

**INF-AX1-MA  
Sécurité des technologies de l’information  
Principaux enjeux de la sécurité**

**Groupe 21609  
Travail pratique En équipe de 2 ou 3 étudiants  
Pondération 20% de la note finale  
Date de remise Vendredi, 10 mars 2023 (en fin de journée)**

**Grille d’évaluation**

|  |  |
| --- | --- |
| **Description** | **Note** |
| Partie 01 -- **Définitions** | 03,0 |
| Partie 02 -- **BYOD** | 05.0 |
| Partie 03 -- **Identification des menaces** | 12,0 |
| **Total :** | **20,0** |

Noms  Johns Roberto Perrier

Mario Arturo

**Louis Savard, M. Ing. TI  
AEC en Gestion de réseaux et sécurité des systèmes**Formation continue  
Collège de Maisonneuve  
3800, rue Sherbrooke est  
Montréal (Québec)  
H1X 3M3

**Partie 01  
Définitions**

**Question 01**Pour chacun des enjeux, donnez votre propre définition, puis trouvez un exemple d’attaque.

|  |  |  |
| --- | --- | --- |
| **Enjeu** | **Définition** | **Exemple** |
| **Intégrité** | C’est le fait de garantir que les données sont bien celles que l’on croit être. Ils ne subissent aucun changement. | Quand on supprime ou modifie intentionnellement ou non des données. Une attaque de type homme du milieu, c’est quand un attaquant modifie le contenu du message après son envoie, mais avant sa réception par le destinataire. |
| **Confidentialité** | C’est le fait de rendre l’information inintelligible a d’autre personne que les seuls destinataires. | Papier confidentiels mis a la poubelle peuvent être récupéré par un membre du personnel malveillant. |
| **Disponibilité** | C’est le fait de garder le bon fonctionnement de l’information. | Attaque par déni de service (DoS) et par déni de service distribué (DDoS) qui empêchent les utilisateurs légitimes d’accéder a la ressource en envoyant une quantité écrasante de données au serveur cible saturant ainsi le processeur, la mémoire et les disques. |
| **Imputabilité** | Est la capacité a identifier qui est responsable d’une violation de sécurité et de la protéger contre des attaques illégales ou des intrusions de la part de tierces personnes. | L'interception ou la modification des messages d'authentification, d'autorisation ou de certification pour usurper l'identité ou les privilèges d'un utilisateur ou d'un système. |
| **Authentification** | C’est le fait de s’assurer de l’identité d’un utilisateur. | Attaque par hameçonnage |
| **Traçabilité** | C’est être capable lors de la moindre attaque d’avoir le plus information possible sur les failles de sécurité. Ou encore capable a retrouver l’historique, l’utilisation et la localisation d’une entité au moyen d’identifications enregistrés. | La falsification des enregistrements de journalisation pour tromper les enquêteurs ou les outils de détection d’intrusion |

**Partie 02  
BYOD**

**Question 02.1**Expliquez ce qu’est le BYOD.

Bring Your Own Devise est une pratique qui consiste à autoriser les employés à utiliser leurs appareils personnels pour l’accès aux données et applications professionnelles.

**Question 02.2**Quels sont les avantages du BYOD?   
Pourquoi est-ce si populaire ?

Les avantages de BYOD

Plus grande productivité : les employés disposants de matériel informatique personnel sont plus à l’aise et maitrise mieux leur environnement de travail. Réduction des couts : les entreprises économisent sur les couts d’achats, de maintenance et d’entretien liés a des matériels et logiciels informatiques couteux. Flexibilité : les employés peuvent travailler n’importe où et à tout moment, ce qui favorise leur motivation et leur productivité.

Pourquoi le BYOD est si important

Parce qu’il permet aux employés de travailler plus efficacement et plus intelligemment. En plus de ça, les avantages du BYOD incluent des économies de couts et des gains de productivités.

**Question 02.3**En quoi le BYOD constitue une menace pour les entreprises ?

Parce qu’il augmente le risque de fuite de données et peut faciliter le piratage des réseaux de l’entreprise. Les employés qui utilisent leurs propres appareils pour l’accès au réseau de l’entreprise ne sont pas soumis à la même rigueur que les appareils d’entreprises autorisés.

**Question 02.4**En tant qu’administrateurs, quels seraient vos conseils à une entreprise qui voudrait adopter le BYOD ?

1 – Mettez en place un code de conduite clair. Cela devrait inclure des directives pour la responsabilité des appareils, le partage des données, la sécurité et les politiques de soutient.

2 – Assurez vous que vos stratégies de sécurité s’appliquent aux appareils personnels ainsi qu’aux appareils professionnels.

3 -Mettez en ouvre des solutions de sécurité adaptatives et des outils de contrôles de données qui garantissent que les données sont cryptées et sécurisées sur chaque appareils.

4 -Établissez une plate-forme de gestion des appareils mobile ou une console de BYOD qui vous permettra de gérer l’inventaire des appareils et déployer les applications de manière uniforme.

**Question 01.5**Vous êtes le patron d’une entreprise.   
Donnez trois exemples de mesures visant à sécuriser votre réseau concernant les postes nomades.

1 – Utiliser des solutions de chiffrement et de sécurité pour protéger les données contre la perte, le vol et l’accès non autorisé. Les solutions de sécurité telles que l’identification a deux facteurs et les solutions de chiffrement des disques sont particulièrement importantes pour les postes nomades car les données sont plus susceptibles d’être volées ou perdues.

2 – Configurer des points d’accès sécurisés pour permettre l’accès a des outils spécifiques. Ils ne devraient permettre uniquement l’accès aux outils nécessaire pour le travail.

3 – Développer des politiques et procédures visant à limiter l’accès aux données sensibles, en plus de définir clairement les exigences de chiffrement, il est important que les utilisateur comprennent et respectent les protocoles de sécurité.

**Partie 03  
Identification des menaces**

Détailler les sources et la vraisemblance des menaces.  
**Sources de menaces externes**

* **Développeurs**
* **Script**
* **Enfants**
* **Pays et** **états**
* **Espionnage** **industriel**
* **Criminels**
* **Hacktivisme**

**Sources de menaces internes**

* **Employés** **mécontents**
* **Entrepreneurs voyous** **(Rogue)**
* **Employés qui éprouvent des difficultés** **financières**   
  (financés par des gens sans scrupules)

**Vraisemblance**

* **Minime** ;
* **Significative** ;
* **Forte**   
  ou
* **Maximale**.

**Question 03 – BYOD**

|  |  |  |
| --- | --- | --- |
| **Menaces 01 concernant le BYOD** | | |
| **Menace**  Perte ou vol de l'appareil | **Vraisemblance**  Significative : Si l'appareil personnel d'un employé est perdu ou volé, cela peut mettre en danger les données de l'entreprise stockées sur cet appareil. | **Réponse et/ou Contre-mesures**  Utiliser des solutions de chiffrement et de sécurité pour protéger les données contre la perte, le vol et l`accès non autorisé . |

|  |  |  |
| --- | --- | --- |
| **Menaces 02 concernant le BYOD** | | |
| **Menace**  Utilisation de réseaux non sécurisés | **Vraisemblance**  Forte : Les employés qui utilisent leurs propres appareils pour accéder aux réseaux de l'entreprise peuvent se connecter à des réseaux non sécurisés (comme des réseaux Wi-Fi publics), ce qui augmente le risque d'attaques de type man-in-the-middle ou d'interception de données sensibles. | **Réponse et/ou Contre-mesures**  Mettre en place un système de gestion des droits d`accès, par le biais d`un pare-feu et d`un serveur d`authentification |

|  |  |  |
| --- | --- | --- |
| **Menaces 03 concernant le BYOD** | | |
| **Menace**  Utilisation d'applications non approuvées | **Vraisemblance**  Significative : Les employés peuvent télécharger des applications non approuvées sur leurs appareils personnels, ce qui peut potentiellement compromettre la sécurité des données de l'entreprise | **Réponse et/ou Contre-mesures**  -Utiliser des outils de contrôle d`accès, tels que des stratégies de groupe et des listes de contrôle d`accès (ACL). D`autres mesures comprennent la mise en œuvre de pare-feu, des systèmes d`authentification forte, des mise a jour automatique et un traçage des modifications |

**Question 04 – Rançongiciels**Donner trois exemples de rançongiciels (exemples d'actualité).

Décrire le fonctionnement (ex : réception courriel, exécution code malveillant, communication avec Command and Control du Pirate, …)   
et   
les impacts sur l'entreprise (arrêt de service, exfiltration de données, perte de productivité, impact sur les clients, ...)

|  |  |  |
| --- | --- | --- |
| **Rançongiciels 01** | | |
| **Fonctionnement**  Ryuk : Est un rançongiciel sophistiqué utilisé pour cibler des organisations et des entreprises de grande envergure. Il est souvent propagé via des courriels de phishing contenant des pièces jointes malveillantes. Une fois que Ryuk infecte un système, il utilise un chiffrement fort pour chiffrer les fichiers de la victime, puis demande une rançon importante en échange de la clé de déchiffrement. | **Impact**  Les impacts peuvent inclure l'arrêt de service, la perte de données critiques et une forte demande de rançon qui peut nuire à la situation financière de l'entreprise | **Réponse et/ou Contre-mesures**  -Utilisation d'un logiciel de sécurité de qualité : l'utilisation d'un logiciel de sécurité de qualité peut aider à détecter les attaques de Ryuk et à empêcher leur propagation.  -Utilisation d'un pare-feu efficace : l'utilisation d'un pare-feu efficace peut aider à bloquer les connexions suspectes et à protéger le système contre les attaques de Ryuk. |

|  |  |  |
| --- | --- | --- |
| **Rançongiciels 02** | | |
| **Fonctionnement**  Sodinokibi, également connu sous le nom de REvil, est un rançongiciel qui utilise des vulnérabilités de sécurité connues pour infecter les systèmes. Il utilise ensuite un chiffrement fort pour chiffrer les fichiers et les données de la victime et exige une rançon importante en échange de la clé de déchiffrement. Sodinokibi est souvent diffusé via des kits d'exploitation de logiciels malveillants, des courriels de phishing et des logiciels de téléchargement malveillants | **Impact**  Les impacts peuvent inclure une perte de productivité, des temps d'arrêt prolongés et une forte demande de rançon. | **Réponse et/ou Contre-mesures**  Surveiller l'activité du réseau : la surveillance de l'activité du réseau peut aider à détecter les activités suspectes et à identifier rapidement les attaques de Sodinokibi. |

|  |  |  |
| --- | --- | --- |
| **Rançongiciels 03** | | |
| **Fonctionnement**  Maze : Ce rançongiciel est souvent distribué via des e-mails d'hameçonnage et des logiciels malveillants téléchargés depuis des sites web compromis | **Impact**  Les impacts peuvent inclure la perte de données critiques et la violation de la confidentialité des clients. | **Réponse et/ou Contre-mesures**  Pour se protéger contre Maze, il est important de sensibiliser les utilisateurs aux risques de sécurité et de mettre en place des politiques de sécurité pour empêcher l'installation de logiciels non autorisés |

|  |  |  |
| --- | --- | --- |
| **Rançongiciels 04** | | |
| **Fonctionnement**  GandCrab : Ce rançongiciel est généralement distribué via des campagnes de phishing et des kits d'exploitation de vulnérabilités | **Impact**  -Temps d'arrêt : Les opérations commerciales peuvent être affectées en raison de la perte de données et de la restauration des systèmes, ce qui peut entraîner des temps d'arrêt coûteux pour l'entreprise.  -Le rançongiciel GandCrab a des impacts significatifs sur les victimes. Lorsque le rançongiciel infecte un système, il chiffre les fichiers de l'utilisateur et demande ensuite le paiement d'une rançon pour fournir la clé de déchiffrement. | **Réponse et/ou Contre-mesures**  Pour éviter GandCrab, il faut maintenir à jour votre logiciel et votre système d'exploitation, et utiliser un logiciel antivirus de qualité pour détecter les menaces |

**Question 05 – Télétravail**Détailler les sources et la vraisemblance des menaces portant sur le **télétravail**.

|  |  |  |
| --- | --- | --- |
| **Menaces concernant le télétravail** | | |
| **Menace**  Vol de données : Les employés en télétravail peuvent être tentés de voler des données confidentielles de l'entreprise pour leur propre bénéfice | **Impact**  Cela peut entraîner une violation de données et des problèmes de conformité. | **Réponse et/ou Contre-mesures**  La contre-mesure consiste à mettre en place des politiques de sécurité solides, à surveiller les activités suspectes des employés et à mettre en place des contrôles d'accès et de séparation des tâches |

|  |  |  |
| --- | --- | --- |
| **Menaces concernant le télétravail** | | |
| **Menace**  Accès non autorisé au réseau : Les employés en télétravail peuvent se connecter à des réseaux non sécurisés ou utiliser des appareils personnels pour accéder aux données de l'entreprise. | **Impact**  Cela peut entraîner une violation de données et des problèmes de conformité | **Réponse et/ou Contre-mesures**  La contre-mesure consiste à mettre en place des politiques de sécurité solides et à fournir des connexions VPN pour les employés en télétravail |

|  |  |  |
| --- | --- | --- |
| **Menaces concernant le télétravail** | | |
| **Menace**  Logiciels malveillants : Les logiciels malveillants peuvent infecter les appareils des employés en télétravail, qui peuvent ensuite accéder aux données de l'entreprise. | **Impact**  Les conséquences peuvent inclure la perte de données et la propagation de logiciels malveillants à travers l'ensemble de l'entreprise | **Réponse et/ou Contre-mesures**  La contre-mesure consiste à fournir des logiciels de sécurité à jour sur les appareils des employés et à mettre en place des politiques de sécurité solides |

**Question 06**Détailler les sources et la vraisemblance des menaces portant sur les **appareils d’inter-réseautage**.

|  |  |  |
| --- | --- | --- |
| **Menaces concernant les appareils d’inter-réseautage (concentrateur, commutateur et routeur)** | | |
| **Menace**  Attaques par déni de service (DDoS) : Les attaques DDoS peuvent surcharger les appareils inter-réseautages, les rendant indisponibles pour les utilisateurs légitimes | **Impact**  Cela peut avoir un impact sur la disponibilité des services et la productivité de l'entreprise | **Réponse et/ou Contre-mesures**  La contre-mesure consiste à mettre en place des dispositifs de protection contre les attaques DDoS et à surveiller en temps réel le trafic réseau. |

|  |  |  |
| --- | --- | --- |
| **Menaces concernant les appareils d’inter-réseautage (concentrateur, commutateur et routeur)** | | |
| **Menace**  Attaques de type man-in-the-middle (MITM) : Les attaques MITM visent à intercepter les données transitant entre les appareils inter-réseautages et à les modifier ou à les voler | **Impact**  Cela peut entraîner une violation de données et des problèmes de confidentialité | **Réponse et/ou Contre-mesures**  La contre-mesure consiste à utiliser des protocoles de communication sécurisés et à mettre en place des contrôles d'accès et d'authentification |

|  |  |  |
| --- | --- | --- |
| **Menaces concernant les appareils d’inter-réseautage (concentrateur, commutateur et routeur)** | | |
| **Menace**  Accès non autorisé : Les pirates peuvent accéder aux appareils inter-réseautages en utilisant des identifiants volés ou des techniques d'ingénierie sociale. | **Impact**  Cela peut entraîner une violation de données et des problèmes de confidentialité. | **Réponse et/ou Contre-mesures**  La contre-mesure consiste à mettre en place des politiques de sécurité solides et à fournir une formation régulière aux employés sur les risques de sécurité. |