12

Les bonnes pratiques en cas d'incident sur un système d'information

CENTRE DE RECHERCHE
SUR L'INFORMATION
SCIENTIFIQUE ET TECHNIQUE
cerist

LES BONNES PRATIQUES EN CAS D'INCIDENT SUR UN SYSTÈME D'INFORMATION

Aujourd'hui, aucune personne ou organisation n'est à l'abri des incidents de sécurité. Bien que des mesures pour assurer la sécurité du système d'information sont mises en place, il peut arriver que cette sécurité soit compromise par des attaques informatiques. Un plan de réponse aux incidents de sécurité doit faire partie intégrante de la stratégie de sécurité globale de l'entreprise pour se préparer /réagir aux incidents.

▪ Préparation

L'étape de préparation est sans aucun doute la plus importante puisque c'est durant celle-ci que s'élabore l'équipe qui intervient lors des incidents ainsi que les procédures qui vont permettre de traiter rapidement et efficacement les incidents qui peuvent affecter le système d'information. Il est également important de disposer des sauvegardes à jours des données critiques.

▪ Identification

Tout d'abord, il faut procéder à l'examen du système pour mettre en évidence les comportements suspects et les signaler aux personnes appropriées (le responsable de la sécurité et de la hiérarchie). Certains signes indiquent que le système a peut-être été

Figure 1 : Processus de gestion d'incidents de sécurité

Ce document propose les étapes à suivre pour mieux gérer les incidents de sécurité. Un petit conseil avant de commencer : « PAS DE PANIQUE! » Concentrez-vous pour éviter de faire des erreurs d'inattention.

compromis. Ils peuvent être recherchés systématiquement par des outils de détection d'intrusion, mais peuvent également être remarqués ponctuellement par : l'analyse des fichiers de journalisation, les programmes en cours d'exécution et les tâches planifiées, les programmes configurés pour être exécutés automatiquement au démarrage du système, les détails de la configuration réseau, les paramètres DNS et ARP, les connexions et les sessions et ports ouverts, les comptes des utilisateurs et leurs privilèges et les fichiers inhabituels laissés par l'intrus.

▪ Confinement des dommages

Après avoir identifié l'incident sur le système, la première action à faire est de limiter l'extension de l'incident. Il s'agit d'isoler les

machines infectées et protéger les machines saines. Une combinaison appropriée des actions suivantes peut être adoptée selon la nature de l'incident :

- Déconnecter la machine compromise du réseau. En revanche, il faut maintenir la machine sous tension et ne pas la redémarrer pour ne pas perdre des informations nécessaires à l'analyse de l'incident.
- Modifier les règles de filtrage d'un pare-feu ou d'un routeur.
- Désactiver le service concerné par l'attaque.
- Désactiver les comptes utilisateurs suspects.
- Changer les mots de passes.

La deuxième action à faire consiste à préparer une copie de sauvegarde du système pour une investigation numérique. Cette analyse permettra de comprendre la nature de l'incident et les vulnérabilités exploitées. Enfin, décider si le système sera nettoyé ou réinstallé à partir d'une version saine.

▪ Éradication

D'une manière générale, il est recommandé de réinstaller entièrement le système afin de s'assurer qu'une machine ne possède plus de porte dérobée ou autre modification laissée par l'intrus. Restaurer les données et les applications affectées à partir des sauvegardes (étape 1). Ensuite, valider la sécurité du système avec un scanner de vulnérabilités et corriger les vulnérabilités identifiées avant de remettre le système en production.

▪ Retour à la normale

Mettre le système nouvellement reconstruit en production et maintenir une surveillance sur ce système afin de détecter d'éventuels futurs incidents.

▪ Tirer des leçons

Rédiger un rapport décrivant l'incident et ce qui a été fait pour le traitement de cet incident. Enfin, identifier les améliorations à apporter au système d'information.