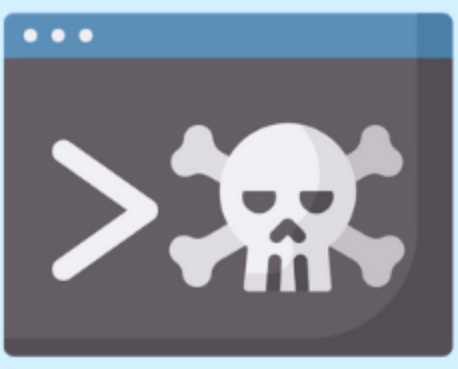

Cyber KILL CHAIN

1

RECONNAISSANCE

Le cyber attaquant sélectionne la cible, effectue des recherches et tente d'identifier les vulnérabilités du réseau cible.

2

ARMEMENT

Le cyber attaquant crée une arme malveillante d'accès à distance, comme un virus, adaptée à une ou plusieurs vulnérabilités.

3

LIVRAISON

Le cyber attaquant transmet l'arme à la cible (par exemple, via des pièces jointes à des courriels, des sites web ou des clés USB).

4

ACTIONS SUR L'OBJECTIF

Le cyber attaquant prend des mesures pour atteindre ses objectifs, telles que l'exfiltration des données, la destruction des données ou le chiffrement contre rançon.

5

INSTALLATION

L'arme malveillante installe un point d'accès (par exemple, une "porte dérobée") utilisable par un intrus.

6

COMMANDE ET CONTRÔLE

Le logiciel malveillant permet au cyber attaquant d'avoir un accès permanent au réseau cible "à partir du clavier".

7

EXPLOITATION

Le code du programme d'une arme malveillante se déclenche, ce qui permet d'agir sur le réseau cible pour exploiter la vulnérabilité.

BESOIN D'AIDE ?

Cabinet de conseil, d'audit et de formation indépendant, MANIKA propose des prestations de Sécurité de l'Information (GRC – Cybersécurité – RGPD), de Résilience (Continuité d'activité –Gestion de crise – Sûreté) et de maîtrise des processus SI.

Nos experts peuvent vous aider dans la définition et la mise en place de votre stratégie de gouvernance.

COMMERCIAL@MANIKA-CONSULTING.COM
PARIS : +33 (0)1 47 49 81 93
ROUEN : +33 (0)2 78 77 5 80
LYON : +33 (0)6 84 76 42 92
ABIDJAN : +225 22 43 18 56

MANIKA