SAE 1.01:Sensibilisation à l'hygiène numérique

Les vulnérabilités générales:

Tout d'abord,une vulnérabilité,c'est les faiblesses ou points faibles d'un système ou d'une infrastructure qui peuvent compromettre sa sécurité.
Les vulnérabilités peuvent tant être dues aux faiblesses physiques(défaut de conception/réalisation du système) que numériques(bugs,mauvaise configuration du système…) d'un système.

- Mode de vie ultra connectée(dépendant d'un réseau)qui rend possible les intrusions dans le système d'information sur lequel sont reliés nos objets du quotidien comme professionnel (ordinateur, téléphone, réseau d'un établissement, …)
  ex attaque: déni de service distribué (DDoS) (rend indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser); botnet ()

- Dans les systèmes d'entreprises,les mots de passe par défaut non modifiés (qui généralement ne sont pas complexe) facilite l'accès à des tiers personne au données de l'entreprise (car mot de passe facilement crackable/devinable)(exemple d'attaque:brute force par dictionnaire,qui consiste à craquer

les systèmes en utilisant des mots de passe évident/connus contenue dans ce qu'on appelle un dictionnaire.)

- Tout simplement,la manipulation habile de l'être humain(exemple d'attaque:attaque par ingénierie sociale,qui consiste à subtiliser habilement des informations confidentielles en se faisant passer pour une tiers personne,ou en utilisant tout autre procédés sociale pour ce faire.)

-Une vulnérabilité courante peut également provenir de logiciels installés sur le système informatique,exploitant les failles de cette dernière pour s'introduire dans le système.(exemple d'attaque:l'attaque buffer overflow exploite les failles d'appli en envoyant une trop grande quantité de données à l'appli,ce qui peut créer un faille de sécurité dans le système.)

-dans le cas des architectures réseaux,si son matériel est mal configuré,peut également permettre la compromission d'un système.(exemple d'attaque:attaque IP spoofing qui permet à un attaquant de se faire passer pour une source légitime de trafic réseau. Ces vulnérabilités liées aux réseaux peuvent également inclure les vulnérabilités les protocoles sans fil tels que le Wi-Fi ou le Bluetooth.)

-Toujours axé sur les éléments "externes" d'un système,la communication via une boite mail virtuelle peut également compromettre un système.(exemple d'attaque:attaque hameçonnage,qui consiste à se faire passer pour un mail légitime dans le but d'obtenir des données sensibles tel que des données bancaires ou autre information confidentielle.)

Qu'est-ce qu'un ransomware ?

Le malware de rançonnage, ou ransomware, est un type de malware qui empêche les utilisateurs d'accéder à leur système ou à leurs fichiers personnels(en chiffrant ou cryptant les données) et exige le paiement d'une rançon en échange du rétablissement de l'accès de ou des systèmes corrompus.

comment se protéger d'un ransomware (wannacry):

Voici quelques moyens de s'en protéger:

- Effectuez des sauvegardes régulières de vos données (sur un disque dur, clef usb,...)

- ne pas ouvrir les messages dont la provenance ou la forme est douteuse (fichiers douteux, liens inconnus)

- mettez à jour vos principaux outils

- utilisez un compte « utilisateur » plutôt qu'un compte « administrateur »(L'administrateur d'un ordinateur dispose d'un certain nombre de privilèges sur celui-ci, comme réaliser certaines actions ou accéder à certains fichiers cachés de votre ordinateur)

Exemple de ransomware:Wannacry

Qu'est ce que Wannacry ?

WannaCry est l'une des pires cyberattaques de tous les temps,ayant fait plus de 200 000 victimes dans le monde,tout en engendrant plusieurs milliards de dollars de dégâts.

Initialement déployé le 12 mai 2017, WannaCry est un malware (variété de logiciels hostiles ou intrusifs) de type cryptoworm ransomware ciblant les ordinateurs fonctionnant sous le système d'exploitation Microsoft Windows.

Ce logiciel malveillant chiffrait les données stockées sur l'ordinateur, et réclamait une rançon allant de 300 à 600 dollars à payer en Bitcoin.

Une fois installé sur une machine, WannaCry crée aussi une porte dérobée sur le système infecté via l'envoie de nombreux e-mail par des botnet.L'une des caractéristiques de ce ransomware réside dans sa rapidité d'action,puisque ce dernier se propage ensuite sur d'autres ordinateurs vulnérables de manière autonome,ce qui peut engendrer plusieurs milliers d'ordinateurs en quelques jours seulement .

La propagation de WannaCry a été permise par l'exploit zero-day EternalBlue. Cette vulnérabilité était présente sur les vieux

ordinateurs Windows utilisant une version obsolète du protocole **Server Message Block** (SMB).

Ce malware est un ver de réseau doté d'un mécanisme de transport lui permettant de se propager automatiquement. Le code de transport scanne le réseau à la recherche de systèmes vulnérables à l'exploit **EternalBlue**, puis installe **DoublePulsar** et exécute une copie de lui-même.

Ainsi, WannaCry peut se propager automatiquement sans même que la victime intervienne. C'est une différence majeure avec d'autres ransomwares reposant sur le phishing ou l'ingénierie sociale pour se répandre.