PSSI

Plan de Sécurisation des Systèmes d'Information

1er août 2019

Table des matières

1. Sécurité organisationnelle

1.1 Introduction

1.2 Acteurs de la sécurité

1.2.1 Responsable de sécurité des systèmes d'information
1.2.2 Responsables de domaine SI
1.2.3 Correspondants métier
1.2.4 Administrateurs racines des droits d'accès
1.2.5 Collaborateurs
1.2.6 Comité de Direction
1.2.7 Fonctions support

1.3 Interlocuteurs externes

1.3.1 Clients
1.3.2 Prestataires et fournisseurs

1.4 Processus organisationnel de gestion de la sécurité

1.4.1 Mise à jour et gestion de version de la Politique de Sécurité
1.4.2 Diffusion de la Politique de Sécurité
1.4.3 Mise en application des règles de sécurité par domaine
1.4.4 Délégation du pouvoir d'attribution des moyens d'accès logiques et physiques
1.4.5 Comité de Pilotage
1.4.6 Contrôles de la SSI
1.4.7 Contrôle des droits d'accès physiques et logiques
1.4.8 Actions de sensibilisation
1.4.9 Gestion des incidents de sécurité
1.4.10 Processus propres aux interlocuteurs externes

2. Sécurité physique des environnements de bureaux

2.1 Définition

2.2 Identification des sites

2.3 Etats des risques naturels et technologiques

2.4 Organisation de l'espace de travail

2.5 Protection des locaux

2.5.1 Protection contre l'intrusion
2.5.2 Vidéosurveillance
2.5.3 Gestion technique du bâtiment
2.5.4 Maintenance des dispositifs de lutte contre l'incendie

2.6 Protection des locaux techniques d'étage

2.6.1 Contrôle d'accès
2.6.2 Energie
2.6.3 Climatisation
2.6.4 Détection incendie

2.7 Contrôle d'accès aux locaux

2.7.1 Mise en œuvre
2.7.2 Fermeture des locaux

2.8 Traçabilité

3. Sécurité informatique des environnements de bureaux

3.1 Contrôle d'accès à l'infrastructure

3.1.1 Architecture d'authentification des utilisateurs
3.1.2 Architecture d'authentification des administrateurs
3.1.3 Inscription des postes de travail dans l'annuaire
3.1.4 Gestion des comptes utilisateurs
3.1.5 Attribution des droits
3.1.6 Moindre privilège
3.1.7 Stratégies de sécurité
3.1.8 Répertoires partagés et serveurs de media

3.2 Protection du réseau

3.2.1 Cloisonnement du réseau
3.2.2 Mise à jour des équipements réseau
3.2.3 Administration des équipements réseau
3.2.4 Protection contre les attaques réseau internes
3.2.5 Accès Internet
3.2.6 Wifi

3.3 Protection des postes de travail contre les codes malveillants

3.3.1 Inventaire du parc
3.3.2 Protection du système
3.3.3 Mises à jour de sécurité
3.3.4 Antivirus
3.3.5 Réponse à une suspicion de compromission
3.3.6 Imprimantes et périphériques réseau
3.3.7 Messagerie et courrier électronique

3.4 Mesures spécifiques aux ordinateurs portables

3.5 Traçabilité des opérations

3.6 Sauvegarde et restauration des données

4. Sécurité des plateformes de traitement

4.1 Salle serveur locale

4.1.1 Responsabilité
4.1.2 Localisation
4.1.3 Assurance
4.1.4 Contrôle d'accès
4.1.5 Energie
4.1.6 Climatisation
4.1.7 Incendie
4.1.8 Dégât des eaux
4.1.9 Continuité et reprise d'activité
4.1.10 Monitoring et traçabilité des opérations

4.2 Service d'hébergement en datacenter

4.2.1 Périmètre du service
4.2.2 Politique de sécurité, standards et certifications
4.2.3 Contrats, engagements et procédures
4.2.4 Sécurité du personnel et des sous-traitants
4.2.5 Sécurité physique
4.2.6 Environnement électrique, climatisation
4.2.7 Protection contre les risques environnementaux
4.2.8 Accès opérateurs
4.2.9 Inventaire des équipements présents
4.2.10 Disponibilité, SLA, Gestion des incidents
4.2.11 Continuité d'activité et gestion de crise
4.2.12 Suivi, indicateurs
4.2.13 Auditabilité

4.3 Hébergement cloud, IAAS

4.4 Externalisation d'applications (SAAS)

5. Sécurité des serveurs et des services de traitement

5.1 Security by design des architectures

5.1.1 Projet initial
5.1.2 Modifications
5.1.3 Evolutions

5.2 Gestion des mises à jour

5.2.1 Suivi des vulnérabilités
5.2.1.1 Suivi des technologies stratégiques
5.2.1.2 Suivi des actifs
5.2.2 Traitement des vulnérabilités et déploiement des mises à jour
5.2.3 Traitement des zero-days

5.3 Gestion de la configuration

5.3.1 Définition des configurations
5.3.2 Déploiement des configurations
5.3.3 Suivi des changements

5.4 Cloisonnement

5.4.1 Cloisonnement réseau
5.4.2 Cloisonnement de la couche virtuelle

5.5 Gestion de l'authentification

5.5.1 Inventaire
5.5.2 Moyens mis en œuvre
5.5.3 Protection des moyens d'authentification et de chiffrement
5.5.4 Génération des moyens d'authentification
5.5.5 Révocation
5.5.6 Traçabilité
5.5.7 Audit

5.6 Protection des données

5.6.1 Traçabilité
5.6.2 Chiffrement
5.6.3 Sauvegarde et archivage

5.7 Sécurité Internet

5.8 Collecte et analyse des logs

5.9 Organisation

5.10 Intrusions et anomalies

5.11 Réponse aux compromissions isolées

5.12 Incidents généraux et APT

5.13 Disaster Recovery Plan (DRP)

5.14 Audits techniques

6. Glossaire

7. Annexes