Concours section : TSIC CN externe Est

Epreuve matière : CAS PRATIQUE Sujet SLSI

15.4 / 20

(Remplir cette partie à l'aide de la notice)

Concours / ~~Examen~~ : Externe - EST Recrutement : TSIC CN

Epreuve : Cas Pratique Spécialité : SLSI Session : 2021

CONSIGNES

- *Remplir soigneusement, sur CHAQUE feuille officielle, la zone d'identification en MAJUSCULES.*
- *Ne pas signer la composition et ne pas y apporter de signe distinctif pouvant indiquer sa provenance.*
- *Numéroter chaque PAGE (cadre en bas à droite de la page) et placer les feuilles dans le bon sens et dans l'ordre.*
- *Rédiger avec un stylo à encre foncée (bleue ou noire) et ne pas utiliser de stylo plume à encre claire.*
- *N'effectuer aucun collage ou découpage de sujets ou de feuille officielle. Ne joindre aucun brouillon.*

1) UEFI : Unified Extensible firmware Interface

Il s'agit du remplaçant du BIOS, dont l'objet est la gestion de bas niveau du matériel, en liaison avec une OS.

Il permet par exemple la sélection des partitions de démarrage, d'activer des options de démarrage (fast boot, secure boot), de régler les paramètres de périphériques (vitesse du ventilateur CPU).

3) Le protocole de la couche application qui permet l'envoi de courriels sur internet est SMTP : Simple Message Transfer Protocol

4) Dans l'ordre croissant des couches OSI :

1- Physique
2- Liaison de données
3- Réseau
4- Transport
5- Session
6- Présentation
7- Application

5) SNMP : Simple Network Management Protocol est un protocole de gestion des équipements informatiques. Il permet d'obtenir des informations sur le fonctionnement d'un équipement réseau connecté au et même de le configurer.

A.1.8..

Concours section : TSIC CN externe Est

Epreuve matière : CAS PRATIQUE Sujet SLSI

15.4 / 20

Par exemple : - récupérer le nombre de copie imprimées pendant une période sur un copieur
- récupérer les erreurs / logs d'un switch

Le protocole implémente un schéma organisationnel des informations et objets (OID), et utilise des agents pour récupérer des informations de manière automatisée (MIB)

6) Open Data : Open → Ouvert
Data → Données
L'open Data est l'usage de collecter des données diverses, habituellement en grande quantité, et de mettre en accès libre à leur consultation.
Site institutionnel : opendata.gouv.fr.

7) DICT : - Disponibilité (des services et données)
- Intégrité (des données)
- Confidentialité (des données)
- Traçabilité (des accès aux services, ressources)

8) - Pierre signe avec sa clé privée le fichier qu'il souhaite envoyer à Sophie
- Pierre chiffre avec la clé publique que Sophie lui a fourni. Elle déchiffrera le message avec sa clé privée

9) Un rançongiciel (Ransomware) est un logiciel malveillant qui va chiffrer toute ou partie des données de la victime, et l'inciter à payer (habituellement en monnaie crypto) pour obtenir la clé de déchiffrement.
Exemple populaire et récent de rançongiciel : Wannacry

.2.1.8..

9) TPM : Trusted Platform Module
(Module de confiance d'une plateforme)

Il s'agit d'un module intégré aux cartes mères permettant de générer de clés uniques, qui vont être utilisés par des OS ou applications.

Par exemple, la solution logiciel de chiffrement Cryhod utilise la puce TPM pour valider le fait que le disque dur (HDD/SSD) chiffré est installé sur la bonne plateforme. Cela évite les tentatives de déchiffrement sur une autre plateforme.

- les clés générées par la puce TPM peuvent être exportées
- les clés comporte différents niveaux d'algorithme de chiffrement
- la rétrocompatibilité des logiciels utilisent des versions récentes (TPM 2.0 → TPM 1.2)

2)

Cas 1 :

1) La gestion électronique de documents (GED) est un système permettant de centralisé, répertorié, sécurisé les données et leurs accès.

Elle se compose de services suivants :

- Gestion des permissions pour les accès (lecture et modif)
- Traçabilité des accès (lecture et modif)
- Sauvegarde et intégrité des données
- Chiffrement possible des données.
- Accès en ligne des documents.

2) Pour les différents type d'hébergement :

- type public : solution cloud comme AWS, Azure, google cloud, OVH cloud
- type privé : hébergement sur des serveurs de la société / administration
- type hybride : communication entre le type privé et public. Authentification sur le partie privée avec redirection vers l'hébergement public par exemple.

Solution d'hébergement choisi : type privé.
Dans un cadre de gouvernance numérique lié à des documents traités et détenus par un service de l'Etat, le fait de concéder l'hébergement et la sauvegarde des données à un tiers / une société privée, pourrait compromettre la sécurité des données en question.
Le cloud a pour avantage de minimiser très largement des coûts d'infrastructure, cependant cette gestion est invisible et inaccessible au client, il est donc difficile d'auditer la sécurité de l'infrastructure.

Concours section : TSIC CN externe Est

Epreuve matière : CAS PRATIQUE Sujet SLSI

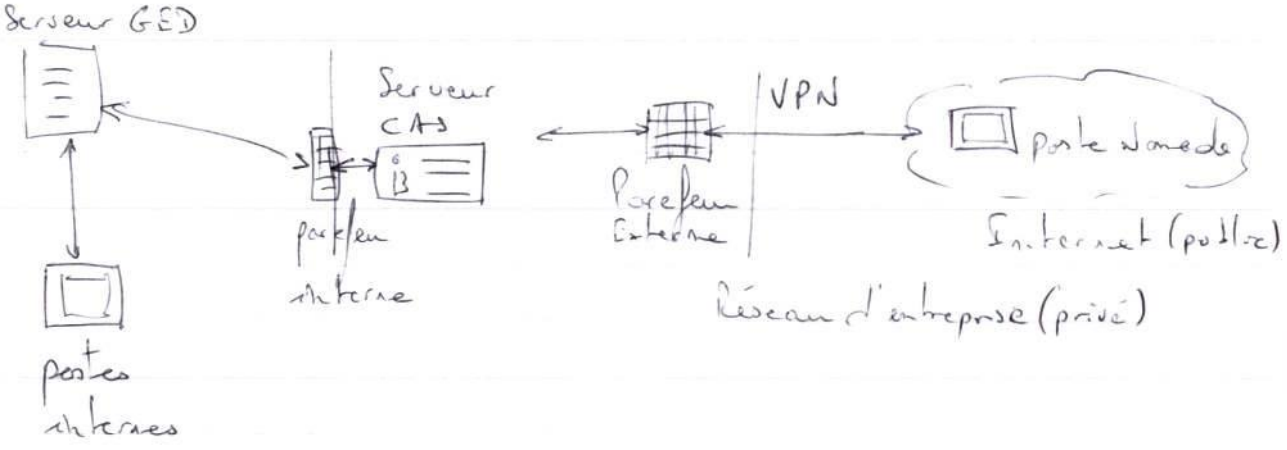
15.4 / 20

(Remplir cette partie à l'aide de la notice)
Concours / Examen : Externe - Est **Recrutement :** TSIC CN
Epreuve : Cas pratique **Spécialité :** SLSI **Session :** 2021

CONSIGNES
- *Remplir soigneusement, sur CHAQUE feuille officielle, la zone d'identification en MAJUSCULES.*
- *Ne pas signer la composition et ne pas y apporter de signe distinctif pouvant indiquer sa provenance.*
- *Numéroter chaque PAGE (cadre en bas à droite de la page) et placer les feuilles dans le bon sens et dans l'ordre.*
- *Rédiger avec un stylo à encre foncée (bleue ou noire) et ne pas utiliser de stylo plume à encre claire.*
- *N'effectuer aucun collage ou découpage de sujets ou de feuille officielle. Ne joindre aucun brouillon.*

3) - Pour permettre un accès en mobilité, les postes nomades (pc portables habituellement) peuvent être équipés et utiliser un VPN (Virtual Private Network) pour accéder depuis un réseau public au réseau interne de l'entreprise/administration.
Les données sont chiffrées lors de la connexion.

- l'authentification pourra être faite avec un portail SSO (single signed on) avec une authentification forte par exemple (carte à puce + certificat + code p.in) et redirection vers le service de GED.



4) + la mise en place ou achat du matériel par l'administration publique doit passés par des marchés publics ; type accord-cadre à bons de commande ; Marché à procédure adaptée selon les coûts et besoin, par exemple. Le fait de mettre en place ce ou ces marchés, peut avoir des délais long jusqu'à son exécution (plusieurs mois)
+ la structure devra faire l'objet de qualification avant mise en production (plusieurs mois)

.5./.8..

15.4 / 20

+ le personnel (usagers et techniciens) devront être formés (délai et coût)
+ les imprévus exceptionnel (délai) comme une crise sanitaire (Covid-19)
+ une mauvaise étude du besoin : sur ou sous-dimensionnement des serveurs par rapport au nombre de connexion (qualité et coût)
+ manque de disponibilité du matériel par les fabricants (délai).

Cas 2 :

1) le CMS recommandé : Joomla. D'après l'extrait du CCT, la version 3.x a été qualifiée pour être utilisée spécifiquement pour la création de site intranet institutionnel. De plus, c'est la DINUM qui en assure l'hébergement, ce sera donc plus aisé pour la configuration et maintenance. (étant affecté en tant que technicien à la DINUM)

- les fonctionnalités principales d'un CMS :
  - Administration simplifiée des rôles (éditeur, administrateur, relecteur)
  Il n'est pas nécessaire de faire la jonction (bootstrapping) entre les pages web et la BDD
  - Une interface WYSIWYG (what you see is what you get), l'édition d'un article se fait comme sous un éditeur de texte (word ou writer) et donc pas besoin de connaissance technique
  - Aggrégation des statistiques (consultations)
  - fonctionnalité des recherches

- Optimisation des recherches (SEO) et indexation
- Intégration aisée de fonctionnalités développées en interne ou externe (modules)
- Gestion facilitée des différents types de médias (vidéo, sons, texte)
- Sauvegarde des données
- Organisation du contenu par critères (date, objet)
- Création de thème CSS

2)
```
<H3> Titre 1 </H3>
    <p> Lorem ... </p>
<H3> Titre 2 </H3>
    <p> Aliquam ... </p>
<H3> Titre 3 </H3>
    <p> Donec est diam... </p>

<H1> Titre </H1>
  <p> Morbi sollicitudin [...]
      [...] <a href="#"><img src="Ministere de l'interieur.
      -png" alt="logo du Ministère de l'intérieur"/></a>
  </p>

  <p> Cette image n'est pas importante ...
      <a href="#"><img src="accueil.png" alt=""/></a>
  </p>
```

3) * Protocole HTTPS : est la version sécurisée de HTTP (Hyper text transfer protocol). Lorsqu'un client requête une adresse web (url), une communication est établie entre le client et le serveur. Cette communication est en clair avec HTTP et donc non sécurisé.
SSL / TLS permettent d'encapsuler cette communication en la chiffrant, et rend (en théorie) quasiment toute interception du trafic.

..7.1.8..

* Des organismes de confiance (OCSP) gère des certificats SSL. Ils peuvent être payants ou gratuits et possèdent différents niveaux de sécurité en fonction du statut et de l'identité du demandeur.
On peut également créer ses propres certificats et être son propre gestionnaire (IGC)
Les certificats sont ensuites intégrés dans les OS, navigateurs, registre de certificats, applications.

* En HTTPS sont garantis deux choses:
  - l'identité de l'émetteur du certificat
  - la sécurité, par chiffrement, des données transmises.