Réponse à incident

Etapes:

1. Informer l'ANSSI de l'incident de sécurité
    a. Affectant la sécurité ou le fonctionnement
    b. Affectant un SIIV
    c. Pour les OIV du secteur financier – notifier les incidents informatiques selon un processus harmonisé et centralisé.
2. Respecter les obligations relatives à la gestion d'une crise cyber
3. Qualifier la détection ou le signalement
    a. Observer pour caractériser les constats
        i. Effectuer une première évaluation du périmètre
            1. Détections
            2. Dysfonctionnements informatiques
            3. Perturbation des métiers
        ii. Déterminer la source précise de l'accident
        iii. Déterminer le périmètre concerné
4. S'orienter pour identifier les impacts potentiels et les actions à prendre
    a. L'incident est-il confirmé ou nécessite-t-il plus de recherches ?
    b. Estimer les impacts potentiels de la situation
    c. Qui sont les acteurs déjà impliqués dans l'incident ?
    d. Quels sont les actifs à mettre en sûreté en cas d'aggravation de l'incident ?
    e. Où sont les traces connues et potentielles laissées par un attaquant ?
    f. Identifier les obligations contractuelles ou réglementaires qui s'appliquent sur une OIV
    g. Notifier à la CNIL tout incident entraînant une violation de données personnelles
5. Réagir
    a. Décider
        i. Synthétiser le sûr et l'incertain sous une forme concise pour les décideurs
        ii. Notifier les décideurs métiers et direction de votre organisation
        iii. Prendre conseil auprès de spécialistes
    b. Agir
        i. Prendre les premières mesures d'endiguement adaptées à la situation
        ii. Préserver les traces
        iii. Mobiliser les équipes internes et l'infogérant le cas échéant

        iv. Contacter les propriétaires d'applications concernées
6. Obtenir de l'aide
    a. ANSII/CERT-FR
    b. Prestataires de réponse à incident (PRIS)
        i. Orange Cyberdefense
        ii. Thales Cyber Solutions
        iii. Wavestone
    c. Assureurs
7. Déclarations
    a. Dépôt de plainte
    b. Cnil
    c. Autres autorités..

Obligation:

1. Informer l'ANSSI de tout incident de sécurité « affectant la sécurité ou le fonctionnement » du SIIV[1].
2. Communiquer à l'ANSSI un point de contact fonctionnel pouvant prendre connaissance à toute heure des signalements de l'ANSSI.
3. Pour les OIV du secteur financier – notifier les incidents informatiques selon un processus harmonisé et centralisé.
4. Notifier à la CNIL tout incident entraînant une violation de données personnelles
5. Traiter les incidents de sécurité affectant le SIIV concerné
6. Respecter les obligations relatives à la gestion d'une crise cyber

Réponse à incident

Sources:

1. Obligation
2. Réflexe
3. Dispositif SAIV
4. CERT-RF
5. Qualification PDIS
6. Prestataire PRIS