Thème 2 : La Cyber conflictualité La Cyber Guerre

29 mai 2009, Président Obama

« La prospérité de l’Amérique passera par la cybersécurité »

I/ Notions Cyberespace, Cyber conflictualité

Définition du Cyberespace

Selon l’agence nationale de la sécurité des systèmes d’information (ANSSI),

Le cyberespace est l’espace de communication constitué par l’interconnexion mondiale d’équipements de traitement automatisé de données numérisées.

Il est généralement caractérisé par une approche sédimentaire en trois couches.

Une première couche « physique » ou « matériel » qui regroupe les appareils d’extrémité (ordinateurs, box de fournisseur d’accès internet, disques durs, carte de crédit, distributeur de billet de banque…) ainsi que les infrastructures de réseau.

Une deuxième couche « logique » ou « logicielle » regroupe les dispositifs de codage et de programmation qu’utilisent les machines.

La pensée humaine est transformée en information via des interfaces homme-machine et des protocoles permettant la communication entre machines au sein d’un réseau, afin qu’elles puissent se transmettre l’information.

Enfin une troisième couche « sémantique », « cognitive » ou « informationnelle » regroupent les données ou métadonnées qui sont transportées par le réseau.

Ces métadonnées sont qualifiées de données de masse. Elles peuvent permettre de déterminer les goûts des consommateurs et influencer ou favoriser la prise de décision.

Définition métadonnées :

Les métadonnées sont des données qui en décrivent d’autres.

Dans la plupart de ses usages informatique, le préfixe méta signifie « définition ou description de référence ».

Exemples de métadonnées : L’auteur, la date de création, la date de modification et la taille du fichier

Les métadonnées et leur corollaire, le filtrage des données, aident à localiser un document spécifique.

Exemples de métadonnées d’une page web :

* Titre d’une page
* Description d’une page (résumé)
* Compte Twitter de l’auteur
* Mots-clefs

Remarque : comment insérer une métadonnée ?

Pour les pages web, ces données sont insérées dans le code html au travers de balises spécifiques.

Définition d’un cyberconflit <3

Un cyberconflit est l’échange d’actions qui utilisent des outils cyber ou des agression cyber pour aider chaque partie à obtenir un avantage sur l’autre dans le cadre de la rivalité qui les oppose.

Caractéristiques ?

Les attaques peuvent être l’œuvre d’un Etat, d’une entreprise, de militants, de particuliers et avoir diverses cibles.

Il s’agit d’une guerre asymétrique :

* Faibles coûts (comparativement)
* Accessible par tous
* Et avantage offensif !

Remarque : l’attaquant est en situation de force, de supériorité car le coût de l’attaque est faible alors que se défendre à un coup très élevé

Plus un pays est connecté, plus il est vulnérable aux attaques informatiques.

Exercice la cyberguerre est déclarée

1/ Il s’agit d’une guerre asymétrique :

* Faibles coûts (comparativement)
* Accessible par tous
* Et avantage offensif !

2/ Stuxnet :

Virus saboteur, structure complexe, découvert par les biélorusses et sa cible c’est les systèmes Scada. Créateur possible : USA et Islande.

3/ DuQu :

Espionnage en Iran

4/ Flame :

Espion des pcs

5/ Gauss :

Virus qui permettait de s’attaquer aux banques libanaises. Voler les mots de passes, les identifiants, voir les montants

6/ Il n’y a pas de certitudes sur le commanditaire de l’attaque.

7/

8/ Parce que le coup est bien moins cher. Si on découvre d’où vient le virus, ça peut être le début d’une guerre.

9/ Il y a une véritable course à l’armement.

10/

2015 attaques Charlie Hebdo, le même jour, 20 000 sites web hacké par l’état islamique

Gemalto, puces hacké

TV5 monde

II/ Les types d’attaques ?

Les conflictualités dans le cyber peuvent être caractérisées par une ou plusieurs combinaisons :

D’actions cyber espionnage de recherches d’informations

Ou d’actions correspondant à des cyberattaques :

* D’actions de perturbation
* De destruction
* Ou de prise de contrôle à distance de système informatique
* Ou d’actions de propagande et de manipulation de l’information assimilable à de la perturbation pour modifier l’opinion
* En effet, la dimension informationnelle et les opinions qui y circulent sont aujourd’hui le support de mouvement de contestations, d’influence, de recrutement, voire l’objet de manipulation

III/ Les conséquences des attaques ?

Conséquence d’une attaque ?

Conséquence physique pour la population : paralysie des services médicaux, risque accrus d’accident de la route suite au défaut de signalisation…

Conséquences psychologiques

Conséquences pour l’environnement : effets sur la maintenance des sites nucléaires, dysfonctionnement des égouts…

Conséquences économiques : pertes industrielles, financières, sociales…

Conséquences politiques : émeutes

Conséquences liées au cumul et à la combinaison des circonstances ci-dessus

IV/ La réponse des Etats

Etats Unis

* Le cybercommand
* Annoncée en 2007
* Création effective en 2009
* Organisation d’opérations de simulation d’attaques

France

L’ANSSI : Agence Nationale de la Sécurité des Système d’Information 🡪 défense

Crée en juillet 2009

Missions ?

* Détecter les attaques
* Prévenir la menace
* Conseiller les administrations et les opérateurs d’importance vitale
* Informer régulièrement les entreprises et le grand public

Force Offensive, mise en œuvre Décembre 2017

D’ici 2019, 2600 combattants numériques

4400 réservistes

Budget : 250 millions d’€ par an

🡪 Objectif offensif

Data Dome

Une menace persistante avancée est une attaque par laquelle une personne non-autorisé accède au réseau et passe inaperçu pendant une période prolongée. Une attaque APT vise à voler des données. Les secteurs particulièrement visés sont : la défense nationale, la fabrication et la finance. Si les attaques APT s’avèrent difficiles à repérer, le vol de données n’est jamais totalement invisible. La détection d’anomalies dans les données sortante est probablement le meilleur moyen dont un administrateur dispose pour repérer une menace persistante avancé.

2) Les techniques de détection sont nouvelles, elles font partie de l’ensemble des moyens d’action de cyber défense.

3) Tromper, duper l’attaquant

4) Rapidité d’analyse, pour stopper ou arrêter l’attaque

5) But : amener les attaquants vers de fausses pistes et repérer les attaques

7) faible

8) IoT : c’est un scénario dans lequel les objets se voient attribuer des identifiants uniques ainsi que la capacité de transférer des données sur un réseau sans interactions humaines

9) Il s’agit d’une catégorie de logiciels destiné au contrôle de processus en temps réel et de vérifier les conditions d’exploitation. La technologie SCADA s’utilise notamment dans les centrales électriques, nucléaires, les télécommunications, les transports, la gestion de l’eau et des déchets.