TD Chapitre 10

Quizz

Q1- La disponibilité d'un système d'information correspond à

A- La capacité de ce système à répondre rapidement o
B- Le fait que ce système a un DSI à sa tête o
C- Le fait que le système d'information soit accessible et utilisable o
D- Le fait que le SI demande un mot de passe pour l'accès o

Q2- Un virus informatique

A- A un code source public o
B- Est développé dans le but de nuire o
C- Utilise un autre programme pour se diffuser o
D- Se repère par sa signature o

Q3- Un antivirus

A- Scanne le disque dur de manière régulière o
B- Observe les adresses IP des paquets qui entrent dans le système o
C- Doit être mis à jour régulièrement o
D- Peut empêcher le fonctionnement correct de certains logiciels o

Q4- Une attaque par déni de service

A- Consiste à faire disparaître les applications d'un système pour que les utilisateurs ne puissent plus les accéder. o
B- Consiste à saturer un système de manière à ce qu'il ne puisse plus répondre de manière normale. o
C- Consiste à ce qu'un pirate se fasse passer pour un prestataire de service et en profite pour voler des données. o
D- Peut empêcher le fonctionnement correct de certains logiciels o

Q5- Les responsables de la sécurité du SI

A- Doivent régulièrement se former et s'informer o
B- Doivent assurer une rotation de manière à ce qu'il y ait une présence permanente o
C- Doivent réaliser des audits sécuritaires o
D- Travaillent indépendamment des autres salariés o

Q6- Parmi les organismes suivants, lesquels sont des ressources pour la sécurité informatique :

A- Club de Sécurité de l'Information Français - CLUSIF o
B- Agence Nationale de la Sécurité des SI - ANSII o
C- Autorité de régulation des télécommunication -ARCEP o
D- Commission Nationale Informatique et Libertés - CNIL

Q7- Pour réaliser un audit de sécurité

A- Il faut s'adresser à un organisme externe - CLUSIF o
B- Agence Nationale de la Sécurité des SI - ANSII o
C- Autorité de régulation des télécommunication -ARCEP o
D- Commission Nationale Informatique et Libertés - CNIL o

Q8- Une zone démilitarisée

A- Permet de gérer différents niveaux de sécurité au sein d'une organisation. o
B- Contient les serveurs de l'entreprise qui doivent pouvoir être accédés depuis l'extérieur du réseau o
C- Est gérée par un antivirus o
D- Est gérée par un firewall o

Q9- La signature d'une charte informatique par le salarié
A- Permet de le sanctionner s'il ne respecte pas les engagements qu'il a pris dans ladite charte o
B- Est un substitut au règlement intérieur de l'entreprise o
C- Permet d'informer le salarié des comportements qu'il convient de tenir ou d'éviter o

Q10- La notion d'intégrité
A- Correspond au fait que des données et des applications ne sont pas corrompues o
B- Garantit la source de l'information o
C- Indique que les personnels d'un SI sont honnêtes. o
D- Indique que l'administrateur d'un SI a un casier vierge. o

Q11- Un firewall
A- Peut empêcher le bon fonctionnement de certaines applications o
B- Scanne les applications disponibles sur la machine pour trouver des virus o
C- Peut-être configuré par l'utilisateur o
D- On peut ne pas mettre de firewall si on a un antivirus. o

Q12- La technologie RAID
A- Est une technologie pour auditer la sécurité des systèmes d'information o
B- Est une technologie pour échanger des messages sécurisés o
C- Est une technologie pour optimiser les sauvegardes en utilisant plusieurs disques durs. o

Q13- Si Agnès a une clé publique d'encryption et que Daniel a la clé privée de décryption correspondante
A- Agnès peut envoyer des messages cryptés à Daniel o
B- Daniel peut envoyer des messages cryptés à Agnès o

Q14- Si Agnès a une clé publique de decryption et que Daniel a la clé privée d'encyprtion correspondante
A- Agnès peut envoyer des messages cryptés à Daniel o
B- Daniel peut envoyer des messages cryptés à Agnès o
C- La situation est dangereuse et un pirate pour retrouver la clé privée d'encryption à partir de la clé publique de decryption o
D- Daniel pourrait envoyer des messages et Agnès pourra s'assurer qu'il en est bien l'auteur o

Q15- Quelles sont les affirmations vraies concernant la sauvegarde ?
A- La technologie RAID permet de mieux gérer les droits des utilisateurs o
B- La technologie RAID permet d'optimiser la vitesse et la robustesse du système de sauvegarde o
C- On peut recourir à un prestataire externe pour la sauvegarde des données o
D- Les clés USB modernes ont de grandes capacités de stockage et peuvent à ce titre constituer des supports de sauvegarde intéressants. o
E- La conception de la sauvegarde d'une organisation doit prendre en compte les événements qui ont une faible probabilité de survenir o

Q16- La non répudiation
A- Garantit qu'une personne ne soit pas déconnectée abusivement d'un système o
B- Correspond au fait que les ressources d'un système sont constamment disponibles. o
C- Prouve qu'un personne a pris part à une transaction. o

Questions
1- Pourquoi conserver des fichiers de logs sur les connexion des utilisateurs ?
2- Comment fonctionne un cheval de Troie ?
3- Donner des exemples d'usages abusifs d'un système d'information.

Cas 1 : intrusion réseau / Dell

Dell victime d'une intrusion informatique Par L'agence EP | Jeudi 29 Novembre 2018, vu sur zdnet.fr

Dell vient de révéler avoir été visé par une intrusion sur son réseau informatique cherchant à extraire des données clients depuis son site Dell.com (noms, adresses e-mail et mots de passe hachés). L'attaque a été détectée le 9 novembre, visiblement le jour où elle s'est produite, et le constructeur texan dit avoir immédiatement pris les mesures nécessaires pour la contrer. "Bien qu'il soit possible qu'une partie de cette information (les données clients, ndlr) ait été supprimée du réseau de Dell, nos enquêtes n'ont trouvé aucune preuve concluante qu'elle en ait été extraite", indique l'entreprise dans un communiqué.

Dell assure que ni les données liées aux cartes de crédit ni d'autres informations sensibles n'ont été affectées. Mais rien n'est dit concernant l'ampleur de cette attaque et la quantité de données potentiellement "supprimées" du réseau. Dell dit avoir immédiatement pris plusieurs mesures : réinitialisation de tous les mots de passe clients sur Dell.com, appel à une société indépendante pour mener l'enquête et signalement aux forces de l'ordre.

Une page d'information détaillant l'incident et fournissant des conseils pour créer un mot de passe fort a également été mise en ligne. (Eureka Presse)

1- Quels sont les principes de la sécurité informatique qui ont été remis en question ici ?
2- Pourquoi faire appel à une société indépendante pour mener l'enquête ?
3- Que pourrait-on recommander à l'entreprise Dell ?

Cas 2 : Areva victime d'une intrusion informatique

Le Monde avec AFP Publié le 30 septembre 2011 à 09h55 - Mis à jour le 30 septembre 2011 à 11h14

Le groupe Areva a été victime d'une attaque informatique qui l'a contraint à renforcer la sécurité de ses réseaux. "On a subi une attaque et c'est pour cela que nous avons pris des mesures de renforcement de nos systèmes de sécurité avec le support de l'Agence nationale de la sécurité des systèmes d'informations [Anssi]", a déclaré jeudi 29 septembre à l'Agence France-Presse, une porte-parole du groupe nucléaire.

L'Anssi est un organisme de l'Etat français chargé de la sécurité informatique, rattaché au secrétariat général de la défense et de la sécurité nationale, dépendant lui-même des services du premier ministre. Selon la porte-parole d'Areva, il y a eu un "accès frauduleux" au "réseau commun d'infrastructure, un réseau qui permet l'échange d'informations non critiques entre les différentes entités du groupe".

DES INFORMATIONS SENSIBLES DÉROBÉES ?

Interrogée sur un possible impact sur les activités militaires d'Areva, la porte-parole a dit que le réseau attaqué portait sur "des informations non critiques et pas sur des informations sensibles".

Mais d'après le site Web du mensuel économique L'Expansion, qui a révélé l'affaire et cite des sources internes, Areva a été victime d'une intrusion "de grande ampleur", qui s'est traduite par trois jours de renforcement des mesures de sécurité autour du 16 septembre. L'Expansion évoque au conditionnel une "origine asiatique" de ces intrusions qui "dureraient depuis deux ans".

Quelle(s) procédure(s) l'entreprise devrait elle revoir au vu de l'intrusion dont elle a été victime.

Cas 3 : Manipulation de BD

Un stagiaire recruté dans une cellule de recrutement de patrimoine se voit charger de supprimer les comptes des clients décédés il y a plus d'un an (délai de conservation légale). A ce titre, et parce qu'il sait maîtriser le langage SQL, on lui fournit un accès à la base de données centrale qui se compose notamment des tables suivantes :

CLIENT(idClient, nomCli, prenCli, dateNaissance, tel, mail, dateDeces)
COMPTE(numCompte, dateOuverture, dateFermeture, #idClient)

Le stagiaire exécute la commande suivante :

```
DELETE FROM Compte
WHERE idClient IN (SELECT idClient FROM Client WHERE dateDeces IS NOT NULL)
```

1) Que produit cette requête ? Quelles sont ses conséquences néfastes ?
2) Comment aurait-on pu rendre le système résilient à l'erreur du stagiaire ?

Cas 4 : Un cas de déni de service.

Telegram victime d'une cyberattaque, la Chine accusée Publié le 13 juin 2019 à 12h35

La messagerie cryptée Telegram a été victime d'une cyberattaque majeure qui semble provenir de Chine, a annoncé jeudi 13 juin son cofondateur sur Twitter, faisant le lien avec les troubles politiques en cours à Hong Kong.

L'application a été largement utilisée ces derniers jours par les manifestants à Hong Kong pour échapper à la surveillance en ligne et coordonner leurs actions contre un projet de loi controversé visant à autoriser les extraditions vers la Chine continentale.

L'ancienne colonie britannique a été ébranlée mercredi par les pires violences politiques depuis sa rétrocession à la Chine en 1997, la police ayant tiré des balles en caoutchouc sur les manifestants qui bloquaient les grandes artères de la ville et tentaient de pénétrer dans le Parlement.

Telegram a annoncé mercredi soir subir une « puissante » attaque par déni de service (DDoS) – qui consiste à inonder un serveur de requêtes inutiles pour le submerger – et indiqué que de nombreux utilisateurs pourraient rencontrer des problèmes de connexion.

Ces requêtes provenaient principalement de Chine, selon le cofondateur russe de Telegram, Pavel Durov, qui a fait le lien avec la situation à Hong Kong.

« Historiquement, toutes les attaques DDos que nous avons rencontrées en provenance d'un acteur étatique de par leur taille (200-400 Gb/s de requêtes inutiles) ont coïncidé avec des manifestations à Hong Kong (organisées via @telegram) », a-t-il indiqué sur Twitter. « Ce n'était pas une exception. »

Telegram a par la suite publié une série de tweets pour expliquer la nature de l'attaque.

« Imaginez qu'une armée de lemmings saute la file d'attente devant vous chez McDonald's – et que chacun commande un Whopper », a expliqué la messagerie, faisant référence au produit phare de l'enseigne concurrente Burger King. « Le serveur est occupé à expliquer aux lemmings qu'ils sont au mauvais endroit mais ils sont si nombreux que le serveur ne peut même pas vous voir pour prendre une commande. »

Interrogé à ce sujet, le ministère chinois des Affaires étrangères a affirmé jeudi « ne pas être au courant ». « La Chine s'est toujours opposée à toute forme de cyberattaque » et « est également victime de cyberattaques », a indiqué lors d'un point de presse le porte-parole de la diplomatie, Geng Shuang.

Basée à Dubaï, la messagerie Telegram, utilisée par plus de 200 millions d'utilisateurs dans le monde, offre une confidentialité élevée pour l'échange de messages texte, de photos et de vidéos et permet d'effectuer des appels vocaux cryptés. Ses « chaînes » permettent également à un utilisateur de diffuser des messages à un grand nombre d'abonnés.

1- Qu'est ce que Telegram ? Par qui a été fondée cette application ?

2- Résumer l'attaque qu'a subi Telegram.

3- Comment comprendre les motivations du gouvernement chinois mis en cause par le fondateur de Telegram ?