Scénarios et tactiques de sécurité

[1.Personne non autorisée tente de retirer de l’argent à un compte du GAB à l’aide d’une carte volé.](#_30j0zll)

[Tactique: Detect Intrusion – Athenticate Actors – Lock Access – Maintain Audit Trail](#_1fob9te)

[2.Un employé mécontent vole de l’information à l’entreprise](#_3znysh7)

[Tactique: Encrypt important data](#_2et92p0)

[3.Un hacker chinois envoie un attaque Distributed Denial of Service aux serveur de l’entreprise](#_tyjcwt)

[Tactique: Inform actors](#_1t3h5sf)

[4.Un utilisateur attaque le serveur transactionnel par “brute force”](#_2s8eyo1)

[Tactique: Detect Intrusion](#_17dp8vu)

[Tactique: Inform Actors](#_26in1rg)

[Tactique: Restore](#_lnxbz9)

[5.Un voleur essaye de se connecter au compte d’un client avec une carte de débit volé.](#_35nkun2)

[Tactique: Détecter l’intrusion](#_1ksv4uv)

[Tactique: Authentifier les acteurs](#_44sinio)

[Tactique: Verrouiller le compte du client](#_2jxsxqh)

[Tactique: Maintenir une trace d’audit](#_z337ya)

[6.Un employé essaye de voler de l’argent lorsqu’il est en train de remplir le guichet.](#_3j2qqm3)

[Tactique: Identifier les acteurs](#_1y810tw)

[Tactique: Informer les acteurs](#_2xcytpi)

[Tactique: Maintenir une trace d’audit](#_3whwml4)

[7.Prévenir vol de PIN](#_1pxezwc)

[Tactique: Encrypt Data](#_2p2csry)

[Tactique: Verify Message Integrity](#_3o7alnk)

[Tactique: Detect Intrusion](#_23ckvvd)

[8.Un utilisateur entre un NIP invalide 3 fois.](#_ihv636)

[Tactique: Revoke access](#_32hioqz)

| **Scénario** | 1. Une personne non autorisée tente de retirer de l’argent à un compte du GAB à l’aide d’une carte volé. |
| --- | --- |
| **objectifs d'affaires** | Rendre le compte hors d’usage si la double vérification d’un retrait à échoué |
| **Source** | Voleur de carte |
| **Stimulus** | Accès au système de retrait du GAB afin de retirer de l’argent |
| **Artéfact** | Argent du détenteur du compte |
| **Environnement** | GAB connecté à un réseau |
| **Réponse** | Argent du compte et services du GAB bloqué du à l’identification d’un accès non autorisé |
| **Mesure de la réponse** | A quel point le solde du compte bancaire a-t-il été affecté lors de l’attaque |
| **Questions** | 1. Qu’est-ce qu’on sous-entend par « double vérification » ? 2. De quelle manière rendra-t-on le compte hors d’usage ? 3. Doit-on considérer les achats frauduleux au même titre qu’un retrait au GAB? |

### Tactique: Detect Intrusion – Athenticate Actors – Lock Access – Maintain Audit Trail

**Description & Justification**: La détection de l’intrusion se fera à l’aide de la géolocalisation du GAB utilisé. Si deux utilisations successives de la carte sont distancées de plusieurs villes, le système lèvera un « flag ». Ce flag sera utilisé pour une double-vérification qui identifierait la personne via SMS qu’une transaction a eu lieu. Si la vérification de localisation ainsi que l’identification échouent, alors nous utiliserons le lock accès qui rendra le compte inutilisable. Le système s’occupera de garder une trace des dernières transactions louches pour vérification ultérieur (footage vidéo des GAB, localisation, montant de transaction, etc.).

| **Scénario** | 2.Un employé mécontent vole de l’information à l’entreprise |
| --- | --- |
| **objectifs d'affaires** | Les informations confidentielles doivent être protégées. |
| **Source** | L’employé |
| **Stimulus** | Un employé veut voler des informations pour les revendre et se faire du cash. |
| **Artéfact** | L’intégrité des informations sur le serveur |
| **Environnement** | Mode normal, en ligne |
| **Réponse** | Le système doit trouver les traces d’une infraction dans le système venant toucher l’intégrité des données |
| **Mesure de la réponse** | Le temps détecter l’intrusion à l’intégrité des données. |
| **Questions** | 1. Y-a t-il eu des informations volées? 2. Y-a t-il eu des dommages logiciels ou hardware 3. Quel sanction doit t-on attribuer aux employés |

### Tactique: Encrypt important data

**Description**: Encrypter les données pour les rendre illisibles sans le décrypteur.

**Justification**: Il est important d’encrypter les informations confidentielles sur le serveur pour ne pas que les personnes malveillantes volent de l’information.

| **Scénario** | 3.Un hacker chinois envoie un attaque Distributed Denial of Service aux serveur de l’entreprise |
| --- | --- |
| **objectifs d'affaires** | L’entreprise doit avoir un serveur sécuritaire |
| **Source** | Le hacker |
| **Stimulus** | Le hacker chinois veut faire planter les serveurs de l’entreprise. |
| **Artéfact** | Les serveurs |
| **Environnement** | Mode normal en ligne |
| **Réponse** | Le système doit remarquer que certains paquets avec des signatures similaires sont envoyés en grande quantité. |
| **Mesure de la réponse** | Le temps pour remettre les serveurs en marche |
| **Questions** | 1. Y a-t-il eu des informations perdues 2. Y a-t-il une grande vulnérabilité dans le système |

# 

### Tactique: Inform actors

**Description**: Lorsqu’on se fait attaquer, il est sage de trouver un moyen de réagir aux attaques. Un DDOS est trop puissant pour que le système le détecte et réussisse à bannir toutes les adresses IP. Il est alors nécessaire de contacter l'administrateur pour qu’ils puissent suivre une procédure mise en place d’avance. Par exemple, fermer les serveurs.

**Justification**: Lorsqu’un DDOS survient sur un serveur, il est impératif de couper les communications. Un virus peut être envoyé et le serveur pourrait ne jamais le voir passé. Il y a aussi beaucoup d’informations qui sont à risque d’être découvertes et transmissent par erreur à d’autres destinataire.

| **Scénario** | 4.Un utilisateur attaque le serveur transactionnel par “brute force” |
| --- | --- |
| **objectifs d'affaires** | Minimiser l’impact engendré par l’attaque de l’utilisateur externe. |
| **Source** | Utilisateur externe |
| **Stimulus** | Tentative d’accès non autorisée au serveur transactionnel |
| **Artéfact** | Serveur, données sur le serveur |
| **Environnement** | Système en ligne et opérationnel. Pare-feu activé. |
| **Réponse** | Données protégées contre les multitudes accès non autorisés provenant d’une même source.  Notifier les responsables du système de l’attaque effectué.  Sauvegarder l’état du serveur. |
| **Mesure de la réponse** | Quantité de données vulnérables à l’attaque  Le temps de détection d’une attaque  Quantité de failles dans le système  Quantité d’attaque que le système peut prévenir |
| **Questions** | 1. Qui a la responsabilité de réagir à l’attaque? 2. Combien de temps est entre le début de l’attaque et la contre-réaction? 3. Après combien de requêtes l’alerte est déclenchée? 4. Combien de temps est nécessaire pour restaurer le système à l’état initial avant l’attaque? |

### Tactique: Detect Intrusion

**Description**: Un système cherche des intrusions et/ou les attaques sur le serveur.

**Justification**: On veut détecter les attaques, réagir rapidement selon l’attaque et minimiser les dégâts.

# 

### Tactique: Inform Actors

**Description**: Alerter les responsables du système de l’attaque.

**Justification**: Avertir les responsables du système pour qu'ils puissent suivre les protocoles mises en place pour sécuriser et minimiser les dégâts.

### Tactique: Restore

**Description**: Mettre en place un système de sauvegarde de l'état du serveur avant une attaque en vue de restaurer les données

**Justification**: Étant donné l'importance des informations transactionnelles, il est donc évident de restaurer ces données après une attaque dans le but de conclure les transactions échouées.

| **Scénario** | 5.Un voleur essaye de se connecter au compte d’un client avec une carte de débit volé. |
| --- | --- |
| **objectifs d'affaires** | Offrir la tranquillité d'esprit aux clients de la banque (c'est-à-dire qu'ils ont confiance que l'argent qui se trouve dans leur compte de banque est en sécurité). |
| **Source** | Voleur de carte de débit |
| **Stimulus** | essai de se connecter au compte d’un client en utilisant une carte volée. |
| **Artéfact** | Le système d’authentification du guichet. |
| **Environnement** | Le système est connecté au réseau et opère normalement. |
| **Réponse** | Le données sont protégées pour accès aux personnes légitimes seulement |
| **Mesure de la réponse** | Après trois tentatives de connexion infructueuses, le compte de l'utilisateur doit être bloqué et la banque doit le contacter dans un délais de deux jours maximum. |
| **Questions** | 1. Quoi faire si on ne réussit pas à rejoindre le client dans un délais raisonnable ? 2. Est-ce qu'il y a une procédure en place pour permettre au client de recevoir une nouvelle carte et de changer son code d'accès une fois que sa carte est déclarée volée ? 3. Quelle est la meilleure façon de contacter le client (courriel,téléphone, texto, etc.) ? |

### Tactique: Détecter l’intrusion

**Description**: Après trois tentatives de connexion avec un mauvais code d'accès, on peut supposer raisonnablement que la personne qui tente d'accéder au compte n'est pas le propriétaire légitime du compte.

**Justification**: Il est peu probable qu'une personne oublie une information aussi importante que son code d'accès.

### Tactique: Authentifier les acteurs

**Description**: Avant de pouvoir exécuter des transactions, ou simplement pour consulter son compte, un client doit s'identifier.

**Justification**: Une banque doit protéger l'avoir de ses clients si elle ne veut pas faire faillite.

### Tactique: Verrouiller le compte du client

**Description**: Après trois tentatives infructueuses, le compte du client est verrouillé jusqu'à ce qu'il puisse être contacté.

**Justification**: Ce moyen de restriction temporaire permet à la banque de valider que la personne qui tente d'accéder au compte est bien le propriétaire légitime du compte et non un voleur.

### Tactique: Maintenir une trace d’audit

**Description**: Chaque connexion ou tentative de connexion est enregistrée sur le serveur de la banque.

**Justification**: En conservant des traces d'audit, on peut prouver que des tentatives de fraudes ont été commises.

| **Scénario** | 6.Un employé essaye de voler de l’argent lorsqu’il est en train de remplir le guichet. |
| --- | --- |
| **objectifs d'affaires** | Les employées de la banque doivent remplir les guichets avec un certain montant afin d'éviter que les guichets soient vides. |
| **Source** | Un employé |
| **Stimulus** | décide de remplir le guichet avec seulement 90 billets au lieu de 100 comme il le devrait, selon la procédure de la banque. |
| **Artéfact** | Le système de remplissage du guichet. |
| **Environnement** | Le système est opérationnel et il est connecté au réseau de la banque. |
| **Réponse** | Le système compte le nombre de billets inséré dans la machine et communique l'anomalie au système de la banque. |
| **Mesure de la réponse** | Le système de la banque envoie un message aux employés qui s'occupent de la sécurité pour les informer du problème. (Les informations concernant le guichet et l'employé concernés sont attachés au rapport de problème). |
| **Questions** | 1. Qui sont les employés chargés de la sécurité ? 2. Le système de remplissage du guichet doit-il compter une deuxième fois les billets afin de s'assurer que l'erreur n'est pas dû à un autre problème ? 3. Que faire si le guichet n'est pas connecté au réseau ou s'il ne parvient pas à communiquer avec le système de la banque ? |

# 

### Tactique: Identifier les acteurs

**Description**: Les informations concernant le guichet et l'employé concernés sont attachés au rapport de problème qui est envoyé aux employés chargés de la sécurité.

**Justification**: La banque peut facilement identifier le coupable.

### Tactique: Informer les acteurs

**Description**: Les gens responsables de prendre des mesures ou des actions correctives sont informés de la situation.

**Justification**: La banque possède probablement un processus à suivre pour ce genre de scénario.

### Tactique: Maintenir une trace d’audit

**Description**: Le système de la banque conserve des traces des événements qui se sont produits afin de comprendre ce qui s’est réellement produit et de pouvoir corriger la situation par la suite.

**Justification**: La banque ne peut porter d’accusation sans preuve.

| **Scénario** | 7.Prévenir vol de PIN |
| --- | --- |
| **Objectifs d'affaires** | Fournir un service de guichet automatique sécuritaire en tout temps. |
| **Source** | Un pirate potentiel (source externe malveillante inconnue) |
| **Stimulus** | Le pirate tente d’intercepter et d’accéder au NIP et compte bancaire d’un usager. (tentative d’accès des données non autorisée) |
| **Artéfact** | Les données utilisées lors du processus d’authentification de l’usager |
| **Environnement** | Runtime, en mode fonctionnel complet et connecté au réseau de communication client serveur |
| **Réponse** | Les données et les services ne sont pas manipulés ou accédés par des tiers non-autorisés.  En cas de tentative d’accès aux données non autorisées, un ‘’flag’’ et la banque est informé de la potentielle brèche de sécurité. |
| **Mesure de la réponse** | Le temps nécessaire pour détecter une attaque et prendre les mesures correctives (aviser le client, changer de NIP, révision des transactions).  Si on détecte une brèche de sécurité, on augmente la sécurité sur les lignes de communication afin de rendre l’opération plus sécuritaire. |
| **Questions** | Comment détecter plus rapidement les attaques potentielles ?  Quels sont les points d’entrées les plus probables pour ce type d’attaque?  Quel est le délai habituel de l’opération d'authentification usager?  Quel est le pattern habituel de la transmission de données usager? Quelle est la signature attendue?  Quelles sont les tactiques qu’on peut développer pour se protéger des technologies futures ? (informatique quantique) |

# 

### Tactique: Encrypt Data

**Description**: Encrypter les données envoyées du GAB au serveur et en retour

**Justification**: Encrypter les requêtes pour empêcher les hackers de décoder les messages transmis. Empêcher le vol d’information.

# 

### Tactique: Verify Message Integrity

**Description**: Vérifier si les requêtes envoyés entre le serveur et le GAB sont intègres.

**Justification**: Pour empêcher un utilisateur non authentifié de lire et modifier les messages transmis.

### Tactique: Detect Intrusion

**Description**: Faire le monitoring des communications entrantes et sortantes du GAB et du serveur.

**Justification**: Pour s’assurer que les données sont seulement envoyés aux personnes autorisés.

| **Scénario** | 8.Un utilisateur entre un NIP invalide 3 fois. |
| --- | --- |
| **objectifs d'affaires** | Empecher les utilisateurs d'accéder au compte auquel il n’ont pas accès |
| **Source** | L'utilisateur |
| **Stimulus** | Un NIP invalide est entré pour la troisième fois. |
| **Artéfact** | Code |
| **Environnement** | système opérationnel |
| **Réponse** | Le système garde la carte  Le système averti l’utilisateur que sa carte est bloqué à cause des trois tentatives avec le mauvais NIP  Le système envois un message à la banque pour les informer de la situation  Le système reviens en mode d’attente de carte pour être disponible aux autres utilisateurs |
| **Mesure de la réponse** | Combiens de carte ont été bloqué, par mois/ans  Combiens de temps avant que la carte soit rendu à son propriétaire, heure/jour |
| **Questions** | 1. Après combien d’essais bloque-t-on la carte? 2. Est-ce qu le système doit rester disponible? 3. Permet-t-on l’utilisation d’une carte appartenant au même usager que la carte bloqué? |

### Tactique: Revoke access

**Description:** On empêche l’utilisateur d'accès au compte de la carte

**Justification:** Cela permet de s’assurer qu’une personne tentant d’utilisé une carte qui ne lui appartient pas ne puisse pas faire des transactions illégale.