Sécurité ANSSI

La Norme ISO 27001

Cette norme traite de la sécurité de l'information, et fournit un cadre de management de la sécurité de l'information (MSI).

Elle permet de répondre à 3 questions :

+ Quels sont les actifs à sécuriser ? -> QUI
+ De quoi protéger les actifs ? -> QUOI
+ Comment protéger les actifs ? -> COMMENT

PROBLEME : Trop souvent, une entreprise investit le strict minimum de moyen dans la cybersécurité, et réagit trop tard, souvent après une cyberattaque.

REPONSE :

+ Anticiper et améliorer la sécurité en permanence
+ Veille technologique et s'informer sur l'évolution de l'écosystème numérique
+ Suivre l'évolution de l'entreprise dans ses pratiques

La norme ISO 27001 établit un cadre de gestion des risques selon 3 axes :

+ Suivre et être informé des objectifs stratégiques de l'entreprise et de son évolution
+ Impliquer les responsables sur les risques de cybersécurité
+ Contrôler l'efficacité des mesures de sécurité mise en place

Gestion des Risques : le budget et les ressources étant limités, il est important de :

+ Prioriser les éléments à sécuriser
+ Identifier les menaces pour choisir les solutions adaptées
+ Accompagner et Sensibiliser les acteurs du Système d'Information
+ Monitorer les mesures pour les améliorer et les mettre à jour.

Quoi sécuriser ? Les Composants du Systèmes d'Information

2 types d'actifs :

ACTIFS PRIMORDIAUX

+ Processus métiers : un ensemble d'activités réalisées pour atteindre un objectif.
Exemple : quels sont les étapes pour réaliser une vente.

+ Données : Mots de passes, fichiers, BDD, documents, ...

ACTIFS SUPPORTS

+ Application : il est important de connaître les applications et leur versions. En fonction de leur version les failles ne seront pas les même.

+ Système d'Exploitation : connaître les différentes solutions (Windows, Linux, Android, ...), les types (client, serveur,) et les versions. Chacun aura des failles différentes.

+ Mobile : téléphones, tablettes sont identifiés par un numéro IMEI

+ Ordinateur, Serveur, Switch, et Routeur sont identifiés par leur adresse MAC

+ Types de réseaux : pour sécuriser son infrastructure i lest important de se poser la question Quel est l'étendu de mon réseau ? (LAN, MAN, WAN ...)

+ Interconnexion avec d'autres réseaux : est-ce que l'infrastructure est interconnectée avec d'autres réseaux (prestataire, partenaire, ...) ? Et comment (VPN, liaison dédiée...)

Identifier les menaces

IDENTIFIER LES MENACES

+ Menace : Cause potentielle d'un incident
+ Vulnérabilité : Faiblesse au niveau d'un actif. Une attaque ne peut avoir lieu que s'il y a vulnérabilité
+ Risque : Conséquence d'une vulnérabilité

Pour identifier les menaces, il est important :

+ Tenir à jour sa veille sur des sites tels que ANSSI, OWAPS, MITRE ATT&CK, ...
+ Garder l'historique des incidents de sécurité au sein de l'entreprise (fichier LOG)
+ Réaliser des tests d'intrusions (et garder une trace du process)

Identifier les Risques :

+ Critère d'acceptation
+ Niveau d'acceptation

Attention, cela veut dire que l'on accepte le risque. La direction doit le valider car les mesures de sécurité ne seront pas mis en œuvre pour réduire ce risque.

Pour chaque élément à risque identifié, il va falloir répertorier :

+ Les menaces auxquels ils sont confrontés
+ Leurs vulnérabilités
+ Les impacts en termes de disponibilité, intégrité, et confidentialité

Exercice

1. IDENTIFIER LES MENACES

Identifier les menaces potentielles concernant le cycle de vie d'une application :

+ HTML/CSS
+ UML : Use Case, Diagramme d'activité, séquence, classe
+ Conception : MCD-MLD, SQL, Hébergement (serveur, liaison, ...)
+ Back-End
+ Front-End

2. DICPT

Identifier, pour chaque élément, les impacts en termes de disponibilité, intégrité, et confidentialité (impact Faible, Moyen, Fort, Très Fort)

3. Impacts pour l'entreprise

Identifier, pour chaque élément, les impacts vis à vis de l'entreprise :

+ Impacts financiers
+ Impacts sur l'image, la réputation
+ Impacts juridique, réglementaire
+ Impacts organisationnel

Matrice de Criticité

Pour déterminer les éléments primordiaux à l'entreprise, lors d'un audit, il est possible de se baser sur la matrice de criticité.

			Fréquence			
			1	2	3	4
			Improbable	Peu Probable	Probable	Très probable
Gravité	1	Sans influence	Risque Mineur (1)	Risque Mineur (2)	Risque Mineur (3)	Risque Mineur (4)
	2	Peu critique	Risque Mineur (2)	Risque Mineur (4)	Risque Majeur (6)	Risque Majeur (8)
	3	Critique	Risque Mineur (3)	Risque Majeur (6)	Risque Majeur (9)	Risque Inacceptable (12)
	4	Très critique	Risque Mineur (4)	Risque Majeur (8)	Risque Inacceptable (12)	Risque Inacceptable (16)

Système de Management de la Sécurité de l'Information - PDCA

Le PDCA, Plan Do Check Act, est définit par la norme ISO27001.
Il doit être mis en place et mis à jour régulièrement.
Il permet d'améliorer en continue la sécurité du SI afin de maîtriser les risques.

Phase Plan :

Elaboration d'une politique de sécurité.
Dans le Plan, il faut préciser :

- Les actifs
- L'analyse et la maitrise des risques
- Le périmètre d'intervention
- Les objectifs
- Les plans d'actions

Phase Do :

Procédure de déploiement des mesures de sécurité.
Sensibilisation et formation des acteurs du SI.
Détecter les incidents en continue pour les résoudre rapidement
Mise en place d'indicateur de suivi de la sécurité

Check :

Audit et contrôle Interne qui permettent de mesurer les résultats suite à la mise en place d'actions correctives et mettre à jour la politique de sécurité en fonction de l'évolution de l'environnement de l'entreprise

Act :

Planifier, améliorer les actions correctives et préventives.

PRA (Plan de Reprise d'Activité) / PCA (Plan de Continuité d'Activité)

Le PCA, Plan de Continuité d'Activité, opère en préventif. Il vise à éviter au maximum tout arrêt de l'activité.

Le PRA, Plan de Reprise d'Activité, intervient une fois que le sinistre a eu lieu. Il doit permettre à l'entreprise de reprendre son activité normalement ou en mode dégradé.

Il faut identifier les ressources à risque selon 2 critères :

- **RPO :** Durée maximum d'enregistrement des données qu'il est acceptable de perdre (Recovery Point objectif)
- **RTO :** Durée maximale d'interruption des services (Recovery Time Objectif)

Pour réaliser le PRA et le PCA, il est important de se référer à l'audit réalisé pour déterminer les ressources à risque.

Pour chaque ressource à risque, il faudra mettre en œuvre une solution pour redémarrer au plus tôt et la tester. (Réplication, redondance, sauvegarde, …)

Les procédures à suivre, permettant de faire face à une situation de crise, contiendront :

- La description du contexte
- Les activités essentielles, les obligations et objectifs de l'entreprise
- Les risques, la gravité et leur impact
- La stratégie pour assurer la reprise d'activité
- Les rôles de chaque acteur du SI, les procédures à suivre et les moyens nécessaires

Le PRA et PCA Doivent être testés et mis à jour régulièrement.