Orange CyberSchool, Direction de la formation
Notes de cours éditées le 6 décembre 2024, 21 h 10 CET

Introduction générale à la Cybersécurité d'entreprise

Eric DUPUIS[1,2]*

Résumé
Ce document présente comment s'exprimer dans le même langage que les acteurs du domaine, en ayant compris leurs valeurs, leurs codes, leur environnement et ses contraintes. Disposer des éléments de langages du domaine en comprenant les enjeux et le cadre de la Cybersécurité en entreprise. Cette première leçon donne les premiers éléments pour positionner le contexte et les enjeux de la cybersécurité en entreprise.
Il fait partie du cours introductif aux fondamentaux de la sécurité des systèmes d'information, de la cybersécurité, et de la cyberdéfense. Le cours est constitué d'un ensemble de notes de synthèse indépendantes compilées en un document unique, mais édité par chapitre dans le cadre de ce cours.
Ce document ne constitue pas à lui seul le référentiel du cours CYBERDEF101. Il compile des notes de cours mises à disposition de l'auditeur comme support pédagogique partiel à ce cours introductif à la cyberdéfense d'entreprise.

Mots clefs
Contexte, Enjeux, attaquants, biens primordiaux

[1] *Enseignement sous la direction du Professeur Véronique Legrand, Conservatoire National des Arts et Métiers, Paris, France*
[2] *Directeur Orange Campus Cyber*
***email** : eric.dupuis@lecnam.net – eric.dupuis@orange.com

1. https://github.com/edufaction/CYBERDEF/raw/master/Builder/L-Orange-Cyberdef101-M1a-Cyber.doc.pdf

Table des matières

1. Contexte

Pour démarrer la leçon plongeons nous dans quelques attaques qui ont marqué une époque, ou du moins ont été révélatrice de la monté rapide des cybermenaces sur l'environnement.

Avant d'être un affaire de criminalité et de cybercriminalité, les attaques informatiques ont été des affaires d'état, ou impliquant des états. De nos jours il y a un retour aux sources dans ce cyberespace qui est devenu un enjeu géostratégique.

On peut parler de Stuxnet, il y a plus de dix ans.

Stuxnet est le premier malware ayant causé des destructions physiques dans le monde réel. Ce virus fut développé par les services secrets d'Israël et des États-Unis, dans le but de faire échouer le programme nucléaire de l'Iran.

Histoire de Stuxnet [2].

Mais on peut plonger plus loin, dans la guerre de l'information, l'espionage avec le réseau ECHELON. avec leur station d'interception ROEM située à Menwith Hill, au Royaume-Uni. ECHELON est le nom de code utilisé pendant de nombreuses années par les services de renseignement des États-Unis pour désigner un réseau utilisé pour la surveillance et l'interception des télécommunications.

Mais revenons au 21ième siécle.

1.1 Quelques fuites de données célèbre

Sony

AsthonWhesley

TV5monde

WannaCry

1.2 Les chaines logiciels

SolarWind

Log4J

1.2.1 Libwebp

Libwebp est une bibliothèque open-source que les programmes intègrent pour obtenir la capacité d'encoder et de décoder des images au format WebP, un format moderne de compression sans perte/avec perte largement utilisé dans les applications web publiées par Google. Des centaines d'applications utilisent libwebp pour prendre en charge le format d'image WebP, de sorte qu'une vulnérabilité dans cette bibliothèque peut avoir des conséquences en cascade.

Après quelques jours de confusion dans la communauté de la sécurité suite à la divulgation initiale de la faille, répertoriée sous le nom de CVE-2023-4863, les analystes se sont rendu compte que l'impact du problème était vaste, allant au-delà des navigateurs web. Comme il a été rapporté que des pirates informatiques ont exploité activement CVE-2023-4863 dans des attaques, le risque pour des millions de personnes utilisant des logiciels encore affectés est élevé.

Pole-emploi, différents CHU

2. les attaquants

2.1 Les script kiddies

2. https://fr.wikipedia.org/wiki/Stuxnet