pas à lui seul le référentiel du cours. Il compile des notes de cours mises à disposition de l'auditeur comme support pédagogique.

Mots clefs
Stratégie, Cyberdéfense, anticiper

[1] *Enseignement sous la direction du Professeur Véronique Legrand, Conservatoire National des Arts et Métiers, Paris, France*
[2] *RSSI Orange Cyberdefense*
***email** : eric.dupuis@cnam.fr – eric.dupuis@orange.com

Pour être prêt à faire face aux cyberincidents inévitables, il ne suffit pas de se préparer à simplement réagir pour neutraliser une attaque isolée. Cela nécessite la capacité d'intervenir efficacement et de manière répétitive pour planifier proactivement, défendre énergiquement vos systèmes et vos actifs informationnels vitaux, devancer l'évolution des menaces, et assurer une reprise complète des activités après les attaques. Dans un contexte où les cyberattaques grèvent de plus en plus les résultats financiers et ternissent la réputation des grandes sociétés, la mise sur pied d'une solide capacité d'intervention en cas de cyberincident (ICC) devient impérieuse pour les entreprises qui tiennent à sauvegarder leur sécurité, leur vigilance et leur résilience. Une solide capacité d'intervention en cas de cyberincident peut aider votre entreprise à faire ce qui suit : Comprendre rapidement la nature d'une attaque pour mieux faire face aux questions quoi, où, comment et combien, et y répondre Réduire le plus possible les coûts – en temps, en ressources et en perte de confiance des clients – associés à la perte de données Instaurer un niveau accru de gestion et de contrôle pour renforcer les TI et les processus opérationnels et, ainsi, pouvoir vous concentrer sur vos activités de base génératrices de valeur

1. Orchestration

CyberDefenseMatrix (1)

2. Cyberrange

2.1 les grandes fragilités des infrastructures

La résiliance est dépendante de composantes

- Sur l'identité : Les annuaires : (AD ...)
- Sur l'infrastructure de routage (DNS, AS ..)

Mitre Acttack

Références

(1) Ashutosh DUTTA et Ehab AL-SHAER. « Cyber defense matrix : a new model for optimal composition of cybersecurity controls to construct resilient risk mitigation ». In : *Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security*. ACM. 2019, page 14 (cf. page 1).

3. Contributions

3.1 Comment contribuer

Les notes et les présentations sont réalisées sous LaTeX.

Vous pouvez contribuer au projet des notes de cours CNAM SEC101 (CYBERDEF101). Les contributions peuvent se faire sous deux formes :

- Corriger, amender, améliorer les notes publiées. Chaque semestre et année des modifications et évolutions sont apportées pour tenir compte des corrections de fond et de formes.
- Ajouter, compléter, modifier des parties de notes sur la base de votre lecture du cours et de votre expertise dans chacun des domaines évoqués.

Les fichiers sources sont publiés sur GITHUB dans l'espace : (edufaction/CYBERDEF) [1] . Le fichier Tex/Contribute/Contribs.tex contient la liste des personnes ayant contribué à ces notes. Le guide de contribution est disponible sur le GITHUB. Vous pouvez consulter le document **SEC101-C0-Contrib.doc.pdf** pour les détails de contributions.

3.2 Les contributeurs/auteurs du cours

Les auteurs des contributions sont :

3.2.1 Années 2020

- **David BATANY** (Contributeur LATEX) : BOTNET
- **Charly Hernandez** : User and Entity Behavior analytics, UEBA
- **Florian PINCEMIN (Orange)** : SIEM en quelques mots

3.2.2 Années 2019

- **François REGIS** (Orange) : CyberHunting

3.2.3 Années 2018

- **Julia HEINZ** (Tyvazoo.com) : ISO dans la gouvernance de la cybersécurité

1. https://github.com/edufaction/CYBERDEF

Table des matières

Table des figures