Rapport du projet de Risk dans le cadre du Master 2 Cybersécurité et e-Santé

# Question 1 – Analyse de risque du smartphone avec EBIOS RM

Année universitaire 2021 – 2022

Projet réalisé par Quentin GUARDIA, quentin.guardia@etu.u-paris.fr
Sous la direction de Patrice Martin

# Table des matières

# Atelier 1 : Cadrage et socle de sécurité

| **Mission** | **Utiliser le téléphone portable** | | | |
|---|---|---|---|---|
| Dénomination des valeurs métier | Communication | Paiement | Accès au web | Contenu privé |
| Nature de la valeur métier | Processus | | | |
| Description | - Envoi et réception de messages textuels ou audiovisuels<br>- Mail et messageries standard ou internet<br>- Appels standard ou internet<br>- Réseaux sociaux<br>- Conversation individuelle ou en groupe | - Autoriser un paiement<br>- Effectuer un virement<br>- Bloquer la carte bancaire<br>- Accès au solde bancaire<br>- Accéder à l'historique des paiements | - Divertissement<br>- Renseignement | Accès et création de :<br>- média<br>- compte en ligne<br>- mot de passe des applications<br>- Cloud |
| Entité ou personne responsable | Utilisateur principal (moi) et propriétaires des applications et serveurs associés | | | |

| Dénomination des biens supports associés | Application cliente | Serveur | Application client | Serveurs de la banque | Application cliente | Serveur | Espace de stockage |
|---|---|---|---|---|---|---|---|
| Description | Les autres et moi | Si pas P2P | | Serveurs e la banque ou associé (paypal) | Les autres et moi | Serveur web | Espace de stockage où sont stockées les informations |
| Entité ou personne responsable | Utilisateur principal (moi) et propriétaires des applications et serveurs associés | | | | | | |

| Échelle | Conséquences |
|---|---|
| G4<br>CRITIQUE | De l'argent est volé. La réputation de l'utilisateur est atteinte, manipulation. |
| G3<br>GRAVE | Le fonctionnement du téléphone est entravé. Des données sensibles sont collectées. |
| G2<br>SIGNIFICATIVE | Certaines applications ou services ne fonctionnent plus correctement. Des données peu sensibles sont collectées. |
| G1<br>MINEURE | Aucun impact notable. |

| Valeur métier | Évènement redouté | Impacts | Gravité |
|---|---|---|---|
| Communication | Usurpation | Impact sur l'image professionnelle ou personnelle | 4 |
| | Phishing | Impact sur la confidentialité d'informations sensibles | 3 |
| | Denis de services | Impact sur la disponibilité de la personne voire sa sécurité | 3 |
| | Altération de la communication | Impact sur le confort de la communication | 2 |
| | Harcèlement | Impact sur le bien-être | 4 |
| | Chantage | Impact sur le bien-être, voire impact financier | 4 |
| | Paiement sans contact inopiné | Impacts financiers | 4 |
| | Détournement d'argent/broutage | Impacts financier | 4 |
| Accès au web | Denis de service | Impact sur l'accès à certaines informations | 2 |
| | Phishing | Impact sur la confidentialité d'informations sensibles | 3 |
| Contenu privé | Perte d'informations | Impact sur la vie pratique ou données affectives | 2 |
| | Diffusion | Impact sur la réputation | 4 |
| Toutes les valeurs métiers | Chute | Impact financier voire sur la disponibilité | 4 |
| | Vol | Impact financier et sur la disponibilité | 4 |
| | Écoute / vol de données | Impact sur la confidentialité, l'image, financier | 4 |
| | Addiction | Impact sur le bien-être | 4 |

**Le socle de sécurité se trouve en annexe**

| Échelle | Description |
|---|---|
| V4<br>quasi certain | La source de risque va certainement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est très élevée. |
| V3<br>Très vraisemblable | La source de risque va probablement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est élevée. |
| V2<br>Vraisemblable | La source de risque est susceptible d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est significative. |
| V1<br>Peu vraisemblable | La source de risque a peu de chance d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est faible. |

# Atelier 2 : Sources de risque

| Source de risque | Objectif visé | Retenu | Justification |
|---|---|---|---|
| Pirate | Revendre des informations, détourner de l'argent | Oui | |
| Technophile | Se tester à accéder au système, voire le manipuler | Oui | |
| Voleur | Revendre le téléphone | Oui | |
| Personne proche | Faire un canular | Non | Peu probable et sans conséquences |
| Personne proche | Se venger | Non | Peu probable |
| GAFAM et autres géants | Traiter des données en masse pour favoriser une orientation politique, et une addiction ou du moins se rendre indispensable | Oui | |
| Applications | Voler des informations de l'utilisateur, vulnérabilité involontaire | Oui | |
| Patrice Martin | Nous prouver l'utilité de son cours | Non | Sa bonté est infinie |

| Sources de risque | Objectifs visés |
|---|---|
| Pirate cherchant des utilisateurs vulnérable | Revendre des informations, détourner de l'argent |
| Technophile | S'entraîner à accéder au système, voire le manipuler |
| Voleur | Revendre le téléphone |
| GAFAM et autres géants | Traiter des données en masse pour favoriser une orientation politique ou une addiction |
| Applications | Voler les informations de l'utilisateur, vulnérabilité involontaire |

| Sources de risque | Objectifs visés | Motivation | Ressources | Activité | Pertinence |
|---|---|---|---|---|---|
| Pirate | Faire du bénéfice à partir des informations soustraites | ++ | ++ | ++ | Moyenne |
| Technophile | Compromettre le téléphone | ++ | + | + | Faible |
| Voleur | Revendre le téléphone | + | + | + | Faible |
| GAFAM & Co | Orienter politiquement | + | +++ | ++ | Moyenne |
| Applications | Voler les informations de l’utilisateur | + | + | + | Faible |

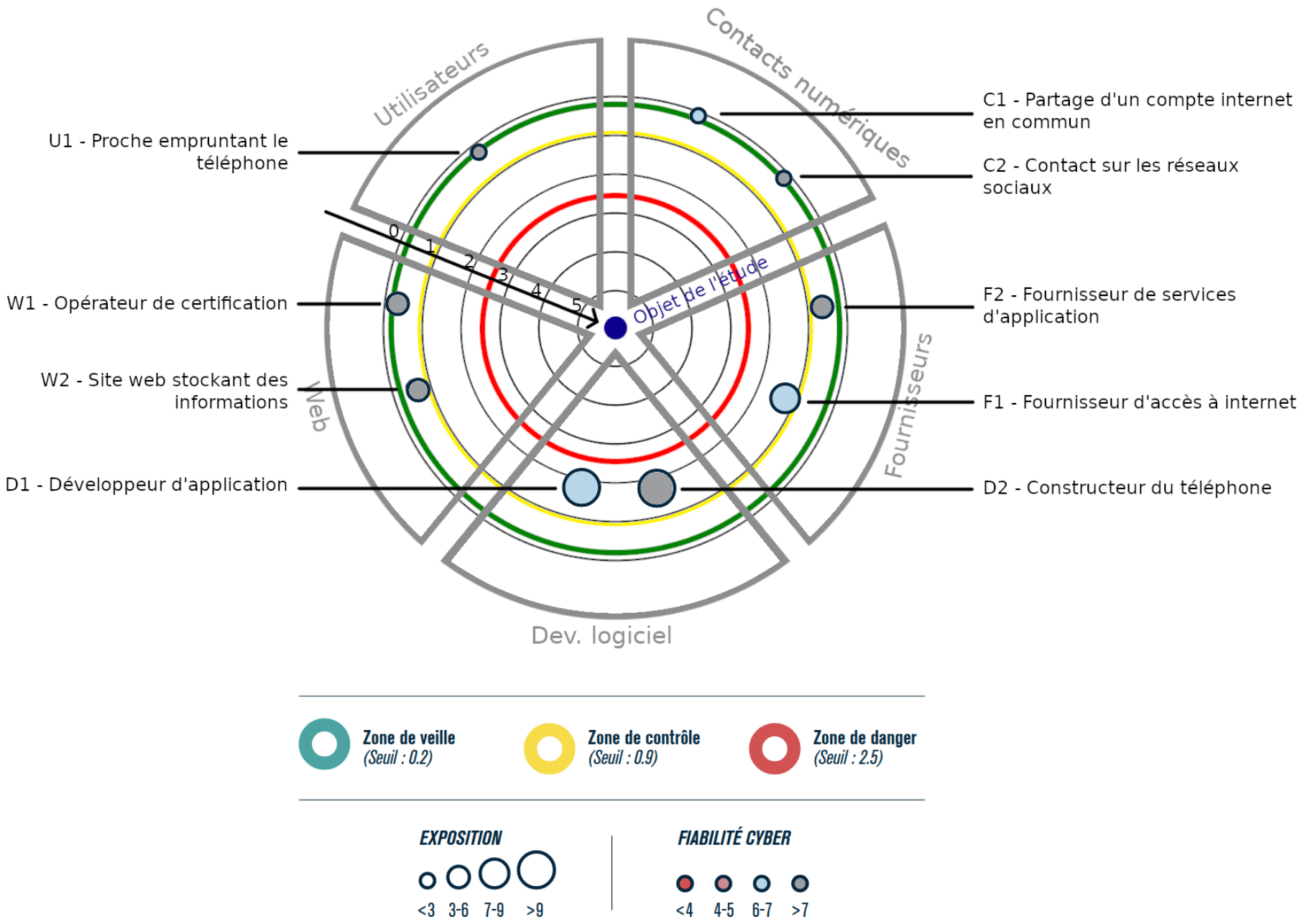
# Atelier 3 : Scénarios stratégiques

| | Dépendance | Pénétration | Maturité cyber | Confiance |
|---|---|---|---|---|
| **1** | Relation non nécessaire au fonctionnement des services de l'appareil. | Presque aucune autorisation sur l'appareil. | Des règles d'hygiène informatique sont appliquées ponctuellement et non formalisées, la capacité de réaction sur incident est incertaine. | Les intentions de la partie prenante ne peuvent être évaluées |
| **2** | Relation utile aux fonctionnement des services de l'appareil. | Accès l'espace de stockage. | Les règles d'hygiène et la réglementation sont prises en compte, sans intégration d'un politique globale. La sécurité numérique est conduite selon un mode réactif. | Les intentions de la partie prenante sont considérées comme neutre |
| **3** | Relation indispensable mais non exclusive. | Accès l'espace de stockage et certaines fonctionnalités. | Une politique globale est appliquée en matière de sécurité numérique. Celle-ci est assurée selon un mode réactif, avec une recherche de centralisation et d'anticipation sur certains risques. | Les intentions de la partie prenant sont connues et probablement positives |
| **4** | Relation indispensable et unique (pas de substitution possible à court terme). | Accès à tout le téléphone avec prise de contrôle possible. | La partie prenante met en œuvre une politique de management du risque. La politique est intégrée et se réalise de manière proactive. | Les intentions de la partie prenante sont parfaitement connues et pleinement compatibles av celles de l'organisation étudiée |

| Catégorie | Partie prenante | Dépendance | Pénétration | Maturité | Confiance | Niveau de menace |
|---|---|---|---|---|---|---|
| Utilisateurs | U1 – Proche empruntant le téléphone | 1 | 2 | 2 | 5 | 0,2 |
| Contacts numériques | C1 – Partage d'un compte internet en commun | 1 | 1 | 2 | 4 | 0,13 |
| | C2 – Contact sur les réseaux sociaux | 1 | 1 | 2 | 3 | 0,17 |
| Fournisseurs | F1 – Fournisseur d'accès à internet | 4 | 2 | 3 | 2 | 1,33 |
| | F2 – Fournisseur de services d'application & SaaS | 4 | 1 | 4 | 2 | 0,5 |
| Développeurs logiciel | D1 – Développeur d'application | 5 | 2 | 3 | 2 | 1,67 |
| | D2 – Constructeur du téléphone | 5 | 4 | 4 | 3 | 1,67 |
| Web | W1 – Opérateur de certification | 3 | 1 | 4 | 3 | 0,25 |
| | W2 – Site web stockant des informations & Cloud | 4 | 1 | 4 | 2 | 0,5 |

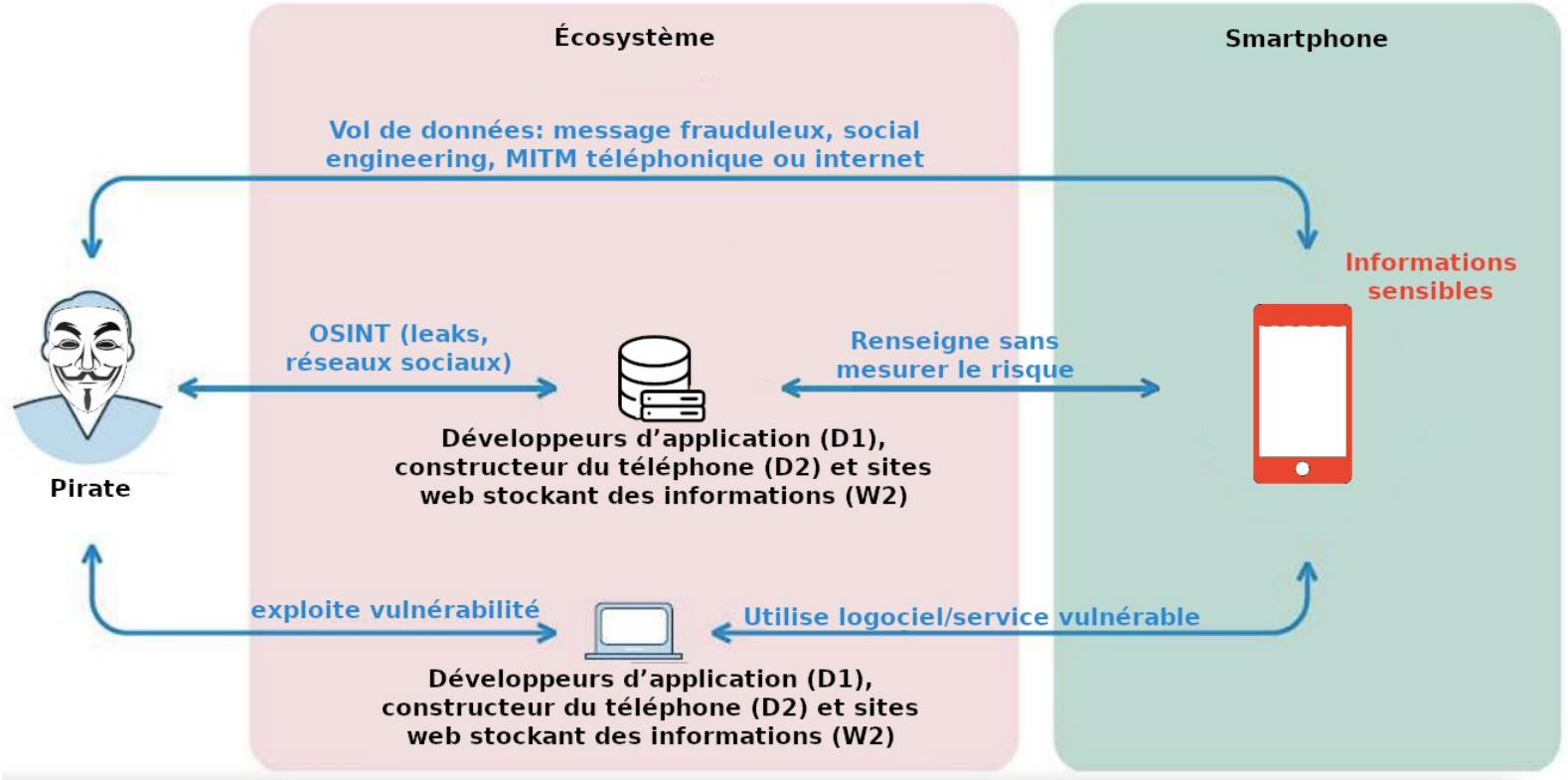
Apparaît de ce tableau que les parties prenantes représentant les plus grosses menaces pour le téléphone sont les développeurs d'application, le constructeur du téléphone et le fournisseur d'accès à internet. Il est à noter que les réseaux sociaux sont inclus parmi les développeurs d'application.

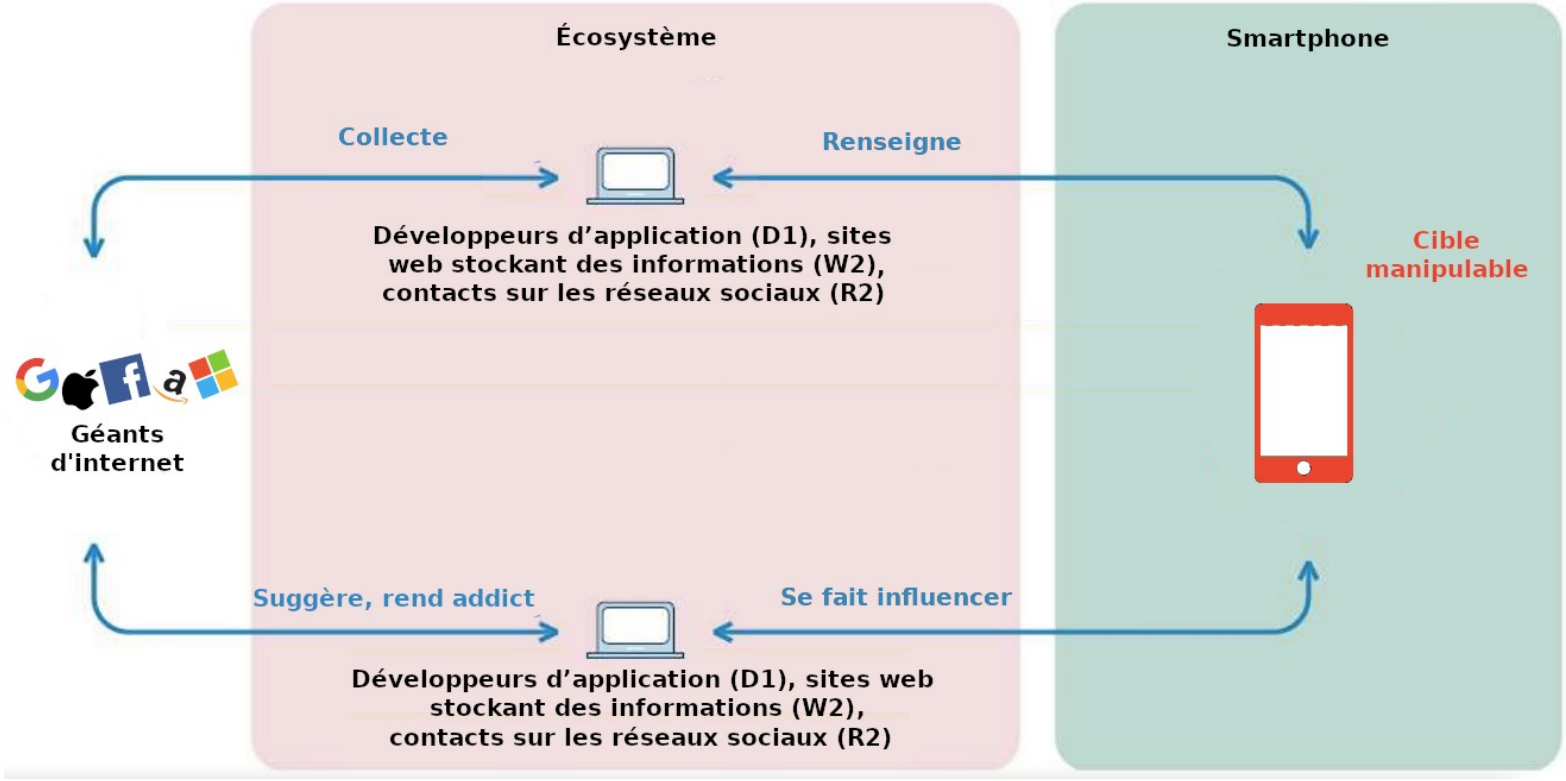
Ci-dessous la cartographie de menace numérique.

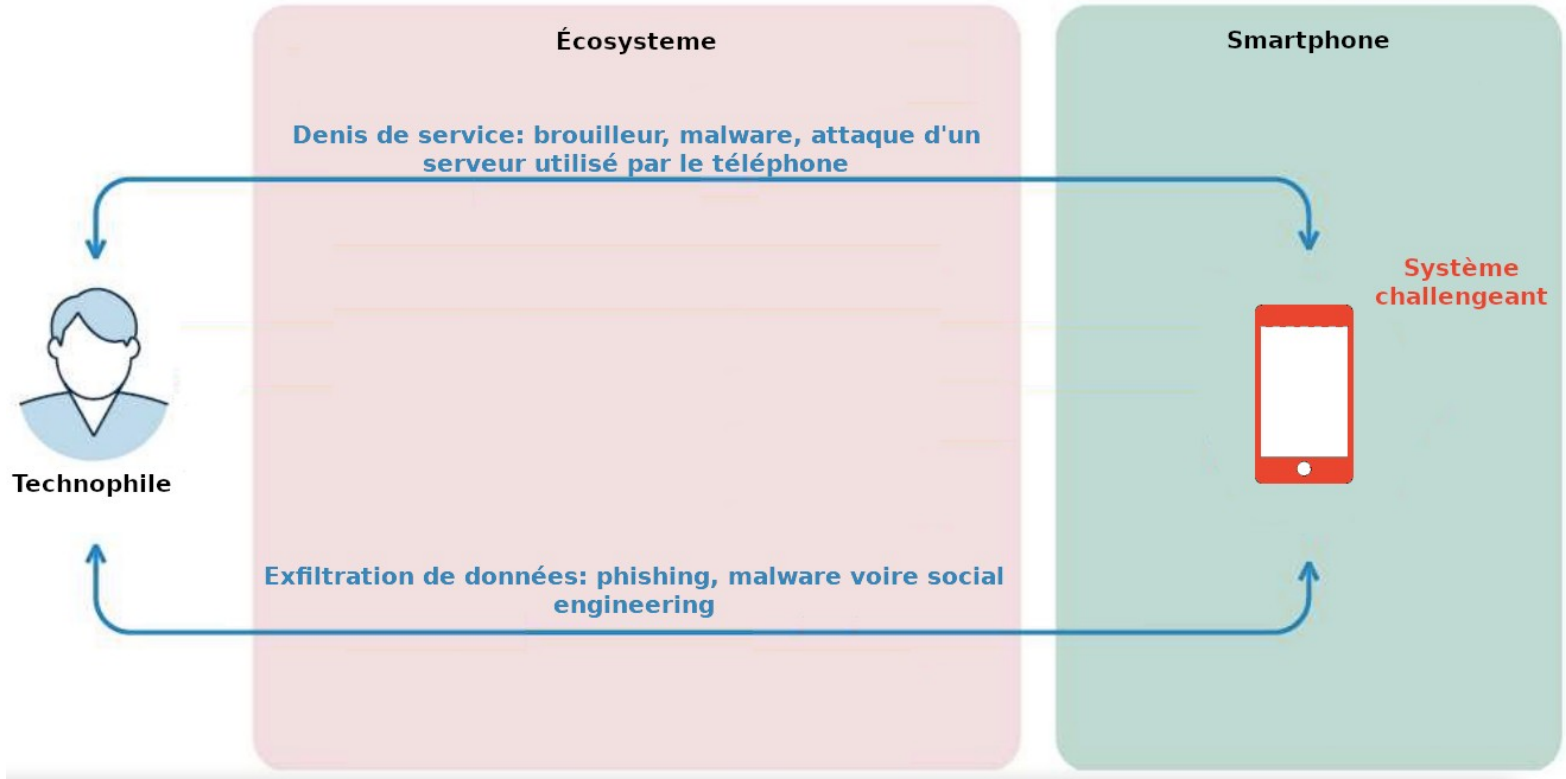

Utilisateurs
Contacts numériques
Web
Fournisseurs
Dev. logiciel
0
1
2
3
4
5
Objet de l'étude
U1 - Proche empruntant le téléphone
W1 - Opérateur de certification
W2 - Site web stockant des informations
D1 - Développeur d'application
C1 - Partage d'un compte internet en commun
C2 - Contact sur les réseaux sociaux
F2 - Fournisseur de services d'application
F1 - Fournisseur d'accès à internet
D2 - Constructeur du téléphone
Zone de veille
(Seuil : 0.2)
Zone de contrôle
(Seuil : 0.9)
Zone de danger
(Seuil : 2.5)
EXPOSITION
<3 3-6 7-9 >9
FIABILITÉ CYBER
<4 4-5 6-7 >7

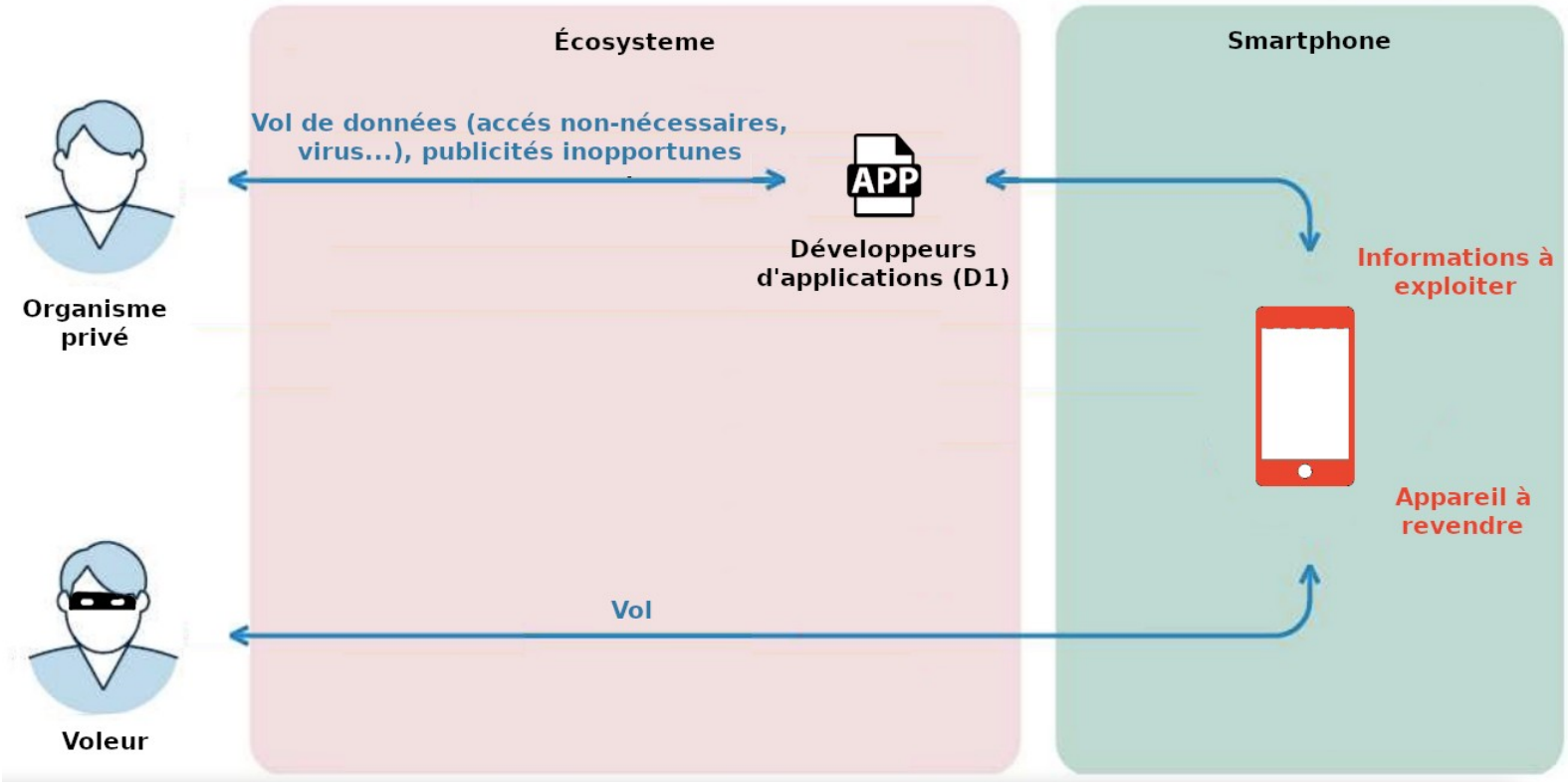
| Sources de risque | Objectifs visés | Chemins d'attaque stratégique | Partie prenante associée, les utilisateurs (U1) étant toujours impliqués, et comment si ce n'est pas évident | Gravité |
|---|---|---|---|---|
| Pirate | Revendre des informations, détourner de l'argent (chantage, broutage, vol direct...), usurpation | Logiciel pas à jour | | 4 |
| | | Mail/message frauduleux | ASP & SaaS (F2) et développeurs d'application (D1) par le manque de détection et de filtre, contacts sur les réseaux sociaux (C2) par diffusion | |
| | | Réseau mal sécurisé | Fournisseurs d'accès à internet (F1) | |
| | | Social engineering | Contacts sur les réseaux sociaux (C2) | |
| | | Leaks : données utilisateurs ou vulnérabilités connues d'applications | Développeurs d'application (D1), constructeur du téléphone (D2) et sites web stockant des informations (W2, notamment réseaux sociaux) | |
| | | Récupération d'informations sur les réseaux sociaux | Contact sur les réseaux sociaux (C2) par partage public, sites web stockant des informations (W2) | |
| | | Écoute téléphonique par MITM | Fournisseurs (F1, F2) et développeurs (D1, D2) | |
| | | Faille 0-day | Développeurs d'application (D1), constructeur du téléphone (D2) et sites web stockant des informations (W2) | |
| Technophile | Accéder au système, voire le manipuler | Spam sur messageries | ASP & SaaS (F1) par manque de filtrage | 3 |
| | | Brouilleur | | |
| | | Phishing | ASP & SaaS (F1) et développeurs d'application (D1) par le manque de détection et de filtre ; opérateurs de certification (W1) par la certification d'un imposteur ou auto-certification ; contact sur les réseaux sociaux (C2) par diffusion | |
| | | Malware | Contact sur les réseaux sociaux (C2) par diffusion | |
| | | Serveurs nécessaires à certains services du téléphone | Développeurs d'application (D1), constructeur du téléphone (D2) et sites web stockant des informations (W2) | |
| Voleur | Revendre le téléphone | Mégarde physique | | 4 |
| GAFAM et | Traiter des données | Collecte d'informations | ASP & SaaS (F1), développeurs d'application (D1) ; sites | 3 |

| | | | | |
|---|---|---|---|---|
| autres géants | en masse pour favoriser une orientation politique | | web stockant des informations (W2) via les cookies, redirections et comptes associés ; autres utilisateurs (U1) par leurs éventuelles recherches | |
| | | Suggestion d'informations, renforcement de l'addiction | ASP & SaaS (F1) et développeurs d'application (D1) via l'inclusion des RS ; sites web stockant des informations (W2) via les publicités ; contacts sur les réseaux sociaux (U1) par leurs capacités à être influencés et influençables | |
| Autres applications et entreprises privées | Voler les informations de l'utilisateur, vulnérabilité involontaire (chemin d'attaque d'un pirate) | Mauvais chiffrement des données ou autres vulnérabilités | Développeurs d'applications (D1) | 3 |
| | | Installation de malwares, publicités inopportunes | Développeurs d'applications (D1) et constructeur (D2) qui n'a pas prévu ce cas de figure | |
| | | Accès à des données du système non-nécessaires | Développeurs d'applications (D1) | |



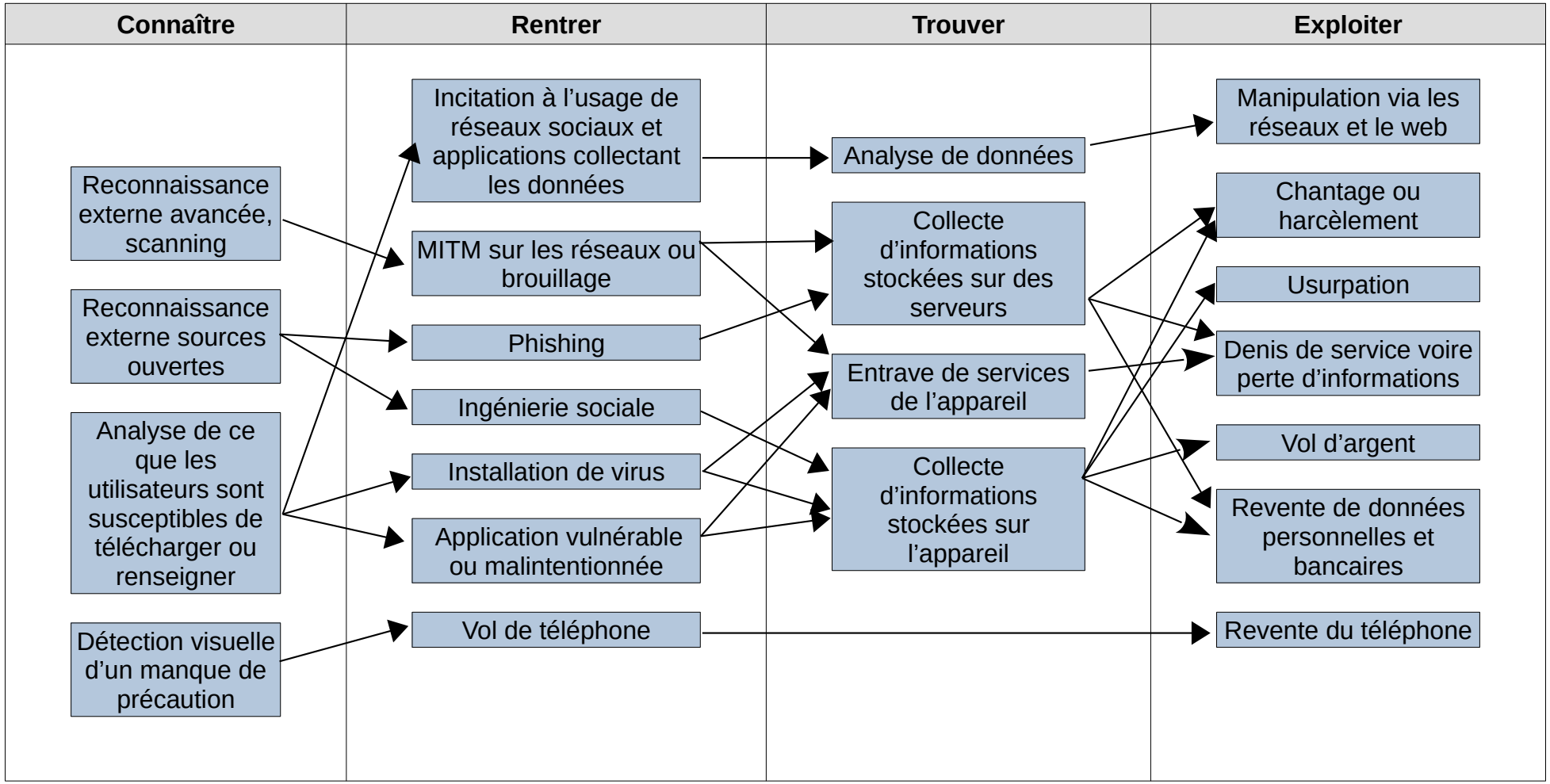

Écosystème
Smartphone
Collecte
Renseigne
Développeurs d'application (D1), sites web stockant des informations (W2), contacts sur les réseaux sociaux (R2)
Cible manipulable
Géants d'internet
Suggère, rend addict
Se fait influencer
Développeurs d'application (D1), sites web stockant des informations (W2), contacts sur les réseaux sociaux (R2)


Écosysteme
Smartphone
Denis de service: brouilleur, malware, attaque d'un serveur utilisé par le téléphone
Système challengeant
Technophile
Exfiltration de données: phishing, malware voire social engineering


Écosysteme
Smartphone
Vol de données (accés non-nécessaires, virus...), publicités inopportunes
APP
Développeurs d'applications (D1)
Informations à exploiter
Organisme privé
Appareil à revendre
Vol
Voleur

| Partie prenante | Chemins d’attaque stratégique | Mesure de sécurité | Menace initiale | Menace résiduelle |
|---|---|---|---|---|
| U1 – Proche empruntant le téléphone | Accès au contenu privé et possibilité d’installer du contenu peu sûr | Sensibilisation aux mesures de sécurité, surveillance | 0,2 | 0,1 |
| C1 – Partage d’un compte internet en commun | Divulgation du mot de passe par social engineering ou phishing | Sensibilisation aux mesures de sécurité, surveillance | 0,13 | 0,06 |
| C2 – Contact sur les réseaux sociaux | Envoie de liens ou fichiers malveillants | Vérifier un lien ou un fichier avant de les ouvrir, avec Virustotal par exemple | 0,17 | 0,14 |
| F1 – Fournisseur d’accès à internet | Écoute du contenu consulté | Mise en place d’un VPN | 1,33 | 0,67 |
| F2 – Fournisseur de services d’application | Accès à du contenu privé, accès aux données peu protégées | Vérifier les certifications de l’ASP en terme de protection des données | 0,5 | 0,25 |
| D1 – Développeurs d’application | Faille sur une application | Mettre à jour les applications, limiter aux accès nécessaires | 1,67 | 0,83 |
| D2 – Constructeur du téléphoné | Faille sur le système | Mettre à jour le système | 1,67 | 1,25 |
| W1 – Opérateurs de certification | Certificat auto-signé | Vérifier la sécurité des connexions | 0,25 | 0,15 |
| W2 – Sites web stockant des informations | Accès à la base de donnée | Vérifier la réputation des sites web avant d’enregistrer des données et diversifier les mots de passe | 0,5 | 0,25 |

# Atelier 4 : Scénarios opérationnels



| Chemins d’attaque stratégiques (associés aux scénarios opérationnels) | Vraisemblance globale |
|---|---|
| Un pirate fait du phishing pour récupérer des informations sensibles | V3 |
| Téléchargement d’un fichier contenant un malware | V2 |
| Vols d’informations à partir d’applications, sites web ou réseau public | V3 |
| Chantage et divulgations par un pirate, concernant des données privées | V1 |
| Vol du téléphone par un voleur à la tire | V2 |
| Manipulation de l’opinion publique et du comportement par les géants du web | V4 |

**Les exigences, leurs impacts et leurs conformités sont en annexe**

# Atelier 5 : Traitement du risque

| Niveau de risque | Acceptabilité du risque | Intitulé des décisions et des actions |
|---|---|---|
| Faible | Acceptable en l'état | Aucune action n'est à prendre |
| Moyen | Tolérable sous contrôle | Un suivi en termes de gestion du risque est à mener et des actions sont à mettre en place dans le cadre d'une amélioration continue sur le moyen et long terme |
| Élevé | Inacceptable | Des mesures de réduction du risque doivent impérativement être prises à court terme pour la sécurité de l'utilisateur (moi) |

| gravité | | | | | |
|---|---|---|---|---|---|
| 4 | R4 | R5 | | | |
| 3 | | R1<br>R2 | R3 | R6 | |
| 2 | | | | | |
| 1 | | | | | |
| | 1 | 2 | 3 | 4 | vraisemblance |

R1 : Un pirate fait du phishing pour récupérer des informations sensibles
R2 : Téléchargement d'un fichier contenant un malware
R3 : Vols d'informations à partir d'applications, sites web ou réseau public
R4 : Chantage et divulgations concernant des données privées
R5 : Vol du téléphone par un voleur à la tire
R6 : Manipulation de l'opinion publique et du comportement par les géants du web

| Mesure de sécurité | Scénarios de risques associés | Freins et difficultés de mises en œuvre | Coût/ complexité |
|---|---|---|---|
| Sensibilisation au phishing des utilisateurs du téléphone | R1 | Réceptivité des autres utilisateurs | + |
| Effectuer les mises à jours régulièrement | R3 | | + |
| Varier et mettre à jour régulièrement les identifiants | R3 | Peu pratique | ++ |
| Installer uniquement des applications officielles | R3 | | + |
| Ne pas se connecter à des réseaux publics | R3 | | + |
| Vérifier la fiabilité d'un site web | R3 | Chronophage pour l'intérêt apporté | ++ |
| Ne pas laisser son téléphone hors de sa vue et le surveiller régulièrement en extérieur | R5 | | + |
| Analyser les fichiers télécharger | R2 | Pas nécessairement le temps | ++ |
| Utiliser un VPN | R3, R6 | | + |
| Filtrage des mails | R1 | | + |
| Ne pas publier de données privées en public | R4 | | + |
| Favoriser une authentification à deux facteurs | R1, R3, R4 | Chronophage | ++ |
| Veille concernant les compromissions de données massives | R3 | | + |

En appliquant toutes les mesures précédemment énoncées, on peut espérer en arriver à ces niveaux de vraisemblances des scénarios stratégiques :

| gravité | | | | | |
|---|---|---|---|---|---|
| 4 | R4 | R5 | | | |
| 3 | R1<br>R2 | R3 | R6 | | |
| 2 | | | | | |
| 1 | | | | | |
| | 1 | 2 | 3 | 4 | vraisemblance |

R1 : Un pirate fait du phishing pour récupérer des informations sensibles
R2 : Téléchargement d'un fichier contenant un malware
R3 : Vols d'informations à partir d'applications, sites web ou réseau public
R4 : Chantage et divulgations concernant des données privées
R5 : Vol du téléphone par un voleur à la tire
R6 : Manipulation de l'opinion publique et du comportement par les géants du web

# Annexes

Socle de sécurité

| Thématique | Type de référentiel | Nom du référentiel | État d'application | Écarts | Justification des écarts |
|---|---|---|---|---|---|
| Client | Règles d'hygiène informatique et bonnes pratiques | Guide hygiène informatique de l'ANSSI | Appliqué avec restriction | I.2. : Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique | Connaissances basiques des pratiques élémentaires de sécurité informatique |
| Fonctionnel | | | | II.4. : Identifier les informations, applications et fonctionnalités les plus sensibles | Pas évident en pratique et peu de traitement possible |
| Réseau | | | | II.7. : Autoriser la connexion au Réseau qu'aux applications maîtrisés | Peu de possibilités pour gérer les applications et leur connectivité |
| Logiciel | | | | III.10. : Définir et vérifier des règles de choix et de dimensionnement des mots de passe | Choix de mots de passe complexes, sans règle stricte cependant |
| Réseau | | | | III.12. : Changer les éléments d'authentification par défaut sur les équipements et services | Certains équipements n'ont pas la possibilité de changer le mot de passe (ex : écouteurs) |
| Réseau | | | | IV.18. : Chiffrer les données sensibles transmises par voie Internet | Utilisation du chiffrement par défaut |
| Réseau | | | | V.20. : S'assurer de la sécurité des Réseau d'accès Wi-Fi et de la séparation des usages | Séparation des usages pas évidente |

| | | | | | |
|---|---|---|---|---|---|
| Réseau | | | | V.21. : Utiliser des protocoles sécurisés dès qu'ils existent | Utilisation des protocoles par défaut |
| Logiciel | | | | V.24. : Protéger sa messagerie professionnelle | Messagerie protégée par défaut |
| Matériel | | | | VII.30. : Prendre des mesures de sécurisation physique du téléphone | Souvent dans la poche pour des raisons pratiques |
| Fonctionnel | | | | VII.31. : Chiffrer les données sensibles, en particulier sur le matériel potentiellement perdable | Il faut une clé pour accéder au système, hors carte SD |
| Réseaux | | | | VII.32. : Sécuriser la connexion réseau du téléphone | Sécurisation par défaut |
| Organisation | | | | IX.37. : Définir et appliquer une politique de sauvegarde des données importantes | Il faut trouver un bon Cloud pas trop cher ou acheter un disque dur |
| Fonctionnel | Règles d'hygiène informatique et bonnes pratiques | EBIOS 2010 | Appliqué avec restriction | Identifier et réexaminer régulièrement les exigences en matière d'engagements de confidentialité ou de non-divulgation, conformément aux besoins | Exigences statiques en matière d'engagements de confidentialité ou de non-divulgation, conformément aux besoins |
| Fonctionnel | | | | Mesure de sécurité concernant les tiers: Identifier les risques provenant des tiers | Peu de risque de manière générale |
| Fonctionnel | | | | Mettre en œuvre des règles permettant l'utilisation correcte de l'information et des biens associés aux moyens de traitement de l'information. | Règles nativement présentes |
| Matériel | | | | Mettre au rebut de façon sûre les téléphones qui ne servent plus, en suivant des procédures formelles | Ancien téléphone stocké chez soi ou vendu |
| Matériel | | | | Mettre en place des procédures pour la gestion des supports amovibles. | Procédures natives, on ne peut pas modifier grand chose |
| Matériel | | | | Établir des procédures de manipulation et de | Pas de procédure |

| | | | | | |
|---|---|---|---|---|---|
| | | | | stockage des informations pour protéger ces informations d'une divulgation non autorisée ou d'un mauvais usage. | particulière à mettre en place |
| Fonctionnel | | | | Journaliser et analyser les éventuels défauts et de prendre les mesures appropriées. | Une application le fait en partie |
| Réseau | | | | Gestion de la sécurité des réseau: Identifier les fonctions réseau, les niveaux de service et les exigences de gestion, et de les intégrer dans tout accord sur les services réseau, qu'ils soient fournis en interne ou en externe | Pas évident en pratique |
| Client | | | | Gestion des incidents liés à la sécurité de l'information: Signaler des failles de sécurité | Failles de sécurité rarement connues |
| Logiciel/Mat. | | | | Empêcher toute possibilité de fuite d'informations. | Pas forcément évident |
| Logiciel/Mat. | | | | Restreindre l'accès à l'information | Chiffrement par défaut |
| Logiciel | | | | Protection contre les codes malveillant et mobile: Mettre en place des mesures contre le code mobile | Applications installées depuis des sources sûres |
| Logiciel | | | | Protection contre les codes malveillant et mobile: mettre en place des mesures contre les codes malveillants | Applications installées depuis des sources sûres |
| Client | | | | Éviter toute utilisation de moyens de traitement de l'information à des fins illégales. | Pas de fin illégale |
| Matériel | | | | Sécurité physique: entretenir le téléphone | Téléphone normalement entretenu |
| Matériel | | | | Sécurité physique: choisir un emplacement sécurisable | Dans la poche pour des raisons pratiques |
| Matériel | | | | Sécurité physique: supprimer les données sensibles en fin de vie du téléphone | À appliquer |
| Matériel | | | | Sauvegarde: réaliser des copies de sauvegarde des informations et logiciels | Compliqué à mettre en place pour les logiciels |

| | | | | | |
|---|---|---|---|---|---|
| Logiciel/ Matériel | Réglementation en vigueur | Instruction Interministérielle n°901 | Appliqué avec restriction | Obj. 19 : protection des informations sensibles en confidentialité et en intégrité | Informations difficilement cloisonnables |
| Logiciel | | | | Obj 20. : Configuration des ressources informatiques | Jamais eu de recommandations de durcissent du système |
| Logiciel | | | | Obj. 21 : Contrôle systématique de la qualité des mots de passe | Certains mots de passe sont simples |
| Fonctionnel | | | | Obj. 18 : Système d'échanges sécurisés : journaliser et imputer des données échangées | Journalisation des appels et messages par défaut sur les applications |
| Logiciel | | | | Obj. 22 : Protection contre les codes malveillants | Pas d'antivirus par défaut |
| Logiciel | | | | Obj. 22 : Configuration du navigateur Internet | Configuration par défaut du navigateur internet |
| Fonctionnel | | | | Obj. 23 : Gestion dynamique de la sécurité. | Peu de possibilités de gérer les flux et journaux |
| Client | | | | Obj. 23 : Appliquer les recommandations de l'ANSSI relatives au nomadisme numérique | Connaissances basiques appliqués |
| Matériel | | | | Obj. 24 : passerelle d' échange de fichiers | Peu de moyen de choisir le protocole à partir du téléphone |
| Logiciel | Règles d'hygiène informatique et bonnes pratiques | MITRE \| ATT&CK | Appliqué avec restriction | T1566 : L'antivirus peut mettre automatiquement en quarantaine les fichiers suspects | Pas d'antivirus par défaut |
| Logiciel | | | | T1176 : S'assurer que les extensions installées sont bien celles prévues, car de nombreuses extensions malveillantes existent | Confiance aveugle aux extensions du navigateur |
| Logiciel | | | | T1530 : Vérifier fréquemment les autorisations sur le Cloud pour s'assurer que les autorisations appropriées sont définies pour filtrer l'accès aux ressources | Pas de vérification fréquente par manque de temps |

| | | | | | |
|---|---|---|---|---|---|
| Fonctionnel | | | | T1552 : Chercher les fichiers contenant des mots de passe et prendre des mesures pour réduire le risques d’exposition | Quelques mots de passe sont notés sur le bloc-note |
| Fonctionnel | | | | T1240 : Auditer les images déployées dans l'environnement pour s'assurer qu'elles ne contiennent pas de composants malveillants. | Confiance aveugle aux images téléchargées |
| Logiciel | | | | T1495 : Vérifier l'intégrité du BIOS existant et du micrologiciel du périphérique pour déterminer s'ils sont vulnérables à la modification. | Manipulation difficile et peu intuitive |
| Matériel | | | | T1486 : S’assurer d’avoir suffisamment de sauvegardes en cas de problème avec les données | Trop chronophage |
| Logiciel | | | | T1048 : La prévention des pertes de données permet de détecter et de bloquer l’upload de données sensibles via les navigateurs web. | Peu d’outils le permettent |
| Matériel | | | | T1052 : La prévention des pertes de données permet de détecter et de bloquer la copie de données sensibles sur des périphériques USB. | Il faut seulement déverouiller le téléphone pour autoriser la copie par USB, pas de traitement spécifique pour les données sensibles |
| Logiciel | | | | T1098 : Utiliser l'authentification à plusieurs facteurs pour accéder au compte utilisateur | Seulement un modèle de déverrouillage ou une reconnaissance |
| Logiciel | | | | T1098.002 : Utiliser l'authentification à plusieurs facteurs pour accéder aux comptes mails | Les sessions restent ouvertes |
| Logiciel | | | | T1176 : S’assurer que les systèmes d'exploitation et les navigateurs utilisent la version la plus récente. | Mises à jour automatiques, mais parfois délayées par l’utilisateur ou un espace de stockage trop rempli |

| | | | | | |
|---|---|---|---|---|---|
| Logiciel | | | | T1606 : Configurer les navigateurs/applications pour qu'ils suppriment régulièrement les cookies web persistants. | Manque de connaissance sur cette pratique |
| Logiciel | | | | T1616 :Les applications pourraient être contrôlées quant à leur utilisation des API de gestion du presse-papiers, avec un examen approfondi des applications qui les utilisent. | Difficulté à contrôler les accès de chaque application |
| Logiciel | | | | T1605 : L'attestation de l'appareil peut souvent détecter les appareils jailbreakés ou rootés. | Il faudrait apprendre à utiliser Android SafetyNet ou Samsung Knox TIMA Attestation |
| Réseau | | | | T1466 : Le cryptage de la couche application (par exemple, l'utilisation de TLS) ou un VPN (par exemple, l'utilisation du protocole IPsec) peuvent contribuer à atténuer les faiblesses du cryptage du réseau cellulaire. | Les bons VPN sont payants |
| Réseau | Règles d'hygiène informatique et bonnes pratiques | NIST Special Publication 800-124 | Appliqué avec restriction | 2.2.3 : Utiliser un VPN pour assurer la confidentialité et l'intégrité des communications, favoriser l'authentification mutuelle si possible, ne pas se connecter aux réseaux Wi-Fi peu sûrs et réduire les surfaces réseau | Les bons VPN sont payants |
| Fonctionnel | | | | 2.2.4 : Vérifier les applications avant de les installer, regarder les permissions qu'elles demandent, voire utiliser une sandbox | La sandbox est peut-être un peu excessive |
| Fonctionnel | | | | 2.2.5 : Faire attention au contrôle à distance par synchronisation ou au contrôle physique, en chargeant son téléphone sur un appareil inconnu par exemple | Confiance aveugle aux batteries externes utilisées |
| Client | | | | 2.2.6 : Se sensibiliser sur les contenus inconnus et leur ouverture inopinée, comme lors de l'ouverture d'URL automatique à la lecture d'un QR code. Dans | Difficile de configurer un proxy sur le téléphone |

| | | | | | |
|---|---|---|---|---|---|
| | | | | ce cas, un proxy pourrait empêcher l'automatisme | |
| Logiciel | | | | 2.2.7 : De nombreux sites web et de nombreuses applications peuvent localiser le téléphone. On peut alors désactiver la localisation ou ne pas autoriser certaines sources à localiser le téléphone. | La localisation peut-être utile en cas de perte ou de vol. Je la supprime cependant lorsqu'elle est inutile |

Exigences, leurs impacts et leurs conformités

J'ai jugé conforme des exigences considérées comme des écarts dans le socle de sécurité lorsqu'elles sont appliquées par défaut. En effet, j'ai mis beaucoup d'exigences dans les écarts du socle de sécurité alors qu'elles sont parfois appliquées par défaut pour que celles-ci apparaissent et ainsi pour prouver mon travail de recherche.

| **Règle** | **Endroit de l'impact sur le scénario opérationnel** | **Conforme** |
|---|---|---|
| Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique | Rentrer : phishing, ingénierie sociale, téléchargement de virus et application vulnérable, usage de réseaux collectant les données | Non |
| II.7. : Autoriser la connexion au Réseau qu'aux applications maîtrisés | Rentrer : MITM sur les réseaux | Non |
| III.10. : Définir et vérifier des règles de choix et de dimensionnement des mots de passe | Trouver : collecte d'information stockées sur l'espace de stockage | Non |
| III.12. : Changer les éléments d'authentification par défaut sur les équipements et services | Trouver : collecte d'information stockées sur l'espace de stockage et les serveurs | Oui |
| IV.18. : Chiffrer les données sensibles transmises par voie Internet | Rentrer : MITM sur les réseaux | Oui |
| V.20. : S'assurer de la sécurité des Réseau d'accès Wi-Fi et de la séparation des usages | Rentrer : MITM sur les réseaux | Non |

| | | |
|---|---|---|
| V.21. : Utiliser des protocoles sécurisés dès qu'ils existent | Rentrer : MITM sur les réseaux | Oui |
| V.24. : Protéger sa messagerie professionnelle | Rentrer : collecte d'informations stockées sur le serveur | Oui |
| VII.30. : Prendre des mesures de sécurisation physique du téléphone | Connaître : détection visuelle d'un manque de précaution | Non |
| VII.31. : Chiffrer les données sensibles, en particulier sur le matériel potentiellement perdable | Trouver : collecte d'information stockées sur l'espace de stockage | Oui |
| VII.32. : Sécuriser la connexion réseau du téléphone | Rentrer : MITM sur les réseaux | Oui |
| IX.37. : Définir et appliquer une politique de sauvegarde des données importantes | Exploiter : perte d'informations, DoS | Non |
| Identifier et réexaminer régulièrement les exigences en matière d'engagements de confidentialité ou de non-divulgation, conformément aux besoins | Trouver : collecte d'informations stockées sur le serveur et sur l'appareil | Non |
| Mesure de sécurité concernant les tiers: Identifier les risques provenant des tiers | Rentrer: téléchargement de virus, application vulnérable ou collectant les données | Non |
| Établir des procédures de manipulation et de stockage des informations pour protéger ces informations d'une divulgation non autorisée ou d'un mauvais usage. | Trouver : collecte d'information stockées sur l'espace de stockage | Non |
| Gestion de la sécurité des Réseau: Identifier les fonctions réseau, les niveaux de service et les exigences de gestion, et de les intégrer dans tout accord sur les services réseau, qu'ils soient fournis en interne ou en externe | Rentrer : MITM sur les réseaux | Non |
| Empêcher toute possibilité de fuite d'informations. | Trouver : analyser les données | Non |
| Restreindre l'accès à l'information | Trouver : collecte d'informations stockées sur l'appareil | Oui |
| Protection contre les codes malveillant et mobile: Mettre en place des mesures contre les codes malveillants | Rentrer : installation de virus | Non |
| Sécurité physique: Choisir un emplacement sécurisable | Connaître : détection visuelle d'un manque de précaution | Oui |
| Sécurité physique: Supprimer les données sensibles en fin de vie du téléphone | Trouver : collecte d'information stockées | Oui |

| | | |
|---|---|---|
| | sur l’espace de stockage | |
| Sauvegarde: Réaliser des copies de sauvegarde des informations et logiciels | Exploiter : perte d’informations, DoS | Non |
| Obj. 19 : protection des informations sensibles en confidentialité et en intégrité | Trouver : collecte d’informations stockées sur le serveur et sur l’appareil | Non |
| Obj. 21 : Contrôle systématique de la qualité des mots de passe | Trouver : collecte d’informations stockées sur le serveur et sur l’appareil | Oui |
| Obj. 22 : Protection contre les codes malveillants | Rentrer : installation de virus | Non |
| Obj. 22 : Configuration du navigateur Internet | Rentrer : MITM | Non |
| Obj. 23 : Appliquer les recommandations de l'ANSSI relatives au nomadisme numérique | Rentrer : phishing, ingénierie sociale, téléchargement de virus et application vulnérable, usage de réseaux collectant les données | Oui |
| T1566 : L'antivirus peut mettre automatiquement en quarantaine les fichiers suspects | Rentrer : installation de virus | Oui |
| T1176 : S’assurer que les extensions installées sont bien celles prévues, car de nombreuses extensions malveillantes existent | Rentrer : installation de virus | Oui |
| T1530 : Vérifier fréquemment les autorisations sur le Cloud pour s’assurer que les autorisations appropriées sont définies pour filtrer l'accès aux ressources | Trouver : collecte d’informations stockées sur des serveurs | Non |
| T1552 : Chercher les fichiers contenant des mots de passe et prendre des mesures pour réduire le risques d’exposition | Trouver: collecte d’informations stockées sur l’appareil | Non |
| T1240 : Auditer les images déployées dans l'environnement pour s'assurer qu'elles ne contiennent pas de composants malveillants. | Entrer : installation de virus | Non |
| T1495 : Vérifier l'intégrité du BIOS existant et du micrologiciel du périphérique pour déterminer s'ils sont vulnérables à la modification. | Entrer : application vulnérable | Non |
| T1486 : S’assurer d’avoir suffisamment de sauvegardes en cas de problème avec les données | Exploiter : perte d’informations, DoS | Non |
| T1048 : La prévention des pertes de données permet de détecter et de bloquer | Trouver: collecte d’informations stockées | Non |

| | | |
|---|---|---|
| l’upload de données sensibles via les navigateurs web. | sur l’appareil | |
| T1052 : La prévention des pertes de données permet de détecter et de bloquer la copie de données sensibles sur des périphériques USB. | Entrer : ingénierie sociale<br>Trouver: collecte d’informations stockées sur l’appareil | Non |
| T1098 : Utiliser l'authentification à plusieurs facteurs pour accéder au compte utilisateur | Trouver: Collecte d’informations stockées sur l’appareil | Non |
| T1098.002 : Utiliser l'authentification à plusieurs facteurs pour accéder aux comptes mails | Trouver: Collecte d’informations stockées sur des serveurs | Non |
| T1176 : S’assurer que les systèmes d'exploitation et les navigateurs utilisent la version la plus récente. | Rentrer: application vulnérable | Oui |
| T1606 : Configurer les navigateurs/applications pour qu'ils suppriment régulièrement les cookies web persistants. | Trouver : collecte d’informations sur l’appareil, analyse de données | Non |
| T1616 : Les applications pourraient être contrôlées quant à leur utilisation des API de gestion du presse-papiers, avec un examen approfondi des applications qui les utilisent. | Rentrer : application vulnérable | Non |
| T1605 : L'attestation de l'appareil peut souvent détecter les appareils jailbreakés ou rootés. | Rentrer : application vulnérable | Non |
| T1466 : Le cryptage de la couche application (par exemple, l'utilisation de TLS) ou un VPN (par exemple, l'utilisation du protocole IPsec) peuvent contribuer à atténuer les faiblesses du cryptage du réseau cellulaire. | Rentrer : MITM sur les réseaux | Non |
| 2.2.3 : Utiliser un VPN pour assurer la confidentialité et l’intégrité des communications, favoriser l’authentification mutuelle si possible, ne pas se connecter aux réseaux Wi-Fi peu sûrs et réduire les surfaces réseau | Rentrer : MITM sur les réseaux | Non |
| 2.2.4 : Vérifier les applications avant de les installer, regarder les permissions qu’elles demandent, voire utiliser une sandbox | Rentrer: téléchargement de virus ou application vulnérable | Non |
| 2.2.5 : Faire attention au contrôle à distance par synchronisation ou au contrôle physique, en chargeant son téléphone sur un appareil inconnu par exemple | Rentrer : application vulnérable, téléchargement de virus | Non |
| 2.2.6 : Se sensibiliser sur les contenus inconnus et leur ouverture inopinée, comme lors de l’ouverture d’URL automatique à la lecture d’un QR code. Dans un tel cas, un | Entrer : ingénierie sociale, installation de virus | Non |

| | | |
|---|---|---|
| proxy pourrait empêcher cette automatisme | | |
| 2.2.7 : De nombreux sites web et de nombreuses applications peuvent localiser le téléphone. On peut alors désactiver la localisation ou ne pas autoriser certaines sources à localiser le téléphone. | Trouver : analyser les données | Oui |
| (ANSSI) Privilégier lorsque c'est possible une authentification forte | Trouver : collecte d'information stockées sur l'espace de stockage, MITM sur réseaux internet | Oui |
| (EBIOS 2010) Protéger le téléphone contre les accès non autorisés. | Trouver : collecte d'information stockées sur l'espace de stockage | Oui |
| (EBIOS 2010) Définir un système de gestion des mots de passe | Trouver : collecte d'information stockées sur l'espace de stockage, MITM sur réseaux internet | Oui |
| (ANSSI) Protéger les mots de passe stockés sur les systèmes | Trouver : collecte d'information stockées sur l'espace de stockage | Oui |