LA DÉFIGURATION

CENTRE CYBER DU PACIFIQUE

EN BREF

QU'EST-CE QUE C'EST ?

La défiguration est une attaque informatique consistant à modifier sans autorisation l'apparence d'un site Internet, en y remplaçant tout ou partie de son contenu par des messages, images, vidéos ou slogans étrangers à son objet initial. Visible par tous, elle prouve que le pirate a pris le contrôle du serveur, ce qui peut lui permettre d'accéder à des données sensibles. Au-delà de l'interruption du service, cette altération porte atteinte à l'image et à la crédibilité du propriétaire du site, tout en pouvant entraîner des pertes financières et de productivité.

BUT RECHERCHÉ : Démontrer la prise de contrôle d'un site pour nuire à son image, revendiquer une cause ou voler des données.

Voici 9 bonnes pratiques à adopter si vous êtes victime

1. DÉCONNEXION DE LA MACHINE OU ALERTE À L'HÉBERGEUR
2. RÉCUPÉRATION DES JOURNAUX DE CONNEXION (LOGS)
3. RÉALISATION D'UNE COPIE PHYSIQUE COMPLÈTE DE LA MACHINE
4. IDENTIFICATION DES ÉLÉMENTS SENSIBLES COMPROMIS
5. NOTIFICATION À LA CNIL EN CAS DE DONNÉES PERSONNELLES
6. IDENTIFICATION DE LA SOURCE DE L'INTRUSION
7. DÉPÔT DE PLAINTE AVEC PREUVES
8. CORRECTION DES FAILLES ET CHANGEMENT DES MOTS DE PASSE
9. ASSISTANCE PAR DES PROFESSIONNELS QUALIFIÉS

▶ Voir détail page "9 BONNES PRATIQUES À ADOPTER"

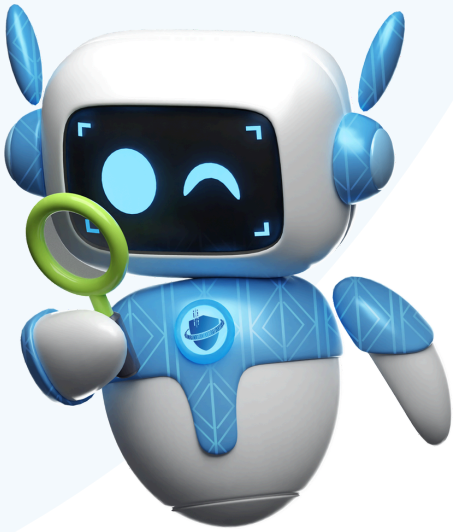
LA DÉFIGURATION

CENTRE CYBER DU PACIFIQUE

9 BONNES PRATIQUES À ADOPTER

1. DÉCONNEXION DE LA MACHINE OU ALERTE À L'HÉBERGEUR

Si possible, déconnectez d'Internet la machine concernée ou alertez votre hébergeur pour qu'il prenne les mesures nécessaires.



2. RÉCUPÉRATION DES JOURNAUX DE CONNEXION (LOGS)

Récupérez les fichiers de journalisation de votre pare-feu, proxy et serveurs touchés, utiles pour l'investigation.

3. RÉALISATION D'UNE COPIE PHYSIQUE COMPLÈTE

Effectuez une copie complète de la machine attaquée et de sa mémoire pour préserver les preuves.

4. IDENTIFICATION DES ÉLÉMENTS SENSIBLES COMPROMIS

Repérez les données qui ont pu être copiées ou détruites.

5. NOTIFICATION À LA CNIL EN CAS DE DONNÉES PERSONNELLES

Si des données à caractère personnel ont été compromises, signalez l'incident à la CNIL.

6. IDENTIFICATION DE LA SOURCE DE L'INTRUSION

Analysez l'attaque pour en déterminer la source et éviter toute récurrence.

7. DÉPÔT DE PLAINTE AVEC PREUVES

Déposez plainte auprès de la police, de la gendarmerie ou du procureur, en fournissant toutes les preuves recueillies.

8. CORRECTION DES FAILLES ET CHANGEMENT DES MOTS DE PASSE

Corrigez toutes les failles de sécurité et changez l'ensemble des mots de passe avant remise en ligne.

9. ASSISTANCE PAR DES PROFESSIONNELS QUALIFIÉS

Faites appel à des experts en sécurité informatique si nécessaire.

LA DÉFIGURATION

CENTRE CYBER DU PACIFIQUE

COMMENT S'EN PROTÉGER ?

Appliquez de manière régulière et systématique les mises à jour de sécurité :
du système d'exploitation et des logiciels installés sur vos serveurs.

Ayez un pare-feu correctement paramétré :
fermez tous les ports inutilisés et ne laissez que les adresses des machines indispensables accéder aux fonctionnalités d'administration du site.

Consultez régulièrement les fichiers de journalisations (logs) :
de votre pare-feu afin de détecter toute tentative d'intrusion, ainsi que les logs de vos serveurs exposés pour identifier les tests de mots de passe suspects en particulier.

Vérifiez que les mots de passe sont suffisamment complexes et changés régulièrement :
mais également que ceux créés par défaut sont effacés s'ils ne sont pas tout de suite changés (tous nos conseils pour gérer vos mots de passe).

Sensibilisez les utilisateurs à ne jamais communiquer d'éléments d'accès administrateurs et d'authentification à un tiers non identifié :
(ingénierie sociale, hameçonnage, etc.).

Ne conservez pas de manière accessible :
la liste nominative des personnes possédant les droits d'administrateur sur le serveur.

EN FONCTION DU CAS D'ESPÈCE, LES INFRACTIONS SUIVANTES PEUVENT ÊTRE RETENUES :

L'incrimination principale qui peut être retenue ici est celle de l'entrave à un système de traitement automatisé de données (STAD ou système d'information).

Les articles 323-1 à 323-7 du code pénal disposent que sont passibles de trois à sept ans d'emprisonnement et de 100 000 à 300 000 euros d'amende :

- « le fait d'accéder ou de se maintenir, frauduleusement » dans un système de traitement automatisé de données (par exemple en utilisant le mot de passe d'un tiers ou en exploitant sciemment une faille de sécurité) ;

- « le fait d'introduire frauduleusement des données » dans un système de traitement automatisé de données. Ce texte peut s'appliquer dans le cadre de la défiguration de site Internet. La défiguration désigne la modification non sollicitée de la présentation d'un site Internet, à la suite d'un piratage du site ;

- le fait « d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données » d'un système de traitement automatisé de données. La copie frauduleuse de données (souvent improprement qualifiée de « vol » de données) pourra être donc sanctionnée sur ce fondement ;

- « le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données » ;

Les tentatives de ces infractions sont punies des mêmes peines (article 323-7 du code pénal).

En fonction du cas d'espèce, les peines encourues sont de deux ans à sept ans d'emprisonnement et de 60 000 euros à 300 000 euros d'amende.