En cas d'incident ? : plan administratif

- Informer le chargé de la SSI et le Directeur d'unité : s'il s'agit du CNRS : la coordination régionale du CNRS, et le cas échéant la chaîne fonctionnelle SSI d'autres tutelles éventuelles.
- Supprimer l'accès au système depuis l'extérieur ... faire une sauvegarde du système sur disque dans son état pour garder des traces (cf plus bas)
- Remplir la fiche "suivi d'incident"
  - *http://www.urec.cnrs.fr/IMG/txt/secu.CNRS.fiche_suivi_incident.txt*
- l'envoyer au CERT-Renater certsvp@renater.fr
- avec copie à l'équipe du CMSSI et aux coordinateurs sécurité de la Délégation Régionale (contacter le RSSI de la Délégation)
- Contacter en concertation avec le Directeur du laboratoire, le Fonctionnaire de Sécurité de Défense si un dépôt de plainte est envisagé. *http://www.urec.cnrs.fr/article117.html*

Pour porter planite?

1. Qui porte plainte au CNRS ?

1) Pour les ***vols ou dégradations de matériels informatiques professionnels*** :

- dépôt de plainte par le Délégué Régional : tous les cas de vols ou dégradations de matériels informatiques professionnels. (dépôt de plainte par l'agent lui-même s'il s'agit d'un matériel privé.)

Si ce matériel contient des données dont la compromission serait préjudiciable au CNRS, une plainte est également à déposer par le Délégué Régional

2) Pour ***les intrusions dans les systèmes d'information***

https://intranet.cnrs.fr/extranet/cnrs/fsd/documents/procedure_depot_p

- Si ERR Unité à régime restreint : Plainte par le FSD auprès de la CDRI
- Si ES : Plainte par le FSD auprès de l'OCLCTIC, DCRI en cas d'incident grave, ou par le délégué régional auprès du SRPJ compétent, sur délégation ponctuelle
- Si ERO : Plainte par le FSD auprès de l'OCLCTIC ou par le délégué régional auprès du SRPJ compétent, sur délégation ponctuelle du DG

En cas d'incident ? : plan technique

- Ne pas commencer par mener une enquéte approfondie sur les raisons et les conséquences de l'incident :
  - passer le minimum de commandes sur la machine
  - documenter les actions que vous réalisez (horodater dans une main courante les actions entreprises et les commandes tapées)
  - Ne pas réinstaller pas ou ne pas reformater la machine avant d'avoir pris une décision par rapport à un dépot de plainte.
- il est nécessaire de préserver les preuves qui seront indispensables en cas de dépot de plainte.
  - Il faut donc faire une sauvegarde du systéme compromis dans son état, selon la méthodologie recommandée par les CERT et l'UREC
  - *https://www.urec.cnrs.fr/IMG/pdf/secu_corres.InfoG.documentation-a2imp-linux.pdf*

En cas d'incident ? : plan technique

- Regarder les dégâts, c’est à dire examiner les traces et tous les répertoires pour déterminer le type d’intrusion et quels sont les fichiers compromis et/ou ceux qui ont été ajoutés
- Un outil de prise d'empreinte système come ”tripwire” ou ”aide” facliteront la détection des fichiers modifiés, rajoutés ou détruits (cf. conseil- recherche-piratage pour unix & pour windows).
- Examiner les autres machines pouvant être compromises et en particulier changer tous les mots de passe si vous avez détecté l’installation d’un renifleur.
- Réinstaller la machine compromise en ayant soin d’avoir corrigé la/les failles de sécurité.
- Faire une sauvegarde et une empreinte du système.
- Réinstaller les comptes utilisateurs.
- Reconnecter la machine au réseau.

Principes de base

- Ne pas faire de modifications sur le système en cours d'acquisition d'informations
- Ne pas faire confiance aux outils installés sur le système en cours d'acquisition d'informations
- Garder une trace horodatée des actions réalisées
- Récupérer les informations et les enregistrer :
- Vérification de la date et de l'heure sur le système compromis
- Création de la main courante
- Montage de la boîte à outils (CDROM) contenant des commandes linkées avec des librairies statiques (pour ne pas utilsier les commandes du système compromis)
- La formation A2IMP fournir un script qui permet d'enregister automatiquement toutes les informations interessantes du système compromis

Principes de base

•***Sauvegarde de l'espace de stockage des partitions système***

•Les partitions que l'on va sauvegarder sont principalement les partitions systèmes, celles où un intrus aurait pu déposer ses outils ou fichiers utilisés pour la compromission.
•La sauvegarde des disques ou partitions systèmes est à répéter pour chaque partition et/ou disque à sauvegarder (liste des partitions données par la commande fdisk /dev/sda1, /dev/sda3, /dev/sdb1 et /dev/sdb2...)

Avoir un disque de sauvegarde... de capacité suffisante... le monter sur le système compromis [les cables USB<-->IDE ou USB<-->SCSI sont très utiles

•utiliser les commandes linkées en statique
•utiliser des commande de copies de blocs physiques!! ”dd” et non pas logiques

copie de partition dans une partition
`/mnt/cdrom/dd if=/dev/sda1 of=/dev/sdb1`