1	**Préparation Examen Cybersécurité 2 BTS SIO SLAM**	

Table des matières

Préparation Examen Cybersécurité 2 BTS SIO SLAM

Partie 1 : QCM

Question 1 : L'authentification, l'imputation* et la traçabilité assurent

a. La vérité
b. La disponibilité
c. La confidentialité
d. La non-répudiation

* : L'imputation permet de déterminer qui est responsable d'une activité particulière. Cela peut être crucial pour l'analyse des incidents, la responsabilité légale, la conformité réglementaire, etc.

Question 2 : Quel terme est associé à la prévention des actes de malveillance ?

a. La sureté
b. La sécurité
c. La cybercriminalité
d. La vraisemblance

La sécurité consiste à protéger les systèmes, les données et les utilisateurs contre les actions malveillantes, telles que les cyberattaques, les intrusions ou tout autre acte intentionnel ayant pour but de causer des dommages.

Question 3 : Qu'est-ce qu'une vulnérabilité ?

a. C'est une faiblesse de la sécurité du SI, qui peut affecter son fonctionnement normal
b. C'est une cause intentionnelle ou non-intentionnelle qui peut entraîner des dommages sur le SI
c. C'est de rendre un SI inopérant par l'envoi d'une multitude d'injonctions
d. C'est une cause intentionnelle ou non-intentionnelle qui vise à perturber ou arrêter les services d'un SI.

Une vulnérabilité est une faille ou une faiblesse dans le système d'information (SI) qui peut être exploitée par des menaces pour compromettre la sécurité, affectant ainsi la confidentialité, l'intégrité ou la disponibilité du système.
Exemple : faille logicielle
Une application web pourrait avoir une vulnérabilité de type **injection SQL**, où un utilisateur malintentionné pourrait manipuler une requête SQL pour accéder à des données sensibles ou même modifier le contenu de la base de données.

Préparation Examen Cybersécurité 2 BTS SIO SLAM

Question 4 : Qu'est-ce que la vraisemblance dans le contexte de la gestion des risques en cybersécurité ?

a. La capacité à résoudre des incidents
b. La probabilité que la menace se matérialise
c. L'impact potentiel d'une menace
d. Le coût associé à la gestion des risques

Dans le contexte de la gestion des risques en cybersécurité, la vraisemblance correspond à l'évaluation de la probabilité qu'une menace donnée se concrétise et exploite une vulnérabilité présente dans le système.
Exemple : La probabilité qu'une attaque par phishing réussisse dans une entreprise où les employés n'ont pas reçu de formation sur la reconnaissance des courriels suspects.

Si l'entreprise n'a pas de mesures de sensibilisation en place, la vraisemblance que les employés cliquent sur des liens malveillants ou divulguent des informations sensibles serait élevée.

Question 5 : Que signifie l'impact potentiel dans le contexte de la gestion des risques ?

a. La probabilité qu'une menace se matérialise
b. La conséquence ou la gravité d'une menace se matérialisant.
c. Le coût de la mise en place de mesures de sécurité
d. La fréquence à laquelle des menaces se produisent

Dans le contexte de la gestion des risques, l'impact potentiel désigne les conséquences ou les dommages que peut entraîner la réalisation d'une menace, affectant par exemple la disponibilité, l'intégrité ou la confidentialité des systèmes et des données.

Question 6 : Comment appelle-t-on l'action visant à tromper un utilisateur pour l'inciter à communiquer des données personnelles.

a. Déni de service
b. Défiguration
c. Rançongiciel
d. Par point d'eau
e. Hameçonnage

Question 7 : Quelle est l'action malveillante qui vise à rendre les données inaccessibles par le chiffrement de celle-ci

a. Déni de service
b. Défiguration
c. Par point d'eau
d. Rançongiciel
e. Hameçonnage

Question 8 : Quels peuvent être les impacts des risques informatiques (plusieurs réponses) ?

a. L'attraction de nouveau client
b. Une mauvaise image de marque
c. Des pertes financières
d. Des conséquences juridiques par suite d'un non-respect de la réglementation

Question 9 : Identifiez les données à caractère personnel (plusieurs réponses)

a. Code de carte bancaire
b. Mot de passe
c. Conviction religieuse
d. Loisirs
e. Données biométriques
f. Opinion politique

Toutes ces options (a, b, c, d, e, f) sont des données à caractère personnel, mais certaines, comme les convictions religieuses et les opinions politiques, sont considérées comme des données sensibles.
a. Code de carte bancaire : Le code de la carte bancaire est directement lié à une personne physique. Bien qu'il ne fournisse pas directement le nom de la personne, il permet de réaliser des transactions qui peuvent être retracées jusqu'à l'individu propriétaire de la carte.
b. Mot de passe : Le mot de passe est une donnée qui permet d'accéder à un compte personnel. Il est directement associé à une identité spécifique dans le cadre d'une authentification, même s'il ne contient pas d'informations sur l'identité lui-même.
c. Conviction religieuse : Les convictions religieuses sont des informations sensibles, car elles révèlent des aspects intimes de la vie privée d'une personne. Selon le Règlement général sur la protection des données (RGPD), ces informations nécessitent une protection accrue.
d. Loisirs : Les loisirs d'une personne peuvent être considérés comme des données personnelles, car ils permettent d'établir un profil de l'individu. Bien que cette information ne soit pas nécessairement sensible, elle peut contribuer, avec d'autres données, à identifier quelqu'un ou à déduire des aspects de sa vie privée.
e. Données biométriques : Les données biométriques (empreintes digitales, reconnaissance faciale, etc.) sont des informations qui permettent d'identifier de façon unique une personne physique. Elles sont considérées comme des données personnelles sensibles car leur traitement présente un risque accru pour la vie privée.
f. Opinion politique : Comme les convictions religieuses, les opinions politiques sont des données sensibles. Elles peuvent révéler des aspects privés et intimes de la personne, nécessitant une protection particulière sous le RGPD.

Préparation Examen Cybersécurité 2 BTS SIO SLAM

Question 10 : Comment appelle-t-on l'ajout ou le remplacement de pages d'un site WEB, afin de revendiquer un message idéologique

a. Déni de service
b. Défiguration
c. Rançongiciel
d. Hameçonnage
e. Par point d'eau