Sécurité du Système d'Information

Information	Qualités d'une information	Accessible, Exacte, Actualisée, Pertinente et Exhaustive.	
	Acteurs du SI	Direction des Systèmes d'Information (DSI) + Informaticiens (Chef de projet, développeurs…) + Partenaires (**ESN** (notion de contrat), fournisseurs, éditeurs) +Utilisateurs finaux.	
	Logiciels du SI	Commerciaux, Shareware, Freeware et Libre.	
Réseaux (LAN : privé)	Principe	TCP/IP	Permet à chaque appareil d'avoir une adresse UNIQUE sur le réseau.
	Serveur	Serveur **DHCP** : distribue automatiquement une configuration IP aux équipements. Serveur **DNS** : traduit les noms de domaines en adresse IP. Serveur d'**authentification** (**annuaire**) : valide les couples login/mdp et détermine les droits des utilisateurs. Serveur **Web** (http, ftp) : internet, intranet, extranet. Serveur **SGBD** : support des bases de données. Autres types de serveurs : serveurs d'applications, de messagerie, de fichiers.	
	Matériel	**Concentrateur** (hub) **Commutateur** (switch) **Routeur** (Gateway)	Une « box » cumule les rôles de commutateur et de routeur.
	Administration - Facilité de gestion - Sécurisation - Économie	**Sous-réseaux**	Découpage d'un LAN en plusieurs LAN dédiés (ex : par service) de plus petites tailles.
		VPN	Liaison totalement sécurisée par le cryptage et l'encapsulation des échanges. Cryptage peut être symétrique ou asymétrique (le plus robuste).
		VLAN (réseau privé virtuel)	Regroupement virtuel de matériels dans un LAN existant.
Sécurité	Contre quoi lutter ? Une information doit rester inaccessible, intègre (non altérée) et disponible (même si crash)	Des failles	Mises à jour non réalisées. Mot de passe faibles. Droits d'accès laxistes. Nomadisme. Absence de sensibilisation.
		Des menaces	**Déstabilisation** (déni de service, divulgation d'infos) + **Espionnage** (à des fins éco. et/ou scientifique) + **Sabotage** + **Cybercriminalité** (Ransonware, Phising).
		Programmes et pratiques	Virus, Vers, Trojans, Ransonware + Phising, Spam.
	Quelles mesures ?	Organisationnelles	Gestion de la disponibilité (redondance stockage). Politique de sauvegarde (complète, différentielle ou incrémentale). Sensibilisation et formation des utilisateurs. Plan de reprise d'activité (PRA).
		Techniques	Serveur d'authentification + Antivirus à jour + **Proxy** : anonymat, filtrage + **DMZ** : isolation de certains serveurs + **Pare-Feu (Firewall)** : filtrage, analyse des flux.
		Pour les échanges	Cryptage + Certificat numérique + Signature électronique.

Sécurité du Système d'Information

Sécurité du Système d'Information

<table>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td rowspan="4">Cadre juridique national et européen</td><td>Une donnée personnelle ?</td><td colspan="2">« Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ».</td></tr>
<tr><td>CNIL : Commission Nationale de l'Informatique et des Libertés</td><td colspan="2">Sa mission : protéger la vie privée et les libertés individuelles ou publiques en veillant au respect de la loi Informatique et Libertés.</td></tr>
<tr><td rowspan="2">RGPD : Règlement Général sur la Protection des Données</td><td>6 principes</td><td>Légalité : demande de consentement avant le recueil.
Finalité : les personnes doivent être informées de l'usage et de la finalité de la collecte.
Pertinence : une collecte de données doit être limitée à l'utilisation prévue.
Conservation : les données collectées ne doivent être conservées que pour une durée limitée.
Sécurité : toutes les mesures nécessaires doivent être mises en œuvre afin de garantir la sécurité et la confidentialité des données collectées.
Respect des droits : droit d'accéder, de rectifier et de s'opposer à leur utilisation (sauf exceptions).</td></tr>
<tr><td>Des étapes de mise en place</td><td>Nomination du DPO (Délégué à la Protection des Données).
Cartographie des traitements des données personnelles (registre des traitements).
Documentation de la conformité.</td></tr>
<tr><td rowspan="4">Cloud</td><td>3 Catégories</td><td colspan="2">Privé, Publique et Hybride.</td></tr>
<tr><td>3 Services</td><td colspan="2">Iaas (infrastructure comme le stockage par ex.).
PaaS (services).
Saas (logiciels : cf Office 365, Google Doc etc.).</td></tr>
<tr><td>Avantages</td><td colspan="2">Libre-service (on paie pour un usage en libre-service).
Adaptabilité (selon les besoins).
Budgétisation des coûts.</td></tr>
<tr><td>Limites</td><td colspan="2">Dépendance forte vis-à-vis des prestataires (FAI et opérateur Cloud).
Propriété intellectuelle : à qui appartient l'information d'une entreprise A stockée/gérée par une entreprise B ?</td></tr>
<tr><td>XML

Extensible Markup Language</td><td colspan="2">Langage à balises
Une balise est encadrée par des <>
Balise de début <..> et une balise de fin </..>
Le XML permet de transférer des informations entre deux systèmes hétérogènes grâce à la standardisation de son format.</td><td>
<bibliographie>
<livre cle="Michard01" langue="fr">
<titre>XML langage et applications</titre>
<auteur>
<nom>Michard</nom>
<prenom>Alain</prenom>
</auteur>
<isbn>2-212-09206-7</isbn>
</livre>
</bibliographie>
</td><td>
Racine du document
Nœud : livre (début)
Sous-nœud titre
Sous-nœud : auteur
Sous-nœud nom
Sous-nœud prenom
Sous-nœud : isbn
Fin du document
</td></tr>
</table>