RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

PIRATAGE D'UN SYSTÈME INFORMATIQUE Pro

Un système informatique (ou système d'information) désigne tout appareil, équipement ou ensemble de ces matériels, permettant de traiter et stocker des données (ordinateur, appareil mobile, objet connecté, serveur, réseau...). Le piratage d'un système informatique se définit comme l'accès non autorisé à ce système par un tiers. En pratique, les pirates peuvent s'introduire dans un système informatique par l'utilisation d'une faille de sécurité ou d'un défaut de configuration d'un équipement; l'infection par un logiciel malveillant (virus); le vol d'identifiants de connexion suite à un appel ou un message frauduleux (hameçonnage); etc. L'origine de l'intrusion peut être interne (collaborateur, prestataire) ou externe (cybercriminels). Une fois introduits, les cybercriminels peuvent chercher à se propager aux autres équipements du réseau attaqué. Une intrusion peut entraîner le vol, voire la destruction, des informations du système touché.

BUT RECHERCHÉ

Prendre le contrôle ou utiliser les ressources d'un équipement pour en faire un usage frauduleux : gain d'argent, espionnage, sabotage, revendication, chantage ou vandalisme.

SI VOUS ÊTES VICTIME

METTEZ EN QUARANTAINE LES ÉQUIPEMENTS concernés par l'incident.

IDENTIFIEZ LA SOURCE DE L'INTRUSION (faille de sécurité, message malveillant...) pour la corriger.

IDENTIFIEZ TOUTE ACTIVITÉ INHABITUELLE : création de comptes, ajout de fichier dans le système, etc.

ÉVALUEZ L'ÉTENDUE DE L'INTRUSION à d'autres appareils ou équipements.

COLLECTEZ LES PREUVES : journaux (logs) des pare-feu et serveurs, copie complète (physique) des équipements compromis et de leur mémoire...

DÉPOSEZ PLAINTE au commissariat de police ou à la brigade de gendarmerie dont vous dépendez avec toutes les preuves en votre possession.

RÉALISEZ UNE ANALYSE ANTIVIRALE COMPLÈTE de l'ensemble de vos équipements.

RÉINSTALLEZ LE SYSTÈME compromis depuis une sauvegarde antérieure à l'attaque.

CHANGEZ LES MOTS DE PASSE d'accès aux équipements touchés.

METTEZ À JOUR LES LOGICIELS ET ÉQUIPEMENTS avant la remise en service de votre système.

NOTIFIEZ L'INTRUSION À LA CNIL en cas de violation de données à caractère personnel.

FAITES-VOUS ASSISTER AU BESOIN PAR DES PROFESSIONNELS SPÉCIALISÉS que vous pourrez trouver sur www.cybermalveillance.gouv.fr.

MESURES PRÉVENTIVES

Utilisez, paramétrez et mettez à jour régulièrement votre antivirus et les équipements de sécurité de votre système informatique (pare-feu, etc.).

Mettez à jour régulièrement les appareils, les systèmes d'exploitation ainsi que les logiciels installés de vos équipements.

N'installez pas de logiciels, programmes, applications ou équipements « piratés » ou dont l'origine ou la réputation est douteuse.

N'utilisez les comptes administrateurs qu'en cas de nécessité.

Limitez les privilèges et les droits des utilisateurs au strict nécessaire.

Vérifiez régulièrement les fichiers de journalisation de vos équipements afin d'identifier toute activité inhabituelle.

Utilisez des mots de passe suffisamment complexes et changez-les au moindre doute (tous nos conseils pour gérer vos mots de passe).

Faites des sauvegardes régulières et déconnectées de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine au besoin.

N'ouvrez pas les messages suspects, leurs pièces jointes et ne cliquez pas sur les liens provenant d'expéditeurs inconnus ou dont le contenu est inhabituel.

EN PARTENARIAT AVEC :
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION