PROTECTION DES SYSTEMES D'INFORMATION

Protégez votre système d'information

Les entreprises ne peuvent plus se passer de l'informatique pour leur propre fonctionnement, ainsi que le travail en réseaux et la communication indispensables avec les fournisseurs, donneurs d'ordre et administrations.

Ce besoin de communication tant interne qu'externe crée une vulnérabilité des systèmes de l'entreprise, aggravée ces dernières années par la généralisation des outils nomades : Smartphones, tablettes, ordinateurs portables.

La mise en œuvre d'une politique de sécurité des systèmes informatiques s'impose.

LES RISQUES

Catégories de risques ...

Vol et **destruction** d'informations

Usurpation d'identités

Intrusion et **captation** des ressources systèmes par des tiers dans des attaques en déni de service d'autres systèmes informatiques via un réseau BOTNET

Mise hors service des systèmes et ressources informatiques

... et leurs conséquences

↘ **Perte d'informations** et de **données** menaçant la vie de l'entreprise

↘ **Mise en cause sur le plan légal**

LES 13 COMMANDEMENTS + 1 DE L'HYGIENE EN ENTREPRISE PAR L'ANSSI

1 - BATIR UNE POLITIQUE DE SECURITE

◊ Connaître la législation en vigueur et la jurisprudence :
- ↘ guide pour les employeurs et les salariés - source CNIL *
- ↘ règlementation - source ANSSI *

◊ Connaître précisément le système d'information et ses utilisateurs (cartographie des SI, disposer d'un inventaire exhaustif des comptes et les maintenir à jour)

◊ Rédiger des procédures d'arrivée et de départ des utilisateurs

2 - MAITRISER LE RESEAU

◊ Limiter le nombre d'accès à Internet

◊ Interdire la connexion d'équipements personnels (Bring Your Own Device) au système d'information de l'entreprise

Communication SGAR PACA - Création : Marina LOISEAU

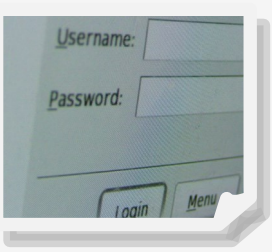
3 - METTRE A NIVEAU LES LOGICIELS

◊ Se tenir informé des vulnérabilités et des mises à jour nécessaires (fiches CERTA)

◊ Avoir un système d'exploitation des logiciels à jour (navigateur, antivirus, bureautique, pare-feu, etc.)

◊ Ne pas télécharger de programmes sur internet sans être sûr de la source : vérifier l'EURL et l'intégrité des fichiers MD5

4 - AUTHENTIFICATION ET MOT DE PASSE



◊ Identifier nominativement chaque personne ayant accès au SI et utiliser les mots de passe forts : éviter 123456. Minimum 8 caractères en intégrant des caractères spéciaux, type majuscules …

◊ Ne pas enregistrer les mots de passe par défaut sur le SI et supprimer les éléments d'authentification par défaut (remplacer admin)

5 - SECURISER LES EQUIPEMENTS TERMINAUX

◊ Désactiver par défaut les services / composants inutiles (fiches pratiques sur le portail SI)

◊ Interdire techniquement la connexion des supports informatiques sauf si c'est nécessaire : clé USB

◊ Utiliser un outil de gestion de parc informatique

◊ Gérer les terminaux nomades (portables, tablettes) comme les postes fixes

◊ Mettre en œuvre des moyens appropriés à la confidentialité des données (outils de chiffrement certifiés de l'ANSSI)

6 - PROTEGER LE RESEAU INTERNE DE L'INTERNET

◊ Interdire la navigation sur l'internet depuis les comptes d'administration

◊ Limiter le nombre d'accès à internet

◊ Eviter l'usage de technologies sans fil (wi-fi, bluetooth)

◊ Créer un sous réseau protégé par un pare-feu

◊ Installer un logiciel antivirus fiable

7 - SURVEILLER LES SYSTEMES

◊ Mettre en place un système de journalisation des évènements

8 - SECURISER LES POSTES ADMINISTRATEURS

◊ Utiliser un réseau dédié à l'administration des équipements

◊ Ne pas donner aux utilisateurs des privilèges administrateurs

9 - SEGMENTER LE RESEAU

◊ Mettre en place des réseaux cloisonnés

◊ Etablir une barrière entre les données externes et internes (travail à distance)

Communication SGAR PACA - Création : Marina LOISEAU

10 - CONTROLER L'ACCES AUX LOCAUX ET SECURITE PHYSIQUE

- ◊ Utiliser des mécanismes de contrôle d'accès robustes
- ◊ Gérer rigoureusement les clés et les badges permettant l'accès aux locaux et codes des alarmes

11 - ORGANISER LA REACTION EN CAS D'INCIDENT

- ◊ Traiter l'infection d'une machine en considérant que le code a déjà pu se propager ailleurs
- ◊ Disposer d'un plan de reprise ou de continuation d'activité
- ◊ Mettre en place une chaîne d'alerte
- ◊ Effectuer des sauvegardes régulières (plan de sauvegarde)
- ◊ Cassettes de stockage à stocker dans les armoires ignifugées

12 - SENSIBILISER LES SALARIES

- ◊ Former les utilisateurs aux règles d'hygiène élémentaires (plan de formation)
- ◊ Contrôler la diffusion d'informations personnelles, internet est une rue peuplée d'inconnus (Viadeo, Facebook etc.)
- ◊ Soyez vigilants avant d'ouvrir des pièces jointes, elles comportent souvent des codes malveillants

13 - FAIRE AUDITER LA SECURITE

- ◊ Faire réaliser des audits tous les ans et y associer un plan d'action

14 - PLAN ASSURANCE RISQUE

- ◊ Comparer les prestations des sociétés d'assurance proposant des services de couverture de risques

+ D'INFORMATIONS ET DE LIENS …

ANSSI Agence Nationale de la Sécurité des Systèmes d'Information:

www.ssi.gouv.fr
www.clusif.asso.fr
ozssi-zds@interieur.gouv.fr

CNIL Commission Nationale de l'Informatique et des Libertés: www.cnil.fr

Communication SGAR PACA - Création : Marina LOISEAU