LES RISQUES INFORMATIQUES
La défiguration de site

OU COMMENT PERDRE LA FACE !

La défiguration d'un site web se caractérise par une ***altération visuelle*** de l'une de ses pages par un attaquant dont les motivations peuvent être très diverses**.** La nouvelle apparence du site web attaqué peut alors comporter des messages, images et vidéos sans rapport avec l'objet initial du site. Si l'attaque revêt un caractère virtuel, le préjudice subi peut quant à lui avoir des conséquences bien réelles sur la continuité de l'activité de l'entité visée (discrédit, vol de données, perte d'exploitation, etc.).

ENTRE QUÊTE DE NOTORIÉTÉ ET IDÉOLOGIE

Dans la très grande majorité des cas, l'auteur d'une défiguration de site web cherchera à la revendiquer et à faire la démonstration de son « exploit ». Ses motivations peuvent être toutefois de plusieurs natures, à savoir:

- Rechercher à accroitre sa ***notoriété*** dans l'univers des hackers,
- Transmettre un ***message*** à caractère ***idéologique*** ou ***politique***,
- Entamer ***la réputation*** de l'entité visée,

Quelles que soient ses motivations, l'attaquant pourra profiter de l'accès frauduleux au système de traitement de données automatisé (STAD) pour commettre un ***vol de données sensibles***, pour ensuite les revendre ou poursuivre ses activités frauduleuses.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

ENTRE SANCTIONS ET OBLIGATIONS

Réprimer les atteintes aux systèmes de traitement automatisé de données (STAD)

Fondées à l'origine sur la loi dite « Godfrain » de 1988, la sanction des atteintes aux STAD a depuis été sensiblement renforcée. Les articles 323-1 et suivants du Code pénal prévoient notamment que le fait « *d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données (…)* » contenues dans un STAD est puni de 5 ans d'emprisonnement et de 150 000€ d'amende (initialement fixé à 75 000€, ce montant a été révisé par l'art 4 de la loi du 24 juillet 2015 relative au renseignement).

Obligation de notifier toute violation à un traitement de données automatisé

Depuis le 25 mai 2018, le Règlement général européen sur la protection des données (RGPD) impose aux entreprises et aux organisations de revoir toute leur architecture de collecte et de traitement des données personnelles de leurs utilisateurs.

Ainsi, l'art 33 du règlement oblige le responsable du traitement de données victime d'une atteinte à son STAD de notifier la violation dans les 72H à l'autorité de contrôle (CNIL), sous peine de sanctions et amendes administratives !

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Si vous êtes victime d'une défiguration de site web, ou souhaitez réduire votre exposition au risque, vous devez:

- Observer une politique rigoureuse de sécurité de vos systèmes d'information et tenir régulièrement à jour votre système d'exploitation,
- Suivre les conseils d'assistance et de prévention de cybermalveillance.gouv.fr et consulter notamment la fiche guide relative à la défiguration de site web,
- Sensibiliser votre entourage et inciter au renforcement des mots de passe en suivant les conseils de l'ANSSI et en en appliquant la méthode proposée par la CNIL,
- Conscients des enjeux pour la sécurité, la justice et les libertés publiques, l'INHESJ et l'IHEDN ont décidé, avec leurs partenaires, de proposer une formation de haut niveau, candidatez !
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT