FICHE REFLEXE INCIDENT CYBER

Ce document générique est destiné à toutes les personnes qui ont en charge l'administration d'ordinateurs reliés à un réseau de type internet (protocole TCP/IP). Il recense, de manière non exhaustive, les bons réflexes à acquérir lorsque l'on soupçonne une intrusion sur l'un ou plusieurs de ces ordinateurs.
Il peut être complété par les mesures spécifiques à votre secteur d'activité.

CONFINER LES MACHINES COMPROMISES

- DECONNEXION : **Déconnecter le Système d'Information d'Internet**

  Le pirate étant installé dans le SI il peut piloter les PC à distance et continuer de compromettre vos outils informatiques

- ISOLATION : **Isoler les machines compromises**

  Débrancher le câble Ethernet du PC et/ou couper les points d'Accès WIFI afin d'éviter toute latéralisation de l'attaque

- CONSERVATION DES PREUVES : **Ne pas éteindre les machines compromises**

  Les systèmes compromis doivent faire l'objet d'une sauvegarde complète avant reconstruction : Copie physique des disques durs et Copie de la RAM qui peut contenir des éléments cruciaux pour l'enquête. Ces techniques de sauvegarde nécessitent des compétences et des outils particuliers
  > Demander conseil au service enquêteur (Police / Gendarmerie)

PERSONNES A CONTACTER

	QUI	POURQUOI	CONTACT
En Priorité	Votre responsable de sécurité		
	La Police ou la Gendarmerie pour déposer plainte	Votre organisme pourrait, dans certains cas, être considéré comme pénalement et civilement responsable des dégâts qui seraient causés par un intrus, à partir de vos systèmes d'information. Votre assureur pourrait exiger un dépôt de plainte pour couvrir les dommages.	**Police Judiciaire :** cybermenaces-bordeaux@interieur.gouv.fr **Gendarmerie :** securite-economique-nouvelleaquitaine@gendarmerie.gouv.fr
	LA CNIL	La notification d'un vol ou fuite de données personnelles est une obligation légale	https://notifications.cnil.fr/notifications/index
	Votre prestataire informatique		
Acteurs spécifiques	Votre Banque et/ou votre Assureur	En cas de fraude financière votre banquier peut geler les versements des sommes d'argent. Votre Assureur dispose peut-être de moyens techniques pour la remédiation du système d'information	
	Vos clients et partenaires	En cas de vols de données prévoir un plan de communication pour informer ses clients et partenaires pour limiter l'impact médiatique et le risque de compromission des systèmes de vos contacts (attaque par rebond)	
	ANSSI	Si vous êtes un OIV ou un OSE vous devez informer l'ANSSI dont vous dépendez.	https://www.ssi.gouv.fr/administration/protection-des-oiv/la-cybersecurite-en-action/

AUTRES RESSOURCES

www.cybermalveillance.gouv.fr	Assistance et prévention du risque cyber pour les entreprises, les particuliers et les collectivités. Le site référence les sociétés de service spécialisées en réponse à incident pour les PME
https://www.cert.ssi.gouv.fr/pdf/CERTA-2002-INF-002.pdf	Note d'information sur la conduite à suivre en cas d'attaque cyber
https://www.cert.ssi.gouv.fr/	Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques
https://www.ssi.gouv.fr/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/	Liste des prestataires de service qualifiés par l'ANSSI
https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action	Portail du ministère de l'intérieur pour signaler des contenus ou comportements illicites sur Internet.

INFORMATION A COMM UNIQUER AU SERVICE ENQUETEUR

- Le Contexte de l'incident
- Un descriptif de l'architecture du système informatique compromis.
- l'ensemble des données réseaux sur la période de l'incident (protocoles, statistiques de flux…).
- Une copie physique des supports compromis : la copie bit à bit permet de récupérer l'ensemble des données y compris les données effacées
- En cas de fourniture de données provenant d'un prestataire de service, il conviendra d'identifier précisément ce dernier qui attestera de leur origine.