1

Préparation Examen Cybersécurité 2 BTS SIO SLAM

Table des matières

Préparation Examen Cybersécurité 2 BTS SIO SLAM

Objectif

- Vous permettre de vous étalonner par rapport au référentiel de l'épreuve E6 du BTS sur les données à caractère personnel, leurs traitements, gestion des risques. Cette épreuve doit être réalisée de façon individuelle.

Rappel

1.1 Piliers de la sécurité

Les piliers de la sécurité sont :

1- **La confidentialité :** Il s'agit de garantir que l'information est accessible uniquement par des personnes autorisées et que les données sensibles ne tombent pas entre de mauvaises mains.

- Seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées.

2- **La Disponibilité :** La disponibilité assure que les systèmes, réseaux et données sont accessibles et utilisables lorsque nécessaire. Cela implique de minimiser les temps d'arrêt non planifiés et de garantir l'accès aux ressources.

- L'accès aux ressources du système d'information doit être permanent et sans faille durant les plages d'utilisation prévues.

3- **L'Intégrité :** L'intégrité concerne la garantie que les données n'ont pas été modifiées de manière non autorisée. Cela signifie que les données restent exactes, complètes et non altérées.

- Les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante.

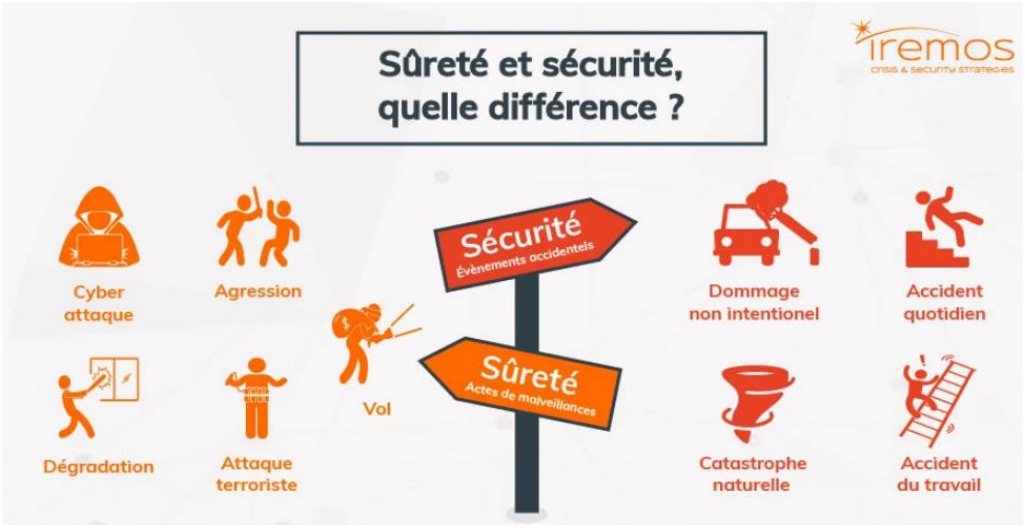
4- **Preuve** (également appelée non-répudiation)**:** elle est souvent considérée comme une composante complémentaire qui garantit qu'une action ou une transaction peut être vérifiée et attribuée à une entité spécifique.

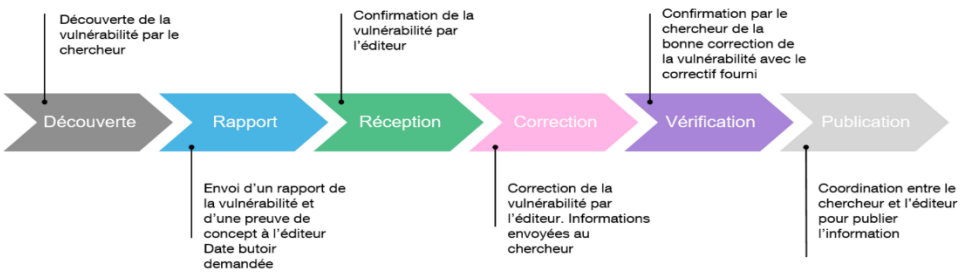
- Elle garantit que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.

Préparation Examen Cybersécurité 2 BTS SIO SLAM

Pilier	Scenario	Mise en œuvre du pilier
Confidentialité	L'entreprise stocke des informations personnelles des employés, y compris les numéros de sécurité sociale, les salaires, etc.	Les accès au système de gestion de base de données sont limités aux employés autorisés. Des politiques de confidentialité sont en place pour régir l'accès aux données sensibles, et le chiffrement est utilisé pour protéger les données lors de leur transmission.
Intégrité	Les employés mettent à jour leurs informations personnelles dans la base de données.	Des contrôles d'intégrité sont appliqués pour garantir que seuls les utilisateurs autorisés peuvent modifier les données. Des journaux d'audit enregistrent les modifications apportées aux données, et des mécanismes de contrôle des versions sont en place pour restaurer les données en cas de corruption.
Disponibilité	Les employés ont besoin d'accéder aux informations stockées dans la base de données pour effectuer leurs tâches.	Le système de gestion de base de données est conçu pour minimiser les temps d'arrêt planifiés et non planifiés. Des sauvegardes régulières sont effectuées pour prévenir la perte de données en cas de défaillance matérielle ou de catastrophe. Des procédures de reprise après sinistre sont en place.
Preuve	Un employé effectue une transaction financière dans le système.	Les transactions sont horodatées et enregistrées dans des journaux d'audit. Des mécanismes de non-répudiation sont mis en place, tels que la signature électronique, pour garantir que les actions des utilisateurs peuvent être attribuées de manière indiscutable à des individus spécifiques.

Les piliers de la sécurité





1.2 La gestion des risques

L' indicateur qui permet de mesurer la probabilité de réalisation d'une menace est **la vraisemblance.**

La vraisemblance, dans le contexte de la cybersécurité et de la gestion des risques, se réfère à la probabilité ou à la plausibilité qu'une menace particulière se réalise ou qu'un événement indésirable se produise. C'est un indicateur qui évalue à quel point il est probable qu'une menace spécifique se matérialise et affecte un système, une organisation ou des données.

En d'autres termes, la vraisemblance mesure la crédibilité ou la réalité perçue d'une menace. Elle peut être exprimée en termes de probabilité, par exemple improbable, possible, probable, ou en pourcentages pour une évaluation plus quantitative.

Elément d'occurrence		Probabilité d'occurrence	
Expérience passée	Élément externe		
Ne s'est jamais produit	Pas d'événement similaire dans la presse spécialisée	Improbable	1
Se produit plusieurs fois dans l'année	Événement similaire dans la presse spécialisée	Possible	2
Se produit plusieurs fois par mois	Événement similaire dans la presse courante	Probable	3
Se produit plusieurs fois par semaine	Événement récurrent dans la presse courante	Fréquent	4

Tableau de probabilité d'occurrence du scénario de risque

La gestion des risques en cybersécurité prend en compte non seulement la probabilité, mais aussi l'impact potentiel d'une menace sur l'organisation. L'utilisation de ces indicateurs aide à hiérarchiser les actions de sécurité et à allouer les ressources de manière efficace pour atténuer les risques identifiés.

Exemple d'un scénario de risque : **Attaque par Phishing**

Menace	Description du Scénario	Vraisemblance
Un attaquant pourrait lancer une attaque de phishing en envoyant des e-mails malveillants à des employés de l'organisation	1- L'attaquant envoie des e-mails semblant provenir d'une source légitime (par exemple, la direction de l'entreprise). 2-L'attaquant envoie des e-mails semblant provenir d'une source légitime (par exemple, la direction de l'entreprise). 3- Les employés, trompés par l'apparence authentique des e-mails, cliquent sur les liens ou ouvrent les pièces jointes, ce qui peut entraîner la compromission de leurs identifiants ou l'installation de logiciels malveillants.	Élevé (probable, peut se produire).

1.3 RGPD

Le Règlement Général sur la Protection des Données (RGPD) dans le contexte de la cybersécurité est une législation européenne mise en œuvre en mai 2018 pour renforcer la protection des données personnelles, imposant des normes strictes de collecte, de traitement et de sécurisation des informations sensibles. Les organisations sont tenues de mettre en place des mesures de sécurité adéquates, d'informer les individus sur l'utilisation de leurs données et de signaler toute violation de données aux autorités compétentes, afin de garantir la confidentialité et l'intégrité des informations personnelles.

Données Personnelles :

Définition : Les données personnelles désignent toute information permettant d'identifier directement ou indirectement une personne physique, telle que le nom, l'adresse, l'adresse électronique, le numéro d'identification, ou tout autre élément spécifique à l'identité de cette personne.

Contexte RGPD : Le RGPD accorde une protection spécifique aux données personnelles en établissant des principes clairs sur leur traitement, leur collecte, et leur conservation. Les individus ont des droits sur leurs données personnelles, y compris le droit à l'information, d'accès, de rectification, et le droit à l'oubli.

Données Sensibles :

Définition : Les données sensibles, dans le cadre du RGPD, englobent des catégories particulières de données personnelles qui révèlent des informations spécifiques telles que l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques, l'appartenance syndicale, la santé, ou l'orientation sexuelle.

Contexte RGPD : Le RGPD accorde une protection accrue aux données sensibles en interdisant leur traitement à moins que des conditions spécifiques ne soient remplies. Les organisations doivent démontrer une base légale pour le traitement de telles données et respecter des mesures de sécurité renforcées pour préserver leur confidentialité.

L'hameçonnage (*phishing* en anglais) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance.

https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/Phishing-hameconnage

Un rançongiciel ou ransomware est un logiciel malveillant ou virus qui bloque l'accès à l'ordinateur ou à ses fichiers et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.

La défiguration de site web est l'altération par un pirate de l'apparence d'un site Internet, qui peut devenir uniformément noir, blanc ou comporter des messages, des images, des logos ou des vidéos sans rapport avec l'objet initial du site, voire une courte mention comme « owned » ou « hacked ».