Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 04 avril 2016
N° CERTFR-2016-ACT-014

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-014

1 - L'organisation de la réponse à incident

Les choses ont bien évolué depuis 1998 et la publication de la RFC 2350 *Expectation for Computer Security Incident Response* (cf. Documentation) décrivant pour la première fois de manière formelle l'organisation, la structure, les services et les modes opératoires d'une structure de réponse aux incidents, CERT ou CSIRT dans notre langage. Cet article propose un premier état des lieux en matière de normes et de modèles applicables à la gestion d'incidents de sécurité.

Une norme

La norme ISO 27035:2011 *Information Security Incident Management* décrit un modèle d'organisation de l'activité de réponse aux incidents s'appuyant sur le cycle de vie d'un incident. Celui-ci se décompose en cinq phases :

1. phase de planification et de préparation ('Plan and prepare') ;
2. phase de détection et de rapport ('Detection and reporting') ;
3. phase d'analyse et de décision ('Assessment and decision') ;
4. phase de réponses ('Responses') ;
5. phase de retour d'expérience ('Lessons learnt').

Une nouvelle version de cette norme est en cours d'élaboration. Son objectif est de détailler chacune des activités devant être menées au sein des cinq phases identifiées. Cette version se déclinera en trois volets dont les deux premiers devraient être publiés en août 2016 :

1. la norme 27035-1 *Principle of incident management* reprendra dans la norme actuelle dans ses grandes lignes ;
2. la norme 27035-2 *Guidelines to plan and prepare for incident response* précisera les activités qu'une organisation doit engager pour être à même de traiter un incident conformément aux meilleures pratiques. Ce volet couvre de fait les phases 1 et 5 du modèle ;
3. la norme 27035-3 *Guidelines for incident response operation* devrait détailler les phases 2, 3 et 4 du modèle. Aucune date de publication n'est actuellement avancée.

Des modèles

D'autres approches de la gestion d'incident sont proposées par ailleurs, en particulier celles de deux grands acteurs du domaine, le NIST (l'Institut américain en charge des normes et de la technologie) et l'ENISA (l'Agence européenne chargée de la sécurité des réseaux et de l'information).

NIST SP800-61r2

Le NIST détaille un modèle d'organisation et de traitement (cf. Documentation) lui aussi basé sur le cycle de vie d'un incident dans le guide intitulé 'Computer Security Incident Handling Guide' initialement publié en 2004 et dont la dernière révision date de 2012. Ce modèle, qui prend ses racines dans les travaux menés par l'US Navy puis par le SANS Institute, est semblable au modèle de l'ISO 27035:2011 au nombre de phases près, soit quatre phases sont identifiées au lieu de cinq, les deux phases post-incident de l'ISO étant regroupées en une seule :

1. la phase 'Préparer' (Preparation) organisée autour de deux volets : préparer et éviter les incidents ;
2. la phase 'Détecter et Analyser' (Detection and Analysis) contenant sept volets : les vecteurs d'attaque, les signes d'un incident, les sources d'information, l'analyse de l'incident, la documentation de l'incident, la gestion des priorités et la notification de l'incident ;
3. la phase 'Contenir, Eradiquer et Restaurer' (Containment, Eradication and Recovery) présentée en quatre volets : choisir une stratégie d'isolation, relever et gérer les éléments de preuve, identifier les systèmes attaquant, éradiquer et restaurer ;
4. la phase 'Gérer l'après-incident' (Post-Incident Activity) scindée en trois volets : les leçons acquises, l'utilisation des données collectées et la conservation des éléments de preuve.

Il discerne l'existence d'un cycle entre les deux phases actives du traitement, les phases 2 et 3, lesquelles peuvent être déroulées alternativement pour affiner le traitement et ceci au fur et à mesure de la progression dans l'analyse et de la connaissance que l'on acquiert de l'incident, de ses atteintes et de ses conséquences.

ENISA

Publié fin 2010 et en anglais uniquement, le guide 'Good Practice Guide for Incident Management' (cf. Documentation) traite de l'ensemble de la problématique de la mise en oeuvre d'une structure de gestion des incidents. Il propose à ce titre une organisation de la gestion des incidents autour des différents services susceptibles d'être offerts et dont le traitement d'un incident n'est qu'une composante. L'ENISA s'inspire ici du modèle fondateur initié en 2004 par le CERT Carnegie Mellon dans son document 'Defining Incident Management Processes for CSIRTs: A Work in Progress' (cf. Documentation) :

- la détection
- le triage
- l'analyse
- la réponse

Ce document ne détaille toutefois ni le contenu des quatre étapes ni les actions à engager. Au lecteur d'adapter à son besoin et à son contexte les exemples proposés qui s'inspirent de cycles de traitement mis en oeuvre par différentes structures européennes.

Conclusion

On retiendra de ce très bref tour d'horizon l'existence de modèles, guides, méthodes et bonnes pratiques de gestion et de traitement des incidents de sécurité éprouvés et sur lesquels il est possible de s'appuyer efficacement. Il y aura bien entendu toujours nécessité d'adapter le modèle à la structure de l'organisation et à son périmètre de responsabilité, les méthodes et pratiques aux équipes et aux contextes techniques.

Documentation

- RFC 2350 *Expectation for Computer Security Incident Response* :
  https://www.ietf.org/rfc/rfc2350.txt
- 'Computer Security Incident Handling Guide' :
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- 'Good Practice Guide for Incident Management' :
  https://www.enisa.europa.eu/activities/cert/support/incident-management/files/good-practice-guide-for-incident-management/
- 'Defining Incident Management Processes for CSIRTs: A Work In Progress' :
  https://www.sei.cmu.edu/reports/04tr015.pdf

2 - Rappel des avis émis

Dans la période du 28 mars au 03 avril 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-110 : Multiples vulnérabilités dans le noyau linux de Suse
- CERTFR-2016-AVI-111 : Multiples vulnérabilités dans les produits Cisco

Gestion détaillée du document

04 avril 2016 version initiale.