Audit Sécurité

Objectif

Cet audit cible les entreprises et cabinets comptables souhaitant un état des lieux sur le respect des bonnes pratiques de base en matière de sécurité informatique de leur Système d'information.

Il est mené sur quatre périmètres essentiels de la sécurité du système d'information :

- La sécurité de vos infrastructures informatiques
- La protection contre le piratage
- La confidentialité des données
- Votre résilience informatique

Contenu

Sécurité des infrastructures informatiques

Ici il est question des aspects matériels :

- Redondance du lien Internet ;
- Fiabilité et maintenance des composants ;
- Sécurité des accès physiques aux éléments du système d'information ;
- Protection électrique, incendie, vol, climatisation.

Protection contre le piratage

Dans cet audit, « Piratage » s'entend au sens large : il s'agit de couvrir autant que faire se peut les risques d'intrusions et d'exfiltrations pouvant avoir des conséquences négatives sur la réputation de l'entreprise, son fonctionnement, ses finances, ou susceptibles d'entraîner des conséquences juridique (RGPD par exemple) voire de sa survie.

L'analyse réalisée dans le cadre de l'audit couvre :

- Les protections destinées à contrôler l'entrée dans le système d'information (dites « protections périmétriques ») :
  - Organisation du réseau, en particulier des pare-feux ;
  - Protection du réseau Wi-Fi ;
  - Paramétrage de la DMZ[1] ;
  - Couverture et application des patchs de sécurité ;
- Les protections sur le réseau :
  - Protection des serveurs et des postes (physique et logique) ;
  - Pertinence de la politique antivirus ;
  - Imprimantes et autres périphériques.
- Les risques sur les applications :
  - Bureautique ;
  - Applications « métier » ;
  - Messagerie électronique.
- La présence et la pertinence de la communication interne sur les risques encourus.

[1] DMZ : « Demilitarized zone », zone sécurisée permettant les accès à un serveur à partir d'internet sans compromission du réseau interne.

Confidentialité des données

La confidentialité des données est à gérer sur plusieurs axes.

L'audit analyse les principaux, à savoir :

- La gestion des accès des utilisateurs au système d'information (mode de connexion, traitement des comptes avec droits étendus, contrôle des utilisateurs externes, cartographie des droits sur les données…) ;
- La prise en compte du cycle de vie des matériels ;
- Le respect du RGPD.

Résilience informatique

Ce chapitre étudie tous les aspects du retour en production après une mise hors service du système informatique (panne matérielle ou logicielle, attaque virale, catastrophe naturelle, vol, …).

Cette analyse part des éléments classiques de prévention, comme le plan de sauvegarde ou la maintenance préventive des matérielles, pour aller jusqu'à l'étude de la pertinence du PRA[2] ou du PCA[3] en place, en passant par le respect du RGPD.

Livrables

1. Un rapport de restitution de l'ensemble des constatations et des recommandations.
2. Un indice chiffé et un graphique vous permettant de situer votre niveau de protection par rapport à ce qui est souhaitable compte-tenu de la taille de votre entreprise.

[2] PRA : Plan de Reprise d'Activité = en cas de mise hors service du système informatique, la remise en production nécessite un délai qui peut aller de quelques heures à quelques jours.

[3] PCA : Plan de Continuité d'Activité = en cas de problème, plus ou moins grave selon la profondeur du PCA, le système continue à fonctionner sans conséquence pour les utilisateurs et le système lève une alerte pour les administrateurs.