Gestion des Incidents de Sécurité de l'Information Le rôle du DPO

Security Forum – 23 octobre 2018

Jean Luc Allard, CSI & DPO @ CHC

Agenda

- I. Posons le problème
- II. La gestion des incidents...
- III. Le rôle du DPO
- Conclusion

I. Posons le problème

- Erreurs habituelles
- C’est quoi une information?
- Définitions
- Exemples

Erreurs habituelles

- Système d'information = système informatique
  - Information = données informatiques
  - … c'est trop court !
- Sécurité = Confidentialité
  - « secret médical »
  - On oublie l'intégrité et la disponibilité

L'information…

- C'est Virtuel, Immatériel et Intangible.
- Ce n'est donc pas géré (de l'acquisition à la mise au rebut) comme les biens matériels
- ***L'information… c'est une donnée qui, dans un contexte spécifique possède une signification et, donc, une valeur.***

Définitions - ITIL

- An **event** may indicate that something is not functioning correctly, leading to an incident being logged.
- **Incident** (V2) An event which is not part of the standard operation of a service and which causes or may cause disruption to or a reduction in the quality of services and customer productivity.
- **Incident** (V3) An unplanned interruption to an IT serviceor a reduction in the quality of an IT service.Failure of a configuration item that has not yet impacted servic

Definitions ISO/IEC 27035

- **Event**: occurrence indicating a possible breach of information security or failure of controls
- **Incident**: one or multiple related and identified information security events that can harm an organization's assets or compromise its operations

RGPD: Violation de données

- « Une violation de la sécurité entrainant, de manière accidentelle ou illicite, la perte, l'altération, la divulgation non autorisés de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données. » *(RGPD Art 4. 12)*

Références

- ISO/IEC 27035 Information technology – Security Techniques – Information security incident management
  - Part 1: Principles of incident management
  - Part 2: Guidelines to plan and prepare for incident response
  - Part 3: Guideline for CSIRT operations

- « CYBERSÉCURITÉ - GUIDE DE GESTION DES INCIDENTS »
  Centre for Cyber security Belgium/ Cyber security Coalition

Exemples…

- Vol d'une mallette dans la voiture… (oubli dans le train)
- Piratage informatique
- Erreur d'encodage ou de lecture
- Crash informatique avec pertes de données
- Erreur d'aiguillage d'un email
- Bavardage autour d'un verre
- …

II. La gestion des Incidents

- Principes & Objectifs
- Processus (5 phases)
- Problèmes !

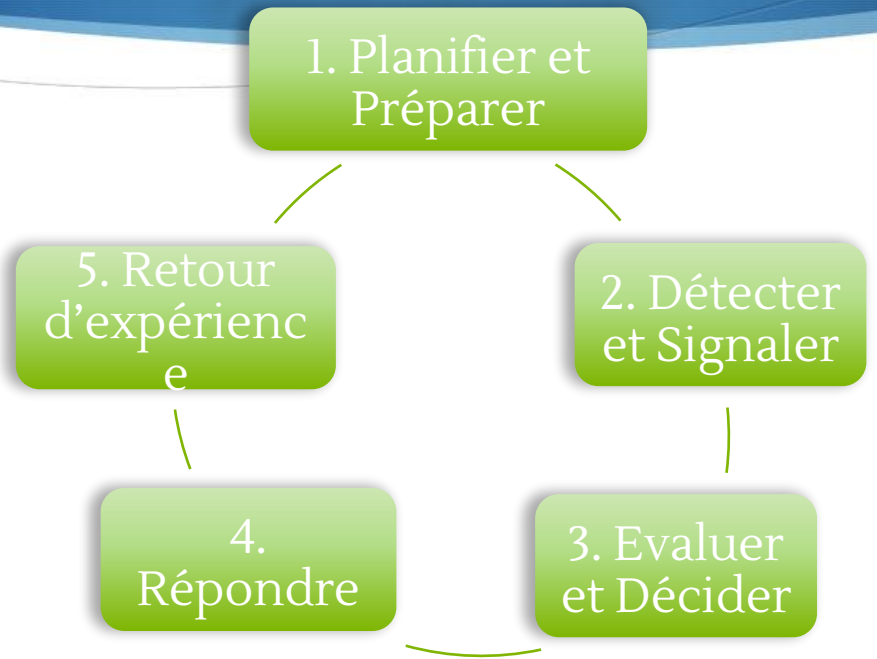
Principes et Objectifs

- Il y aura toujours des incidents… pour des raisons diverses
- Objectif : “Toujours prêt !”
  - Sinon… stress, erreurs, inefficacité et catastrophes
- **Détecter, contenir, neutraliser … et réparer**
- Bénéfices d’une approche structurée
  - Contrôle de l’Impact
  - Priorisation
  - Efficacité et efficience
  - Amélioration
- Besoin d’une ‘capacité’ adaptée au contexte.

Processus: transversalité

- Documentation nécessaire et suffisante
- Coordination et communication
- Notification à la direction et aux parties prenantes

Les Phases


1. Planifier et Préparer
2. Détecter et Signaler
3. Evaluer et Décider
4. Répondre
5. Retour d'expérience

1. Planifier et Préparer

- Une politique
- Organisation: de la réponse ***et du suivi***
- Plans de réponse détaillés
- Mécanismes de détection et de signalement
- Informer les parties prenantes *sur ce qui existe*

2. Détecter et signaler

- De bons indicateurs et les détecteurs adaptés
- Un ‘format’ de signalement
- Un canal de transmission d’alerte
- Collecte et sauvegarde des traces (*forensics*)
  - *ISO/IEC 37037 – Guidelines for identification, collection, acquisition and preservation of digital evidence*

3. Evaluer et Décider

- Evaluation
  - Importance et Urgence
  - Envergure et portée de l'événement
- Décision
  - Ressources
  - Délais
- Gestionnaire d'incident '*de bout en bout*'

4. Répondre

- Contenir & Neutraliser
- Escalade
  - Horizontale (plus de moyens)
  - Verticale (dépasse l'autorité du gestionnaire)
  - *Connexion avec la gestion de crise*
- Communiquer
  - Équipe(s) de réponse
  - 'victimes'
  - Parties prenantes et décideurs
- Rapport 'continu' & calcul du coût (réponse + '*victimes*')

5. Retour d'expérience

- Qu'est-ce qui a bien marché?
- Qu'est-ce qui a 'foiré'?
- Que doit-on améliorer?
  - La détection - signalement
  - La réponse
  - Le suivi
  - La communication
  - Les « Contrôles »
  - La Politique de sécurité de l'information … et les directives qui en dépendent

Change management

Problèmes

- Il faut
  - Le soutien de la direction
  - Une directive claire
  - Une capacité
    - Une organisation
    - Des Procédures de réponse pour chaque type d'incident + *workarounds*
  - Un 'formulaire' de signalement

Ca existe quelque part ?

III. Le rôle du DPO

- Incidents sur les DCP
- Intervention
- Notification

Evènements et Incidents sur DCP

- Quelle(s) information(s)
  - Type
  - Quantité
- Quelles personnes concernées
- Quel(s) traitement(s)
- Quel impact sur la vie privée

Intervention du DPO

- Collecter les informations
  - Via la capacité de gestion des incidents
- Enquêter
  - Juge d'instruction
  - Compléter le 'dossier'

Notifier

- Formulaire « Notification » https://www.autoriteprotectiondonnees.be/formulaire-notification-de-fuites-de-donnees)
  - Initiale
  - Avancée
  - Finale
- Délai de 72 heures (chrono) si l'incident peut avoir « un impact grave » sur la vie privée des personnes concernées.
- Sinon: Registre des incidents
  - Rapports factuels
  - Rapports 'coût'
  - Rapports 'amélioration'

4. Conclusion

-
-
-
- *… il faut souvent ‘créer’ la capacité et la directive……*


C'EST FINI, ÇA Y EST !
MERCI POUR VOTRE ATTENTION
makeameme.org

- Jean Luc ALLARD
  - CISM,CISA, ExM IT Governance (Solvay)
  - DPO certified (PECB)
  - CISO & DPO @ CHC (Liège) – jean-luc.allard@chc.be
- MISIS: jeanluc.allard@misis.be - www.misis.be
- Info-Attitude (blog): www.info-attitude.com