Cybersécurité - BTS SIO 1

Fiche savoirs technologiques 3

Sécurité et sûreté

I Définitions

La sûreté vise à prévenir les risques et conséquences d'un événement accidentel ou involontaire.

La sécurité consiste à prévenir les actes de malveillance en combinant des moyens humains, techniques et organisationnels. Cette notion est souvent englobée dans le terme de sûreté informatique. Elle doit permettre de faire face aux risques de vol de données, d'intrusion dans le système informatique, ou d'effectuer la recherche de dégradation de service du SI.

II Les périmètr es r espectif s

1. Le périmètre de la sûreté informatique

a. Les menaces non intentionnelles

Le périmètre de la sûreté informatique englobe les menaces non intentionnelles qui sont, par définition, peu prévisibles et non-volontaires.

b. Les types de menaces

Menace d'accident naturel	Menace humaine	Menace liée au matériel
Un risque naturel (orage, inondation, etc.) est un élément imprévu ou difficilement prévisible qui peut être dangereux lorsqu'il impacte une vulnérabilité du SI.	L'erreur humaine, la maladresse ou la négligence peuvent mettre à jour une faiblesse du SI et mettre en échec sa stabilité.	Le choix du matériel informatique peut rendre plus ou moins vulnérable le SI. La réduction de certains coûts d'acquisition peut être source de menaces pour le SI.

2. Le périmètre de la sécurité informatique

a. Les menaces délibérées

Le périmètre de la sécurité informatique regroupe les menaces délibérées qui proviennent de personnes malveillantes, et qui peuvent nuire au SI. Ces personnes sont internes ou externes à l'organisation, et disposent de capacités plus ou moins importantes dans les possibilités de détérioration du SI, selon leur niveau de compétence technique et leurs droits d'accès au SI.

b. Les catégories d'attaquants

D'après l'ANSSI, les profils des attaquants peuvent être regroupés selon trois grandes catégories :

- les organisations structurées guidées par une logique d'efficacité et de gain disposant de moyens sophistiqués et conséquents, voire quasi illimités (États, crime organisé) ;
- les organisations ou groupes guidés par une motivation idéologique disposant de moyens significatifs mis en œuvre de façon relativement coordonnée (terroristes, activistes) ;
- les attaquants disposant de moyens limités mais spécialisés (individus isolés, groupes d'individus).

3. Les principaux types de menaces

Quatre principaux types de menaces sont mis en avant par l'ANSSI : la déstabilisation, l'espionnage, le sabotage et la cybercriminalité.

Menaces	Types d'attaques
Déstabilisation	• Déni de service : action qui rend un service inaccessible, par l'envoi d'une multitude de requêtes vers un serveur pour provoquer sa panne ou sa dégradation. • **Défiguration** : ajout ou remplacement des pages d'un site Web afin de revendiquer un message idéologique. • **Divulgation de données** : récupération de données confidentielles d'une organisation en exploitant une vulnérabilité du réseau informatique.
Espionnage	• **Attaque par « point d'eau » (*wateringhole*)** : infection du site Internet d'une organisation pour contaminer les ordinateurs des visiteurs, afin d'accéder au réseau de l'organisation. • **Attaque par hameçonnage ciblé (*spearfishing*)** : usurpation de l'identité d'une personne connue du destinataire pour envoyer un message ciblé à un membre d'une organisation, afin de lui faire ouvrir une pièce jointe malveillante qui permettra d'accéder au réseau de l'organisation.
Sabotage	Les modes d'attaques sont nombreux, mais ils visent tous à créer une panne dans un périmètre ou sur l'ensemble du système d'information d'une organisation.
Cybercriminalité	• **Rançongiciel (*ransomware*)** : données confidentielles rendues inaccessibles jusqu'au paiement d'une rançon. Le chantage peut parfois toucher des données gênantes, que l'on menace de rendre publiques sur Internet. • **Hameçonnage (*phishing*)** : action visant à tromper un utilisateur pour l'inciter à communiquer des données personnelles, souvent des données bancaires. Les formes peuvent être diverses, telles que l'utilisation des réseaux sociaux, un courriel ou encore un SMS.

D'après www.ssi.gouv.fr