Le rôle et l'expérience du Cert-Renater

■ David CROCHEMORE, crochemo@renater.fr
CERT Renater

Des structures appelées CERT (Computer Emergency Response Team) ont été mises en place dès le début des années 90 suite à des incidents de sécurité de grande ampleur survenus à cette époque sur les réseaux de la recherche américains. Dans les années qui ont suivi, des CERTs ont été mis en place dans la plupart des autres pays dans lesquels l'Internet s'est développé.
Les CERTs veillent à limiter l'envergure et le nombre des attaques malveillantes :
- *en organisant les moyens de défense et de réaction,*
- *en assurant une certaine prévention par la diffusion d'information.*

■ Les fonctions d'un CERT

La mission d'un CERT est d'assister ses adhérents en matière de sécurité informatique, et notamment dans le domaine de la prévention, détection et résolution d'incidents.

Sa fonction première est d'être le point de contact, c'est-à-dire la structure que l'on appelle à l'aide et qui organise les secours en cas d'accident. Afin d'organiser les secours efficacement, un CERT doit pouvoir se mettre en rapport avec :

- les responsables (ou correspondants) sécurité des instances gouvernementales,
- les organismes sur le réseau (en descendant éventuellement jusqu'au niveau des sites raccordés),
- les autorités de police,
- les autres CERTs.

Un CERT doit s'entourer de techniciens permanents et d'experts externes pour pouvoir faire une première analyse technique du problème et ceci, le cas échéant, avec l'aide des constructeurs pour trouver la parade. Là encore, un bon carnet d'adresses s'impose.

Quand une parade est trouvée à un « trou de sécurité », découvert à l'occasion d'un incident récent, le CERT diffuse très largement un avis public qui décrit sommairement le problème (cette description ne doit pas permettre de reproduire l'incident !) et détaille la correction ou les méthodes de protection.

L'Internet ne connaît pas les frontières. Que pourra faire un site français victime d'une attaque et qui soupçonne un site hollandais ? Il pourrait essayer de contacter directement un responsable du site hollandais. Mais comment connaître le responsable sécurité de ce site ? Faut-il lui faire confiance ? D'abord, quel est ce site ? De plus il est fortement possible que ce site hollandais ne serve que de tremplin, à un attaquant venu d'ailleurs !

La démarche qu'impose la prudence et l'efficacité : avertir le responsable sécurité de son organisme (ou de son établissement), qui lui-même contacte le CERT de sa communauté ; par exemple le CERT-Renater, ce dernier contacte le CERT hollandais...

Ce circuit, qui peut paraître long, possède des avantages :

- s'organiser autour d'une chaîne humaine de responsables se reconnaissant mutuellement un certain degré de confiance,
- globaliser l'information au niveau le plus haut de façon à favoriser tout recoupement avec d'autres incidents récents ou en cours. Ceci permet notamment de faciliter la résolution de cas d'attaques internationales,
- garantir un meilleur suivi des incidents, et de l'information auprès des sites membres.

Les CERTs, grâce à leur expérience, établissent des recommandations générales (pour les administrateurs de machines, de réseaux...) et font de la sensibilisation auprès des responsables et des utilisateurs. Certains d'entre eux organisent même des cycles de formations.

Un rôle, également important, est la pression mise sur les constructeurs pour qu'ils corrigent rapidement des erreurs grossières « de sécurité » dans la conception de certains logiciels ou matériels.

Les CERTs ne se substituent jamais aux autorités des organismes, encore moins aux autorités de police et/ou de justice. Ce sont les sites attaqués qui doivent (s'ils le jugent opportun) faire appel aux autorités de police. Néanmoins, les CERTs maintiennent des liens de coopération avec ces autorités.

Un CERT sert une communauté définie, mais ne refuse généralement pas d'aider les personnes extérieures à celle-ci.

■ La structure du CERT Renater

Au niveau opérationnel, le CERT-Renater est un des service du département technique du GIP Renater. Ce service est assuré durant les jours et heures ouvrables.

Pour fonctionner efficacement, le CERT s'appuie sur :

- un réseau de correspondants sécurité au niveau des organismes membres du GIP Renater, (CEA, CNES, CNRS, INRIA, Universités) et des autres organismes ou entités qui ont passé un contrat avec le GIP pour utiliser ses services ;
- chaque organisme, membre du GIP ou contractant, désigne un ou deux correspondants sécurité, seuls interlocuteurs du CERT. Ils sont les destinataires des informations du CERT et doivent les diffuser conformément aux restrictions demandées ;
- en retour, ils informent le CERT de tout incident sécurité survenant sur un site appartenant à leur communauté et pouvant nuire au reste de la communauté Internet.

■ Le champ d'action du CERT Renater

La préoccupation du CERT-RENATER est celle de tout CERT. Dans un premier temps le CERT-RENATER privilégie les actions liées à la circulation et la diffusion des informations, et à la mise en place du réseau de correspondants sécurité.

La diffusion d'informations

Actuellement, le CERT diffuse les informations de type bulletin, notes, recommandations, alertes..., en provenance :

- des CERTs étrangers,
- des correspondants sécurité au niveau des organismes,
- des experts techniques.

Ces informations sont diffusées vers les correspondants sécurité au niveau des organismes. Ceux-ci assurent la responsabilité de la diffusion interne, conformément aux restrictions de diffusion que le CERT leur a communiquées.

La coordination en cas d'alerte

En cas d'alerte (attaque de sites, virus...), le responsable sécurité du site informe le responsable sécurité de son organisme de tutelle, et contacte le CERT-Renater (Mél : Certsvp@renater.fr, Tél. : 01.53.94.20.44, Fax : 01.53.94.20.31).

Le CERT pourra alors conseiller sur l'attitude à adopter (protections immédiates, demande d'enquête par les autorités nationales de sécurité, dépôt de plainte, et diffuser l'alerte vers d'autres organismes ou vers les CERTs étrangers, en cas d'attaque extérieure.

Un des principes du CERT-Renater est de ne pas se substituer aux organismes impliqués dans des incidents de sécurité. Il ne diffuse d'informations sur l'incident qu'avec l'accord du site attaqué et du correspondant sécurité de l'organisme.

Relations avec les entités de sécurité compétentes

Au-delà des relations avec les entités évoquées plus avant comme sources d'informations directes, c'est-à-dire :

- CERTs étrangers,
- correspondants sécurité au niveau des organismes,
- experts techniques.

Le CERT est en relation avec les autorités nationales de sécurité et peut conseiller les sites victimes de tentatives malveillantes sur les démarches à engager vis-à-vis des autorités compétentes.

Cependant, le CERT n'a pas vocation à se substituer aux sites pour leurs relations avec les autorités telles que la police ou la justice. La saisie des autorités judiciaires est de la responsabilité du site concerné ou de son autorité de tutelle. Le fait d'informer le CERT-RENATER ne décharge en aucune façon la direction du site de ses responsabilités civiles et pénales.

■ Comment réagir en cas d'incident de sécurité

Au niveau de l'utilisateur ou du responsable d'un équipement informatique :

- informer votre direction (seule habilitée à porter plainte),
- informer le responsable sécurité de votre organisme, afin que celui-ci mette tout en œuvre (via son réseau interne de contacts) pour traiter l'incident,
- arrêter les services compromis ou mieux, isoler la (ou les) machine(s) du réseau,
- sauvegarder le système pour garder les traces qui serviront comme éléments de preuve en cas de plainte. Essayer de ne pas détruire d'informations utiles pour l'analyse ultérieure de l'incident,
- ne pas donner d'information sur l'incident à des tiers qui ne seraient pas directement concernés,
- informer le CERT-Renater (certsvp@renater.fr) et le correspondant sécurité de votre tutelle,
- analyser les informations disponibles pour évaluer l'étendue des dégâts et comprendre la stratégie utilisée pour l'intrusion. Cette stratégie s'est appuyée sur une vulnérabilité. La connaître peut être utile pour vos collègues,
- réinstaller le(s) système(s),
- faire changer les mots de passe et vérifier qu'ils ont bien été changés sinon fermer le compte. Vérifier leur solidité. Pour cela utiliser des outils comme CRACK,
- pour les .rhost (pour tous les utilisateurs) :
  - s'ils n'ont pas de besoin de se connecter de l'extérieur les inviter à supprimer leur .rhost,
  - s'ils en ont besoin, qu'ils « élaguent » surtout le superflu. qu'ils le « brident » et en vérifient la validité,
  - leur dire de supprimer le « + + » à la fin.
- ne pas laisser le répertoire utilisateur comme premier chemin par défaut (mettre le chemin ./ en dernière position dans la variable PATH des utilisateurs),
- et les sniffeurs étant la bête noire, il faut rechercher leur présence sur toutes les machines du parc.