

Affaire suivie par :
CERTA

NOTE D'INFORMATION DU CERTA

Objet : Les bons réflexes en cas d'intrusion sur un système d'information.

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002>

Gestion du document

Référence	CERTA-2002-INF-002-003
Titre	Les bons réflexes en cas d'intrusion sur un système d'information.
Date de la première version	17 juin 2002
Date de la dernière version	07 janvier 2008
Source(s)	–
Pièce(s) jointe(s)	Aucune

TAB. 1 – gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

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.

Ce document, même s'il s'adresse en priorité aux membres de la communauté du CERTA (administrations, collectivités territoriales et organismes publics) pourra être utile à d'autres. Il y est notamment fait référence à l'aide que peut apporter le CERTA en cas d'intrusion sur une machine. Cette aide n'est apportée systématiquement qu'aux membres de la communauté du CERTA. Si vous n'êtes pas membre de la communauté du CERTA, essayez d'identifier, de préférence avant qu'un incident ne se produise, l'équipe de réponse et de traitement des incidents de sécurité informatique qui pourra vous aider au moment où l'attaque se produit. Pour plus d'information sur les CERTs et leurs rôles, consultez la page :

<http://www.certa.ssi.gouv.fr/certa/cert.html>

Le FIRST (Forum of Incident Response and Security Teams) est une organisation internationale qui regroupe plus d'une centaine de CERTs. La liste des CERTs membres du FIRST se trouve à l'adresse suivante :

<http://www.first.org/about/organization/teams/index.html>

Remarques Préliminaires Importantes

- 1° Toutes les actions entreprises devront être conformes à la politique de sécurité et aux procédures définies au sein de votre organisme. Si la politique de sécurité est plus précise que ce document, ou en contradiction avec celui-ci, c'est bien entendu la politique de sécurité de votre organisme qui doit s'appliquer.
- 2° Un certain nombre de manipulations très délicates ne sont pas décrites dans ce document. Elles concernent en particulier l'analyse de l'intrusion. Nous considérons en effet qu'il est préférable de confier cette analyse à des professionnels expérimentés.
- 3° Beaucoup d'effets néfastes d'une intrusion sur un système d'information découlent directement, ou sont très amplifiés, par une mauvaise réaction après la découverte de l'intrusion. Le CERTA ne pourra pas être tenu pour responsable d'éventuels dégâts causés par l'application des conseils contenus dans ce document. Cependant, s'ils sont appliqués correctement, ils éviteront beaucoup de problèmes.

2 Comment déterminer si l'on a été victime d'une intrusion ?

2.1 Utiliser des outils de détection d'intrusion

Note : Les outils de détection d'intrusion ne peuvent être efficaces que s'ils sont couplés à une surveillance humaine. Ces outils devraient en réalité être appelés outils « d'aide à la détection d'intrusion ».

Il existe deux grandes familles d'outils de détection d'intrusion :

- ceux qui analysent les journaux des événements se produisant sur les équipements (en anglais, cette méthode est appelée *host-based*) ;
- ceux qui capturent et analysent le trafic en certains points du réseau (en anglais, cette technique est appelée *network-based*).

Chacune des techniques de détection d'intrusion (sur l'équipement ou sur le réseau) possède ses avantages et ses inconvénients, et il est donc préférable d'utiliser si possible les deux types d'outils pour obtenir une meilleure efficacité.

En ce qui concerne les contraintes juridiques de l'utilisation de tels outils, on peut se référer au rapport thématique de la CNIL de 2004 intitulé : *La cybersurveillance des salariés*.

Ce rapport est disponible en ligne sur le site de la documentation Française :
<http://lesrapports.ladocumentationfrancaise.fr/BRP/044000175/0000.pdf>

Note : il est important que les horloges des outils de détection d'intrusion en particulier, et de tous les équipements en général, soient synchronisées, pour que les traces soient exploitables.

Le tableau 2 dresse une liste non exhaustive des avantages et inconvénients des deux types d'outil.

2.2 Prendre au sérieux les messages provenant des CERTs

Si l'un de vos systèmes d'information est compromis, il est probable que cette compromission sera aussi découverte par des personnes totalement extérieures à votre organisme. En effet, lorsqu'une machine est compromise, elle est souvent utilisée par le pirate pour effectuer une recherche de machines vulnérables sur le réseau (on parle de « scans »). Si l'une de vos machines est utilisée pour cela et qu'elle est repérée, une des victimes prendra contact avec un CERT, et vous pouvez être contacté et prévenu par ce CERT ou par un autre membre du réseau des CERTs. Prenez ce type de message très au sérieux.

En cas de doute, la liste des CERTs membres du FIRST (Forum of Incident Response and Security Teams) peut être trouvée à l'adresse suivante :
<http://www.first.org/team-info>

2.3 Mettre en évidence 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 (voir paragraphe 2.1), mais peuvent également être remarqués ponctuellement :

- impossibilité de se connecter à la machine ;

<p>Avantages d'un outil de détection d'intrusion « host-based »</p> <ul style="list-style-type: none"> - indépendant de la topologie du réseau ; - fonctionne dans un environnement où le trafic réseau est chiffré ; - donne l'information sur le succès ou l'échec d'une tentative de connexion ; - aucun équipement supplémentaire n'est nécessaire. 	<p>Avantages d'un outil de détection d'intrusion « network-based »</p> <ul style="list-style-type: none"> - indépendant des systèmes d'exploitation sur les équipements ; - surveille tout le trafic réseau sur des services connus (par exemple http, port 80) ; - l'information donnée est fiable, même après la compromission d'un ou plusieurs équipements sur le réseau.
<p>Inconvénients d'un outil de détection d'intrusion « host-based »</p> <ul style="list-style-type: none"> - plus difficile à gérer, car chaque équipement doit être configuré individuellement ; - si plusieurs équipements d'un réseau sont attaqués, pas de vision d'ensemble de l'attaque ; - non fiable lorsque l'équipement est compromis ; - utilise des ressources de l'équipement-hôte (performance et espace disque). 	<p>Inconvénients d'un outil de détection d'intrusion « network-based »</p> <ul style="list-style-type: none"> - vulnérable à certaines attaques ; - des paquets peuvent être perdus lorsque le réseau est saturé ; - certains protocoles réseau obsolètes ne seront pas pris en charge.
<p>Exemples d'outils de détection d'intrusion « host-based »</p> <ul style="list-style-type: none"> - chkrootkit (http://www.chkrootkit.org) - Tripwire (http://tripwire.org) - md5sum - AIDE 	<p>Exemples d'outils de détection d'intrusion « network-based »</p> <ul style="list-style-type: none"> - Snort (http://www.snort.org) - TCPdump

TAB. 2: Les outils de détection d'intrusion

- 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.

2.4 Suivre les conseils des CERTs

Certains types d'intrusion spécifiques peuvent laisser des traces précises qui seront décrites dans les bulletins du CERTA et des autres CERTs.

3 Quels sont les bons réflexes en cas d'intrusion sur une machine ?

3.1 Déconnecter la machine du réseau

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.

3.2 Prévenir le responsable sécurité

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 Prévenir le CERT dont vous dépendez

En France, le CERT dont dépendent les administrations est le CERTA. Il peut être contacté :

- par courrier électronique : certa-svp@certa.ssi.gouv.fr ;
- par téléphone : 01-71-75-84-50 ;
- par fax : 01-71-75-84-20.

Pour en savoir plus sur les CERTs (Computer Emergency Response Team), vous pouvez consulter la page de présentation :

<http://www.certa.ssi.gouv.fr/certa/cert.html>

3.4 Faire une copie physique du disque

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

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.

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.

Comment faire un copie physique du disque ?

Sur un système Unix, vous pouvez utiliser la commande `dd1` 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.

Si vous n'avez jamais utilisé ce type de commandes ou d'outils, ne le faites pas dans l'urgence car vous risqueriez de détruire toutes les traces. Faites appel à votre CERT pour plus de détails sur la façon de procéder.

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

3.5 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.

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.

De toute façon, le taux de réussite pour contacter l'administrateur de la machine source sera beaucoup plus élevé si c'est un CERT qui s'en charge. Il y a plusieurs raisons à cela :

- 1° les CERTs disposent de nombreux outils, de contacts et de correspondants, ce qui leur permet de contacter plus rapidement la personne adéquate ;
- 2° les messages à entête d'un CERT sont en général pris plus au sérieux que les messages de particuliers ;
- 3° les CERTs représentent une autorité neutre qui permet d'entamer si nécessaire un dialogue constructif, sans accusation abusive d'un côté ou de l'autre.

4 Quels sont les aspects légaux d'une intrusion ?

4.1 Dépôt 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 Dégâts à 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.

4.3 Services centraux spécialisés

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

OCLCTIC

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

¹man dd pour plus d'information

Tel : 01 47 44 97 55
<http://www.interieur.gouv.fr/>

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.prefecture-police-paris.interieur.gouv.fr/>

DCRI

Direction centrale du renseignement intérieur
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/>

Dans le cas des services déconcentrés et des collectivités locales, le CERTA pourra vous orienter utilement vers le service régional comportant des enquêteurs spécialisés.

5 Comment analyser l'intrusion a posteriori ?

Rappel

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 techniques d'analyse de l'incident ne seront pas détaillées dans ce document. Si vous souhaitez de l'aide, il est très fortement conseillé d'en demander au CERT dont vous dépendez. En vous adressant au CERTA, celui-ci pourra soit vous aider directement, soit vous indiquer le CERT qui pourra vous aider dans l'analyse.

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 recherche 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 après une intrusion

6.1 Ré-installer complètement le système d'exploitation à 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 ré-installer 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 Nessus²) 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 ;

²<http://www.nessus.org>

- 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 sécurité préconisés pour le système d’exploitation et les logiciels utilisés

Assurez-vous que vous disposez de tous les correctifs de sécurité nécessaires. Vous pouvez vérifiez ces informations sur le site du CERTA (<http://www.certa.ssi.gouv.fr>) et sur les sites des éditeurs des systèmes d’exploitation et des logiciels utilisés.

6.4 Restaurer les données d’après 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` dans leur répertoire personnel.

6.5 Changer tous les mots de passe du système 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, la récupération du fichier `/etc/passwd` ou tout autre moyen.

7 Comment améliorer sa sécurité après une intrusion

7.1 Se poser les bonnes questions et apporter les réponses 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 entrer plus facilement en relation avec le CERT qui s’est occupé de votre cas ;
- 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 déduire les choses à améliorer

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 écrite complète de tout ce qui s'est passé

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.

Gestion détaillée du document

17 juin 2002 version initiale.

24 novembre 2003 changement des numéros de téléphone du CERTA.

8 décembre 2003 modification de quelques liens hypertextes.

25 novembre 2005 corrections des liens vers First et CERT et prise en compte du dernier rapport de la CNIL.

07 janvier 2008 modification des coordonnées de la B.E.F.T.I.