Parc d'Activités Schweitzer
26 rue du bois Fossé
85300 CHALLANS
Tél. 02 51 49 31 31

espace technologie

FICHE CONSEIL

CYBER SECURITE : REPONSES APRES INCIDENTS

TABLE DES MATIERES

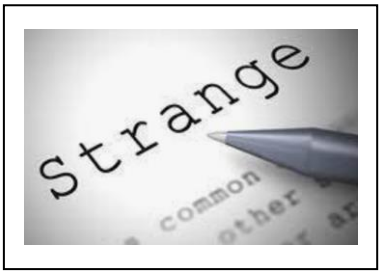
1. introduction 3
2. mettre en evidence des comportements inhabituels 3
3. Quels sont les bons réflexes en cas d'intrusion sur une machine ? 4
   3.1 Déconnecter la machine du réseau 4
   3.2 Prévenir le responsable sécurité 4
   3.3 Faire une copie physique du disque 4
   3.4 Pourquoi faire une copie du disque ? 4
   3.5 Pourquoi faire une copie physique – du disque ? 5
   3.6 Comment faire un copie physique du disque ? 5
   3.7 Rechercher les traces disponibles 5
   3.8 Remarque importante 5
4. Quels sont les aspects légaux d'une intrusion ? 6
   4.1 Dépôt de plainte 6
   4.2 Dégâts à des tiers 6
   4.3 Services centraux spécialisés 6
5. Comment analyser l'intrusion a posteriori ? 8
6. Comment repartir sur de saines bases après une intrusion ... 8
   6.1 Ré-installer complètement le système d'exploitation à partir d'une version saine 8
   6.2 Supprimer tous les services inutiles 9
   6.3 Appliquer tous les correctifs de sécurité préconisés pour le système d'exploitation et les logiciels utilisés 9
   6.4 Restaurer les données d'après une copie de sauvegarde non compromise 9
   6.5 Changer tous les mots de passe du système d'information . 9
7. Comment améliorer sa sécurité après une intrusion 10
   7.1 Se poser les bonnes questions et apporter les réponses avec soin 10
   7.2 En déduire les choses à améliorer 10
   7.3 Garder une trace écrite complète de tout ce qui s'est passé 11
   Sources : https://www.cert.ssi.gouv.fr 11

1. INTRODUCTION

Ce document général 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.

On considère qu'il y a intrusion sur un système d'information lorsqu'une personne réussit à obtenir un accès non autorisé sur ce système. En particulier, dans beaucoup de cas d'intrusion, une personne n'ayant en théorie pas le droit d'accès au système d'information parvient à s'octroyer les droits de l'administrateur.

2. METTRE EN EVIDENCE DES COMPORTEMENTS INHABITUELS



Certains signes indiquent que le système a peut-être été compromis. Ils peuvent être recherchés systématiquement par des outils de détection d'intrusion, mais peuvent également être remarqués ponctuellement :

- Impossibilité de se connecter à la machine ;
- Fichier(s) disparu(s) ;
- Système de fichiers endommagé ;
- Signature de binaires modifiée ;
- Connexions ou activités inhabituelles ;
- Activité importante ;
- Services ouverts non autorisés ;
- Présence d'un renifleur de mots de passe (généralement appelé « sniffer ») ;
- Modification intempestive du fichier de mots de passe, date de modification suspecte ;
- Création ou destruction de nouveaux comptes ;
- Création de fichiers, y compris de fichiers cachés.

3. QUELS SONT LES BONS REFLEXES EN CAS D'INTRUSION SUR UNE MACHINE ?

3.1 DECONNECTER LA MACHINE DU RESEAU

Déconnecter du réseau la machine compromise (ou les machines) permet de stopper l'attaque si elle est toujours en cours. S'il était toujours connecté à la machine, l'intrus n'a plus de contrôle sur celle-ci et ne pourra donc pas surveiller ce que vous faites et/ou modifier des fichiers. En revanche, maintenez la machine sous tension et ne la redémarrez pas, car il serait alors impossible de connaître les processus qui étaient actifs au moment de l'intrusion. Vous risqueriez de provoquer une modification sur le système de fichiers et de perdre de l'information utile pour l'analyse de l'attaque.

Il convient de débrancher la prise RJ 45 ou le wifi

3.2 PREVENIR LE RESPONSABLE SECURITE

Prévenez immédiatement le responsable sécurité et votre hiérarchie qu'une intrusion a été détectée. Prévenez-les de préférence par téléphone ou de vive voix, car l'intrus est peut-être capable de lire les courriers électroniques échangés, depuis une autre machine du réseau.

Le responsable sécurité doit être clairement identifié par tous les administrateurs système/réseau avant que l'incident de sécurité ne soit déclaré. C'est la base de toute procédure de réaction sur incident de sécurité.

3.3 FAIRE UNE COPIE PHYSIQUE DU DISQUE

Attention la copie physique d'un disque dur est une opération très délicate.

3.4 POURQUOI FAIRE UNE COPIE DU DISQUE ?

D'une part, en l'absence de copie, l'altération des données provoquée par l'analyse rendrait inefficace toute procédure judiciaire, si vous souhaitiez mener cette démarche. D'autre part, même si aucune action judiciaire n'est envisagée, vous pourrez tout de même avoir besoin dans le futur d'une copie exacte du système tel qu'il était au moment de la découverte de l'intrusion.

3.5 POURQUOI FAIRE UNE COPIE PHYSIQUE – DU DISQUE ?

Une simple sauvegarde de fichiers ne fournit pas l'intégralité des informations contenues sur le disque, il est donc important de procéder à une copie de bas niveau du disque, y compris des secteurs non occupés.

3.6 COMMENT FAIRE UN COPIE PHYSIQUE DU DISQUE ?

Sur un système Unix, vous pouvez utiliser la commande dd pour procéder à la copie exacte du disque. Sur un système Windows, il n'existe pas de telle commande sur le système d'exploitation, mais de nombreuses applications sont disponibles pour effectuer la même opération. (clonezilla)

Attention : l'image produite ne doit en aucun cas être stockée, même temporairement, sur le disque à étudier.

3.7 RECHERCHER LES TRACES DISPONIBLES

Un équipement n'est jamais isolé dans un système d'information. S'il a été compromis, il doit exister des traces dans d'autres équipements sur le réseau (gardes-barrière, routeurs, outils de détection d'intrusion, etc…). C'est pourquoi il est utile de rechercher des traces liées à la compromission dans tout l'environnement, les copier, les dater et les signer numériquement.

3.8 REMARQUE IMPORTANTE

Si vous avez pu déterminer l'origine probable de l'intrusion, n'essayez pas d'entrer en contact directement avec l'administrateur de la machine dont semble provenir l'attaque. Vous risqueriez en effet de communiquer avec le pirate et de lui fournir des informations importantes sur ce que vous savez de lui.

4. QUELS SONT LES ASPECTS LEGAUX D'UNE INTRUSION ?

4.1 DEPOT DE PLAINTE

Gardez à l'esprit que seule la direction de votre organisme, qui en porte l'autorité morale, est habilitée à déposer une plainte.

4.2 DEGATS A DES TIERS

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.Dans tous les cas, si votre S.I. stocke des données personnelles, vous devez signaler l'incident à la CNIL

4.3 SERVICES CENTRAUX SPECIALISES

Voici les services spécialisés auprès desquels la direction de votre organisme peut déposer une plainte si elle le désire :

SDLC/OCLCTIC

Sous-Direction de Lutte contre la Cybercriminalité, Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication.
Dépend de la Direction Centrale de la Police Judiciaire.
Compétence nationale, point de contact international
Tel : 01 47 44 97 55
http://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminalite

BEFTI
Brigade d'enquêtes sur les Fraudes aux Technologies de l'Information.
Dépend de la Direction Régionale de la Police Judiciaire de la Préfecture de Police de Paris.
Compétence sur Paris et la petite couronne.
Tel : 01 55 75 26 19
http://www.prefecturedepolice.interieur.gouv.fr/

DGSI
Direction Générale de la Sécurité Intérieure.
Compétence nationale. Enquête sur les crimes et délits pouvant porter atteinte à la sûreté de l'Etat.

Tel : 01 77 92 50 00
http://www.interieur.gouv.fr/

Gendarmerie Nationale/C3N
Pôle judiciaire de la gendarmerie nationale.
Centre de lutte contre les criminalités numériques.
Compétence nationale.
Tel : 01 78 47 36 52
http://www.gendarmerie.interieur.gouv.fr

CNIL
https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

5. COMMENT ANALYSER L'INTRUSION A POSTERIORI ?

L'analyse de l'incident ne devra être faite que sur une copie physique du disque dur, dans le cas où un dépôt de plainte est envisagé. L'altération des données provoquée par l'analyse rendrait inefficace toute procédure judiciaire.

Les grandes étapes de l'analyse de l'intrusion sont :

1. La recherche des modifications dans le système et les fichiers de configuration ;
2. La rechercher des modifications de données ;
3. La recherche des outils et des données laissés par l'intrus ;
4. L'examen des fichiers de journalisation ;
5. La recherche d'un sniffer sur le réseau ;
6. La vérification des autres machines connectées sur le réseau.

6. COMMENT REPARTIR SUR DE SAINES BASES APRES UNE INTRUSION

6.1 RE-INSTALLER COMPLETEMENT LE SYSTEME D'EXPLOITATION A PARTIR D'UNE VERSION SAINE

N'oubliez pas que sur une machine compromise, n'importe quelle partie du système d'information peut avoir été modifiée : noyau, binaires, fichiers de données, processus et mémoire.

D'une manière générale, la seule manière de s'assurer qu'une machine ne possède plus de porte dérobée ou autre modification laissée par l'intrus est de réinstaller entièrement le système d'exploitation à partir d'une distribution saine et de compléter cette installation en appliquant tous les correctifs de sécurité avant de reconnecter la machine à un réseau. Il est conseillé de tester la machine avec un scanner de vulnérabilités à jour (tel que Nessus) et de corriger les vulnérabilités identifiées, avant de la rebrancher au réseau.

Se contenter de supprimer la vulnérabilité qu'a utilisé l'intrus pour pénétrer le système d'information est très largement insuffisant.

6.2 SUPPRIMER TOUS LES SERVICES INUTILES

La configuration normale d'un système est de n'ouvrir que les services que celui-ci doit offrir et aucun autre.

Vérifiez :

- Qu'il n'y a pas de vulnérabilités dans ces services ;
- Que ces services ne sont offerts qu'aux systèmes extérieurs réellement autorisés par la politique de sécurité.

Une bonne manière de procéder est de désactiver tous les services au départ, et de les activer au fur et à mesure qu'ils sont nécessaires.

6.3 APPLIQUER TOUS LES CORRECTIFS DE SECURITE PRECONISES POUR LE SYSTEME D'EXPLOITATION ET LES LOGICIELS UTILISES

Assurez-vous que vous disposez de tous les correctifs de sécurité nécessaires.

6.4 RESTAURER LES DONNEES D'APRES UNE COPIE DE SAUVEGARDE NON COMPROMISE

Lorsque vous restaurez les données d'après une copie de sauvegarde, assurez-vous que ces données ne proviennent pas d'une machine compromise. Vous pourriez dans ce cas réintroduire une vulnérabilité qui permettrait à un intrus un accès non autorisé.

De plus, si vous restaurez des données sur des comptes utilisateur, gardez à l'esprit que n'importe lequel des fichiers peut contenir un cheval de Troie. En particulier, il peut être conseillé de vérifier, avec l'accord des utilisateurs concernés, les fichiers .rhosts, .ps1 dans leur répertoire personnel.

6.5 CHANGER TOUS LES MOTS DE PASSE DU SYSTEME D'INFORMATION

Une fois que toutes les vulnérabilités connues du système d'information ont été supprimées, il est très fortement recommandé de modifier les mots de passe de tous les comptes de ce système. En effet, lors de la compromission, il est possible que ces mots de

passe aient été récupérés par l'intrus, grâce à un renifleur de mots de passe.

7. COMMENT AMELIORER SA SECURITE APRES UNE INTRUSION

7.1 SE POSER LES BONNES QUESTIONS ET APPORTER LES REPONSES AVEC SOIN

Il est très important de se poser les questions qui permettront d'améliorer la réaction sur incident dans le futur. Même avec la meilleure politique de sécurité vous n'êtes jamais complètement à l'abri d'une nouvelle intrusion. Faites la liste dès maintenant des informations ou des procédures qui vous ont manqué :

- Pour protéger plus fortement le système d'information sur lequel il y a eu une intrusion ;
- Pour détecter plus rapidement qu'un incident de sécurité était en train de se produire ou s'était produit ;
- Pour cerner plus précisément quelles étaient les anomalies de fonctionnement du système ;
- Pour réagir plus calmement, de manière plus adéquate, sans risquer de commettre un geste qui ferait empirer la situation ;
- Pour déterminer plus vite quelle était la marche à suivre et quelles étaient les personnes à contacter ;
- Pour envisager plus sereinement l'analyse du système ;
- Pour trouver plus aisément la ou les vulnérabilités qui avaient été utilisées ;
- Pour reconstituer plus efficacement tout l'historique de l'intrusion sur l'ensemble des systèmes d'information ;
- Pour mieux repartir sur de bonnes bases avec des systèmes d'exploitation sains et sans faille de sécurité connue.

7.2 EN DEDUIRE LES CHOSES A AMELIORER

Les réponses aux questions posées dans le paragraphe précédent se déclinent en deux catégories :

1. Les réponses techniques, qui demandent la mise en place d'outils spécifiques :
    - Outils de protection ou de filtrage ;
    - Outils de détection d'intrusion ;
    - Outils de journalisation des connexions au système d'information.
2. Les réponses organisationnelles, qui demandent des procédures plus claires ou plus adéquates ; la politique de sécurité était-elle suffisante, et a-t-elle été respectée ?

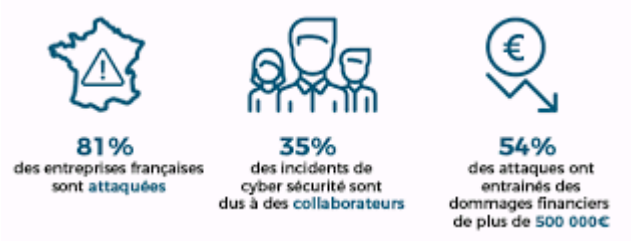
- La recherche systématique et régulière d'une intrusion potentielle est-elle prévue ?
- La marche à suivre détaillée en cas d'intrusion est-elle écrite et à disposition de tous les acteurs ?
- Les relations humaines entre les différentes personnes impliquées (sur le site, et en dehors du site) ont-elles été un facteur positif ou un facteur négatif dans la résolution de l'incident ?

7.3 GARDER UNE TRACE ECRITE COMPLETE DE TOUT CE QUI S'EST PASSE

Oublier l'intrusion le plus vite possible n'est pas la méthode la plus efficace pour en tirer les leçons et éviter une nouvelle intrusion dans le futur.

N'oubliez surtout pas de documenter chronologiquement l'ensemble des faits écoulés depuis la découverte de l'intrusion, et gardez une « version papier » de cette documentation.

SOURCES : HTTPS://WWW.CERT.SSI.GOUV.FR



Mieux vaut prévenir que guérir : Réaliser un Audit Cyber Sécurité