Fiche réflexe

CYBERSÉCURITÉ

CHU AMIENS PICARDIE

Les différents types d'attaques

Attaque par rançongiciel :
- ✓ Votre ordinateur est bloqué sur une page vous indiquant de payer une certaine somme d'argent afin de débloquer vos fichiers
- ✓ Vos fichiers ou programmes ont été renommés avec des suites des caractères et il est impossible des les ouvrir
- ✓ Vos fichiers ou dossiers sont impossibles à ouvrir avec leurs programmes habituels

Attaque par hameçonnage :
- ✓ Vous avez reçu un courriel suspect vous invitant à cliquer sur un lien ou à ouvrir une pièce jointe. Vous avez, sans vous méfier, ouvert les éléments.
- ✓ Vous avez reçu un courriel suspect vous incitant à y répondre et transmettre des éléments personnels (code de carte, téléphone, mot de passe….). Vous avez, sans vous méfier, répondu à ce courriel.

Attaque par déni de service (DddoS) :
- ✓ Votre site Internet est inaccessible ou votre accès Internet ne fonctionne plus

Attaque par défiguration (défacement) :
- ✓ Votre site Internet a changé d'apparence et semble avoir été piraté

Attaque par point d'eau (watering hole) :
- ✓ Vous avez visité un site sur lequel vous avez l'habitude d'aller. Ce dernier a été piégé par des pirates qui souhaitaient que vous fournissiez volontairement des informations personnelles ou confidentielles sans vous méfier.

Attaque par hameçonnage ciblé (spearphishing) :
- ✓ Vous avez trouvé un équipement de stockage usb (clé, lecteur, carte, téléphone...) et l'avez branché sur votre pc afin de voir ce qu'il contenait sans vous méfier et un programme malveillant s'y trouvait.
- ✓ Vous avez reçu un courriel suspect mais envoyé par une connaissance ou une société pour laquelle vous êtes client. Ce courriel paraissant légitime, il vous invitait à cliquer sur un lien ou à ouvrir une pièce jointe ou à transmettre des informations confidentielles (code de carte, mot de passe,...) Vous avez, sans vous méfier, ouvert les éléments ou répondu au courriel.

Que Faut-il faire ?

o Déconnecter la machine suspecte du réseau (PC de bureau)
En 1ère intention, afin de limiter la propagation des virus informatiques sur l'infrastructure de l'établissement, il suffit de débrancher le câble réseau derrière le PC relié à la prise qui clignote.

En cas de problème avec la manipulation ou dans le doute, forcer l'arrêt du PC en appuyant au moins 10 secondes sur le bouton de démarrage du PC ou débrancher électriquement le PC

- **PC portable**

En 1ère intention afin de limiter la propagation des virus informatique sur l'infrastructure de l'établissement,

il suffit de couper le wifi en mettant le pc en veille prolongée.

Appuyer pour cela sur le bouton de démarrage du pc, l'écran doit s'éteindre. Vérifier en bougeant la souris que l'écran reste éteint.
En cas de problème avec la manipulation ou dans le doute, forcer l'arrêt du PC en appuyant au moins 10 secondes sur le bouton de démarrage du PC

PRÉVENIR LE SERVICE INFORMATIQUE

NUMÉRO ALERTE CYBER – CHU AMIENS PICARDIE :

- **EN INTERNE : 14000 HOTLINE INFORMATIQUE 8H-18H**
- **DEPUIS L'EXTERIEUR : 03.22.08.81.08**

EN DEHORS DES PLAGES HORAIRES NUIT & WEEK END :

- **ASTREINTE INFORMATIQUE À CONTACTER DEPUIS LE STANDARD DU CHU**

-EN INTERNE : 9

-EXTÉRIEUR : 0322088000