Gestion des incidents de sécurité de l'information

1. Définition

Un incident de sécurité est un événement causant des dommages, ou susceptible de le faire, à des personnes ou à des organisations. Il s'agit d'un événement ne faisant pas partie du fonctionnement standard d'un service et qui cause, ou peut causer, une interruption ou une diminution de la qualité de ce service.

2. Classification des incidents de sécurité

A. Contenu abusif

A.1. Spam (pourriel ou polluriel) — Communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires.

A.2. Harcèlement — Discrédits, ou discrimination contre une personne d'un point de vue cyber.

A.3. Enfant/Sexe/Violence — Pornographie infantile, glorification de la violence

B. Code malicieux

Virus, Ver, Cheval de Troie, Spyware, Dialler — Logiciel intentionnellement introduit dans un système pour un but nocif. L'interaction d'un utilisateur est normalement nécessaire pour activer ce code.

C. Collecte d'informations

C.1. Scanning — Attaques qui consistent à envoyer des requêtes à un système pour découvrir ses failles. Ceci inclut également tout type de processus de test pour collecter des informations sur les hôtes, les services et les comptes. Exemple : fingerd, requête DNS, ICMP, SMTP (EXPN, RCPT,...)

C.2. Sniffing — Observer et enregistrer le trafic réseau (Ecoute)

C.3. Ingénierie sociale — Collecte d'informations sur un être humain sans utiliser de moyens techniques (ex : mensonges, menaces...)

D. Tentatives d'intrusion

D.1. Exploiter des vulnérabilités connues — Une tentative pour compromettre un système ou interrompre tout service en exploitant les vulnérabilités avec des identifiants standardisés comme un nom CVE (ex : Buffer overflow, Portes dérobées, cross side scripting ,etc).

D.2. Tentatives de connexion — Tentatives de connexion multiples (vol ou crack de mots de passe, force brute).

D.3. Signature d'une nouvelle attaque — Une tentative pour exploiter une vulnérabilité inconnue.

E. Intrusions

Compromission d'un compte à privilèges, Compromission d'un comte sans privilèges, Compromission d'une application — Une compromission réussie d'un système ou d'une application (service). Ceci peut être causé à distance par une nouvelle vulnérabilité ou une vulnérabilité inconnue, mais aussi par un accès local non autorisé.

3. Processus de gestion et de traitement des incidents

Etape 1 Détection de l'incident

Etape 2 Analyse des données

Etape 3 Recherche de solutions

Gestion des incidents de sécurité de l'information

Etape 4 Rapport au client

Etape 5 Réponse à l'incident (traitement des vulnérabilités)

Etape 6 Récupération

Etape 7 Clôture de l'incident

Etape 8 Information finale au client

4. Révisions

1.0 Date of change: 01/09/2021 - Responsible: Technical team - Summary of Change: Initial release