Région de gendarmerie Nouvelle-Aquitaine
Antenne Sécurité Économique et Protection des Entreprises de la formation administrative de Poitou-Charentes
Groupement de gendarmerie départementale de la Vienne.

Défacement des sites internet

DÉFACEMENT (défiguration) : Résultat d'une activité malveillante visant à modifier l'apparence ou le contenu d'un serveur Internet. Cette action est souvent porteuse d'un message politique et d'une revendication.

DE QUOI PARLE T-ON ?

L'actualité récente a montré un accroissement significatif du nombre d'attaques informatiques visant des sites Internet français. La très grande majorité de ces attaques sont des défigurations de sites Internet (ou défacement), ou des dénis de service (DDoS – saturation des serveurs – dysfonctionnement) qui exploitent les failles de sécurité de sites vulnérables. La mise en ligne d'un site Internet chez un hébergeur ne dédouane pas l'administrateur du site d'effectuer régulièrement des mises à jour logicielles.

QUE FAIRE ?

Le site a été défacé (la page d'accueil a été remplacée), 3 origines possibles :
1/ Des «Scripts Kiddies » (hackers débutants) se sont amusés à se prouver qu'ils étaient capables de défacer un site.
2/ Un employé ou un ancien employé a voulu se venger (ce type d'attaque est très fréquente).
3/ Des hackers.
- L'origine peut être des revendications politiques, les pirates n'étaient pas d'accord avec les idées ou principes politiques présentés sur le site.
- L'origine peut être économique afin de nuire à l'image de l'entreprise ou de l'organisme.
- Cela peut être personnel si quelqu'un en veut à la victime.

ATTENTION : Le piratage du site ne correspond pas toujours au défaçage du site, c'est même rarement le cas ! Certains piratages peuvent donc passer inaperçus pendant quelques temps voire de longs moments. Dans tous les cas, cela révèle la présence d'une ou plusieurs failles qu'il faudra corriger.

Précautions :
1/ Effectuer les mises à jour des applications sur les ordinateurs de l'entreprise (antivirus, parefeu, etc.).
2/ Utiliser des mots de passe forts (9 caractères alphanumériques et caractères spéciaux), principalement pour l'administrateur du site. Proscrire le duo login-mot de passe (admin – admin).
3/ Effectuer des sauvegardes régulières de son site et des données contenues dans les bases de données (voir avec hébergeur).
4/ Avoir une politique de hiérarchisation des accès au serveur. Tout le monde ne peut pas mettre à jour les données sur le serveur.
5/ Vérifier la sécurisation de son site régulièrement et notamment à chaque mise à jour importante.
6/ Mettre à jour l'application permettant de créer et de maintenir le site en activité.
7/ Surveiller le trafic du site. Une augmentation significative des visites doit être analysée.

Réactions :
En cas d'attaque avérée, il y a lieu de prendre des mesures en urgence.
1/ Effectuer des captures d'écran de l'attaque.
2/ Prendre attache avec votre hébergeur afin qu'il réalise les mises à jour sécuritaires.
3/ Demander à votre hébergeur de désactiver l'accès à votre site le temps de la mise à jour logicielle de votre site et du nettoyage complet des malwares (vers, virus, chevaux de Troie etc.).
4/ Aviser les clients ou membres du site.

AU MOINDRE DOUTE, ALERTEZ IMMÉDIATEMENT LES FORCES DE L'ORDRE