**Audit du Système d’Information**

**Objectif Pédagogique :**

* Evaluer le niveau de sécurité du système d'Information
* Identifier les vulnérabilités
* Détecter les failles matérielles
* Détecter les failles logicielles
* Définir une liste d'action à mettre en place

**Norme ISO 27001 :**

Cette norme traite la sécurité de l’information.

Elle fournit un cadre de management de la sécurité de l'information (MSI)

Elle liste les exigences techniques et opérationnelles à mettre en œuvre pour gérer la Cybersécurité dans l’entreprise.

L’entreprise pourra donc répondre à ces trois questions :

* Quels sont les actifs à sécuriser ? QUI
* De quoi protéger les actifs ? QUOI
* Comment protéger les actifs ? COMMENT

La certification de l’entreprise à cette norme est de fournir un gage de bonne gestion de la sécurité à ces clients.

Intérêt de la norme ISO 27001 :

Très souvent en entreprise, l’investissement dans la cybersécurité est réduit au strict minimum.

Une entreprise réagira trop tard et bien souvent après une cyberattaque.

Pour assurer la cybersécurité dans l’entreprise et faire face à des cybercriminels, il faut anticiper et améliorer la sécurité en permanence.

La veille technologique permettra de suivre l’évolution de l’écosystème du numérique.

Il faut également suivez l’évolution de l’entreprise dans ses pratiques.

La norme ISO 27001, permet de fournir un cadre de gestion de la sécurité de l’information selon trois axes :

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

Gestion des risques :

Pour gérer les risques cybersécurité de l’entreprise le budget et les ressources ne sont pas illimités, il est donc important de :

* **Savoir quoi sécuriser ?** les éléments dont l’entreprise a le plus besoin
* **Savoir contre quoi ?** sans connaitre le contre quoi, la solution ne sera pas efficace.

Choisir les solutions techniques et opérationnels adaptées efficaces au « contre quoi »

* **Accompagner** les acteurs du SI pour qu’ils deviennent acteur de la sécurité : sensibilisation de tous les collaborateurs
* **Monitorer, piloter** les mesures pour les améliorer, les faire évoluer et les mettre à jour

**Savoir quoi sécuriser ? - Composition du Système d’Information (SI) :**

Afin d’assurer la sécurité de votre infrastructure et établir le SMSI (système de management du système d’information), il est nécessaire de connaitre les **composants** (= les Actifs) de son système d’information, les **valeurs** associées et les dépendances entre eux.

Ce travail est à réaliser en collaboration avec les acteurs du SI.

Les différents types d’actifs composant le SI :

* Actifs Primordiaux : Processus métier et données
* Actifs Supports
  + Sites
  + Acteurs
  + Eléments supports : Application et Système d’exploitation
  + Equipements : Mobile, Ordinateur, Serveur, Switch et Routeur.

Les différents types d’éléments composant le SI :

* Actifs primordiaux :

Processus métier : un ensemble d’activités réalisées pour atteindre un objectif.

Nous verrons par la suite comment analyser les processus métiers avec UML.

Exemple : Processus vente : pour réaliser une vente quels seront les différentes étapes.

Données : mots de passes, fichiers, bases de données, documents …

Application : il est important de connaitre les applications et leurs versions. En fonction de leur version les failles ne seront pas les mêmes.

Système d’exploitation : connaitre les différentes solutions (Windows, Linux, Android, Ios, …), les types (client, serveur) et les versions.

Chacun aura des failles différentes.

Mobile : téléphones, tablette sont identifiés par un numéro IMEI

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

Pour inventorier les composants du SI, il existe des outils tel que OCS Inventory.

Types de réseaux : Pour sécuriser son infrastructure il est important de se poser la question, Quel est l’étendue de mon réseau ? (LAN, MAN, WAN...)

Interconnexion avec d’autres réseaux :

Est-ce que l’infrastructure est interconnectée avec d’autres réseaux (prestataire, partenaires…) ? et comment (VPN, liaison dédiée…) ?

**Identifier les éléments à risque :**

La sécurisation de l’informations devra être concentré sur les actifs qui ont le plus de valeurs pour l’entreprise.

Il faudra également déterminer les besoins en termes de DICPT (disponibilité, intégrité, confidentialité, preuve et traçabilité)

Tous ces éléments permettront de définir les objectifs de sécurité et de choisir les mesures les plus adaptées.

**Contre quoi ? - Identifier les menaces, Vulnérabilités et les risques :**

Menace : Cause potentielle d’un incident CONTRE QUOI

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 technologique sur des sites tel que ANSSI, l'OWASP, MITRE ATT&CK…
* Garder l’historique des incidents de sécurité au sein de l’entreprise.
* Réaliser des tests d’intrusion

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 des mesures de sécurité ne seront pas mis en œuvre pour réduire ce risque.

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

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

**Critère DICPT :**

4 niveaux pour chaque critère : Faible, Moyen, Fort, Très fort

D : Disponibilité

Avoir accès aux ressources au moment voulu.

(Haute disponibilité)

I : Intégrité

Le contenu est intègre, il n’y a pas eu de modification illégitime.

Toute modification illégitime doit être détectée et corrigée

C : Confidentialité

Ressource est accessible qu’aux personnes autorisées

P : Preuve

Retrouver les circonstances dans lesquelles une ressource évolue.

Elle regroupe :

* La traçabilité
* Authentification d’un utilisateur
* Le responsable de l’action effectuée

T : Traçabilité

Ensemble des actions menées sur une ressource

**Impacts :**

Pour l’entreprise, les enjeux de la cybersécurité :

* Impacts financiers
* Impact sur l’image, la réputation
* Impact juridique, réglementaire
* Impact organisationnel

**Pra / Pca :**

Le PCA, Plan de continuité d’activité, opère en préventif. Plan visant 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.

**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 maitriser 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.