La norme ISO 27035

Alexandre Fernandez Toro
Alexandre@Fernandez-Toro.com

ISO 27035

- Généralités
  - Pas de grande surprise
    - La norme ne réinvente pas la roue
  - Norme volumineuse
    - 80 pages
  - Clauses et annexes
  - Très orientée PDCA

ISO 27035

- Intérêt du processus de gestion d'incidents
  - Améliorer la sécurité de l'information
  - Réduire les impacts sur le business
  - Renforcer la prévention d'incident
  - Assurer le recevabilité des preuves
  - Mettre à jour l'appréciation des risques
  - Prévention et sensibilisation

ISO 27035

- Politique de gestion d'incident
  - Document à part entière (free-standing document)
  - Contenu type
    - Importance de la gestion des incidents
    - Présentation brève du processus
    - Répartition des responsabilités en la matière
    - Enregistrement des actions lors de la gestion des incidents
    - Aspects sensibilisation et formation
    - Aspects réglementaires
  - Intégration de cette politique dans les autres documents

ISO 27035

- Schéma de gestion d'incident
  - Objectif
    - Détailler tous les aspects opérationnels de la gestion d'incident
  - Contenu type
    - Plan
    - Evaluation et décision
    - Réponses
    - Retour d'expérience
- Procédures correspondantes

ISO 27035

- Détection de l'incident
  - Détection humaine ou automatique
  - La personne détectant l'incident renseigne
    - Heure/date
    - Observations
    - Contacts éventuels
  - Moyens de communication
    - Mail/téléphone/direct/formulaire/etc..

ISO 27035

- PoC
  - Point of Contact
  - C'est l'intermédiaire entre la personne qui rapporte l'incident et l'ISIRT
  - Missions
    - Vérifie s'il agit d'un incident réel ou d'un faux positif
    - Contrôle que la fiche d'incident est bien renseignée
    - Fait une première évaluation des impacts
      - La norme propose une typologie des impacts
    - Escalade à l'ISIRT, si nécessaire

ISO 27035

- ISIRT
  - Information Security Incident Response Team
  - Selon les cas
    - Equipe dédiée ou Virtual ISIRT
  - Missions
    - Passe en revue la fiche d'incident
    - Corrélation avec d'autres incidents
    - Evaluation complémentaire
      - Plus poussée, plus technique
    - Ordonnancement des priorités en cas d'incidents concurrents

ISO 27035

- Phase de réaction
  - Actions à entreprendre en premier lieu
  - Evaluation de l'efficacité des actions
  - Actions à prendre dans un second temps
  - Escalade en cas de crise
  - Communication

ISO 27035

- Retour d'expérience
  - Prendre du recul
  - Améliorer les mesures de sécurité existantes
  - Mettre à jour l'appréciation des risques
  - Améliorer le processus de gestion d'incidents

ISO 27035

- Outils vivement recommandés par la norme
  - Gestion de tickets
  - Formulaire d'incident
  - Base de données des incidents

ISO 27035

- Conservation des preuves
  - La norme insiste beaucoup sur cet aspect
  - Faire en sorte que les éléments obtenus lors de l'incident puissent être opposables en cas de procédure judiciaire

ISO 27035

- Formation et sensibilisation
  - De tout le personnel
  - Des PoC
  - Des membres de l'ISIRT

ISO 27035

- Annexes de la norme
  - Rapprochement ISO 27001 et ISO 27035
  - Liste de types d'incidents de sécurité
  - Exemples de catégorisation et de classification des incidents de sécurité
  - Formulaires type
  - Aspects réglementaires

Dans la réalité

- Phase où l'on subit l'incident
  - Déferlante des alertes
  - Réactivité inégale des personnes concernées
    - Sous réactions
    - Sur réactions
  - Initiatives individuelles désordonnées

➔ Impossibilité de se concentrer sur un sujet plus de trois minutes !

Dans la réalité

- Questions fondamentales
  - Quel est l'impact réel de l'incident ?
  - Quel est le signalement technique de l'incident ?
  - Quel est le mode de propagation/ aggravation ?

Dans la réalité

- Phase où l'on lutte contre l'incident
  - Actions techniques de stabilisation
  - Actions techniques d'éradication
  - Actions de compensation
  - Actions de communication
    - Interne/externe
  - Pilotage

Dans la réalité

- Phase de retour à la normale
  - Rétablir le service nominal
  - Sécuriser le SI
  - Affiner le processus de gestion d'incident

Dans la réalité

- Tout cet aspect concret me manque dans l'ISO 27035
  - Pourquoi pas une annexe avec des fiches réflexe
    - Techniques
    - Organisationnelles
  - Par type d'incident ?

Conclusion

- Points forts de la norme
  - Donne un bon argumentaire pour mettre en place un processus de gestion des incidents
  - Volonté de donner des éléments concrets
    - Cf, annexes
- Points à améliorer
  - Clauses toujours trop abstraites
  - Manque des schémas de réaction pour les incidents les plus classiques

Conclusion

- On an parle d'ISO 27035 mais…
- …en somme, c'est tout le métier de RSSI qui est e train d'être normalisé par l'ISO
- Qu'est-ce que cela veut dire ?
  - Passé : Sécurité artisanale
  - Présent : Industrialisation de la sécurité
  - Avenir : …

Questions ?