

Comment assurer la sécurité des objets connectés dans les foyers genevois et protéger efficacement les données personnelles des utilisateurs ?

Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES

par :

Nicolas MARTINELLI

Conseiller au travail de Bachelor :

Thibault VATTER, Professeur HES

Genève, le 11 juillet 2024

Haute École de Gestion de Genève (HEG-GE)

Filière économie d'entreprise

Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre de Bachelor of Science en économie d'entreprise.

L'étudiant-e atteste avoir réalisé seul-e le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. Il ou elle atteste par ailleurs que le travail rendu est le fruit de sa réflexion personnelle et a été rédigé de manière autonome. Ce travail a, en outre, été soumis pour analyse par le logiciel de détection de plagiat préconisé par la filière.

L'étudiant-e accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur-e, ni celle du ou de la conseiller-ère au travail de Bachelor, celle du juré-e ou celle de la HEG.

Remerciements

Je tiens à remercier, en premier lieu, mon conseiller en travail de bachelor, Thilbault Vatter, qui s'est montré très disponible tout au long de l'année. Grâce à son expérience et à son savoir-faire, il a su me prodiguer de précieux conseils qui m'ont énormément aidé lors de la rédaction de ma thèse de bachelor.

Je tiens à exprimer également ma profonde gratitude à monsieur Omar Bognuda, directeur de la cybersécurité chez Eyra Group, et à monsieur Axel Baudry, pentester chez Eyra Group, pour leur aide précieuse dans la réalisation de mon cas pratique. Leur expertise et leurs réponses claires et détaillées à mes nombreuses questions ont été d'une grande aide tout au long de ce travail.

Résumé

L'objectif de ce travail de Bachelor est d'explorer les mesures nécessaires pour garantir au mieux la sécurité des objets connectés dans les foyers genevois et protéger les données personnelles des utilisateurs. La recherche met en lumière les principaux défis de sécurité liés à la domotique, un secteur en pleine expansion qui apporte confort, sécurité et efficacité énergétique.

Le cas pratique de l'étude a impliqué l'utilisation de base de données publique pour démontrer comment les cybercriminels peuvent facilement identifier et exploiter les vulnérabilités des objets connectés. L'analyse a révélé des failles dans divers dispositifs domestiques mettant en évidence la nécessité de mettre à jour régulièrement les appareils et d'adopter des pratiques de sécurité robustes.

Les recommandations issues de cette recherche incluent, tout d'abord, l'adoption d'une approche Zero Trust, l'éducation et la sensibilisation des utilisateurs aux risques de cybersécurité. Puis, une marche à suivre de questions à se poser avant l'achat d'un objet connecté. Pour faire suite à l'achat, une liste de mesure détaillée à mettre en place afin de se protéger. Enfin, une dernière recommandation sur les actions à entreprendre si un objet connecté est infecté. La mise en place de ces recommandations renforce notre système de sécurité et permet de réduire grandement nos chances d'être piraté.

Table des matières

Déclaration.....	i
Remerciements.....	ii
Résumé	iii
Liste des figures.....	v
1. Introduction.....	1
2. Contexte	2
2.1 Méthodologie	2
2.2 Définition IOT	3
2.3 Qu'est-ce qu'une maison intelligente ?	3
2.4 Avantages et inconvénients d'une maison intelligente	4
2.5 Identification des principaux défis en matière de sécurité de l'IOT	6
3. Expansion du marché.....	9
3.1 Marché mondial de l'IOT	9
3.2 Marché mondial de la maison intelligente	10
3.3 Marché suisse de la maison intelligente.....	11
4. Analyse des objets connectés dans les maisons genevoises	14
4.1 Données démographiques.....	15
4.2 Cybersécurité des objets connectés.....	16
4.3 Relation des personnes aux objets connectés.....	22
5. Cas Pratique.....	29
5.1 Utilisation de Shodan	30
5.2 Piratage d'un Wi-Fi domestique	33
5.3 Identification des vulnérabilités des IOT.....	35
5.4 Solutions aux vulnérabilités identifiées.....	42
6. Recommandations.....	44
6.1 Quelles questions se poser avant l'achat d'un IOT.....	45
6.2 Les mesures à mettre en place.....	46
7. Conclusion	50
Bibliographie	51
Annexe 1 : Glossaire.....	56
Annexe 2 : Questionnaire	58
Annexe 3 : Retranscription.....	66

Liste des figures

Figure 1: Nombre d'IOT dans le monde de 2022 à 2023, avec des prévisions de 2024 à 2033.	9
Figure 2 : Pyramide des âges	15
Figure 3 : Conscience des risques en fonction du sexe	16
Figure 4 : Conscience des risques en fonction de l'âge.....	17
Figure 5 : Perception de la responsabilité légale en cas de piratage de télévision connectée par sexe	17
Figure 6 : Perception de la responsabilité légale en cas de piratage de télévision connectée par âge	18
Figure 7 : Quels types d'attaques concernant les objets connectés connaissez-vous ?	19
Figure 8 : Quelles raisons qui pousseraient un hacker à attaquer vos objets connectés, connaissez-vous ?	20
Figure 9 : Quelles mesures avez-vous prises afin de sécuriser vos objets connectés contre les cyberattaques ?	21
Figure 10 : Les types d'objets connectés possédés	22
Figure 11 : Période d'achat pour chaque catégorie	23
Figure 12 : Projection du nombre d'objets connectés qui vont être ajouter dans les foyers à l'avenir.....	24
Figure 13 : Objectif des objets connectés dans les foyers.....	25
Figure 14 : Facteurs clé dans le choix d'objets connectés pour la maison	26
Figure 15 : En moyenne, combien d'interaction(s) journalière(s) avez-vous avec vos objets connectés ?	27
Figure 16 : Utilisation de shodan.io.	30
Figure 17 : Information générale de 188.155.247.185.....	31
Figure 18 : Flux vidéo sur Shodan.io.....	32
Figure 19 : Utilisation de la fonction recherche.....	36
Figure 20 : Liste des identifiants des vulnérabilités.	36
Figure 21 : Utilisation de cve.org.....	37

1. Introduction

À l'ère numérique, les objets connectés, également connus sous le nom d'Internet des objets, ont radicalement transformé nos foyers et notre quotidien (PME 2023). La domotique, qui intègre ces objets connectés au sein de l'infrastructure domestique, a apporté des améliorations significatives en termes de confort, de sécurité, d'efficacité énergétique et de bien-être (Gabriele 2023). Les résidences Suisses, à l'instar de nombreuses autres à travers le monde, voient une adoption croissante de ces technologies, créant ainsi des maisons intelligentes où divers dispositifs peuvent être contrôlés et automatisés à distance (Statista 2024a).

Le secteur de la domotique connaît une expansion rapide (Statista 2024b). Cependant, cette croissance s'accompagne de défis majeurs, notamment en matière de sécurité des objets connectés et de protection des données personnelles des utilisateurs (Conseil fédéral 2020, p. 5). En effet, les objets connectés, en raison de leur interconnexion et de leur accès à des réseaux ouverts, sont particulièrement vulnérables aux cyberattaques, posant ainsi des problèmes de confidentialité et de sécurité des informations personnelles (PME 2023; OFCS 2024).

Dans ce contexte, la problématique de la sécurité des objets connectés dans les foyers genevois devient cruciale. Comment assurer la sécurité des objets connectés dans les foyers Genevois et protéger efficacement les données personnelles des utilisateurs ?

Les cybercriminels exploitent ces failles pour accéder aux réseaux domestiques, voler des informations personnelles ou même prendre le contrôle des appareils (Conseil fédéral 2020, p. 6,7). Face à ces enjeux, il est essentiel de développer et de mettre en œuvre des stratégies robustes de cybersécurité pour les objets connectés dans les foyers.

La présente étude vise à explorer ces questions en profondeur, en se concentrant sur les maisons genevoises. Elle analyse les principaux défis de sécurité liés aux objets connectés, les pratiques actuelles des utilisateurs en matière de cybersécurité, et propose des recommandations pour renforcer la sécurité des objets connectés. En adoptant une approche méthodologique mixte, combinant recherche qualitative et quantitative, cette étude apporte des réponses concrètes et applicables aux problématiques identifiées, contribuant ainsi à une meilleure sécurisation des foyers intelligents.

2. Contexte

Pour ce projet, nous nous concentrons exclusivement sur l'analyse des technologies qui sont spécifiquement intégrées dans l'infrastructure domestique. Nous avons mis en place un glossaire afin que les termes techniques spécifiques soient facilement compréhensibles (Annexe 1), Nous excluons délibérément de cette étude l'utilisation de dispositifs mobiles personnels comme les smartphones, les tablettes et les accessoires connectés tels que les montres intelligentes et autres wearables. Cette approche nous permet d'approfondir les implications et les interactions des technologies purement domestiques, sans les interférences des technologies mobiles souvent utilisées à des fins personnelles et en déplacement.

2.1 Méthodologie

Cette section décrit la méthodologie utilisée pour aborder notre question de recherche. Notre étude adopte une approche mixte, combinant des techniques de recherche qualitatives et quantitatives pour obtenir une compréhension complète des défis de sécurité et des solutions pour les objets connectés dans les foyers domestiques.

La conception de la recherche est structurée comme suit :

Les sources tirées d'Internet sont nombreuses dans cette étude, étant donné que les objets connectés sont un sujet très actuel avec une abondance d'informations disponibles. Notre recherche s'appuie sur des rapports de l'OFSC et du Conseil fédéral, des rapports spécifiques sur le sujet, des rapports de vulnérabilité, ainsi que sur des bases de données publiques répertoriant les vulnérabilités.

Un questionnaire non scientifique a été réalisée pour recueillir des données auprès des résidents de Genève concernant leur utilisation, leur niveau de connaissances et leur perception de la sécurité liée aux objets connectés dans leurs foyers. L'enquête a été diffusée via les réseaux sociaux, recueillant 115 réponses.

Une étude d'un cas approfondie d'un foyer équipé de divers types d'objets connectés. Cette étude de cas implique l'identification des vulnérabilités potentielles et de solutions.

Un expert en objets connectés et un pentester ont été consultés tout au long du processus de recherche afin d'obtenir des perspectives sur les pratiques de sécurité avancées et valider les résultats de l'enquête et du cas pratique.

2.2 Définition IOT

L'Internet des objets, également connu sous le nom Internet of Things (IOT), désigne la connexion d'objets physiques intégrés avec des composants électroniques, des logiciels et des capteurs au réseau, à leur identité numérique. Ces objets connectés sont capables de collecter et d'échanger des données, permettant ainsi de modifier leur état via Internet. L'objectif principal de l'IOT est de faciliter une variété d'applications, de l'amélioration du quotidien à l'optimisation de processus industriels complexes, grâce à cette capacité d'interconnexion et d'interaction entre les objets et leurs environnements numériques (OCDE 2018; PME 2023).

En effet, les objets connectés sont conçus pour améliorer l'efficacité, la commodité et la sécurité dans les foyers, tout en offrant des possibilités de contrôle et de surveillance à distance grâce à des interfaces utilisateur conviviales, souvent accessibles via des applications mobiles ou des interfaces web. Cependant, leur interconnexion et leur accès à des réseaux ouverts les exposent à des risques de sécurité et de confidentialité des données, posant des défis importants en matière de protection des informations personnelles des utilisateurs (OFCS 2024).

2.3 Qu'est-ce qu'une maison intelligente ?

Une maison intelligente, aussi appelée smart home, désigne une maison équipée d'une variété d'objets connectés qui facilitent l'automatisation et le contrôle à distance de nombreux aspects de notre vie quotidienne au sein du domicile. Ces dispositifs sont souvent reliés entre eux via un réseau domestique (Wi-Fi de la maison), ce qui permet une gestion centralisée à travers des applications sur nos smartphones ou d'autres interfaces utilisateur, comme des assistants vocaux par exemple. L'intégration de ces technologies dans les maisons vise principalement à améliorer notre confort, à améliorer l'efficacité énergétique (prise connectée) et à renforcer la sécurité. Par exemple, les systèmes d'éclairage intelligents peuvent s'adapter automatiquement selon l'heure de la journée ou détecter une présence dans les pièces. En matière de sécurité, les maisons intelligentes sont équipées de caméras de surveillance, de systèmes d'alarme avancés, de détecteurs de mouvement et même de serrures connectées qui peuvent être verrouillées ou déverrouillées à distance, cela offre ainsi une tranquillité d'esprit. Les alarmes peuvent également être configurées comme pour alerter les propriétaires et les autorités en cas d'activité suspecte, ce qui garantit une réponse rapide en cas d'urgence et une meilleure sécurité. La gestion des appareils électroménagers via des applications permet, elle, une plus grande commodité. De plus, l'expérience utilisateur dans une

maison intelligente est renforcée par l'utilisation d'assistants vocaux qui permettent une interaction sans smartphone ou autre interface utilisateur afin de contrôler les dispositifs connectés. Les maisons intelligentes représentent donc la fusion de la technologie actuelle et du confort domestique, cela offre une multitude de fonctionnalités qui améliorent l'efficacité énergétique, la sécurité, et le confort général de ces dernières. Elles symbolisent une avancée dans la façon dont nous interagissons avec nos environnements de vie, ce qui ouvre la porte à des innovations futures qui continueront de transformer nos habitats et notre quotidien (Hengsberger 2024).

2.4 Avantages et inconvénients d'une maison intelligente

Les maisons intelligentes offrent une multitude de bénéfices comme :

- Le confort

Les dispositifs de maison intelligente offrent la commodité de contrôler les appareils de la maison à distance via un smartphone ou des commandes vocales. Par exemple, il est possible d'éteindre les ampoules intelligentes à l'étage sans y être ou de vérifier le système de sécurité de la maison alors que nous nous trouvons à des centaines de kilomètres. La possibilité de tout contrôler avec un smartphone apporte un niveau de confort et de contrôle sans précédent.

- La tranquillité d'esprit

Avec des dispositifs de sécurité intelligents, tels que les sonnettes connectées et les caméras de surveillance, nous pouvons toujours être informés en temps réel si quelque chose d'anormal se produit chez nous. Ces appareils peuvent notifier immédiatement en cas d'intrusion, ce qui offre ainsi une grande tranquillité d'esprit.

- La sécurité

Les dispositifs comme les serrures intelligentes et les caméras protègent constamment le domicile. Cela permet par exemple de verrouiller ou de déverrouiller les portes à distance, ce qui élimine le besoin de partager des codes de garage ou de donner des clés de rechange. Mais également vérifier si les portes sont bien fermées après notre départ et autoriser l'accès aux personnes de confiance en quelques clics.

- L'économie d'énergie

Les appareils intelligents écoénergétiques, comme les thermostats intelligents ou prise connectée, réduisent considérablement la consommation d'énergie. Ces thermostats par exemple, apprennent les habitudes des occupants et ajustent la température en conséquence, ce qui permet de réaliser des économies et de gérer son énergie (Vivint 2023; Gabriele 2023).

Les maisons intelligentes représentent donc une fusion de la technologie et du confort domestique, offrant des fonctionnalités avancées qui améliorent la qualité de vie et la sécurité des occupants et l'efficacité énergétique des foyers.

Cependant, posséder une maison intelligente présente également des inconvénients comme :

- Le coût élevé

L'installation des technologies de maison intelligente peut être coûteuse. Les dispositifs intelligents, ainsi que leur intégration dans un système d'interopérabilité, représentent un investissement initial important. De plus, les coûts de maintenance et de réparation peuvent s'ajouter avec le temps.

- Les problèmes de sécurité des objets connectés

Les dispositifs intelligents collectent et stockent des données sur les habitudes d'utilisation et des informations personnelles. Si ces données ne sont pas correctement protégées, elles peuvent être accessibles à des tiers non autorisés, posant des risques de violation de la vie privée et de sécurité des données.

- Compatibilité et Complexité :

Avec une grande variété de dispositifs et de systèmes disponibles sur le marché, des problèmes de compatibilité peuvent survenir. Différents fabricants utilisent différents protocoles, ce qui peut compliquer l'intégration des dispositifs et rendre la gestion de la maison intelligente plus difficile.

- Dépendance à la connexion Internet :

La plupart des dispositifs intelligents dépendent d'une connexion Internet stable pour fonctionner correctement. En cas de panne d'Internet, de nombreuses fonctions peuvent être perturbées ou inaccessibles, affectant la sécurité et la gestion de la maison (HAWRYLACK 2024).

Ces inconvénients montrent que bien que les maisons intelligentes offrent de nombreux avantages, elles présentent également des défis qui doivent être pris en compte avant de faire un investissement.

2.5 Identification des principaux défis en matière de sécurité de l'IOT

D'après le rapport du Conseil fédéral sur les normes de sécurité pour les appareils connectés à Internet, le développement rapide des appareils connectés à Internet est principalement guidé par des priorités de fonctionnalité et de coût, plutôt que de sécurité. En raison de la pression sur les coûts, des délais serrés et d'une compréhension limitée des cyberattaques potentielles, de nombreux fabricants ne voient aucun avantage commercial à offrir des mises à jour de sécurité ou à intégrer des fonctions de sécurité spécifiques dans leurs appareils. Les utilisateurs finaux, souvent non sensibilisés aux risques de sécurité, créent également une demande insuffisante pour des produits sécurisés. Par conséquent, il y a une offre et une demande limitées pour des appareils connectés à Internet sécurisés, en particulier dans le segment grand public où les prix bas dominent (Conseil fédéral 2020, p. 5).

Selon ce même rapport, les cyberattaques connues impliquant des appareils IOT peuvent être classées en quatre catégories principales :

- Accès Direct aux Appareils

Les cybercriminels cherchent à manipuler, contrôler ou détourner les appareils IOT directement dans les maisons. Par exemple, ils peuvent attaquer des enceintes connectées ou des babyphones pour écouter clandestinement des conversations privées, compromettant ainsi la vie privée des occupants. Ils peuvent également prendre le contrôle de thermostats intelligents pour modifier les températures de manière inattendue ou désactiver les systèmes de sécurité, mettant en danger la sécurité du domicile.

- Pénétration de Réseaux Locaux

Les attaques utilisent souvent des appareils IOT domestiques comme points d'entrée pour accéder à des réseaux locaux plus vastes. Par exemple, un cybercriminel peut exploiter une caméra de sécurité mal sécurisée pour s'infiltrer dans le réseau domestique, puis accéder à d'autres appareils connectés, tels que des ordinateurs personnels, des smartphones ou des routeurs, sans manipuler directement les appareils IOT eux-mêmes.

- Création de Réseaux de Zombies

Les appareils IOT domestiques sont fréquemment utilisés pour créer des réseaux de zombies, également connus sous le nom de botnets, qui peuvent lancer des attaques DDOS contre d'autres cibles. Par exemple, un cybercriminel peut infecter des dizaines de milliers de caméras de sécurité pour submerger un site web ou un service en ligne, rendant ce dernier inaccessible et causant des perturbations majeures.

- Utilisation des Capacités de Calcul

Les cybercriminels exploitent souvent les capacités de calcul des appareils IOT domestiques pour des activités comme le minage de cryptomonnaie. Par exemple, un attaquant peut utiliser un logiciel malveillant pour détourner les capacités de calcul d'une télévision intelligente ou d'une caméra, les utilisant à leur insu pour générer des cryptomonnaies, ce qui augmente la consommation d'électricité et réduit la durée de vie de l'appareil (Conseil fédéral 2020, p. 6,7).

Les cyberattaques impliquant des appareils IOT dans les foyers peuvent prendre des formes variées, mais elles partagent toutes un potentiel significatif de compromettre la sécurité et la vie privée des utilisateurs. Cela souligne l'importance d'une vigilance accrue et de mesures de sécurité rigoureuses pour protéger les IOT dans les foyers genevois. Il est essentiel de comprendre ces menaces pour pouvoir mettre en place des stratégies de défense appropriées et ainsi sécuriser les environnements domestiques contre les cybercriminels toujours plus ingénieux. Les utilisateurs doivent être proactifs dans l'application des meilleures pratiques de cybersécurité pour atténuer les risques et protéger leurs données personnelles et leurs réseaux domestiques contre les cyberattaques.

De plus, les cybercriminels sont motivés à entreprendre ce genre d'action illégale avec des objectifs spécifiques lorsqu'ils piratent des objets connectés, tels que :

- Appât du Gain

Les cybercriminels peuvent cibler les IOT domestiques mal sécurisés pour créer des réseaux de zombies, qu'ils utilisent pour lancer des attaques DDOS ou qu'ils louent à d'autres criminels. Les rançongiciels sont également utilisés pour chiffrer les données des appareils domestiques et extorquer de l'argent aux propriétaires en échange de la restauration de l'accès.

- Sabotage

Les cyberattaques peuvent viser les IOT dans les maisons pour perturber les systèmes domestiques essentiels, tels que les systèmes de sécurité, le chauffage, ou l'éclairage. En perturbant ces systèmes, les attaquants peuvent causer des désagréments importants et potentiellement des dommages matériels.

- Espionnage

Les IOT domestiques peuvent être exploités pour l'espionnage, avec des logiciels malveillants installés pour surveiller les activités des occupants. Ces programmes peuvent capter et transmettre des informations sensibles, permettant aux attaquants de recueillir des données personnelles ou des habitudes de vie à des fins malveillantes (Conseil fédéral 2020, p. 7).

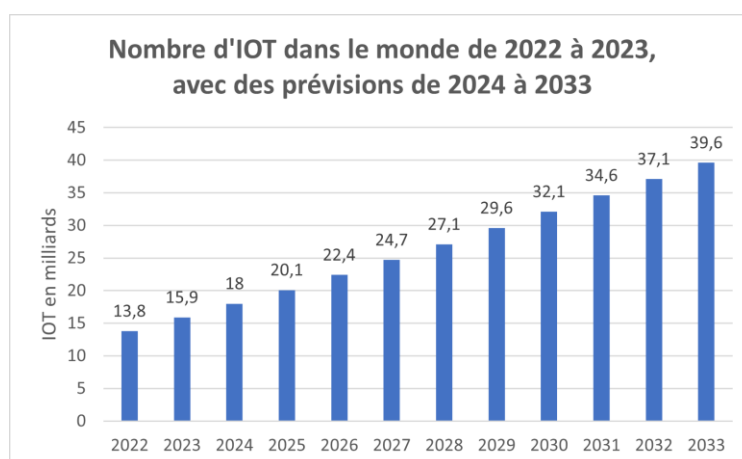
Ces objectifs illustrent la diversité des risques associés aux objets connectés et soulignent la nécessité d'une vigilance accrue et de mesures de sécurité robustes. En comprenant les objectifs des cybercriminels, les utilisateurs peuvent mieux se préparer et mettre en œuvre des stratégies de défense efficaces pour protéger leurs foyers contre les menaces croissantes de cyberattaques.

3. Expansion du marché

3.1 Marché mondial de l'IOT

Selon une analyse approfondie réalisée par Statista, le marché mondial des objets connectés poursuit sa croissance impressionnante. Pour l'année 2024, il est prévu que la valeur de ce marché atteigne les 336 milliards de dollars, avec une projection ambitieuse de 621,6 milliards de dollars d'ici 2030. Le segment le plus dynamique de ce marché est celui des produits destinés aux consommateurs, qui comptait déjà 7,7 milliards d'objets connectés en circulation en 2022 (Statista 2023a, p. 3,7).

Figure 1: Nombre d'IOT dans le monde de 2022 à 2023, avec des prévisions de 2024 à 2033.



(Statista 2024c)

Selon ce graphique reproduit à partir de Statista, le nombre d'IOT dans le monde devrait plus que doubler au cours des prochaines années, passant de 13,8 milliards en 2022 à plus de 32,1 milliards d'ici 2030 (Statista 2024c). Ces données sont basées sur les chiffres de Transforma Insights et englobent non seulement les dispositifs de détection et d'actionnement à distance (capteurs et actionneurs individuels), mais aussi les dispositifs qui assurent la collecte et l'agrégation des données (Transforma Insights 2024).

Les IOT représentés dans ce graphique sont utilisés dans divers secteurs industriels et marchés de consommation, cependant les consommateurs représentant environ 55 % de tous les dispositifs IOT en 2022. Selon Statista, en 2023, le segment des consommateurs représente environ 60 % de tous les dispositifs IOT ou connectés. Cette proportion devrait rester stable au cours des dix prochaines années (Sujay Vailshery 2024).

3.2 Marché mondial de la maison intelligente

Concernant spécifiquement le secteur mondial de la maison intelligente, les prévisions sont également prometteuses. Il est estimé que le nombre de maisons intelligentes dans le monde s'élèvera à 493,5 millions en 2025, avec une augmentation attendue à 785,2 millions d'ici 2028. Le nombre de foyers adoptant les technologies intelligentes est en hausse, cela peut être dû au fait que les consommateurs sont de plus en plus prêts à investir dans des systèmes qui offrent non seulement plus de confort et de sécurité, mais aussi une gestion plus efficace de l'énergie et des ressources, contribuant ainsi à une maison à la fois plus connectée et durable (Statista 2023b, p. 10). À noter que dans ce rapport, Statista inclut les dispositifs connectés directement ou indirectement à Internet via une passerelle, servant à contrôler, surveiller et réguler les fonctions d'un foyer privé. Les appareils dont la fonction première n'est pas l'automatisation ou la commande à distance, comme les smartphones et les tablettes, ainsi que les télévisions intelligentes, ne sont pas inclus dans leur définition (Statista 2023b, p. 6).

De plus, un graphique présenté par Statista sur la répartition détaillée des appareils domestiques intelligents possédés par les ménages (télévisions intelligentes comprises), nous montre les préférences actuelles des consommateurs en matière de technologies de maison intelligente. L'adoption des téléviseurs intelligents est particulièrement élevée, suivis par les assistants virtuels. Les appareils de sécurité et de gestion énergétique montrent également une adoption significative, soulignant l'importance de la sécurité et de l'efficacité dans les foyers modernes. Cependant, il existe encore des segments, comme les contrôles intelligents pour radiateurs et climatiseurs, qui présentent des opportunités de croissance (Statista 2022).

De plus, selon le rapport : 2023 IOT Security Landscape, les foyers américains comptent en moyenne 46 dispositifs connectés, tandis que les foyers européens en comptent 25. Cette densité d'appareils pose des défis significatifs en matière de sécurité et montre que le marché européen est en pleine expansion, mais reste en retrait par rapport aux États-Unis en termes de densité de dispositifs connectés par foyer. Cette différence indique un potentiel de croissance important pour le marché européen des maisons intelligentes. De plus, avec l'augmentation prévue du nombre de dispositifs connectés, il est impératif de mettre en place des mesures de sécurité robustes pour prévenir les intrusions et les violations de données. En effet, les foyers connectés subissent en moyenne huit attaques contre leurs appareils toutes les 24 heures. Cette statistique alarmante souligne la vulnérabilité accrue des environnements domestiques face aux cybermenaces et repose sur des données collectées auprès de 2,6 millions de foyers

intelligents à travers le monde. Environ 120 millions d'IOT ont été analysés, générant 3,6 milliards d'événements de sécurité (2023-IoT-Security-Landscape-Report).

3.3 Marché suisse de la maison intelligente

Pour mieux comprendre et approfondir notre analyse du marché des maisons intelligentes en Suisse, il est essentiel de segmenter ce marché en six catégories distinctes. Cette segmentation nous permet d'examiner plus en détail les différentes facettes de ce marché dynamique et en croissance rapide. Les catégories sur lesquelles nous nous concentrons sont : les appareils intelligents, le contrôle et la connectivité, le confort et l'éclairage, la sécurité, la gestion de l'énergie et le divertissement domestique. En analysant chacune de ces catégories, cela nous permet d'avoir une vision complète et approfondie du marché des maisons intelligentes en Suisse.

Concernant spécifiquement le marché des appareils intelligents, cela comprend les robots aspirateurs, réfrigérateurs intelligents, machines à café connectées, etc. Le chiffre d'affaires de ce marché devrait augmenter à un taux de croissance annuel moyen de 9,78% à partir de 2024. Il est estimé que ce marché passe de plus de 422,2 millions de dollars en 2024 à plus de 613,5 millions de dollars en 2028. Cette croissance sera accompagnée d'une augmentation significative du nombre d'utilisateurs d'appareils intelligents, atteignant 3,1 millions d'utilisateurs d'ici 2028 (Statista 2024d).

Pour le marché du contrôle et de la connectivité, cela comprend les enceintes intelligentes, les prises intelligentes, etc. Le chiffre d'affaires de ce marché devrait augmenter à un taux de croissance annuel moyen de 9.48% à partir de 2024. Il est estimé que ce marché passe de 180,1 millions de dollars en 2024 à 258,7 millions de dollars en 2028. Cette croissance sera accompagnée d'une augmentation significative du nombre d'utilisateurs du contrôle et de la connectivité, atteignant 1,2 million d'utilisateurs d'ici 2028 (Statista 2024e).

Quant au marché du confort et de l'éclairage, cela comprend les ampoules intelligentes, les stores connectés, etc. Le chiffre d'affaires de ce marché devrait augmenter à un taux de croissance annuel moyen de 9.84% à partir de 2024. Il est estimé que ce marché passe de 144.4 millions de dollars en 2024 à 210.2 millions de dollars en 2028. Cette croissance sera accompagnée d'une augmentation significative du nombre d'utilisateurs de confort et éclairage, atteignant 3,4 millions d'utilisateurs d'ici 2028 (Statista 2024f).

Pour le marché de la sécurité, cela comprend les caméras de sécurité, les détecteurs de mouvement, les serrures de porte connectée, etc. Le chiffre d'affaires de ce marché

devrait augmenter à un taux de croissance annuel moyen de 8.62% à partir de 2024. Il est estimé que ce marché passe de 133,7 millions de dollars en 2024 à 186,1 millions de dollars en 2028. Cette croissance sera accompagnée d'une augmentation significative du nombre d'utilisateurs de sécurité, atteignant 2,9 millions d'utilisateurs d'ici 2028 (Statista 2024g).

En ce qui concerne le marché de la gestion de l'énergie, cela comprend les thermostats intelligents, climatiseurs intelligents, etc. Le chiffre d'affaires de ce marché devrait augmenter à un taux de croissance annuel moyen de 12.87% à partir de 2024. Il est estimé que ce marché passe de 96.4 millions de dollars en 2024 à 156.4 millions de dollars en 2028. Cette croissance sera accompagnée d'une augmentation significative du nombre d'utilisateurs de gestion de l'énergie, atteignant 3 millions d'utilisateurs d'ici 2028 (Statista 2024h).

Enfin, pour le marché du divertissement domestique, cela comprend les systèmes audio connectés, les télécommandes intelligentes, etc. Le chiffre d'affaires de ce marché devrait augmenter à un taux de croissance annuel moyen de 3.52% à partir de 2024. Il est estimé que ce marché passe de 106.4 millions de dollars en 2024 à 122.2 millions de dollars en 2028. Cette croissance sera accompagnée d'une augmentation significative du nombre d'utilisateurs de divertissement domestique, atteignant 2,2 millions d'utilisateurs d'ici 2028 (Statista 2024i).

Pour finir, le marché suisse de la maison intelligente augmente continuellement à un taux de croissance annuel moyen de 9.32% à partir de 2024. Il est estimé que ce marché passe de 1,083 milliards de dollars en 2024 à 1,547 milliard de dollars en 2028. De plus, les segments qui devraient générer le plus de revenus dans le domaine des maisons intelligentes en 2028 incluent les appareils intelligents, qui occupent la première place, suivis par les solutions de contrôle et de connectivité. Viennent ensuite le confort et l'éclairage, la sécurité, la gestion de l'énergie, ainsi que le divertissement domestique. Ces domaines reflètent une tendance croissante vers une technologie résidentielle plus intégrée et automatisée (Statista 2024a).

Pour conclure, le marché des maisons intelligentes en Suisse connaît une croissance soutenue et prometteuse, avec des tendances positives dans tous ses segments. Cette dynamique est alimentée par une demande croissante des consommateurs pour des solutions améliorant la qualité de vie. L'intérêt des Suisses pour les technologies de maison intelligente est évident, avec une forte adoption prévue dans les années à venir. Cette évolution vers des technologies résidentielles plus intégrées et automatisées

laisse entrevoir un avenir prospère pour ce marché, offrant de nombreuses opportunités dans ce secteur en expansion.

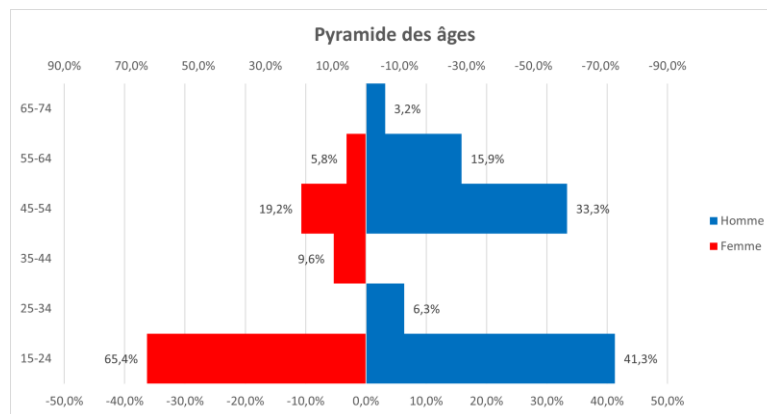
4. Analyse des objets connectés dans les maisons genevoises

Pour mieux comprendre comment assurer la sécurité concernant les objets connectés dans nos maisons genevoises, il semble important de se tourner vers les gens qui composent notre société, ceux qui nous entourent. C'est pourquoi, un questionnaire non scientifique a été mis en place par nos soins en avril à Genève (Annexe 2). Cependant, il convient de noter qu'au moment de la réalisation de ce questionnaire, nous ne disposions pas des connaissances actuelles. Par conséquent, il est possible que le questionnaire présente un léger biais, car nous n'avons pas exclu les wearables (appareils portables connectés) lors de la création de celui-ci. Avec une compréhension plus approfondie de la sécurité des objets connectés, une exclusion des wearables aurait permis de concentrer davantage sur les dispositifs spécifiques à l'infrastructure domestique, ce qui aurait pu affiner les résultats et les conclusions de cette enquête. Cette limitation doit être prise en compte lors de l'interprétation des données recueillies, bien que les informations obtenues restent pertinentes pour identifier les comportements et les préoccupations générales des utilisateurs genevois en matière de sécurité et utilisations des objets connectés. Ce questionnaire est segmenté en 3 parties, la première afin de récolter l'âge et le sexe des participants, la deuxième se concentrant uniquement sur la partie cybersécurité des objets connectés et la dernière se concentrant sur la relation que les participants ont avec leurs objets connectés. Ce questionnaire a été partagé sur mes réseaux sociaux et 115 participations ont été récoltées.

4.1 Données démographiques

Regardons de plus près ce que ce graphique met en évidence : sur ces 115 participations, 54,8% sont des hommes et 45,2% sont des femmes.

Figure 2 : Pyramide des âges

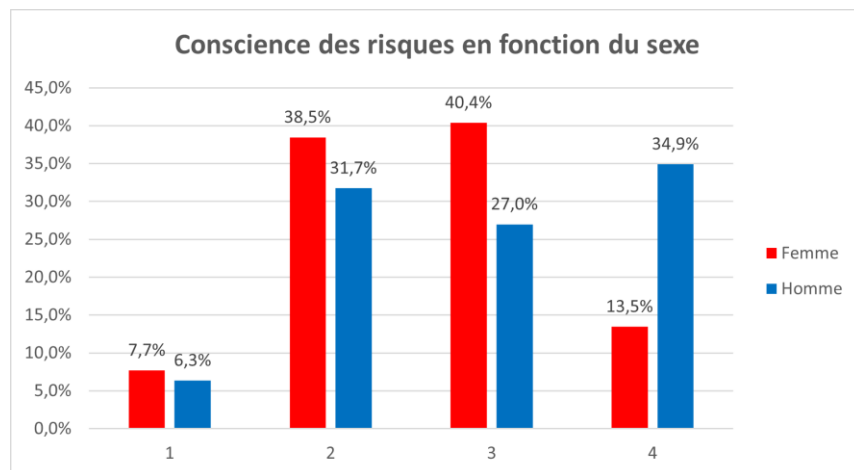


Ce premier graphique est une pyramide des âges de notre échantillon, qui montre la distribution de la population par groupe d'âge et par sexe. Les âges sont divisés en tranches de dix ans. Ce graphique montre une répartition inégale entre les sexes au sein de différentes tranches d'âge. Nous observons une prédominance féminine marquée dans la tranche des 15-24 ans, avec 65,4% des femmes sondées tandis que le reste des femmes est dispersé dans les tranches de 35-65 ans. En ce qui concerne les hommes, 41,3% sont dans la tranche des 15-24 ans. De plus presque la moitié des hommes sondés se retrouve dans les tranches de 45-64 ans. Afin de clarifier les graphiques suivants j'ai créé 2 catégories d'âge à partir de cette pyramide : une catégorie <30 ans et une ≥30 ans.

4.2 Cybersécurité des objets connectés

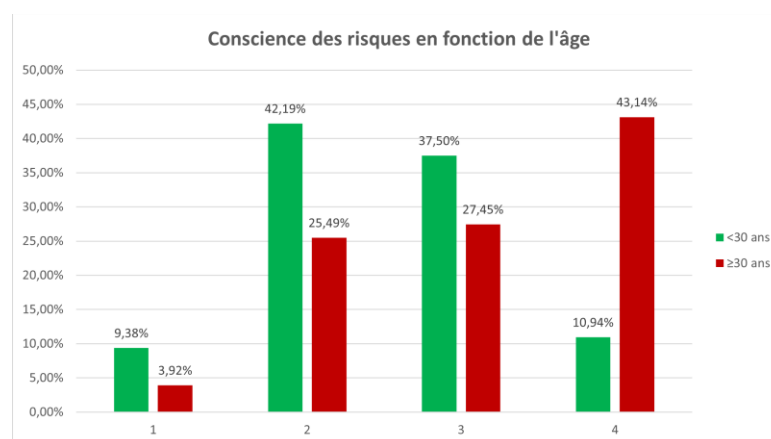
Il est essentiel de comprendre les risques auxquels nous sommes exposés et d'adopter des mesures préventives pour protéger notre vie privée et notre sécurité. C'est pourquoi nous avons interrogé les sondés sur leurs connaissances en matière de cybersécurité, ainsi que sur les mesures qu'ils prennent pour se protéger contre les menaces potentielles associées aux objets connectés dans leurs foyers.

Figure 3 : Conscience des risques en fonction du sexe



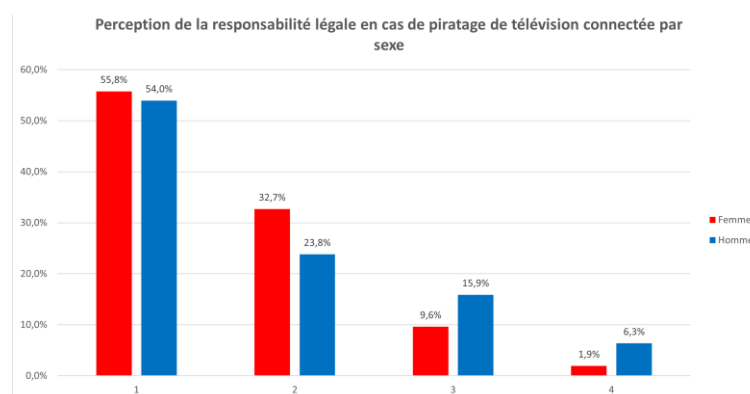
Ces graphiques qui questionnent notre échantillon sur leur conscience des risques de cybersécurité liés à l'utilisation des objets connectés dans leur quotidien, 1 étant pas conscient et 4 étant très conscient. Nous remarquons sur le premier graphique qui filtre en fonction du sexe du sondé que seule une minorité égale d'homme et de femme n'est pas consciente des risques, alors qu'une grande majorité (78,9%) des femmes est modérément consciente des risques contre 58,7% pour les hommes. Cependant 34,9% des hommes se disent très conscients contre seulement 13,5% des femmes. Il semble que les femmes tendent à avoir une conscience modérée des risques de cybersécurité, tandis que les hommes montrent une conscience plus élevée de ces risques.

Figure 4 : Conscience des risques en fonction de l'âge



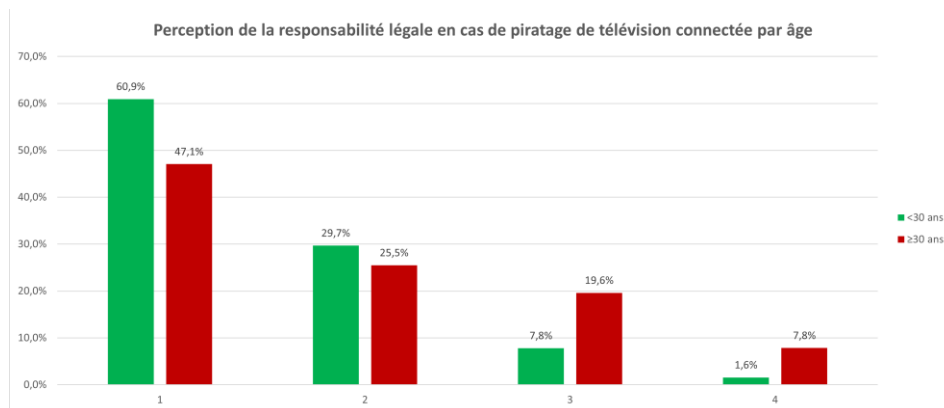
Sur ce graphique qui filtre en fonction de l'âge du sondé, nous remarquons que l'âge semble jouer un rôle important dans la perception des risques de cybersécurité liés aux objets connectés. Les sondés plus âgés (≥ 30 ans) ont tendance à être plus conscients des risques avec 43% qui se sentent très conscients des risques, ce qui peut être causé par une plus grande expérience de vie. Cependant, les jeunes (< 30 ans), se sentent modérément conscients des risques, cela montre un besoin potentiel de renforcer l'éducation et la sensibilisation sur la cybersécurité concernant les objets connectés dans cette catégorie d'âge.

Figure 5 : Perception de la responsabilité légale en cas de piratage de télévision connectée par sexe



Nous avons également mesuré la perception de la responsabilité légale en cas de piratage d'appareils connectés utilisés à l'insu de leur propriétaire pour commettre des infractions (1 étant 0% fautif et 4 étant 100% fautif). Nous observons que la différence entre les hommes et les femmes est assez faible, cependant, moins de femmes atteignent le degré de reconnaissance de faute le plus élevé (4) comparativement aux hommes. Cependant, une majorité des femmes comme des hommes ne se pense pas fautif.

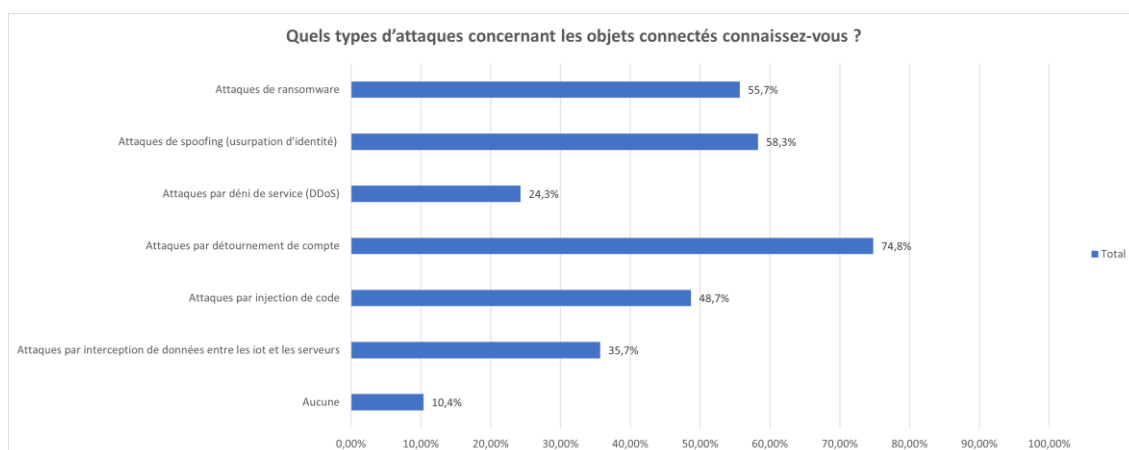
Figure 6 : Perception de la responsabilité légale en cas de piratage de télévision connectée par âge



Nous retrouvons de plus gros écarts lorsqu'on filtre par l'âge, 60,9% des <30 ans ne se pense pas fautif contre 47,1% pour les ≥30 ans. Les individus ≥30 ans sont beaucoup plus susceptibles de se sentir pleinement responsables légalement par rapport aux <30 ans.

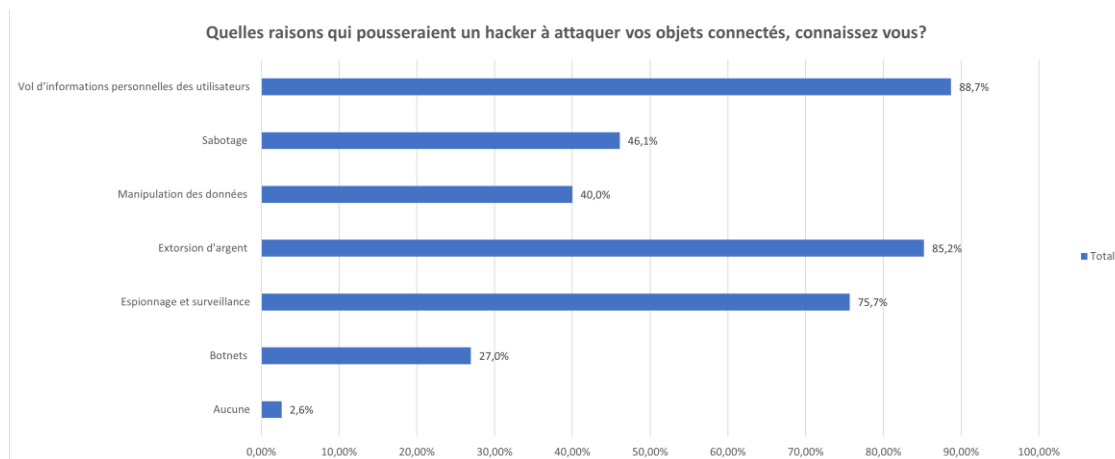
Afin d'avoir la bonne réponse, nous avons posé la question suivante à un expert en objets connectés : « Le propriétaire d'une télévision connectée se fait hacker, et cette dernière est utilisée afin d'attaquer une entreprise, quelle est sa responsabilité ? ». Selon lui, puisque l'attaque est lancée depuis son objet connecté et via sa connexion Internet, le propriétaire est présumé responsable des actions entreprises par ses objets connectés. Cela implique une obligation de surveiller et de sécuriser activement ses objets connectés. En agissant ainsi, il démontre non seulement un effort conscient pour protéger ses données et limiter les dégâts, mais aussi minimiser ainsi sa responsabilité. Par exemple, en cas d'utilisation d'objets connectés piratés afin d'attaquer une autre personne ou entreprise.

Figure 7 : Quels types d'attaques concernant les objets connectés connaissez-vous ?



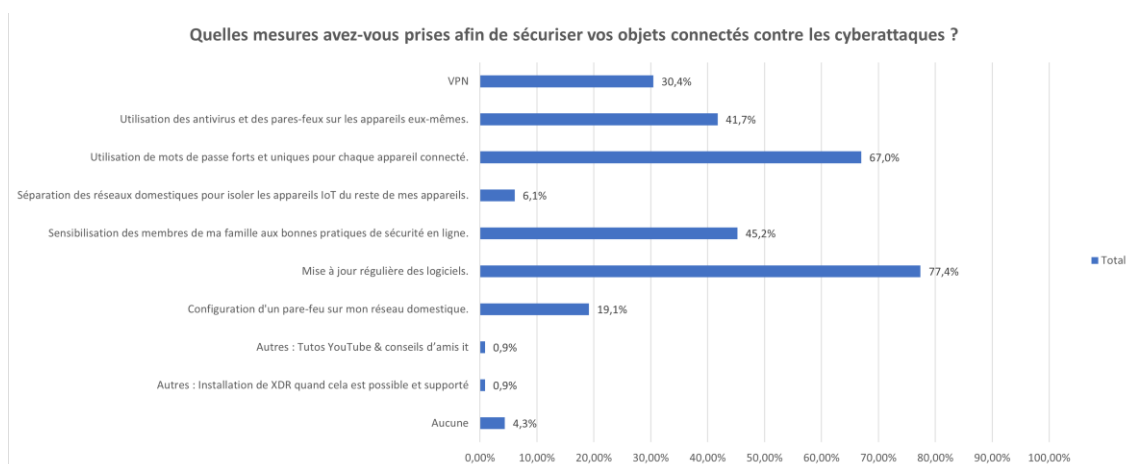
Ce graphique montre la connaissance des différents types d'attaques informatiques liées aux objets connectés par les sondés. Ce que nous remarquons c'est que les attaques les plus connues sont celles dont nous parlons le plus sur les réseaux sociaux comme le détournement de compte et l'usurpation d'identité. Cependant une sensibilisation a tout de même été faite concernant les virus et les injections de code dans ces objets connecté. Peu sont les sondés qui connaissent les interceptions de données et les DDoS. Il y a tout de même 10,4% qui ne connaissent aucun de ces types d'attaque ce qui démontre que la sensibilisation à la sécurité pourrait être tout de même améliorée.

Figure 8 : Quelles raisons qui pousseraient un hacker à attaquer vos objets connectés, connaissez-vous ?



Ce graphique montre les résultats d'un sondage sur les raisons pour lesquelles un hacker pourrait attaquer des objets connectés, selon la connaissance des sondés. Nous remarquons une similitude avec le graphique précédent puisque le vol d'informations personnelles est la raison la plus connue parmi les sondés suivis de l'extorsion d'argent et l'espionnage qui sont souvent médiatisés. Nous l'oublions souvent mais il existe également le sabotage qui a pour but de nuire directement au propriétaire. Nous remarquons également que la manipulation des données et botnets sont les motifs les moins connus ce qui est cohérent avec le graphique précédent, où l'utilisation de botnets pour mener des attaques par déni de service (DOS) contre, par exemple, des entreprises n'est pas très connue.

Figure 9 : Quelles mesures avez-vous prises afin de sécuriser vos objets connectés contre les cyberattaques ?



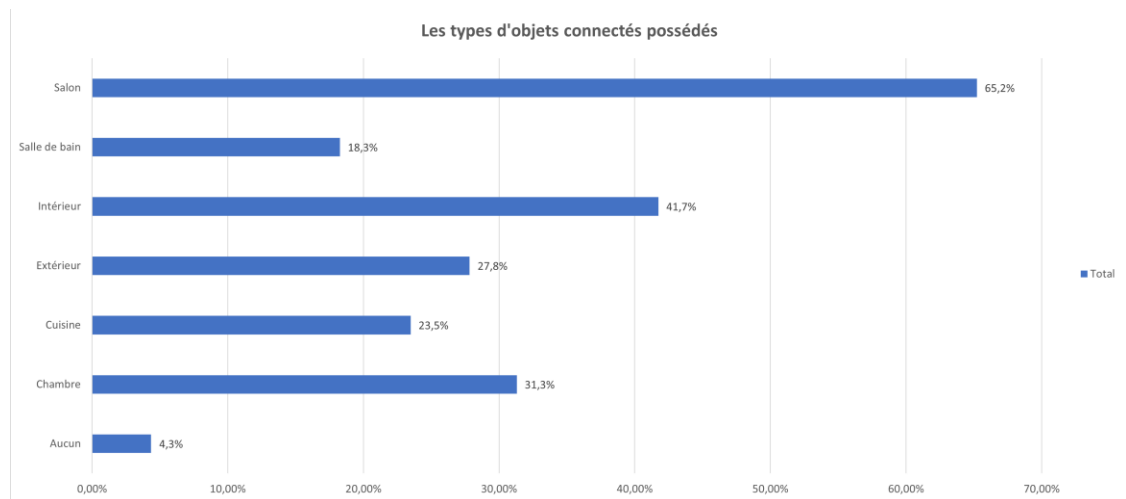
Afin de se protéger de ces possibles attaques, les particuliers mettent en place des mesures de sécurité afin de protéger leurs objets connectés contre les cyberattaques. Nous remarquons que les mesures prises les plus courantes sont aussi les plus simples à mettre en place comme les mises à jour régulière des logiciels, l'utilisation de mots de passe fort et unique ainsi que la sensibilisation de la famille aux bonnes pratiques. Malgré le haut taux de sondés qui mettent en place ces mesures, nous remarquons que beaucoup ne le font pas encore. Pour ce qui est des mesures de sécurité plus avancées comme le VPN, l'utilisation des antivirus/pare-feux sur les appareils eux-mêmes ainsi que l'utilisation d'un pare-feu sur le réseau domestique sont bien moins utilisées mais la plus simple de ces mesures reste tout de même de payer un VPN ou un antivirus sur ses appareils. Une mesure moins courante est la séparation du réseau domestique afin d'isoler les objets connectés du reste des appareils. Nous avons également laissé la possibilité aux sondés de mettre leur propre mesure de sécurité, l'une provient d'une personne ayant suivi des tutoriels sur YouTube ou reçu des conseils d'amis spécialisés dans le domaine de l'informatique et une autre mesure avancée mentionnée par un sondé est l'installation de solutions « Extended Detection and Response » (XDR), lorsqu'elles sont disponibles et compatibles. Cette mesure est une solution de cybersécurité qui combine plusieurs outils et fonctionnalités pour fournir une détection et une réponse intégrée contre les menaces (Microsoft 2024).

Ce graphique nous a permis d'avoir un aperçu de la façon dont les gens sécurisent leurs objets connectés, montrant une préférence pour les pratiques de sécurité de base. Des mesures plus avancées sont moins fréquemment utilisées, ce qui nous montre que même si la sensibilisation aux pratiques de sécurité de base est relativement élevée, les configurations de sécurité un peu plus complexes sont moins connues ou utilisées par le grand public.

4.3 Relation des personnes aux objets connectés

Lorsqu'il s'agit de la relation des sondés avec leurs objets connectés, il est intéressant de comprendre leurs comportements, leurs préférences, ainsi que les facteurs qui influencent leurs décisions lors d'achat.

Figure 10 : Les types d'objets connectés possédés



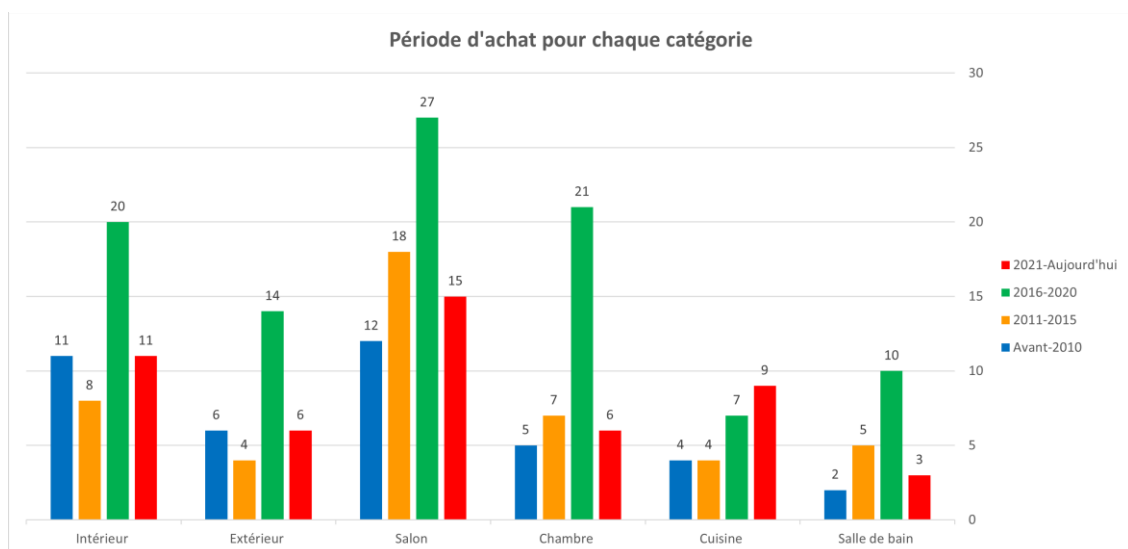
Pour ce graphique, nous avons posé une question sur les types d'objets connectés que les sondés possèdent chez dans leurs maisons. Nous avons donné une liste d'exemples d'objets connectés pour chaque catégorie, en concluant chaque énumération par "autre" afin d'indiquer que cette liste n'est pas exhaustive et que d'autres objets similaires peuvent également être inclus.

Nous avons créé 6 catégories d'objets connectés, nous avons le salon qui comporte des objets connectés comme les aspirateurs robots, les télévisions connectées les assistants vocaux etc. C'est la catégorie qui domine, avec 65,2% possédant ce type d'objet. Cela correspond au graphique de Statista mentionné dans la section précédente, qui indique que les dispositifs connectés les plus populaires sont les télévisions intelligentes et les assistants vocaux (Statista 2022). En ce qui concerne les objets connectés que nous pouvons retrouver dans toutes les pièces, nous avons créé la catégorie intérieure avec 41,7% qui possèdent des objets comme des systèmes d'éclairage, des caméras de surveillance, des stores, des climatiseurs, etc. Toujours dans le même graphique de Statista, nous retrouvons en 3e position les éclairages intelligents ce qui correspond encore une fois aux données récoltées par ce sondage. Ensuite nous avons la chambre qui regroupe des télévisions connectées, des miroirs, des réveils etc. avec 31,3%. Pour l'extérieur nous y retrouvons des sonnettes, des alarmes, des serrures, des arrosages etc. avec 27,8%, cette catégorie mais plus

précisément les systèmes de sécurité étaient eux aussi dans le top des objets les plus possédés selon Statista. Seul 23,5% possèdent des objets connectés dans leurs cuisines ce qui comprends des balances de cuisines, des distributeurs automatiques pour animaux, des réfrigérateurs ou même des assistant culinaire, etc. Pour finir nous avons la salle de bain avec seulement 18,3% qui possèdent des objets comme des brosses à dent électrique connectée, des balances, des miroirs, etc. 4,3% des sondés ne possèdent aucun de ces objets connectés ce qui concorde avec les 4,3% précédent. Globalement, ce graphique nous montre la répartition et la popularité des objets connectés dans différents espaces de la maison, mettant en lumière les tendances actuelles de la domotique dans les foyers genevois.

Dans le prochain graphique, nous examinons la période d'achat des premiers objets connectés pour chaque catégorie. Nous remarquons que beaucoup d'objets connectés ont été achetés pour la première fois dans la période 2016-2020, nous pouvons l'expliquer avec l'arrivée du confinement et le télétravail qui a augmenté le besoin d'un confort à la maison tout en restant très connecté.

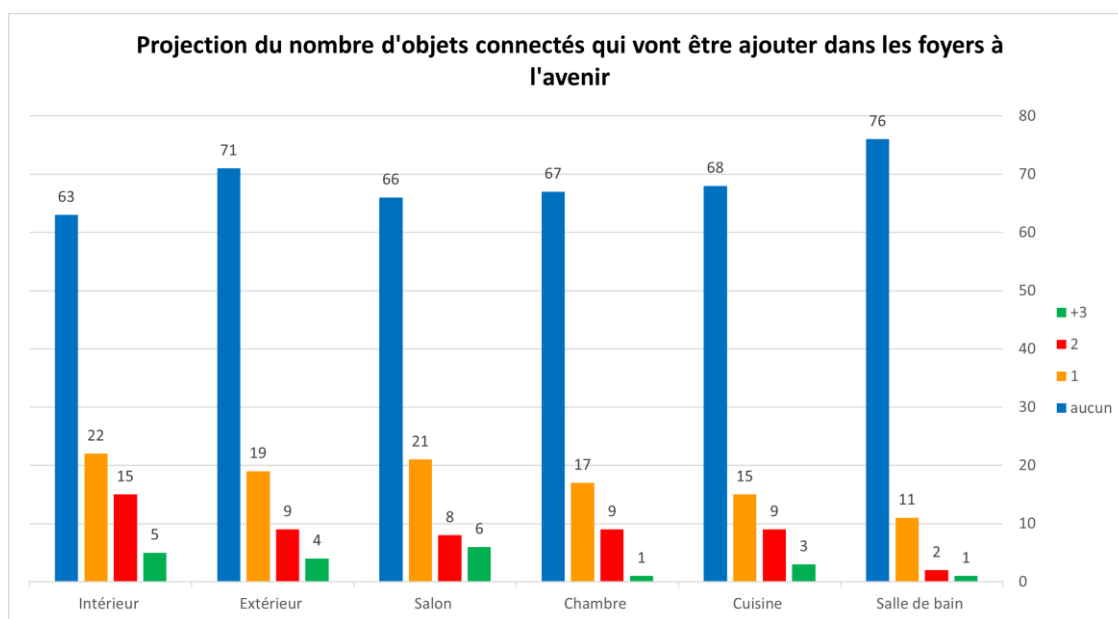
Figure 11 : Période d'achat pour chaque catégorie



Ce graphique nous montre qu'il y a un intérêt constant pour les objets connectés dans les habitations au cours des dernières années, cela est en accord avec la croissance des foyers adoptant la domotique. Cet intérêt est particulièrement prononcé dans les catégories comme le salon ainsi que dans la chambre ou l'intérieur. Nous remarquons que dans presque toutes les catégories, il existe un pic entre 2016 et 2020 correspondant aux premiers achats d'appareils connectés dans ces catégories. Toutefois, la cuisine fait exception à cette tendance en montrant une croissance modérée au fil du temps avec une légère augmentation récente. Malgré le pic observé

entre 2016 et 2020, il y a continuellement de nouveaux consommateurs qui découvrent et s'intéressent à la domotique. Ces nouveaux consommateurs démontrent un engouement persistant pour ces technologies capables d'améliorer le confort, la sécurité et l'efficacité énergétique au sein de leur maison.

Figure 12 : Projection du nombre d'objets connectés qui vont être ajoutés dans les foyers à l'avenir

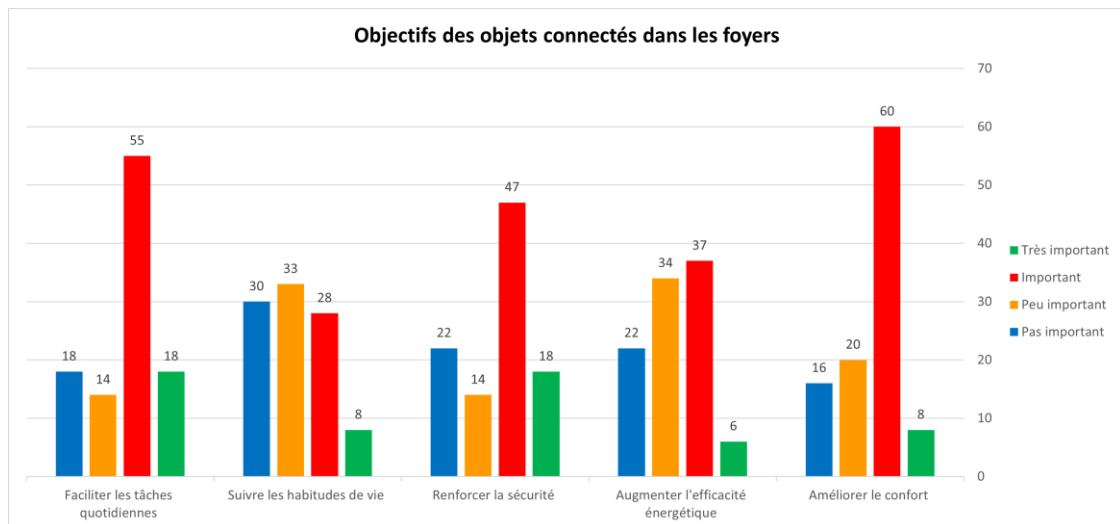


Nous remarquons dans ce graphique que la grande majorité des personnes ne prévoient pas d'ajouter des objets connectés. Les catégories où les gens sont les plus favorables à augmenter le nombre d'objets connectés dans le futur sont l'intérieur, l'extérieur et le salon, tandis que la salle de bain semble être la moins concernée par cette tendance.

Pour continuer l'analyse de ce graphique, nous supposons que la catégorie "3+" représente précisément trois objets connectés supplémentaires, même si elle peut potentiellement indiquer un nombre plus élevé. Cette hypothèse nous permet de simplifier et de quantifier notre analyse des données pour chaque catégorie d'objets connectés. Si nous prenons le total des objets connectés qui seront ajoutés à chaque catégorie de foyer, nous constatons que les trois catégories mentionnées précédemment (intérieur, extérieur, salon) comptent entre 100 et 105 objets connectés chacune. Les trois autres catégories (cuisine, chambre, salle de bain) affichent, quant à elles, un total entre 90 et 95 objets connectés. En additionnant tous les objets connectés qui seront ajoutés, le total atteint 588. Bien que la majorité des personnes n'envisage pas d'en ajouter, en calculant une moyenne pour estimer le nombre d'objets connectés qui seront ajoutés par personne à l'avenir, nous obtenons un minimum de 5 objets par personne. Nous remarquons avec cela que cette moyenne de cinq objets connectés par

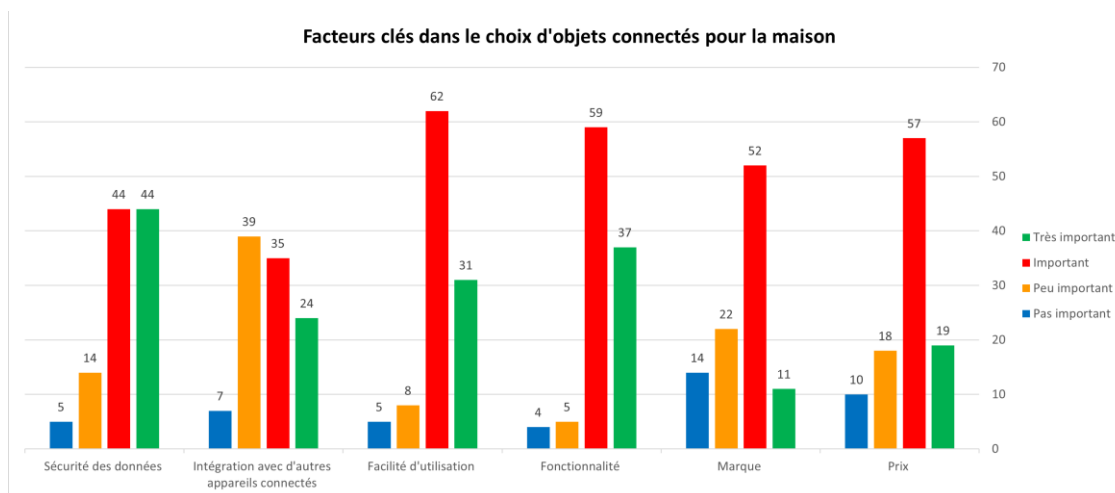
personne reflète des tendances significatives en termes d'adoption technologique et correspond donc bien à ce que nous avons vu en ce qui concerne la tendance croissante du marché.

Figure 13 : Objectif des objets connectés dans les foyers



L'analyse du graphique met en évidence que la majorité des personnes interrogées considèrent l'aide des tâches quotidiennes comme une fonctionnalité essentielle des objets connectés. De plus, le renforcement de la sécurité et l'amélioration du confort sont également perçus comme des aspects essentiels, cela montre un grand intérêt pour les objets connectés qui contribuent à une vie domestique plus sûre et plus agréable. Par ailleurs, bien que le suivi des habitudes de vie et l'augmentation de l'efficacité énergétique nous montre des avis plus partagés, ces objectifs restent tout de même significatifs pour une portion considérable des répondants. En effet, environ un tiers des personnes interrogées attribuent une importance à ces aspects. Ces perspectives mettent en lumière les attentes actuelles des consommateurs concernant les objets connectés.

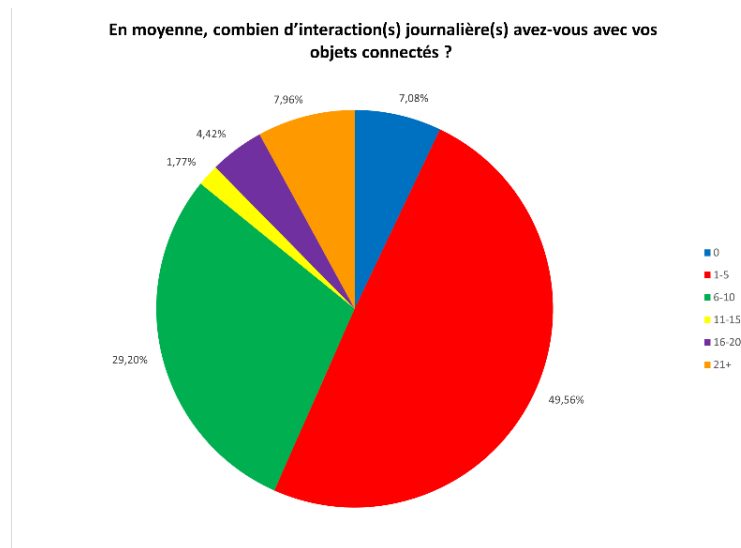
Figure 14 : Facteurs clé dans le choix d'objets connectés pour la maison



L'analyse de ce graphique révèle clairement que la sécurité des données est perçue comme un facteur crucial dans le choix des objets connectés. Cela met en lumière l'importance primordiale que les consommateurs accordent à la protection de leurs informations personnelles, même face à une compréhension limitée des risques de cybersécurité associés à l'utilisation quotidienne de ces technologies. En outre, la facilité d'utilisation et les fonctionnalités sont également valorisées comme des éléments essentiels, soulignant une forte préférence pour des produits qui sont à la fois intuitifs et facilement accessibles à tous les utilisateurs. D'autre part, bien que la marque et le prix soient considérés comme des facteurs importants, environ un tiers des répondants leur accordent moins de priorité, ce qui peut indiquer une disposition à explorer de nouvelles marques ou des options plus économiques si les critères de fonctionnalité et de sécurité sont satisfaits. Par ailleurs, l'intégration avec d'autres objets connectés semble être le facteur le moins prioritaire, avec près de la moitié des participants qui lui accordent une importance moindre, reflétant peut-être une approche plus sélective ou individualisée dans la constitution de leur écosystème domestique connecté.

Ces facteurs indiquent une préférence pour des produits intuitifs et sécurisés, même si cela peut impliquer d'explorer de nouvelles marques ou des options plus économiques.

Figure 15 : En moyenne, combien d'interaction(s) journalière(s) avez-vous avec vos objets connectés ?



Pour élaborer le prochain graphique présenté, nous avons voulu déterminer leur nombre moyen d'interactions quotidiennes avec leurs objets connectés. Il est important de noter que ce chiffre inclut également les interactions avec les wearables (comme les montres intelligentes), ce qui peut introduire un biais dans les résultats. En effet, pour les besoins de cette étude, nous nous intéressons spécifiquement aux interactions avec les technologies utilisées exclusivement à domicile.

Après une analyse des données collectées, nous constatons que la moyenne des interactions quotidiennes, incluant les wearables, s'élève à presque 7. Ce chiffre peut paraître surprenant, car il suggère un niveau d'engagement relativement modeste avec ces technologies, compte tenu de leur omniprésence et de leur capacité à simplifier divers aspects de la vie quotidienne. Mais nous pouvons mettre cela sur la méconnaissance des sondés qui peuvent ne pas prendre en compte qu'allumer sa télévision connectée ou sa lumière intelligente est une interaction par exemple. De plus, cette moyenne peut être sous-estimée pour les technologies domestiques si nous considérons que les wearables, souvent utilisés tout au long de la journée et en dehors du domicile, peuvent contribuer de manière disproportionnée au nombre total d'interactions enregistrées. Ainsi, le nombre d'interaction est très petit ce qui coordonne mal avec l'augmentation du nombre d'objets connecté dans les foyers et donc le nombre d'interaction.

Pour conclure, cette analyse des objets connectés dans les maisons genevoises met en lumière une adoption croissante de ces technologies, largement motivée par le désir de confort, de sécurité et d'efficacité énergétique. Les téléviseurs intelligents et les assistants vocaux sont les plus populaires, soulignant une préférence pour les dispositifs faciles à utiliser et intégrés harmonieusement dans la vie quotidienne. Cependant, cette expansion des objets connectés introduit des défis de sécurité significatifs. Bien que les utilisateurs soient modérément conscients des risques, il existe une disparité notable entre les groupes d'âge, les personnes de plus de 30 ans étant généralement plus sensibilisées aux enjeux de cybersécurité. Cela souligne le besoin urgent de renforcer la sensibilisation et l'éducation, surtout parmi les plus jeunes. La sécurité des objets connectés dépend non seulement des fabricants, mais aussi des utilisateurs qui doivent veiller à appliquer régulièrement les mises à jour et à adopter des pratiques de sécurité robustes. De plus, la perception de la responsabilité légale en cas de piratage reste floue, une majorité des sondés ne se considérant pas fautifs. Pour finir, bien que les objets connectés continuent de transformer les foyers genevois, il est crucial de renforcer les mesures de sécurité et de sensibilisation pour garantir une adoption sécurisée et bénéfique de ces technologies (Annexe 2).

5. Cas Pratique

Pour ce cas pratique, nous prenons une maison conçue pour accueillir une famille de quatre personnes, incluant deux adultes et deux adolescents. Cette maison est équipée de divers objets connectés intégrés dans son infrastructure domestique pour offrir un confort optimal, une sécurité accrue et une gestion efficace de l'énergie.

La maison comprend plusieurs pièces équipées d'IOT. Le salon est doté d'un système de divertissement intelligent incluant une télévision connectée et un assistant vocal. La cuisine est équipée de prises connectées et d'un aspirateur robot. Chaque chambre dispose de dispositifs spécifiques, notamment des éclairages intelligents et des thermostats individuels. Pour renforcer la sécurité de la maison, des caméras de surveillance connectées équipées de capteur de mouvement et une serrure intelligente. Les espaces extérieurs comprennent des dispositifs tels que des stores connectés et une sonnette connectée, permettant une gestion et une surveillance optimales de la propriété.

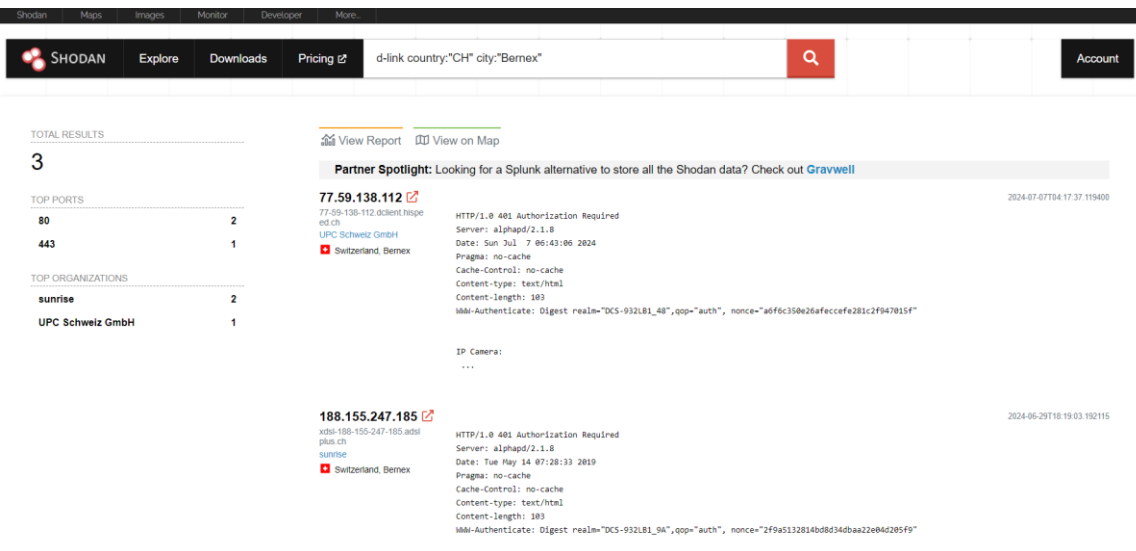
Cette configuration domotique offre un environnement moderne et connecté, mais introduit également des défis en matière de cybersécurité. Les objets connectés utilisés dans ce foyer sont vulnérables aux cyberattaques, ce qui nécessite une analyse approfondie des risques et la mise en place de mesures de sécurité robustes pour protéger les données personnelles des habitants et assurer la fiabilité des dispositifs.

Le cas pratique se concentre sur l'évaluation des vulnérabilités spécifiques des objets connectés présents dans la maison, ainsi que sur la proposition de solutions pour remédier au mieux à ces vulnérabilités. Les résultats de cette analyse vont permettre de sensibiliser les utilisateurs et par la suite, de formuler des recommandations concrètes et applicables afin d'améliorer la sécurité des foyers connectés à Genève.

5.1 Utilisation de Shodan

Il existe un site nommé Shodan.io, qui est un moteur de recherche spécialisé dans les appareils connectés à Internet. Contrairement aux moteurs de recherche traditionnels qui indexent les pages web, Shodan explore les adresses IP connectées à Internet pour trouver des ports ouverts et identifier les dispositifs connectés. Il permet de découvrir une grande variété d'appareils, tels que des caméras de surveillance, des téléviseurs intelligents et des imprimantes, en fournissant des informations détaillées comme les adresses IP, les ports ouverts, et les versions de logiciels installés. Ces données sont stockées dans une base de données consultable par mots-clés et filtres spécifiques, facilitant ainsi l'accès à des informations cruciales pour évaluer la vulnérabilité des dispositifs IOT par exemple. Shodan met en lumière l'importance de la sécurité des technologies IOT, car il permet à quiconque de trouver et potentiellement d'exploiter des appareils connectés. Il peut permettre à des pirates informatiques de s'informer sur divers dispositifs. Cela montre la nécessité de protéger ces technologies pour empêcher les cybercriminels d'accéder à ces informations sensibles et de prendre le contrôle des dispositifs (OFCS 2023; Shodan 2024a).

Figure 16 : Utilisation de shodan.io.



(Shodan 2024b)

Prenons l'exemple d'une caméra D-Link en Suisse, en écrivant dans la barre de recherche « D-Link camera » et en filtrant pour la Suisse à Bernex uniquement, nous pouvons trouver ce type de résultat (188.155.247.185) (Shodan 2024b).

Figure 17 : Information générale de 188.155.247.185.

General Information

Hostnames	xDSL-188-155-247-185.adslplus.ch
Domains	ADSLPLUS.CH
Country	Switzerland
City	Bernex
Organization	sunrise
ISP	Sunrise GmbH
ASN	AS6730

Open Ports

80 3128

// 80 / TCP

4121065381 | 2024-06-29T18:19:03.192115

D-Link DCS-932LB1 webcam http interface 2.18

```
HTTP/1.0 401 Authorization Required
Server: alphasd/2.1.8
Date: Tue May 14 07:28:33 2019
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html
Content-Length: 169
WWW-Authenticate: Digest realm="DCS-932LB1_9A",qop="auth", nonce="2f9a5132814bd8d340baa2e04d285f9"
```

IP Camera:

MAC Address: 88:C5:54:41:A7:9A
Version: 2.18
Hardware Version: B
Name: DCS-932LB
Brand: D-Link
IP Address: 192.168.1.104
Model: DCS-932LB1
Build: 1

MAC Addresses

88:C5:54:41:A7:9A
OUI: 88:C5:54
Organization: D-Link International
Assignment: HA-L
Registration Date: 2011-12-14

(Shodan 2024c)

Nous remarquons que nous avons accès à toutes sortes d'informations concernant cette caméra à Bernex, comme des informations générales sur la caméra (modèle, marque, nom, version du firmware, version du matériel), des informations sur le réseau (adresse IP, adresse MAC) et des détails du serveur web. Les informations sur la caméra IP D-Link DCS-932LB1 révèlent plusieurs détails clés concernant l'utilisateur et l'appareil. Tout d'abord, l'utilisateur possède une caméra de surveillance D-Link, configurée sur un réseau local avec l'adresse IP 192.168.1.104, ce qui indique une utilisation domestique ou de bureau. L'adresse MAC associée et les détails de la version du firmware montrent que l'appareil est potentiellement ancien et peut nécessiter des mises à jour pour rester sécurisé. Le fait que la caméra utilise une authentification Digest pour protéger l'accès indique une certaine conscience des besoins de sécurité, bien que cette mesure puisse ne pas être suffisante sans l'utilisation de SSL/TLS par exemple. Les détails sur le serveur HTTP et les configurations de ports ouverts montrent que l'appareil est accessible à distance, ce qui pose des risques de sécurité s'il n'est pas correctement sécurisé (Shodan 2024c).

De plus, lors de notre recherche de l'exemple précédent de la caméra D-Link, nous avons également trouvé par hasard un flux vidéo localisé à Uetendorf en Suisse. L'image montre la dernière vue captée par la caméra. Selon notre expert en objets connectés, Shodan peut parfois capturer des images ou des flux vidéo si ces dispositifs ne sont pas correctement sécurisés (Shodan 2024d).

Figure 18 : Flux vidéo sur Shodan.io.

D-Link Corporation. | WIRELESS INTERNET ... 2024-06-28T16:48:10.262107
62.2.85.226 HTTP/1.0 200 OK
62-2-85-226.st Server: alphasd
atic.cablecom Date: Fri Apr 12 14:34:39 2024
ch Pragma: no-cache
Sunrise Cache-Control: no-cache
GmbH Content-type: text/html
Switzerland, Uetendorf

IP Camera:
MAC Address: 28:10:7B:10:53:C9
Version: 1.14
Hardware Version: A
Name: IPCAM-T101
Brand: D-Link
IP Address: 172.25.110.60
Model: DCS-93...



(Shodan 2024d)

L'utilisation de Shodan révèle les vulnérabilités potentielles des appareils connectés et met en évidence l'importance cruciale de sécuriser les dispositifs IOT dans nos foyers. Comme démontré par l'exemple de la caméra D-Link dont les données sont disponibles publiquement, des informations sensibles et des flux vidéo peuvent être facilement accessibles si les dispositifs ne sont pas correctement configurés et sécurisés.

5.2 Piratage d'un Wi-Fi domestique

Parmi les principaux risques potentiels liés à la sécurité des objets connectés dans les foyers genevois, l'accès non autorisé aux réseaux Wi-Fi domestiques par un pirate informatique est particulièrement préoccupant. Un hacker peut tenter de se connecter au réseau Wi-Fi domestique en exploitant diverses méthodes pour découvrir le mot de passe et accéder à l'ensemble de nos dispositifs connectés. De nos jours, les Wi-Fi domestiques sont sécurisés avec un protocole de sécurité chiffré qui protège le trafic Internet sur les réseaux sans fil. Il est appelé WPA2 ou WPA3 et a remplacé les précédents protocoles de chiffrement facilement piratables (WEP et WPA). Le WPA2 (Wi-Fi Protected Access 2) est un protocole de sécurité Wi-Fi conçu pour sécuriser les connexions sans fil. Il crypte les données et protège les communications afin d'empêcher les pirates informatiques d'accéder au réseau. Le WPA3 est quant à lui le plus récent des protocoles de sécurité pour les réseaux sans fil. Il utilise un chiffrement avancé, notamment le Perfect Forward Secrecy, pour offrir une sécurité supérieure par rapport au WPA2. Toutefois, le WPA3 n'est pas encore largement adopté et tous les appareils ne le prennent pas automatiquement en charge (Avast 2024).

Dans ce cas pratique nous supposons que le Wi-Fi est sous le protocole de sécurité WPA2. Le tutoriel fourni à l'adresse suivante : <https://www.freecodecamp.org/news/wi-fi-hacking-101/> nous montre une explication détaillée sur la façon de pirater un réseau Wi-Fi utilisant le protocole WPA2. Il commence par expliquer les bases du fonctionnement des paquets réseau, puis présente les différents protocoles Wi-Fi et leurs niveaux de sécurité respectifs. Nous y retrouvons les étapes clés pour mener cette attaque.

Il faut tout d'abord passer le mode réseau en mode *moniteur* ce qui signifie configurer une carte réseau sans fil pour qu'elle capture tous les paquets de données circulant sur le réseau sans fil à portée, indépendamment de leur destination. Cette configuration permet de surveiller le trafic réseau sans se connecter à un point d'accès spécifique. Ensuite il faut identifier la cible à l'aide de *airodump-ng*, puis effectuer une attaque DoS pour forcer la connexion d'un client et capturer les paquets de poignée de main. Il faut également utiliser *aircrack-ng* pour générer des clés de chiffrement (PMK) et tenter de craquer le mot de passe (lwugo 2022).

Si la maison est équipée du protocole de WPA3, des chercheurs en sécurité ont découvert récemment une nouvelle vulnérabilité publiée en mai qui concerne le standard Wi-Fi 802.11 (CVE-2023-52424), aussi appelée attaque de confusion SSID. Cette faille permet à un attaquant de tromper les clients Wi-Fi en les connectant à un réseau non

approuvé, même en utilisant le protocole de sécurité WPA3. Le problème réside dans le fait que le standard 802.11 n'exige pas l'authentification du nom de réseau (SSID), ce qui peut être exploité pour faire croire aux utilisateurs qu'ils se connectent à un réseau de confiance alors qu'il s'agit d'un réseau malveillant. Cette vulnérabilité permet à l'attaquant d'espionner le trafic réseau des victimes. Pour exploiter cette faille, plusieurs conditions doivent être réunies, mais une solution proposée inclut la mise à jour du standard 802.11 pour toujours authentifier le SSID lors de la connexion ou l'adoption de mesures de mitigation par les réseaux, comme éviter la réutilisation des identifiants entre les SSID et renforcer la protection des balises réseau (Newsroom 2024; Jackson 2024).

Une fois qu'un pirate informatique a réussi à accéder au réseau Wi-Fi domestique en récupérant le mot de passe, il peut facilement trouver la liste des dispositifs connectés au réseau avec l'utilisation d'un logiciel nommé *Nmap* par exemple. *Nmap* est un logiciel capable de détecter les dispositifs connectés au réseau ainsi que leurs versions et le système d'exploitation en cours d'exécution (Gordon Lyon 2024).

Lorsque le pirate informatique possède ces informations, il peut cibler spécifiquement les objets connectés vulnérables, comme des caméras de sécurité, des thermostats intelligents, et des assistants vocaux.

Supposons à présent que le pirate informatique trouve la liste suivante d'objets connectés (tous vulnérables) dans la maison avec le modèle, les versions des services et des systèmes d'exploitation en cours d'exécution. Nous y retrouvons :

- Des télévisions connectées (Samsung Smart TV UE40D7000 version T-GAPDEUC-1033.2)
- Une enceinte (Amazon Alexa Echo Dot 4e génération)
- Des lumières (Govee LED Strip v3.00.42)
- Des caméras de surveillance (D-Link DCS-8300LHV2)
- Prise connectée (Belkin Wemo Smart Plug WSP080 v1.2)
- Des thermostats (Sinilink XY-WFT1 WiFi Remote Thermostat, running firmware 1.3.6)
- Une serrure (Nuki Smart Lock 3.0 before 3.3.5)
- Des stores (Third Reality Smart Blind 1.00.54)
- Une sonnette (NightOwl WDB-20-V2)
- Un aspirateur (Shenzhen Jisiwei i3 robot vacuum cleaner)

5.3 Identification des vulnérabilités des IOT

A partir de toutes les informations dont il dispose sur ces objets connectés, le pirate informatique peut tout simplement les mettre dans une base de données publique comme la National Vulnerability Database (NVD) gérée par le National Institute of Standards and Technology (NIST). La NVD est une ressource accessible en ligne qui recense les vulnérabilités connues des logiciels et des matériels informatiques. Les informations partagées dans la base de données NVD peuvent permettre aux pirates informatiques d'identifier et d'exploiter rapidement les faiblesses des objets connectés comme ceux listés dans l'exemple. Le processus est simple, les pirates informatiques recherchent dans la base de données NVD des vulnérabilités spécifiques aux dispositifs connectés trouvés dans le réseau domestique. La NVD offre des détails techniques sur chaque vulnérabilité, y compris des descriptions, des impacts potentiels, et des mesures d'atténuation possibles (NIST 2024a).

En plus de ces détails, la NVD et d'autre base de données utilisent le Common Vulnerability Scoring System (CVSS) pour évaluer la gravité des vulnérabilités. Cette méthode fournit une mesure quantitative de la sévérité, exprimée par un score numérique. Ce score peut ensuite être traduit en termes qualitatifs tels que faible, moyen, élevé et critique, aidant ainsi les organisations à évaluer et prioriser correctement leurs processus de gestion des vulnérabilités. Bien que la quatrième version du CVSS soit la plus récente, nous utilisons la troisième version, car elle est plus largement disponible pour les vulnérabilités identifiées dans ce cas pratique. Le CVSS v3 se compose de trois groupes de métriques : la métrique de base, la métrique temporelle et la métrique environnementale, permettant d'attribuer un score numérique allant de 0 à 10 (NIST 2024b).

Pour accéder à tous ces détails techniques sur chaque vulnérabilité, il faut se rendre sur le lien suivant : <https://nvd.nist.gov/vuln/search> et rentrer dans la fonction recherche la marque de l'objet et sa version (NIST 2024c).

Figure 19 : Utilisation de la fonction recherche.

The screenshot shows the 'Search Vulnerability Database' page. At the top, there's a green 'VULNERABILITIES' button. Below it, the title 'Search Vulnerability Database' is followed by a subtitle: 'Try a product name, vendor name, CVE name, or an OVAL query.' A note states: 'NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions. Search results will only be returned for data that is populated by NIST or from source of Acceptance Level "Provider".' The search form includes sections for 'Search Type' (Basic selected, Advanced unselected), 'Results Type' (Overview selected, Statistics unselected), 'Keyword Search' (with a text input containing 'Samsung Smart TV UE40D7000 version T-GAPDEUC-1033.2' and an 'Exact Match' checkbox), and 'Search Type' (All Time selected, Last 3 Months unselected). On the right, there are checkboxes for 'Contains HyperLinks' (CISA Known Exploited Vulnerabilities, US-CERT Technical Alerts, US-CERT Vulnerability Notes, OVAL Queries) and 'Contains Tags' (Disputed, Unsupported When Assigned, Exclusively Hosted Service). 'Search' and 'Reset' buttons are at the bottom right.

(NIST 2024c)

Prenons l'exemple du premier IOT ressorti lors de l'utilisation de *Nmap* par le pirate. C'est une télévision connectée Samsung Smart TV UE40D7000, version T-GAPDEUC-1033.2. Si nous entrons cela dans le « Keyword Search », nous arrivons sur une page qui liste les identifiants (ID) des vulnérabilités aussi appelés CVE (= Common Vulnerabilities and Exposures) (NIST 2024d; 2024e).

Figure 20 : Liste des identifiants des vulnérabilités.

The screenshot shows the 'Search Results' page. At the top, there are green buttons for 'VULNERABILITIES' and 'SEARCH AND STATISTICS'. The title 'Search Results (Refine Search)' is followed by a 'Sort results by:' dropdown set to 'Publish Date Descending' and a 'Sort' button. Below this, 'Search Parameters:' lists: Results Type: Overview, Keyword (text search): Samsung Smart TV UE40D7000 version T-GAPDEUC-1033.2, Search Type: Search All, and CPL Name Search: false. A message states: 'There are 1 matching records. Displaying matches 1 through 1.' The main table has columns 'Vuln ID', 'Summary', and 'CVSS Severity'. The first row shows 'CVE-2023-41270' with a summary: 'Improper Restriction of Excessive Authentication Attempts vulnerability in Samsung Smart TV UE40D7000 version T-GAPDEUC-1033.2 and before allows attackers to cause a denial of service via WPS attack tools.' The 'Published' date is 'novembre 08, 2023; 2:15:27 AM -0500'. The 'CVSS Severity' column shows 'V4.0:(not available)', 'V3.1: 4.3 MEDIUM', and 'V2.0:(not available)'.

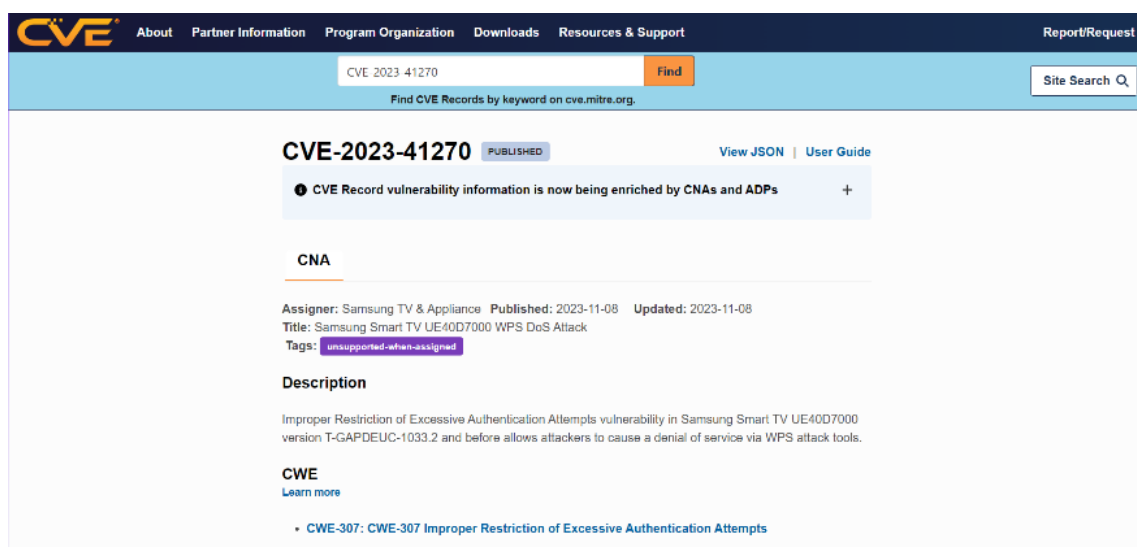
(NIST 2024e)

Cette télévision connectée Samsung Smart TV a une vulnérabilité sous le numéro CVE suivant : CVE-2023-41270 et un score CVSS de 4,3 MEDIUM (NIST 2024f).

Le pirate peut alors se rendre sur le site : <https://www.cve.org>. La mission du programme CVE® est d'identifier, de définir et de cataloguer les vulnérabilités de cybersécurité qui ont été divulguées publiquement. Chaque vulnérabilité est consignée dans un enregistrement CVE spécifique. Ces vulnérabilités sont découvertes, attribuées et publiées par des organisations partenaires du programme CVE à travers le monde (CVE 2024a). Les partenaires du programme CVE qui sont au nombre de 387 publient ces enregistrements pour fournir des descriptions uniformes des vulnérabilités (CVE 2024b). Les professionnels des technologies de l'information et de la cybersécurité utilisent les enregistrements CVE pour s'assurer qu'ils parlent du même problème et pour coordonner leurs efforts en vue de prioriser et de résoudre ces vulnérabilités.

Lorsque nous sommes sur le site <https://www.cve.org> il suffit d'entrer le CVE ID : CVE-2023-41270 et nous arrivons sur une page qui décrit la vulnérabilité de l'objet connecté et la version de l'appareil.

Figure 21 : Utilisation de cve.org.



(CVE 2023a)

Dans cet exemple pour cette télévision Samsung nous remarquons que le problème est dans les versions du firmware T-GAPDEUC-1033.2 et antérieures du Samsung Smart TV modèle UE40D7000 et permet à des attaquants de causer un déni de service (DoS) en exploitant une restriction inappropriée des tentatives d'authentification excessives. Cette faille permet aux attaquants d'utiliser des outils d'attaque WPS pour envoyer un grand nombre de tentatives de connexion, submergeant ainsi le système et rendant le téléviseur inutilisable ou lent pour les utilisateurs légitimes (CVE 2023a). De plus, nous pouvons y retrouver des références qui développe la vulnérabilité plus en détail comme

dans cet exemple où nous pouvons consulter une slideshare qui développe toute la manipulation afin d'effectuer ce déni de service mais aussi une solution afin d'éviter cette vulnérabilité. La solution que nous retrouvons dans ce document est de désactiver la fonctionnalité Samsung Wireless Link (SWL) sur la Samsung Smart TV modèle UE40D7000 (Fuguet 2022).

Suite à cet exemple, nous allons répéter la marche à suivre avec la liste des objets connectés que le pirate informatique a trouvée dans la maison afin de découvrir plusieurs types de vulnérabilité. Le 2^e objet connecté trouvé par le pirate informatique est un assistant Amazon Alexa Echo Dot 4^{ème} génération. Le CVE trouvé est : CVE-2022-25809 et le score CVSS est de 9,8 CRITICAL (NIST 2023a). Pour cette vulnérabilité, nous parlons d'une attaque Alexa versus Alexa (AvA) qui exploite les commandes vocales issues de fichiers audio pour contrôler les appareils Amazon Echo, en utilisant l'auto-émission de commandes. AvA permet aux attaquants de se passer de haut-parleurs malveillants à proximité, en émettant des commandes depuis l'appareil lui-même. Cela peut mener à des actions non désirées comme le contrôle des appareils intelligents, l'achat de produits ou l'espionnage (CVE 2022). Nous pouvons retrouver en référence un lien qui nous permet de consulter un PDF où nous retrouvons la vulnérabilité bien plus détaillée (Esposito, Sgandurra, Bella 2022).

Le 3^e objet connecté trouvé est une lumière Govee LED Strip v3.00.42. Le CVE associé est : CVE-2023-45956 et le score CVSS est de 7,5 HIGH (NIST 2023b). Pour cette vulnérabilité, l'appareil Govee présente une vulnérabilité de déni de service exploitée via l'envoi de messages malveillants, provoquant l'arrêt des dispositifs. Cette faille est liée aux commandes *Move* et *MoveWithOnoff* du groupe *Level Control*, utilisées pour ajuster la luminosité. Ces commandes acceptent deux paramètres : le premier est *MoveMode* (0 ou 1) et le deuxième est *uint8 Rate*. Le dispositif se bloque lorsque le paramètre *Rate* est égal à 0. Nous pouvons retrouver en référence un lien qui nous permet de consulter un rapport de la vulnérabilité sous format PDF (CVE 2023b; IoT-Fuzz 2023).

Le 4^e objet connecté trouvé est une caméra de sécurité qui permet la détection de présence humaine D-Link DCS-8300LHV2 et le CVE associé est : CVE-2023-51629. Le score CVSS est de 6,3 MEDIUM (NIST 2024g). Une vulnérabilité de contournement de l'authentification par code PIN codé en dur est identifiée dans les caméras IP D-Link DCS-8300LHV2 via l'application programming interface (API) ONVIF. Cette faille permet à des attaquants proches du réseau de contourner l'authentification sans nécessiter de connexion préalable. Le problème réside dans l'utilisation d'un code PIN codé en dur dans la configuration de l'API. Exploitée, cette vulnérabilité permet d'accéder au système

sans authentification. D-Link a publié une mise à jour pour corriger cette vulnérabilité. Il est crucial que les utilisateurs mettent à jour leurs appareils IOT pour se protéger contre ce type de faille de sécurité (CVE 2024c). Nous pouvons retrouver en référence des liens qui nous permettent de consulter la vulnérabilité plus en détails ainsi que plus d'information concernant la mise à jour proposée par D-Link (Kheirkhah 2024; D-Link 2023).

Le 5^e objet connecté trouvé est une prise connectée Belkin Wemo Smart Plug WSP080 v1.2. Le CVE associé est : CVE-2023-33768 et le score CVSS est de 6,5 MEDIUM (NIST 2023c). Une vérification incorrecte de la signature du micrologiciel pendant la mise à jour du Belkin Wemo Smart Plug WSP080 v1.2 permet à des attaquants de provoquer un DoS en utilisant un fichier de micrologiciel malveillant. Pour aller un peu plus loin dans la vulnérabilité, lors de la mise à jour du firmware via l'application mobile Wemo, une signature de firmware non valide peut bloquer la prise intelligente. En exploitant l'application Wemo Android, il est possible d'injecter un micrologiciel modifié, changeant un octet spécifique dans le binaire. Le micrologiciel modifié, une fois envoyé et reçu par la prise connectée, provoque son dysfonctionnement complet, le rendant impossible à réinitialiser et indétectable par l'application mobile (CVE 2023c; PurSec Lab 2023).

Le 6^e objet connecté trouvé est un thermostat Sinilink XY-WFT1 WiFi Remote Thermostat, firmware V1.3.6. Le CVE associé est : CVE-2022-43704 et le score CVSS est de 5,9 MEDIUM (NIST 2023d). Le thermostat à distance WiFi Sinilink XY-WFT1, utilisant le firmware 1.3.6, présente une vulnérabilité permettant à un attaquant de contourner les exigences de communication via Message Queuing Telemetry Transport (MQTT). L'appareil ciblé permet de contrôler un relais physique et utilise le protocole MQTT pour transmettre des messages à un broker MQTT hébergé dans le cloud. En conditions normales, une application mobile publie et s'abonne via ce broker MQTT. Les modifications de configuration du client MQTT (le thermostat) sont communiquées et publiées au broker MQTT. Le thermostat écoute ces modifications via les messages d'abonnement MQTT et ajuste son fonctionnement en conséquence. L'état du thermostat est également transmis à l'application mobile via des messages Sinilink sur UDP/1024. En utilisant le protocole Sinilink (UDP/1024), un attaquant peut rejouer des commandes et contrôler le relais du dispositif sans authentification par l'application mobile. Cette faille permet de manipuler la température de l'environnement physique de l'appareil cible, potentiellement créant des conditions inacceptables (CVE 2023d; Hanna 2023).

Le 7^e objet connecté trouvé est une serrure Nuki Smart Lock 3.0, version avant 3.3.5. Le CVE associé est : CVE-2022-32509 et le score CVSS n'est pas mentionné (NIST 2024h). Les dispositifs Nuki Smart Lock et Bridge ne disposent pas de la validation des certificats SSL/TLS, ce qui les rend vulnérables aux attaques de type man-in-the-middle (MITM). Cela permet aux attaquants d'intercepter, d'analyser et de modifier le trafic réseau chiffré entre l'appareil et les services web. Par exemple, le trafic WebSocket en provenance et à destination du dispositif Keyturner peut être capturé par le pirate. Pour atténuer ce risque, il est recommandé pour cette vulnérabilité de mettre en œuvre la validation des certificats SSL/TLS pour toutes les fonctions de communication réseau (NIST 2024h). De plus, lorsque nous nous penchons sur les références mises à disposition par le site CVE.org, nous remarquons que des chercheurs ont découvert onze failles de sécurité différentes dans les produits Nuki Smart Lock et Bridge. Ces vulnérabilités facilitent diverses attaques, y compris l'exécution de code arbitraire et les attaques DoS. Informé en avril 2022, Nuki a rapidement réagi et publié des correctifs pour toutes les vulnérabilités en juin 2022. Toutefois, il est impératif que les utilisateurs mettent régulièrement à jour leur logiciel (Romero 2022; Nuki 2022).

Le 8^e objet connecté trouvé est un store Third Reality Smart Blind 1.00.54. Le CVE associé est : CVE-2023-29780 et le score CVSS est de 7,5 HIGH (NIST 2023e). La version 1.00.54 du Third Reality Smart Blind présente une vulnérabilité de DoS liée à la commande *Down_close*, qui étend les stores au maximum sans accepter d'argument. Lorsqu'un message malveillant Zigbee exploitant cette commande est envoyé, l'appareil ne répond plus. Si une seule commande est envoyée, l'appareil perd sa connexion et se reconnecte automatiquement après environ une seconde. Si plusieurs commandes sont envoyées en peu de temps, l'appareil perd sa connexion et se reconnecte après environ 30 secondes (CVE 2023e; Agatha2333 2023).

Le 9^e objet connecté trouvé est une sonnette NightOwl WDB-20-V2. Le CVE associé est : CVE-2021-31793 et le score CVSS est de 7,5 HIGH (NIST 2022). Un problème de sécurité a été découvert dans les dispositifs NightOwl WDB-20-V2_20190314. Cela permet à un utilisateur non authentifié d'accéder aux instantanés et aux flux vidéo de la sonnette via un serveur web fonctionnant sur le port 80. Le point de terminaison peut être atteint sans authentification, permettant à toute personne ayant accès au réseau de visualiser les flux de caméra et les instantanés, compromettant ainsi la confidentialité et la sécurité des utilisateurs (CVE 2021; tj-oconnor 2021).

Le 10e et dernier objet connecté trouvé est un aspirateur Shenzhen Jisiwei i3 robot vacuum cleaner. Le CVE associé est : CVE-2019-12820 et le score CVSS est de 5,6 MEDIUM (NIST 2023f). Une vulnérabilité a été identifiée dans l'application 2.0 de l'aspirateur robot Shenzhen Jisiwei i3. Les actions effectuées via l'application, comme la modification de mot de passe et la transmission d'informations personnelles, utilisent le protocole HTTP non chiffré. Par exemple, les identifiants de connexion sont envoyés en clair lors de la connexion à un compte Jisiwei. Cette vulnérabilité affecte les versions Android et iOS de l'application. Un attaquant pourrait exploiter cette faille en utilisant une attaque MITM sur le réseau local pour intercepter les identifiants et accéder entièrement à l'aspirateur robot. CVE-2019-12820 (CVE 2019). Dans les références, nous retrouvons un document qui analyse la sécurité des IOT, en particulier un aspirateur robot, à travers des méthodes de modélisation des menaces et de tests de pénétration pour évaluer leur vulnérabilité aux attaques malveillantes. Deux faiblesses majeures ont été identifiées. La première concerne la communication non sécurisée : l'application mobile utilise le protocole HTTP pour échanger des données avec le serveur, ce qui permet à un attaquant sur le même réseau d'intercepter les identifiants de connexion en clair. La seconde faiblesse porte sur la vulnérabilité du QR code : les informations contenues dans le QR code utilisé pour lier l'aspirateur à un compte suivent un modèle prédictible, permettant à un attaquant de deviner l'ID de l'appareil et d'en prendre le contrôle. Ces failles mettent en évidence que la sécurité des appareils IOT, comme l'aspirateur robot Jisiwei i3, est souvent insuffisante et nécessite une révision. Les tests ont démontré que l'absence de chiffrement des communications et les modèles prédictibles des QR codes peuvent exposer les utilisateurs à des risques considérables. De plus, dans ce rapport, les auteurs soulignent que l'absence de chiffrement du trafic réseau est particulièrement préoccupante, car l'utilisateur moyen ne peut pas facilement vérifier si ses communications sont sécurisées. Par conséquent, il ne sait pas si des informations sensibles peuvent être interceptées et lues par des parties non autorisées. Les auteurs suggèrent, afin de renforcer la sécurité, d'adopter des protocoles de communication sécurisés comme HTTPS et de revoir les méthodes d'authentification des appareils (Olsson, Forsberg 2019).

5.4 Solutions aux vulnérabilités identifiées

Pour conclure, l'analyse approfondie des vulnérabilités des objets connectés dans ce cas pratique révèle des failles significatives dans la sécurité de divers dispositifs IOT présents dans une maison typique. Les vulnérabilités identifiées touchent une variété de dispositifs, allant des télévisions intelligentes aux serrures connectées, et exposent les utilisateurs à des risques de sécurité considérables. C'est pourquoi, en plus de notre documentation actuelle, nous avons demandé l'aide d'un pentester et d'un expert en objets connectés (Annexe 3). Ils nous ont fait part de solutions qui s'appliquent pour les vulnérabilités citées lors de ce cas pratique :

Tout d'abord, afin améliorer la sécurité générale du foyer de ce cas pratique, il faut segmenter le réseau Wi-Fi en une partie principale et plusieurs sous-réseaux dédiés pour chaque type d'objet connecté. Ensuite, nous retrouvons les vulnérabilités spécifiques au cas pratique comme les attaques DoS ce qui peut rendre les appareils complètement inutilisables en les submergeant de requêtes malveillantes. Il n'y a pas de protections particulières car il n'y a pas grand intérêt de faire une attaque DoS sur un objet connecté si ce n'est pour nuire personnellement au foyer, par exemple pour la télévision connectée, elle va se déconnecter et se reconnecter. C'est aussi au fabricant de proposer les mises à jour adéquates dès lors qu'une vulnérabilité spécifique de DoS apparaît et par la suite à l'utilisateur de l'effectuer. De plus, déconnecter nos IOT lorsque nous ne les utilisons pas reste aussi une mesure de prévention.

Comme pour certaine vulnérabilité de DoS spécifique à certains objets connectés, beaucoup des IOT du cas pratique nécessitent une mise à jour par le fabricant. Il est crucial que les fabricants de dispositifs connectés publient régulièrement des mises à jour et des correctifs pour corriger les vulnérabilités connues. Cependant, la responsabilité de la sécurité ne repose pas uniquement sur les fabricants. Les utilisateurs doivent également être vigilants et s'assurer d'appliquer les mises à jour que ce soit manuellement ou automatiquement.

Cependant certaines vulnérabilités spécifiques à ce cas pratique peuvent tout de même être protégées. Nous retrouvons les communications non sécurisées qui sont particulièrement vulnérables aux interceptions et manipulations par des attaquants, notamment lorsqu'elles transitent via des protocoles non chiffrés ce qui facilite les attaques de type MITM par exemple. Il est du devoir de l'utilisateur de vérifier si son objet connecté est protégé par du HTTPS par exemple ou utiliser des validations des certificats SSL/TLS pour toutes les fonctions de communication réseau (Olsson, Forsberg 2019; Romero 2022). De plus, l'utilisation de la double authentification sur les appareils offre

une protection renforcée. Par exemple, si le pirate récupère le mot de passe de notre serrure, il ne peut pas rentrer si une validation biométrique est également nécessaire. Lorsque cela est possible mettre en place une double authentification permet de se protéger des informations non chiffrées qui transitent entre les appareils. En effet, le deuxième facteur d'authentification ajoute une couche supplémentaire de protection en demandant une deuxième forme de vérification en plus du mot de passe.

Les failles d'authentification et de contrôle d'accès constituent également un problème majeur, car elles peuvent permettre à des individus malveillants d'obtenir un accès non autorisé aux dispositifs ce qui leur donne la possibilité de les contrôler à distance. L'installation de pare-feu permet d'agir comme une barrière de protection, bloquant les tentatives d'accès non autorisées et surveillant le trafic réseau pour détecter les activités suspectes.

Bien que les objets connectés de cette maison offrent une commodité et des fonctionnalités avancées, ces objets connectés doivent être sécurisés de manière adéquate afin de protéger les utilisateurs contre les attaques potentielles. La sécurité des objets connecté reste une préoccupation majeure, nécessitant une attention continue et des efforts coordonnés entre les fabricants, les chercheurs en sécurité et les utilisateurs finaux. En adoptant des pratiques de sécurité robustes et en restant vigilants quant aux mises à jour de sécurité, les foyers peuvent réduire les risques et assurer une utilisation sûre et fiable des technologies connectées dans leurs foyers.

6. Recommandations

Assurer la sécurité des objets connectés dans nos foyers est essentiel pour protéger nos informations personnelles. Cela, ne doit pas être perçu comme une tâche ardue, mais plutôt comme une série d'étapes essentielles pour garantir un environnement numérique sûr et fiable. Pour ce faire, il est crucial de mettre en place des mesures de sécurité adéquates. Cette section propose un ensemble de recommandations pratiques pour renforcer la protection de nos appareils connectés, tout en étant réalisable par les utilisateurs eux-mêmes.

Afin d'assurer la sécurité des objets connectés dans nos foyers et donc protéger nos informations personnelles, il est important de mettre en place les mesures adéquates. Cela commence par appliquer un concept informatique très important : Zero Trust (Confiance Zéro). Ce modèle de sécurité ne considère aucun élément, qu'il soit interne ou externe, comme digne de confiance par défaut. Chaque tentative d'accès ou de communication doit être vérifiée et authentifiée indépendamment de sa provenance. En appliquant le concept de Zero Trust à un foyer, cela implique de renforcer la sécurité de chaque appareil et de chaque connexion, même à l'intérieur du réseau domestique (Républic Française 2021; Fortinet 2019).

6.1 Quelles questions se poser avant l'achat d'un IOT

Cela commence par se poser les bonnes questions avant l'achat d'un objet connecté :

- Existe-il une fréquence de mise à jour ? Si oui quelle est la fréquence des mises à jour ?
- Est-ce que les mises à jour sont installées automatiquement ou l'utilisateur doit-il les lancer manuellement ?
- Comment l'utilisateur est-il notifié que des mises à jour sont disponibles ?
- Existe-il des mécanismes de sécurité dont l'appareil dispose afin d'empêcher tout accès non autorisé ?
- Est-ce que le système d'exploitation de l'appareil est compatible avec le chiffrement sécurisé de type HTTPS par exemple ?
- Est-il possible de modifier les données d'accès prédéfinies par le fabricant comme le nom d'utilisateur et le mot de passe ?
- Est-ce que mon appareil propose une option de double facteur d'authentification pour renforcer la sécurité ?

Ces questions permettent de choisir des objets connectés qui offrent non seulement des fonctionnalités pratiques et innovantes mais aussi une protection robuste contre les menaces numériques. Elles garantissent une utilisation sécurisée et fiable, minimisant les risques de violation de la vie privée (DDPS 2024 ; Annexe 3).

6.2 Les mesures à mettre en place

Lorsque nous nous sommes posé ces questions et que nous avons acheté les bons objets connectés pour notre maison, il faut par la suite pour tous objets connectés au réseau du foyer mettre en place les mesures suivantes lorsqu'elles sont possibles :

- Segmenter notre réseau Wi-Fi pour renforcer la sécurité de notre réseau domestique, en créant plusieurs sous-réseaux dédiés pour nos objets connectés, tels qu'un pour les caméras de sécurité, un autre pour les stores intelligents, etc. Cela permet de limiter la propagation des pirates dans le réseau principal, rendant plus difficile l'accès à nos informations sensibles et à nos autres appareils. De plus, l'utilisation d'un réseau Wi-Fi invité protégé par une double authentification pour les personnes extérieures au foyer permet d'ajouter une couche supplémentaire de sécurité. Les appareils IOT étant plutôt vulnérables aux cyberattaques en raison de leurs configurations de sécurité parfois faibles, le fait de les isoler sur un sous-réseau distinct, permet de limiter leur accès à nos données personnelles et critiques, ce qui permet de réduire les risques d'attaque. Il faut connecter exclusivement les appareils IOT à ce sous-réseau et limiter leur accès à Internet uniquement. L'appareil est ainsi connecté à Internet sans être relié à notre réseau interne. De cette façon, nous protégeons notre réseau interne de toute attaque menée par le biais de l'un de nos appareils connectés. Cette segmentation protège nos données sensibles contre les attaques potentielles via des dispositifs IOT, réduit les risques d'intrusion et permet une gestion centralisée des mises à jour de sécurité des appareils IOT sans compromettre la sécurité du réseau principal. Adopter cette pratique sécurise notre maison intelligente tout en maintenant un haut niveau de protection pour notre réseau domestique.
- Désactiver la fonction universal plug and play (UPnP) de notre routeur permet la configuration manuelle de la redirection de port et permet de maintenir un réseau sécurisé. Bien que cela demande un effort supplémentaire, cette pratique offre un contrôle accru sur notre réseau et réduit considérablement les risques de sécurité. En choisissant précisément quels ports ouvrir, nous protégeons nos appareils contre les accès non autorisés et les cyberattaques, assurant ainsi la sécurité de notre maison intelligente. Il faut cependant se renseigner auprès de notre fournisseur d'accès afin de s'informer sur les possibilités de configuration et les conséquences que ces mesures peuvent engendrer.

- Utiliser des filtres d'adresses IP et des filtres de géolocalisation d'adresses IP est une mesure efficace pour protéger nos appareils IOT contre les accès non autorisés. En configurant ces filtres, nous pouvons restreindre l'accès à des adresses IP de confiance ou à des régions géographiques spécifiques, renforçant ainsi la sécurité de notre réseau domestique et réduisant le risque de cyberattaques.
- Utiliser uniquement des protocoles qui offrent une connexion sécurisée, tels que des protocoles HTTPS. Ces protocoles offrent un cryptage fort, une authentification sécurisée et une protection contre les interceptions et les modifications des données. Il faut éviter les protocoles non sécurisés comme HTTP, qui laissent nos communications vulnérables et exposées aux attaques. En adoptant des protocoles de connexion sécurisée, nous renforçons considérablement la sécurité de notre environnement numérique. Cela nous permet de renforcer notre protection contre les attaques de type MITM.
- Éviter l'utilisation de ports standards pour nos objets connectés est une stratégie efficace pour renforcer la sécurité de notre réseau domestique. En choisissant des ports plus complexes et moins courants, nous compliquons la tâche des attaquants qui utilisent des scanners de ports pour détecter les dispositifs.
- Ne jamais utiliser les données d'accès par défaut, telles que les noms d'utilisateur et les mots de passe prédéfinis, car ils sont bien connus des cybercriminels et facilement exploitables. Dès la mise en service de l'appareil, il faut immédiatement changer ces informations d'accès. Il est prudent d'utiliser un nom d'utilisateur unique et un mot de passe fort, incluant une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux. Ces combinaisons doivent être différentes pour chaque IOT. En modifiant ces identifiants par défaut, nous empêchons les pirates d'accéder facilement à nos appareils via des listes de mots de passe courants ou des attaques par force brute. Il est également du devoir de l'utilisateur de conserver ces nouvelles informations d'identification dans un endroit sécurisé pour un accès futur.
- Utiliser lorsque cela est possible, un deuxième facteur d'authentification pour renforcer la sécurité des objets connectés. Le deuxième facteur d'authentification ajoute une couche supplémentaire de protection en demandant une deuxième forme de vérification en plus du mot de passe, telle qu'un code envoyé par SMS, une application d'authentification, ou une clé de sécurité physique. Cette méthode rend toute connexion non autorisée beaucoup plus difficile, car même

si un attaquant parvient à obtenir nos identifiants et mots de passe avec une attaque MITM par exemple, il ne pourra pas accéder à nos appareils sans ce second facteur. En activant le deuxième facteur d'authentification, nous augmentons significativement la résistance de nos dispositifs IOT contre les cyberattaques et les intrusions. Cela assure ainsi une meilleure protection de notre réseau et de nos données personnelles. Il est nécessaire de configurer et de tester le deuxième facteur d'authentification dès la mise en service de l'appareil et de le maintenir à jour.

- Déconnecter nos appareils du réseau ou d'Internet lorsqu'ils ne sont pas utilisés. Cela permet de limiter les risques de cyberattaques tout en offrant des avantages supplémentaires comme des économies d'énergie. En intégrant cette habitude dans notre routine quotidienne, nous renforçons la sécurité de notre maison intelligente.
- Effectuer des mises à jour régulières, tant logicielles que micrologicielles. Bien que cela puisse sembler banal, négliger ou retarder les mises à jour expose nos dispositifs à des vulnérabilités de sécurité récemment découvertes, compromettant ainsi la protection de nos données personnelles. Ces mises à jour fournies par les fabricants incluent des correctifs pour des vulnérabilités de sécurité récemment découvertes, ainsi que des améliorations de performances et de nouvelles fonctionnalités. En configurant nos appareils pour recevoir des mises à jour automatiques et en effectuant des vérifications manuelles régulières, nous assurons une protection continue contre les menaces potentielles.
- Installer des pare-feux, qu'ils soient matériels, logiciels ou intégrés aux routeurs. Les pare-feux agissent comme une barrière de protection, bloquant les tentatives d'accès non autorisé et surveillant le trafic réseau pour détecter les activités suspectes. Ils permettent d'éviter que nos appareils soient utilisés pour diverses attaques, telles que les attaques par DDoS. Si possible, activer et configurer les pare-feux via l'interface de gestion de notre routeur ou directement sur nos appareils pour protéger efficacement nos IOT et assurer la sécurité de notre maison intelligente.

Si malgré nos précautions, un de nos objets connectés est infecté, il est crucial d'agir rapidement pour minimiser les dommages et sécuriser réseau.

- Déconnecter immédiatement l'appareil infecté du réseau pour empêcher la propagation du pirate.
- Réinitialiser l'appareil et consulter le manuel d'utilisation ou le site Internet du fabricant.
- Utiliser des outils de diagnostic pour analyser l'infection et effectuer une réinitialisation d'usine de l'appareil.
- Installer les dernières mises à jour du firmware et des logiciels et changer les identifiants de connexion par défaut.
- Après la réinitialisation, réappliquer les mesures préventives recommandées pour minimiser le risque de nouvelles attaques.

Mettre en œuvre toutes ces recommandations de sécurité dans notre foyer réduit considérablement les risques d'attaques sur nos appareils connectés. Il est important de rappeler que nous sommes responsables de la sécurité de nos objets connectés, surtout si par la suite ils sont utilisés à des fins malveillantes par des pirates informatiques afin de nuire à d'autres personnes ou entreprises. De plus, si un pirate informatique entreprend un scan d'objets connectés et découvre que nos dispositifs sont bien protégés, il est beaucoup moins susceptible de persister, à moins qu'il ne nous cible personnellement. En suivant ces pratiques, nous créons des couches de sécurité qui découragent les attaquants. Plus notre système est sécurisé, moins nous avons de chances d'être piraté. En effet, les cybercriminels préfèrent les cibles faciles et se tournent vers des dispositifs moins protégés. Bien que certaines de ces mesures puissent prendre du temps à mettre en place, le gain en sécurité, de tranquillité d'esprit et d'économies potentielles par la suite ne sont pas négligeables. Adopter ces mesures de sécurité est donc essentiel pour protéger notre maison intelligente et assurer la sécurité de nos données personnelles et de nos appareils (DDPS 2024 ; Annexe 3).

7. Conclusion

La sécurité des objets connectés dans les foyers genevois représente un enjeu crucial à l'ère du numérique où l'interconnexion et l'automatisation des appareils domestiques sont en constante expansion. Cette étude a mis en lumière les défis et les opportunités liés à l'adoption des objets connectés dans les foyers genevois. La domotique en pleine expansion apporte un confort, une sécurité et une efficacité énergétique sans précédent, mais elle expose également les utilisateurs à des risques de cybersécurité significatifs.

Les résultats de cette recherche révèlent une adoption croissante des objets connectés tout en soulignant une sensibilisation modérée des utilisateurs aux risques de cybersécurité. L'analyse des vulnérabilités du cas pratique démontre que les objets connectés présentent des failles exploitables par les cybercriminels. Il est donc impératif d'adopter des mesures de sécurité robustes et de sensibiliser davantage les utilisateurs à l'importance de protéger leurs dispositifs connectés.

Les recommandations formulées dans cette étude visent à renforcer la sécurité des objets connectés dans les foyers genevois. Cela inclut l'adoption de bonnes pratiques de sécurité, telles que l'adoption d'une approche "Zero Trust". Puis se poser les bonnes questions avant l'achat d'un objet connecté, évaluer la fréquence des mises à jour, les mécanismes de sécurité et la possibilité de modifier les identifiants par défaut, etc. Après l'acquisition, mettre en place les mesures suivantes lorsqu'elles sont possibles : segmenter le réseau Wi-Fi, désactiver la fonction UPnP, utiliser des filtres d'adresses IP, adopter des protocoles sécurisés comme HTTPS, éviter les ports standards, changer les identifiants par défaut, utiliser une authentification à deux facteurs, déconnecter les appareils inutilisés, configurer les mises à jour automatiques, installer des pare-feux. Ces mesures protègent efficacement le réseau domestique et les données personnelles contre les cyberattaques. Il est également crucial de sensibiliser les utilisateurs à l'importance de la cybersécurité et de leur rôle dans la protection de leurs appareils.

Pour conclure, en adoptant une approche "Zero Trust" et en appliquant les recommandations énoncées, les foyers genevois peuvent continuer à bénéficier des avantages de la domotique tout en minimisant les risques associés. La sensibilisation continue et l'éducation sur les bonnes pratiques de cybersécurité sont essentielles pour garantir la protection des données personnelles et la sécurité des environnements domestiques connectés.

Bibliographie

2023-IoT-Security-Landscape-Report, [en ligne]. Disponible à l'adresse : <https://www.bitdefender.com/files/News/CaseStudies/study/429/2023-IoT-Security-Landscape-Report.pdf> [consulté le 17 juin 2024].

AGATHA2333, 2023. IoT-CVE/Third Reality Smart Blind Vulnerability Report.pdf at main · iot-sec23/IoT-CVE · GitHub. [en ligne]. 24 mai 2023. Disponible à l'adresse : <https://github.com/iot-sec23/IoT-CVE/blob/main/Third%20Reality%20Smart%20Blind%20Vulnerability%20Report.pdf> [consulté le 7 juillet 2024].

AVAST, 2024. Sécurité Wi-Fi : WEP vs WPA ou WPA2. [en ligne]. 2024. Disponible à l'adresse : <https://www.avast.com/fr-fr/c-wep-vs-wpa-or-wpa2> [consulté le 17 juin 2024].

CONSEIL FÉDÉRAL, 2020. Normes de sécurité pour les appareils connectés à Internet (Internet des objets). *Internet des objets*.

CVE, 2019. CVE Record | CVE. [en ligne]. 19 juillet 2019. Disponible à l'adresse : <https://www.cve.org/CVERecord?id=CVE-2019-12820> [consulté le 7 avril 2024].

CVE, 2021. CVE Record | CVE. [en ligne]. 6 mai 2021. Disponible à l'adresse : <https://www.cve.org/CVERecord?id=CVE-2021-31793> [consulté le 7 avril 2024].

CVE, 2022. CVE Record | CVE. [en ligne]. 23 février 2022. Disponible à l'adresse : <https://www.cve.org/CVERecord?id=CVE-2022-25809> [consulté le 7 avril 2024].

CVE, 2023a. CVE Record | CVE. [en ligne]. 8 novembre 2023. Disponible à l'adresse : <https://www.cve.org/CVERecord?id=CVE-2023-41270> [consulté le 7 juillet 2024].

CVE, 2023b. CVE Record | CVE. [en ligne]. 30 octobre 2023. Disponible à l'adresse : <https://www.cve.org/CVERecord?id=CVE-2023-45956> [consulté le 7 avril 2024].

CVE, 2023c. CVE Record | CVE. [en ligne]. 13 juillet 2023. Disponible à l'adresse : <https://www.cve.org/CVERecord?id=CVE-2023-33768> [consulté le 7 avril 2024].

CVE, 2023d. CVE Record | CVE. [en ligne]. 20 janvier 2023. Disponible à l'adresse : <https://www.cve.org/CVERecord?id=CVE-2022-43704> [consulté le 7 avril 2024].

CVE, 2023e. CVE Record | CVE. [en ligne]. 24 avril 2023. Disponible à l'adresse : <https://www.cve.org/CVERecord?id=CVE-2023-29780> [consulté le 7 juillet 2024].

CVE, 2024a. Overview | CVE. [en ligne]. 2024. Disponible à l'adresse : <https://www.cve.org/About/Overview#AbouttheCVEProgram> [consulté le 7 juillet 2024].

CVE, 2024b. List Of Partners | CVE. [en ligne]. 2024. Disponible à l'adresse : <https://www.cve.org/PartnerInformation/ListofPartners> [consulté le 7 juillet 2024].

CVE, 2024c. CVE Record | CVE. [en ligne]. 4 juin 2024. Disponible à l'adresse : <https://www.cve.org/CVERecord?id=CVE-2023-51629> [consulté le 7 avril 2024].

DDPS, Département fédéral de la défense, de la protection de la population et des sports, 2024. Sécurité de l'Internet des objets. [en ligne]. 1 janvier 2024. Disponible à l'adresse : <https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-iot.html> [consulté le 7 juillet 2024].

D-LINK, 2023. D-Link Technical Support. [en ligne]. 13 juillet 2023. Disponible à l'adresse : <https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SA-P10370> [consulté le 7 juillet 2024].

ESPOSITO, Sergio, SGANDURRA, Daniele et BELLA, Giampaolo, 2022. [2202.08619] Alexa versus Alexa: Controlling Smart Speakers by Self-Issuing Voice Commands.

[en ligne]. 17 février 2022. Disponible à l'adresse : <https://arxiv.org/abs/2202.08619> [consulté le 7 juillet 2024].

FORTINET, 2019. Qu'est-ce que le modèle de sécurité Zero-Trust ? Fonctionnement. *Fortinet* [en ligne]. 2019. Disponible à l'adresse : <https://www.fortinet.com/fr/resources/cyberglossary/what-is-the-zero-trust-network-security-model.html> [consulté le 7 juillet 2024].

FUGUET, Gerard, 2022. SMOLD TV: Old & Smart. *SlideShare* [en ligne]. 17 octobre 2022. Disponible à l'adresse : <https://www.slideshare.net/slideshow/smold-tv-old-smart/253658668> [consulté le 7 avril 2024].

GABRIELE, Rob, 2023. 2024 Guide to Home Automation Systems & Smart Home Products. *SafeHome.org* [en ligne]. 23 mai 2023. Disponible à l'adresse : <https://www.safehome.org/home-automation/> [consulté le 8 juillet 2024].

GORDON LYON, 2024. Nmap: the Network Mapper - Free Security Scanner. [en ligne]. 2024. Disponible à l'adresse : <https://nmap.org/> [consulté le 8 juillet 2024].

HANNA, Victor, 2023. CVE-2022-43704 - Capture-Replay Vulnerability in Sinilink XY-WFT1 Thermostat | Trustwave. [en ligne]. 12 janvier 2023. Disponible à l'adresse : <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/cve-2022-43704-capture-replay-vulnerability-in-sinilink-xy-wft1-thermostat/> [consulté le 7 juillet 2024].

HAWRYLACK, SAM, 2024. Smart Home: Definition, Benefits And More | Rocket Mortgage. [en ligne]. 24 avril 2024. Disponible à l'adresse : <https://www.rocketmortgage.com/learn/smart-home> [consulté le 17 juin 2024].

HENGESBERGER, Cynthia, 2024. À quand la démocratisation de la maison intelligente? - Bulletin FR. [en ligne]. 2 avril 2024. Disponible à l'adresse : <https://www.bulletin.ch/fr/news-detail/a-quand-la-democratisation-de-la-maison-intelligente.html> [consulté le 17 juin 2024].

IOT-FUZZ, 2023. IoT-Fuzz/Govee LED Strip Vulnerability Report.pdf at main · IoT-Fuzz/loT-Fuzz · GitHub. [en ligne]. 30 octobre 2023. Disponible à l'adresse : <https://github.com/loT-Fuzz/loT-Fuzz/blob/main/Govee%20LED%20Strip%20Vulnerability%20Report.pdf> [consulté le 7 juillet 2024].

IWUGO, Daniel, 2022. Wi-Fi Hacking 101 – How to Hack WPA2 and Defend Against These Attacks. *freeCodeCamp.org* [en ligne]. 18 octobre 2022. Disponible à l'adresse : <https://www.freecodecamp.org/news/wi-fi-hacking-101/> [consulté le 17 juin 2024].

JACKSON, Mark, 2024. New SSID Confusion Attack Exploits General WiFi Vulnerability. *ISPreview UK* [en ligne]. 14 mai 2024. Disponible à l'adresse : <https://www.ispreview.co.uk/index.php/2024/05/new-ssid-confusion-attack-exploits-general-wifi-vulnerability.html> [consulté le 17 juin 2024].

KHEIRKHAH, Sina, 2024. ZDI-24-049 | Zero Day Initiative. [en ligne]. janvier 2024. Disponible à l'adresse : <https://www.zerodayinitiative.com/advisories/ZDI-24-049/> [consulté le 7 juillet 2024].

MICROSOFT, 2024. Qu'est-ce que la technologie XDR ? | Sécurité Microsoft. [en ligne]. 2024. Disponible à l'adresse : <https://www.microsoft.com/fr-ch/security/business/security-101/what-is-xdr> [consulté le 17 juin 2024].

NEWSROOM, 2024. New Wi-Fi Vulnerability Enables Network Eavesdropping via Downgrade Attacks. *The Hacker News* [en ligne]. 16 mai 2024. Disponible à l'adresse : <https://thehackernews.com/2024/05/new-wi-fi-vulnerability-enabling.html> [consulté le 17 juin 2024].

NIST, 2022. NVD - CVE-2021-31793. [en ligne]. 7 décembre 2022. Disponible à l'adresse : <https://nvd.nist.gov/vuln/detail/CVE-2021-31793> [consulté le 7 avril 2024].

NIST, 2023a. NVD - CVE-2022-25809. [en ligne]. 8 août 2023. Disponible à l'adresse : <https://nvd.nist.gov/vuln/detail/CVE-2022-25809> [consulté le 7 avril 2024].

NIST, 2023b. NVD - CVE-2023-45956. [en ligne]. 11 juin 2023. Disponible à l'adresse : <https://nvd.nist.gov/vuln/detail/CVE-2023-45956> [consulté le 7 avril 2024].

NIST, 2023c. NVD - CVE-2023-33768. [en ligne]. 21 juillet 2023. Disponible à l'adresse : <https://nvd.nist.gov/vuln/detail/CVE-2023-33768> [consulté le 7 avril 2024].

NIST, 2023d. NVD - CVE-2022-43704. [en ligne]. 27 janvier 2023. Disponible à l'adresse : <https://nvd.nist.gov/vuln/detail/CVE-2022-43704> [consulté le 7 avril 2024].

NIST, 2023e. NVD - CVE-2023-29780. [en ligne]. 5 avril 2023. Disponible à l'adresse : <https://nvd.nist.gov/vuln/detail/CVE-2023-29780> [consulté le 7 avril 2024].

NIST, 2023f. NVD - CVE-2019-12820. [en ligne]. 11 juin 2023. Disponible à l'adresse : <https://nvd.nist.gov/vuln/detail/CVE-2019-12820> [consulté le 7 juillet 2024].

NIST, 2024a. NVD - General. [en ligne]. 27 juin 2024. Disponible à l'adresse : <https://nvd.nist.gov/general> [consulté le 7 juillet 2024].

NIST, 2024b. NVD - Vulnerability Metrics. [en ligne]. 27 juin 2024. Disponible à l'adresse : <https://nvd.nist.gov/vuln-metrics/cvss#> [consulté le 7 juillet 2024].

NIST, 2024c. NVD - Search and Statistics. [en ligne]. 2024. Disponible à l'adresse : <https://nvd.nist.gov/vuln/search> [consulté le 17 juin 2024].

NIST, 2024d. NVD - CVEs and the NVD Process. [en ligne]. 2024. Disponible à l'adresse : <https://nvd.nist.gov/general/cve-process> [consulté le 17 juin 2024].

NIST, 2024e. NVD - Results. [en ligne]. 2024. Disponible à l'adresse : https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=Samsung+Smart+TV+UE40D7000+version+T-GAPDEUC-1033.2&search_type=all&isCpeNameSearch=false [consulté le 9 juillet 2024].

NIST, 2024f. NVD - CVE-2023-41270. [en ligne]. 16 mai 2024. Disponible à l'adresse : <https://nvd.nist.gov/vuln/detail/CVE-2023-41270> [consulté le 7 avril 2024].

NIST, 2024g. NVD - CVE-2023-51629. [en ligne]. 5 mars 2024. Disponible à l'adresse : <https://nvd.nist.gov/vuln/detail/CVE-2023-51629> [consulté le 7 avril 2024].

NIST, 2024h. NVD - CVE-2022-32509. [en ligne]. 14 mai 2024. Disponible à l'adresse : <https://nvd.nist.gov/vuln/detail/CVE-2022-32509> [consulté le 7 avril 2024].

NUKI, 2022. Nuki Security Updates. *Nuki* [en ligne]. juin 2022. Disponible à l'adresse : <https://nuki.io/en/security-updates/> [consulté le 7 juillet 2024].

OCDE, 2018. *IoT measurement and applications*. Paris : OCDE. DOI 10.1787/35209dbf-en.

OFCS, 2023. Cyberconseil: précautions à prendre avec l'Internet des objets. [en ligne]. 20 avril 2023. Disponible à l'adresse : <https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/2023/cybertipp-iot.html> [consulté le 17 juin 2024].

OFCS, 2024. Sécurité de l'Internet des objets. [en ligne]. 1 janvier 2024. Disponible à l'adresse : <https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-iot.html> [consulté le 17 juin 2024].

OLSSON, Theodor et FORSBERG, Albin Larsson, 2019. IoT Offensive Security Penetration Testing. .

PME, Portail, 2023. Internet des objets (IoT): applications et opportunités. [en ligne]. 16 mars 2023. Disponible à l'adresse : <https://www.kmu.admin.ch/kmu/fr/home/fakten-und-trends/internet-of-things.html> [consulté le 8 juillet 2024].

PURSEC LAB, 2023. GitHub - purseclab/CVE-2023-33768: DoS against Belkin smart plugs via crafted firmware injection. [en ligne]. 16 juillet 2023. Disponible à l'adresse : <https://github.com/purseclab/CVE-2023-33768> [consulté le 7 juillet 2024].

RÉPUBLIQUE FRANÇAISE, 2021. Le modèle Zero Trust | ANSSI. [en ligne]. 15 avril 2021. Disponible à l'adresse : <https://cyber.gouv.fr/publications/le-modele-zero-trust> [consulté le 7 juillet 2024].

ROMERO, Daniel, 2022. Technical Advisory – Multiple vulnerabilities in Nuki smart locks (CVE-2022-32509, CVE-2022-32504, CVE-2022-32502, CVE-2022-32507, CVE-2022-32503, CVE-2022-32510, CVE-2022-32506, CVE-2022-32508, CVE-2022-32505) | NCC Group Research Blog | Making the world safer and more secure. [en ligne]. 25 juillet 2022. Disponible à l'adresse : <https://research.nccgroup.com/2022/07/25/technical-advisory-multiple-vulnerabilities-in-nuki-smart-locks-cve-2022-32509-cve-2022-32504-cve-2022-32502-cve-2022-32507-cve-2022-32503-cve-2022-32510-cve-2022-32506-cve-2022-32508-cve-2/> [consulté le 7 juillet 2024].

SHODAN, 2024a. What is Shodan? - Shodan Help Center. [en ligne]. 2024. Disponible à l'adresse : <https://help.shodan.io/the-basics/what-is-shodan> [consulté le 8 juillet 2024].

SHODAN, 2024b. Shodan Search. [en ligne]. 2024. Disponible à l'adresse : <https://www.shodan.io/search?query=d-link+country%3A%22CH%22+city%3A%22Bernex%22> [consulté le 8 juillet 2024].

SHODAN, 2024c. 188.155.247.185. [en ligne]. 8 juillet 2024. Disponible à l'adresse : <https://www.shodan.io/host/188.155.247.185> [consulté le 17 juin 2024].

SHODAN, 2024d. 62.2.85.226. [en ligne]. 17 juin 2024. Disponible à l'adresse : <https://www.shodan.io/host/62.2.85.226> [consulté le 17 juin 2024].

STATISTA, 2022. Smart home device ownership US 2022. *Statista* [en ligne]. mai 2022. Disponible à l'adresse : <https://www.statista.com/statistics/1124290/smart-home-device-ownership-us/> [consulté le 17 juin 2024].

STATISTA, 2023a. Les objets connectés. *Statista* [en ligne]. 2023. Disponible à l'adresse : <https://fr.statista.com/etude/35552/les-objets-connectes-dossier-statista/> [consulté le 17 juin 2024].

STATISTA, 2023b. Smart Home: Marktdaten & -Analyse | Statista. [en ligne]. septembre 2023. Disponible à l'adresse : <https://de.statista.com/statistik/studie/id/41155/dokument/smart-home-report/> [consulté le 8 juillet 2024].

STATISTA, 2024a. Smart Home - Switzerland | Statista Market Forecast. *Smart Home - Switzerland* [en ligne]. mars 2024. Disponible à l'adresse : <https://www.statista.com/outlook/cmo/smart-home/switzerland> [consulté le 8 juillet 2024].

STATISTA, 2024b. Smart Home - Worldwide | Statista Market Forecast. *Smart Home - Worldwide* [en ligne]. mars 2024. Disponible à l'adresse : <https://www.statista.com/outlook/cmo/smart-home/worldwide> [consulté le 8 juillet 2024].

STATISTA, 2024c. IoT connections worldwide 2022-2033. *Statista* [en ligne]. juin 2024. Disponible à l'adresse : <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/> [consulté le 17 juin 2024].

STATISTA, 2024d. Smart Appliances - Switzerland | Statista Market Forecast. *Statista* [en ligne]. mars 2024. Disponible à l'adresse : <https://www.statista.com/outlook/cmo/smart-home/smart-appliances/switzerland> [consulté le 27 juin 2024].

STATISTA, 2024e. Control & Connectivity - Switzerland | Market Forecast. *Statista* [en ligne]. mars 2024. Disponible à l'adresse : <https://www.statista.com/outlook/cmo/smart-home/control-connectivity/switzerland> [consulté le 27 juin 2024].

STATISTA, 2024f. Comfort & Lighting - Switzerland | Statista Market Forecast. *Statista* [en ligne]. mars 2024. Disponible à l'adresse : <https://www.statista.com/outlook/cmo/smart-home/comfort-lighting/switzerland> [consulté le 27 juin 2024].

STATISTA, 2024g. Security - Switzerland | Statista Market Forecast. *Statista* [en ligne]. mars 2024. Disponible à l'adresse : <https://www.statista.com/outlook/cmo/smart-home/security/switzerland> [consulté le 27 juin 2024].

STATISTA, 2024h. Energy Management - Switzerland | Statista Market Forecast. *Statista* [en ligne]. mars 2024. Disponible à l'adresse : <https://www.statista.com/outlook/cmo/smart-home/energy-management/switzerland> [consulté le 27 juin 2024].

STATISTA, 2024i. Home Entertainment - Switzerland | Statista Market Forecast. *Statista* [en ligne]. mars 2024. Disponible à l'adresse : <https://www.statista.com/outlook/cmo/smart-home/home-entertainment/switzerland> [consulté le 27 juin 2024].

SUJAY VAILSHERY, Lionel, 2024. IoT connections worldwide 2022-2033. *Statista* [en ligne]. 12 juin 2024. Disponible à l'adresse : <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/> [consulté le 8 juillet 2024].

TJ-CONNOR, 2021. gist:16a4116050bbcb4717315f519b944f1f - GitHub. [en ligne]. 24 avril 2021. Disponible à l'adresse : <https://gist.github.com/tj-oconnor/16a4116050bbcb4717315f519b944f1f> [consulté le 7 juillet 2024].

TRANSFORMA INSIGHTS, 2024. Current IoT Forecast Highlights - Transforma Insights. [en ligne]. 7 juin 2024. Disponible à l'adresse : <https://transformainsights.com/research/forecast/highlights> [consulté le 8 juillet 2024].

VIVINT, 2023. 10 Advantages of Home Automation | Vivint. [en ligne]. 11 juillet 2023. Disponible à l'adresse : <https://www.vivint.com/resources/article/advantages-of-home-automation> [consulté le 17 juin 2024].

Annexe 1 : Glossaire

Adresse IP = Internet Protocol : un identifiant numérique attribué à chaque appareil connecté à un réseau.

Adresse MAC = Media Access Control : adresse physique d'un périphérique réseau.

Aircrack-ng : un ensemble d'outils de sécurité réseau utilisé principalement pour tester la sécurité des réseaux Wi-Fi.

Airodump-ng : logiciel qui permet la capture et l'analyse des paquets (bloc de données) des réseaux Wi-Fi.

API = Application Programming Interface : un ensemble de protocoles qui facilite la création et l'intégration des applications.

ONVIF = Open Network Video Interface Forum : un ensemble de règles qui permet à différents appareils vidéo réseau de communiquer entre eux.

Attaque WPS = Wi-Fi Protected Setup : une méthode d'exploitation de la vulnérabilité du protocole Wi-Fi Protected Setup.

Authentication Digest : un système d'authentification Web.

DDoS = Distributed Denial of Service : une attaque où de nombreux appareils coordonnés visent un service pour le rendre indisponible.

DoS = Denial of Service : une attaque visant à rendre un service indisponible.

Firmware : programme intégré dans un matériel.

MITM = Man-in-the-middle : une attaque où un pirate informatique intercepte et manipule les communications entre l'utilisateur et le système.

MQTT = Message Queuing Telemetry Transport : un protocole de messagerie léger utilisé pour la communication entre appareils connectés.

Pentester : une personne qui teste la sécurité des systèmes informatiques en simulant des attaques.

Port 80 : le port standard utilisé pour les communications HTTP permettant la navigation sur le web.

Rançongiciels : logiciels malveillants qui chiffrent les données d'une victime et exigent une rançon pour les déchiffrer.

Réseaux de zombie : un groupe d'appareils connectés infectés et contrôlés à distance pour mener des cyberattaques.

SSID = Service Set Identifier : nom d'un réseau Wi-Fi.

SSL/TLS = Secure Sockets Layer/Transport Layer Security : un protocole chiffré qui permet de transmettre des informations.

VPN = Virtual Private Network : un réseau privé virtuel.

Wearable : un appareil électronique intégré à un vêtement ou un accessoire.

WEP = Wired Equivalent Privacy : protocoles destinés à assurer la sécurité des connexions WiFi.

Zigbee : un protocole de communication sans fil.

Annexe 2 : Questionnaire

Rubrique 1 sur 3

Les objets connectés dans les maisons

B *I* U  

Madame, Monsieur,

Dans le cadre de mon travail de Bachelor en économie d'entreprise, je mène une analyse sur les objets connectés dans les maisons. Afin de mener à bien cette étude, je vous demande votre aide en répondant à ce questionnaire qui dure environ **5 à 10 min**.

Je vous remercie de consacrer un peu de votre temps pour ce questionnaire, qui me permettra de répondre à la problématique suivante : Comment assurer la sécurité des objets connectés dans les foyers genevois et protéger efficacement les données personnelles des utilisateurs.

Je vous remercie d'avance pour votre participation.

Nicolas Martinelli

Vous êtes ? *

- ☐ Homme
- ☐ Femme
- ☐ Préfère ne pas répondre
- ☐ Autre...

Quel est votre date de naissance ? *

Mois, jour, année



Cybersécurité / Sensibilisation



IOT = objets connectés

Comment mesurez-vous votre conscience des risques de cybersécurité liés à l'utilisation des objets connectés dans votre quotidien ? *

	1	2	3	4	
Pas conscient	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Très conscient

Votre télévision connectée se fait hacker, et est utilisée afin d'attaquer une entreprise, pensez-vous être fautif aux yeux de la loi ? *

	1	2	3	4	
0% fautif	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	100% fautif

Quels types d'attaques concernant les objets connectés connaissez-vous ? *

- ☐ Aucune
- ☐ Attaques par injection de code : injection de codes malveillants pour compromettre leur sécurité.
- ☐ Attaques de ransomware : prise de contrôle des iot et demande de rançons pour éviter la divulgation de données sensibles.
- ☐ Attaques par détournement de compte : utilisation des identifiants volés afin d'accéder aux comptes des iot.
- ☐ Attaques par déni de service (DDoS) : rendre un service indisponible en surchargeant l'iot.
- ☐ Attaques de spoofing (usurpation d'identité) : falsification des adresses IP pour accéder aux réseaux.
- ☐ Attaques par interception de données entre les iot et les serveurs.

Quelles raisons qui pousseraient un hacker à attaquer vos objets connectés, connaissez vous? *

- ☐ Aucune
- ☐ Espionnage et surveillance : utilisation des caméras pour recueillir des informations sensibles.
- ☐ Manipulation des données : modification des données collectées par les iot pour induire en erreur les utilisateurs.
- ☐ Vol d'informations personnelles des utilisateurs.
- ☐ Botnets : utilisation des iot pour constituer un réseaux d'appareils infectés afin de mener des attaques informatiques à distance.
- ☐ Extorsion d'argent en menaçant de divulguer des informations sensibles ou en bloquant l'accès aux appareils.
- ☐ Sabotage : Désactiver ou altérer le fonctionnement des appareils connectés.

Avez-vous déjà été victime d'une cyberattaque visant un de vos objets connectés à domicile ? *

- ☐ Oui
- ☐ Non
- ☐ Ne sais pas

Avez-vous une assurance pour la cybersécurité ? *

- ☐ Oui, au travers de l'assurance ménage
- ☐ Oui, au travers d'une assurance supplémentaire
- ☐ Non
- ☐ Ne sais pas

Relation avec les objets connectés

Quels types d'objets connectés possédez-vous ?

Intérieur (Système d'éclairage intelligent / Caméras de sécurité / Climatiseurs intelligents / Thermostat intelligent / Store ou rideau motorisé connecté / Détecteurs de fumée connectés / autre)

Extérieur (Sonnette connectée / Système d'alarme connecté / Serrure de porte connectée / Système d'arrosage connecté / autre)

Salon (Assistant vocal / Aspirateur robot intelligent / Télévision connectée / autre)

Chambre (Réveil intelligent / Télévision connectée / Miroir connecté / autre)

Cuisine (Machine à café connectée / Distributeur automatique de nourriture pour animaux de compagnie connecté / Réfrigérateur intelligent / Balance de cuisine connectée / Assistant culinaire intelligent / Plaque de cuisson ou cuisinière connectée / autre)

Salle de bain (Brosse à dents électrique connectée / Balance connectée / autre)

Wearable (=objets connecté porter sur soi) (Montre connectée / Casque audio ou écouteurs sans fil / Lunettes connectées / Bague connectée / Vêtements connectés / autre)

- ☐ Intérieur
- ☐ Extérieur
- ☐ Salon
- ☐ Chambre
- ☐ Cuisine
- ☐ Salle de bain
- ☐ Wearable
- ☐ Autre : _____

Parmi les catégories que vous avez cochées précédemment, quand a été votre première acquisition d'un objet connecté ?

Veuillez répondre uniquement aux catégories cochées précédemment

	Avant 2010	2011-2015	2016-2020	2021- aujourd'hui
Intérieur	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Extérieur	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Salon	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Chambre	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cuisine	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Salle de bain	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Wearable (objets connecté que l'on porte sur soi)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Autre	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Combien de nouveaux objets connectés envisagez-vous d'ajouter dans votre maison à l'avenir ?

	Aucun	1	2	+3
Intérieur	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Extérieur	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Salon	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Chambre	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cuisine	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Salle de bain	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Wearable (objets connecté que l'on porte sur soi)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Quels sont les objectifs de l'utilisation de ces objets connectés dans votre maison ?

	Pas important	Peu important	Important	Très important
Améliorer le confort	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Augmenter l'efficacité énergétique	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Renforcer la sécurité	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Faciliter les tâches quotidiennes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Suivre les habitudes de vie	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Quels facteurs sont les plus importants pour vous lors du choix d'un nouvel objet connecté pour votre maison ?

	Pas important	Peu important	Important	Très important
Prix	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Marque	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fonctionnalités	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Facilité d'utilisation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Intégration avec d'autres appareils connectés	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sécurité des données	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

En moyenne, combien d'interaction(s) journalière(s) avez-vous avec vos objets connectés ?

- ☐ 0
- ☐ 1-5
- ☐ 6-10
- ☐ 11-15
- ☐ 16-20
- ☐ 21+

Annexe 3 : Retranscription

Retranscription de la conversation du 18 juin 2024 concernant le cas pratique et les recommandations de mon travail de bachelor

Contexte :

Cette conversation s'est déroulée en présentiel dans un bureau équipé d'un écran retranscrivant le contenu de mon PC. J'étais accompagné d'un Pentester nommé Axel Baudry et d'un expert en objet connecté nommé Omar Bognuda. Nous avons discuté des aspects pratiques ainsi que techniques liés à mon cas pratique et de recommandations à mettre en place. Cette retranscription a été réalisée avec l'aide de <https://turboscribe.ai>.

(00:00) Nicolas : Bonjour, donc concernant shodan, j'ai pris un peu l'exemple de ce qu'on peut retrouver avec une caméra D-Link. Et j'ai trouvé un autre où on voyait une photo. Et après, du coup, cette petite partie, moi je suis parti du principe qu'en gros pour avoir accès à tous les objets connectés de la maison, etc., il arrivait à hacker le Wi-Fi. Bon après, le seul truc c'est que du coup je ne suis pas du tout un expert en Wi-Fi. J'ai trouvé quelques petits trucs qui expliquent comment est-ce qu'on peut plus ou moins hacker un Wi-Fi sous protection WPA2 et 3. Et du coup, j'ai retranscrit en gros ce qu'il fallait faire. Et ça c'est peut-être ce que je voulais regarder avec vous afin de voir juste que ce que je suis en train de dire et ce que j'ai lu, ce n'est pas n'importe quoi vu que c'est la base du début. Et après, du coup, dès qu'il était dans le Wi-Fi, j'ai dit qu'il allait utiliser un logiciel Nmap pour trouver du coup tous les dispositifs. Après, j'ai listé les dispositifs et après, j'ai expliqué en gros ce qu'il peut faire avec le National Vulnerability Database, donc en gros qu'on peut retrouver tous les CVE.

Et après, en les mettant dans CVE.org, on peut trouver encore plus d'informations. Et j'ai répété ça pour les 10 objets connectés que j'avais. Et après, j'ai juste fait une sorte de petite conclusion là-dessus pour lister les plus grosses vulnérabilités qui révèlent souvent les DDoS, les attaques avec man-in-the-middle, ce genre de choses.

Et du coup, après, c'est à voir est-ce que c'est possible avec la liste des objets connectés et tout ce que j'ai résumé, pour ce cas pratique-là, mettre en place des protections et après, dans les recommandations, faire quelque chose de plus globalisé entre ce que je

trouve sur Internet, ce que vous vous dites en tant qu'expert, etc. Puis comme ça, ça peut faire plusieurs parties qui vont ensemble.

(02:12) Expert en objet connecté : Pour l'exemple du man-in-the-middle, s'assurer de mettre en place de l'authentification pour des choses comme ça qui font que c'est un type d'attaque qui va être relativement mitigée par la suite.

(02:23) Pentester : Trafic chiffré aussi. Même si tu parviens à accéder au réseau, tu as quand même du trafic chiffré, même si c'est un peu plus compliqué. Mais il ne peut pas avoir tous les paquets qui passent et intercepter les informations.

(02:42) Nicolas : Parce qu'en fait, j'ai juste listé en gros les vulnérabilités et ce qu'ils pouvaient faire avec les vulnérabilités de chaque objet connecté. Bon, techniquement, après, je ne sais pas pour chaque vulnérabilité vu ils ont réussi à rentrer avec le réseau et les objets connectés. A quoi exactement ils peuvent avoir accès ? Est-ce qu'on peut après aller voler des données sur un autre appareil du style un PC, ce genre de choses qui sont aussi connectées au Wi-Fi ? Ça, après, vu que je ne connais pas plus que ça, j'hésite un peu à rentrer trop là-dedans et plus dire que ça, c'est une vulnérabilité. Après, on peut accéder à nos données personnelles. Mais on peut quand même se protéger en mettant quelques petits trucs en place.

(03:20) Pentester : En fait, c'est accéder au Wi-Fi. Après, comme c'est un réseau à part entière, tout ce qui est dessus, tu peux y accéder. Je veux dire, par exemple, c'est comme si tu étais dans le réseau de l'entreprise. Tu peux pivoter. On appelle ça pivoter. Donc, tu passes d'une machine à une autre. En fait, tu vas trouver une vulnérabilité sur l'autre machine. Par exemple, un mot de passe qui transite en clair. A partir de ta machine, tu vas l'intercepter. Du coup, tu as un mot de passe. Tu vas essayer de te connecter à l'autre machine. Et comme ça, tu te déplaces sur le réseau comme ça. Donc, s'il n'y a pas justement des protections... En fait, tu peux accéder au réseau. Mais si, par exemple, l'objet est connecté... Moi, je prends le cas d'un PC. Si, par exemple, le PC a des vulnérabilités, tu pourras les exploiter pour y accéder. Mais si l'objet est connecté ou le PC, il est suffisamment protégé. Il est suffisamment protégé. Tu peux être sur le

réseau. Mais, par exemple, tu ne pourras pas intercepter le trafic entre les deux appareils. Ou tu ne pourras pas accéder à l'objet connecté en question.

(04:28) Nicolas : OK. Parce que c'était ça, justement. Parce que ce qui revenait le plus, c'était les communications non sécurisées du type man-in-the-middle. Les attaques des DOS qui sont assez fréquentes dans tous les appareils que j'ai retrouvés. Et les failles d'authentification qui permettent des accès non autorisés aux dispositifs et qui permettent ensuite de les contrôler à distance, ce genre de choses. En gros, ça, c'était les trois vulnérabilités qui revenaient dans tous mes objets connectés. Donc, je me suis dit que si j'arrivais à mettre une protection pour chacun des trois, juste pour le cas pratique. Et qu'après, plus en général, qu'est-ce qu'on peut faire ? Comme diviser le réseau, etc. J'avais discuté un peu avec Omar sur comment on pouvait faire ça. On pouvait mettre des pare-feux, se protéger un petit peu comme ça. Et juste dire, après, toujours le même truc. Si vous êtes un peu plus protégés, ce n'est pas sur vous que le pirate va se diriger.

(05:23) Pentester : Par exemple, le principe de segmentation, c'est un peu divisé, comme tu dis. Mais ça s'appelle segmenter. Et en fait, c'est comme si tu avais deux réseaux dans le même réseau. Donc, en fait, tu peux être... Je ne sais pas, le pirate, il est dans un sous-réseau. Il ne sait pas qu'il y a un autre réseau qui existe à côté. Et du coup, il ne peut pas forcément y accéder. Parce qu'on pourrait placer tes objets connectés dans des sous-réseaux à part entière. Et en fait, ils n'interagissent pas avec le reste. Je ne sais pas, par exemple, ton PC personnel.

(05:59) Nicolas : Parce que justement, chaque objet connecté peut avoir un sous-réseau. Il faut quand même qu'ils soient ensemble pour pouvoir communiquer entre eux, etc.

(06:06) Pentester : Théoriquement, ils pourraient tous avoir un sous-réseau. Mais après, dans la pratique, ce n'est pas optimal. Surtout dans un réseau domestique.

(06:20) Expert en objet connecté : En tout cas, par type.

(06:22) Pentester : Mais tu pourrais les dissocier et mettre des objets connectés par catégorie.

(06:26) Expert en objet connecté : Par exemple, le fait d'avoir des caméras de surveillance sur un réseau, même s'il y a un réseau isolé. Ta télé, ton système Wi-Fi, audio, etc. C'est mieux de les regrouper sur un réseau privé. Comme ça, tu sais que si tu te fais attaquer sur un des réseaux, tu limites quand même la propagation gauche-droite.

(06:53) Nicolas : Et ça, par exemple, un consommateur peut le faire seul ?

(06:59) Expert en objet connecté : Ça demande un minimum. Mais disons que l'utilisateur final, celui qui sort le router du carton et puis il a un port WAN et un port LAN, il ne va pas forcément se poser la question. Mais techniquement, la machine est capable de dire j'ai quatre ports en sortie, je peux les séparer avec quatre réseaux différents.

(07:21) Pentester : Déjà, de base, quand tu achètes ta box, normalement tu as une interface d'administration. Déjà, il n'y a pas beaucoup de monde qui vont... Quand tu achètes ta box, tu la branches, tu es à Internet, tu es content. Mais en fait, tu as toute une interface d'administration où tu peux gérer ton réseau. Mais déjà, un utilisateur lambda, pour moi, déjà, il ne va pas sur son interface d'administration, mais encore moins, il va diviser son réseau.

(07:46) Nicolas : Mais du coup, même quelqu'un qui n'a pas vraiment plus de connaissances que ça, il peut quand même aller regarder pour faire ça ou il faut demander à une entreprise. C'était aussi ça la question.

(07:58) Pentester : Non, pas une entreprise, mais... Demander à l'opérateur. Je ne sais pas si à partir juste de la box, tu peux la segmenter.

(08:02) Expert en objet connecté : Oui, après, tu peux demander typiquement. Certains opérateurs mettent en place ça. Tu payes un minimum de plus, et puis ils te donnent des outils supplémentaires ou ils te donnent des conseils supplémentaires.

(08:15) Nicolas : d'accord.

(08:17) Expert en objet connecté : Tout le monde ne le fait pas.

(08:19) Nicolas : Oui, parce que ça pourrait être une bonne recommandation justement parce que j'ai vu plusieurs informations sur l'OFCS suisse, qui nous disaient qu'on pouvait essayer d'avoir des sous-réseaux, utiliser des protocoles HTTPS, ne pas utiliser des ports standards, par exemple aussi.

(08:48) Pentester : c'est parce qu'en fait, les ports standards, la plupart des services utilisent des ports standards et quand tu es un pirate, tu ne vas pas t'embêter, tu vas scanner, tu sais que tel service tourne sous tel port. Par exemple, le port web, c'est 80.

Des fois, c'est soit 80, soit 80-80. Par exemple, tu pourrais le mettre, je ne sais pas, dans un autre port 80-80. Et en fait, quand il va scanner, le pirate, Il ne va pas s'embêter à énumérer tous les ports. En fait, c'est juste pour le ralentir.

(09:20) Nicolas : ok, oui, parce que le but, c'était de... Enfin, les recommandations que je veux faire, je ne veux pas aller trop loin, il faut aller chez une entreprise, etc. Ce serait plus, est-ce qu'on peut le demander à notre opérateur tout simplement, par exemple, éviter après de passer justement sur une solution d'entreprise, etc. Et de rester, du coup, toujours assez général. Ça ne va pas être le meilleur truc, parce que le meilleur truc, ça serait de passer par une entreprise qui est spécialisée à temps.

(09:44) Pentester : Je pense que changer le port, c'est faisable avec l'interface d'administration.

(09:50) Nicolas : Après, il parlait aussi d'une fonction UPnP, Universal Plug and Play, sur le routeur. C'était de la désactiver il fallait se renseigner auprès de vos routeurs pour les possibilités de configuration, ainsi que les restrictions. Parce qu'en gros, du coup, ça pourrait aussi permettre de plus protéger nos appareils. Aussi, quand on n'utilise pas un appareil, le déconnecter tout simplement du réseau pour éviter tout ce qui est, par exemple, des DOS pour qu'il essaie de se reconnecter tout seul quand il n'y a personne et qu'on essaie d'interférer les paquets.

(10:30) Expert en objet connecté : Ça passe aussi du fait de dire typiquement, quand tu te connectes sur un réseau domestique, souvent tu reçois une adresse qui est donnée par défaut. Une adresse d'un pool automatique. C'est quelque chose que, si tu sais que tu n'as pas forcément beaucoup d'autres appareils qui vont se connecter, c'est de réserver des adresses spécifiques pour tel et tel devices. Donc, ton routeur, il va reconnaître ton iPhone, il va lui connaître toujours la même adresse Ip. Et puis, tu sais que quand il se connecte, ton téléphone est reconnu, il reçoit cette adresse IP. S'il y a quelqu'un d'autre qui vient avec un autre téléphone, le téléphone ne va pas être reconnu. Donc, potentiellement, il n'y a pas de réservation. Donc, il n'y aura pas d'adresse IP. Donc, il ne pourra pas se connecter. C'est vrai que, comme toute la sécurité, ça peut être contraignant si tu reçois du monde à la maison et que du coup, tu veux les connecter au Wi-Fi, ce n'est pas pratique. Tu as des systèmes où t'appuies sur un bouton et tu peux enregistrer comme ça. Cette partie-là peut être intéressante pour essayer de limiter justement les appareils qui se connectent tout seul.

(11:42) Pentester : Sur le PNP tu dis ?

(11:44) Expert en objet connecté : oui sur le PNP, oui.

(11:47) Pentester : Et puis, le PNP, en plus, ça t'attribue les ports. En fait, ça te fait tout pour toi. C'est justement là où t'as l'attribution des ports automatiques.

(11:54) Expert en objet connecté : Ça te fait le NAT, le PNP. Ça te permet d'être visible depuis l'extérieur. On sait que si tu viens avec un NAS, par exemple, et que tu le connectes, le téléphone va te voir en tant que tel. Ils vont communiquer sur des ports qui sont spécifiques. Et puis, automatiquement, le NAS est publié à l'extérieur pour faire en sorte que toi, quand t'es à l'extérieur, tu vas pouvoir te connecter sur ton adresse de la maison ou sur un port spécifique. Et ce port est redirigé ensuite et mappé avec ton NAS. C'est comme si tu faisais une communication directe. Il faut une sorte de mapping et de connexion.

(12:32) Pentester : C'est pour faciliter, pour que ce soit accessible à tous les utilisateurs. T'as pas besoin de recevoir ton routeur et tu le configures toi-même.

(12:40) Expert en objet connecté : Quand on parle de ports, comment ça se passe ? La communication entre deux devices qui sont sur du IP. Tu as deux adresses IP. Ça, c'est la couche basse. Après, tu montes dans les couches qui me viennent plus applicatives. Par exemple, si tu dis que je veux parler avec toi, ça c'est ton adresse. Mais je veux te parler web. Si je veux t'interroger et avoir une page web, je vais te poser une question sur le port 80 ou le 443 si c'est du HTTP.

(13:09) Pentester : C'est comme si c'était des portes.

(13:12) Expert en objet connecté : C'est ce port-là qui fait partie de l'adresse. T'as l'adresse IP plus le port. Et le port est spécifique au service que tu vas aller. T'as le fansharing, tu peux avoir des protocoles de transfert de fichiers, tu peux avoir des protocoles web, tu peux avoir des protocoles voice, tu peux avoir... Chaque protocole correspond à un port particulier. Le langage que tu veux parler avec une interface IP, quelqu'un qui prend l'IP, est déterminé par le port.

(13:41) Pentester : Et justement, les firewalls ou les pare-feux, par exemple, des fois, ils viennent bloquer certains ports pour pas que quelqu'un y accède ou il y a un filtrage qu'autorise que certains... Que certaines informations à passer.

(13:54) Nicolas : Ok. Parce que du coup, on pourrait combiner l'histoire de séparer le Wi-Fi en deux et qu'il y en ait un qui... Du coup, on désactive tout ce qui est plug and play et du coup, c'est nous qui mettons à chaque fois les objets connectés dans ce devices-là mais garder l'autre partie pour, du coup, notre...

(14:10) Expert en objet connecté : C'est typiquement ce qui se passe même à la maison, même les opérateurs font ça. Quand t'as un réseau guest, le réseau guest, c'est un réseau qui est ouvert à tout. Tout le monde peut se connecter mais la seule chose qu'il va pouvoir faire, c'est de surfer sur Internet. Tandis que le réseau privé, c'est là que tu peux mettre en place toutes ces limitations et dire, ben voilà, il y a que moi sur mon réseau privé, donc je mets en dur mon adresse IP ou ma sécurité ou je fais une règle qui dit que moi, je vais pouvoir discuter avec mon SAN ou avec mon multimédia que en utilisant le protocole de streaming. Si j'essaie de lui parler autre chose que du streaming, il sait que c'est pas normal, donc il rejette, on rejette.

(14:56) Nicolas : Ok. C'est comme ici, vous avez un réseau guest et un réseau privé, etc.

(15:00) Pentester : Du coup ça c'est une sorte de segmentation comme ça tout le monde est sur le même réseau mais tu ne peux pas parler aux autres.

(15:08) Expert en objet connecté : On a en plus le fait de... dans le réseau guest, une fois que t'es sur le réseau guest tu peux pas tellement tout faire mais pour aller sur le réseau guest, il faut une autorisation de quelqu'un qui est dans l'entreprise. Tu fais une demande, tu as sur le guest, tu rentres à l'adresse e-mail de la personne qui t'a invitée, la personne qui t'a invitée reçoit un e-mail ou un SMS en disant il y a un monsieur qui veut se connecter, est-ce que tu l'autorises ? S'il me fait oui, toi tu vas recevoir un e-mail ou un SMS avec un mot de passe que tu vas pouvoir entrer et t'y autoriser à rentrer. Donc une fois que t'es dedans, tu fais ce que tu veux.

(15:45) Nicolas : Ok, c'est pas mal.

(15:47) Expert en objet connecté : C'est toutes des couches supplémentaires que tu peux rajouter pour sécuriser ta chose. Et à l'occurrence, nous on ne le fait pas pour sécuriser en termes de menaces, mais pour être sûr qu'on log qui fait quoi. Parce que nous on est responsable de, comme x est responsable de sa ligne internet, s'il y a quelqu'un qui fait des trucs malveillants sur notre ligne, on va pouvoir dire, cette communication, c'était, quel était tel monsieur qui l'a faite.

(16:21) Nicolas : Ok. Intéressant ça. Parce que du coup, si je reviens à ce qui retournerait le plus souvent dans mon cas pratique, j'avais mis qu'on y retrouve les communications non sécurisées, vulnérables aux interceptions, manipulations par des attaquants, notamment lorsqu'elles transitent via des protocoles non chiffrés, ce qui facilite les attaques man-in-the-middle. Ça, par exemple, est-ce qu'il y a une protection concrète que je pourrais dire qu'on peut mettre en place, etc.

(16:53) Expert en objet connecté : Man-in-the-middle, c'est surtout une question d'authentification. Différents mécanismes pour t'authentifier. Le mieux, c'est de... Mais ça c'est général, ce n'est pas que pour le man-in-the-middle, c'est vraiment... Ça doit être culturel, c'est d'utiliser l'authentification à deux facteurs.

(17:16) Nicolas : OK. Parce que là, du coup, c'était l'application d'un aspirateur robot, où la modification de mot de passe et les transmissions d'appareils personnels, etc., ils utilisent le protocole HTTP, mais non chiffré.

(17:27) Pentester : Du coup, tu peux intercepter les communications et les voir en clair comme si c'est toi qui l'as envoyé.

(17:32) Nicolas : OK.

(17:33) Pentester : C'est-à-dire que si tu modifies ton mot de passe ou si, par exemple, tu fais un achat sur Internet, en fait, c'est un peu comme quand t'as le petit chiffrement

sécurisé quand t'es sur Internet, par exemple. Mais en fait, c'est que tes communications, elles sont chiffrées. Donc, en fait, personne peut les comprendre. Alors que si t'es, par exemple, HTTP, t'as pas le chiffrement dessus et tout le monde peut lire en clair. Donc, il suffit juste d'être dans le réseau. En gros, il y a des outils qui intercepte les communications et du coup, tu peux lire totalement tout ce qui passe. C'est un peu ce qui... C'est pour ça que sur les réseaux, par exemple, publics, je sais pas, au McDo ou quoi, en fait, il suffit que... Enfin, il suffit que quelqu'un qui soit dans le McDo connecté, il peut voir complètement tout ce que tu fais, quoi. Parce que c'est un Wi-Fi public.

(18:37) Nicolas : OK. Et, par exemple, pour protéger des appareils de DDoS, il y a des protections qu'on peut mettre en place ?

(18:51) Pentester : Après, le problème du DDoS, c'est que... Enfin, c'est vraiment... C'est vraiment juste pour détruire, quoi.

(18:57) Expert en objet connecté : DDoS, dans le cadre d'un privé, je vois pas forcément beaucoup d'intérêt parce que ça va sauter la connexion. Tu lui coupes sa télé, ça va pas aller beaucoup plus loin.

(19:10) Nicolas : Après, c'était comme on avait vu, je crois, dans la vidéo avec toi qu'on avait regardé. C'est qu'il coupe la... Enfin, il envoie... Enfin, il fait faire un DDoS pour après connecter la télé à son réseau.

(19:20) Pentester : Par exemple, t'as une technique comme ça pour le Wi-Fi, justement, en fait, tu vas créer un faux point d'accès et en fait, le mec qui est sur son Wi-Fi, tu vas le bombarder, du coup, tu vas le DoS et ça va le déconnecter une milliseconde et quand il va le voir se reconnecter, il va essayer comme ton point d'accès, ton faux point d'accès, tu l'auras appelé comme son Wi-Fi à lui, il va vouloir tenter de se connecter, il va envoyer les... Il va envoyer son mot de passe pour se connecter au Wi-Fi et là, tu vas l'intercepter, tu vas pouvoir du coup capturer son mot de passe, le déchiffrer et après, tu pourras se connecter à son Wi-Fi. En fait, le fait de le DoS, l'appareil va surcharger et du coup, il va faire une tentative de reconnexion mais après, en soi, au niveau de, comme il disait

Omar, au niveau d'un particulier, ce n'est pas très utile. Mais non, en vrai, il n'y a pas de... Je ne vois pas de protection particulière à part... Non, même au pire, l'appareil va sauter, il va se déconnecter, le temps que ça va arrêter, il va se reconnecter, quoi. Parce qu'en soi, si tu n'as plus accès à ta télé, c'est juste embêtant, c'est tout.

(20:39) Nicolas : Ouais c'est vrai. Est-ce que c'est possible de mettre mon PC sur l'écran ? C'est comme ça, peut-être que je peux vous montrer chaque objet connecté. Du coup, après, on a des vulnérabilités encore de déni de service, l'envoi de messages malveillant... Donc du coup, techniquement, déni de service, de toute façon, on ne peut pas trop...

(21:44) Pentester : Non, tu ne peux pas faire grand-chose.

(21:48) Nicolas : C'est vrai sinon même les entreprises se protégeraient contre.

(21:51) Pentester : Oui, après, c'est complètement différent dans un réseau entreprise qu'un réseau... dans un réseau privé. Après, on est d'accord, toi, tu fais sur le réseau privé, on voit une maison en général, pas uniquement une maison.

(22:11) Nicolas : Oui, Du coup, ça, c'était pour un déni de service. Ça, c'était un contournement de notification par code PIN. C'était à cause d'un code PIN codé en dur dans une API. Après, ils ont...

(22:27) Pentester : Codé en dur, tu comprends.

(22:28) Nicolas : Oui, c'est qu'il est dans l'objets.

(22:30) Pentester : Oui, il est inscrit dans le code directement.

(22:37) Nicolas : Oui, ça, par exemple, à part, du coup, bien se renseigner et mettre à jour ses dispositifs...

(22:43) Pentester : Oui, là, tu ne peux rien, c'est le fabricant. C'est le fabricant qui fait une erreur, c'est son code qui est mauvais.

(22:50) Nicolas : Le cinquième objet, c'était une vérification incorrecte de la signature d'un micro-logiciel permettant... Oui, encore un déni de service. Du coup... Parce que peu importe la manière dont on fait un déni de service, de toute façon, un déni de service, c'est un déni de service. Le but, c'est de surcharger. On ne peut pas empêcher quelqu'un de... Surcharger.

(23:09) Pentester : Oui, ça arrive. Perso, ça sert à rien de mettre les moyens juste pour DOS quelqu'un, quoi. C'est vraiment il t'a tué sur un jeu et... Voilà.

(23:23) Nicolas : les DOS sur Minecraft, quoi.

(23:27) Pentester : oui quand il y avait l'API sur Discord avant.

(23:29) Nicolas : Voilà, après, du coup, il y avait la vulnérabilité de communication avec MQTT.

(23:44) Pentester : C'est quoi ça, c'est une application. Ah, OK. En gros, c'est que tu modifies les informations et après, du coup, le thermostat, il prend en compte ces informations. En gros, c'est qu'il va chercher ces informations dans... C'est quoi c'est au niveau d'une API ? Le thermostat, il va chercher les informations au niveau du broker et en fait, tu peux modifier les informations du broker sans être connecté. Et du coup, par exemple, si tu mets, je ne sais pas, 50° dans le broker et que le thermostat vient de les rechercher, du coup, il va se mettre à 50°.

(24:35) Nicolas : Ça, on peut le faire à distance, du coup ?

(24:38) Pentester : Un attaquant pourra jouer des commandes et contrôler sans authentification par l'application mobile. En gros, ça te permet juste de... Tu vas pouvoir modifier la température.

(24:48) Nicolas : C'est pour embêter toujours.

(24:52) Pentester : Après, ouais, ça dépend de tous les... Là, c'est un thermostat, tu ne peux pas faire grand-chose à part monter la température. Ouais. Ça peut être problématique. Et ça, par exemple, c'est au niveau toujours du fabricant.

(25:12) Nicolas : OK.

(25:15) Pentester : C'est vraiment toujours de tenir à jour les objets et... Tu ne peux pas grand-chose.

(25:23) Nicolas : OK. Après ça, du coup, c'était les attaques man in the middle.

(25:27) Pentester : Bon, là, du coup, pas de validation des certificats, c'est-à-dire que le trafic, il n'est pas chiffré. Il n'est pas chiffré, donc tu peux faire le man in the middle et écouter les communications en clair.

(25:55) Nicolas : Après, celui-là, après, il y avait... 11 failles différentes, ça partait loin mais c'était juste pour montrer que, bah, la serrure, elle avait un problème. Bah, du coup, on peut... On peut tout intercepter, etc., mais après, elle en avait encore plein d'autres. Mais du coup, avec... Avec, du coup, cette attaque man in the middle, on peut tout écouter, mais on peut, du coup, récupérer des mots de passe et ce genre de choses.

(26:19) Pentester : C'est ça oui

(26:22) Nicolas : Donc, imaginons qu'on ait mis le même mot de passe pour cet objets que pour d'autres c'est un problème

(26:26) Pentester : Et après, quand t'as des attaques man in the middle, le problème, c'est que... Par exemple, si tu te mets entre les deux... Enfin, de base, t'es entre les deux, t'écoutes leur trafic, mais par exemple, tu pourrais... Je sais pas, Omar, il m'envoie un truc, toi, t'es au milieu, et en fait, il va t'envoyer à toi, toi, tu pourras modifier ce qu'il m'envoie et me l'envoyer, et du coup, moi, je penserais que c'est Omar qui me l'a envoyé et je prendrais cette réponse comme la sienne.

(26:48) Expert en objet connecté : Tu vois comment ça marche ? T'es à la maison, tu vas aller sur ton site de e-banking. Moi, je fais man in the middle. Toi, tu vas rentrer l'adresse de ton e-banking. UBS.com. Sauf que à la place d'aller chez l'UBS, tu viens chez moi. Moi, je te dis, je suis l'UBS, donc je reçois ta demande, moi, en parallèle, j'ouvre une requête à l'UBS. L'UBS, il m'envoie le numéro de contrat que je te présente, toi, tu m'envoies ton mot de passe, je reçois ton mot de passe, je rentre le mot de passe, et à ce moment-là, je suis connecté. Toi, tu m'as donné les infos, moi, je suis connecté, toi, tu penses être sur ton site de l'UBS, moi, j'y suis. Pendant que toi, t'essaies de faire des opérations sur mon site Web à moi, moi, j'ai vraiment en train faire des opérations sur ton site Web... sur le site Web sur ton compte. Donc, je fais le man in the middle, donc je... Je me fais passer comme ça. Je siphonne ton compte, je ferme ton compte, et en attendant, tu me poses des questions, mon site Web te répond avec des pages qui ne vont rien dire, tu ne comprends rien, qu'est-ce qui se passe ? 3 ou 4 fois, quand moi j'ai fini de faire mes opérations, je ferme ma connexion, toi, tu te reconnectes, vas-y, la connexion est arrêtée, tu es directement sur ton site d'UBS, et là, t'arrives, il n'y a plus rien. Ça, c'est l'attaque man in the middle classique. Et ça peut être utilisé pour ça, le vol d'argent, et ça peut être utilisé aussi pour voler des informations. Je me mets juste au milieu pour écouter ce que toi tu dis avec d'autres personnes. Whatsapp est crypté de point en point, et ça dépend combien de points il y a. Donc si t'en as un au milieu, toi, t'es crypté chez moi, moi je suis crypté là-bas, et puis potentiellement, je vais repasser tous les messages, je les vois en clair, je peux faire tout ce que je veux, je peux même écrire des trucs à la place, et ainsi de suite. D'où le fait de dire, si tu mets

d'authentification forte, un double facteur ou peu importe, un multifacteur, quand l'UBS demande une authentification par SMS par exemple, c'est toi qui reçois les SMS. Mais le gars ici ne va pas pouvoir y accéder. Si tu as ton application d'UBS, donc tu sais que tu as l'application de login, elle ne passe pas par le site web. Le login se passe, l'authentification se passe entre ton téléphone et l'UBS directement. Pas entre ton ordinateur et le serveur de l'UBS. Je ne sais pas si tu es chez l'UBS ou pas, ils sont tous pareils. Quand tu as ton application qui te permet de t'authentifier sur ton téléphone, en plus ton téléphone, tu as du biométrique, donc ton téléphone sait que c'est toi. Ce n'est pas quelqu'un qui t'a piqué le téléphone. Donc tu te fais une première authentification biométrique sur le téléphone. Le téléphone passe par un service direct par la 4G directement au site de la banque. Et puis là, quand tu es sur ton site web, tu as utilisé un autre moyen pour t'authentifier, donc je te donne accès à ta chose à toi. Et là ça te permet de... Qui n'empêche que tu peux quand même avoir un man in the middle. À un moment il fait un hijack de ta connexion, mais ça devient un peu plus compliqué. Bref, le but c'est de le rendre le plus compliqué possible. Et que le hacker se dise, c'est trop compliquer, je vais aller chercher quelqu'un qui est plus facile à hacker.

(30:32) Nicolas : Parce que là du coup il pourrait récupérer le mot de passe, mais si le mot de passe c'est le même que pour d'UBS ou je ne sais quoi, de toute façon il n'a pas la 2e authentification nécessaire.

(30:40) Pentester : exactement, Là justement on imagine par exemple, ce serait la communication entre la serrure et ta box par exemple. Et par exemple si tu as une serrure externe, par exemple avec celle à ta maison, il pourrait voir ton code de PIN qui transite parce qu'il ne serait pas chiffré. Du coup il aura accès à ta maison.

(30:56) Nicolas : Et là par exemple si on a une double authentification, ça veut dire qu'il faudrait avoir un deuxième code sur son téléphone, qui ferait que si on n'a pas la double authentification, on ne peut pas rentrer quand même.

(31:09) Pentester : Oui voilà, le but c'est de se protéger au maximum, et d'éviter justement le principe de la double authentification, c'est pas d'avoir les mêmes dispositifs. Par exemple t'as ta tête, une empreinte digitale. Par exemple tu vois dans

ces serrures des fois, tu mets ton code et après tu mets ton empreinte digitale. Donc quand t'as une double authentification, le pirate il peut avoir ton code mais il ne pourra pas valider ton empreinte digitale.

(31:34) Nicolas : ok, ça c'est bien.

(31:37) Pentester : Après ça reste une faille au niveau fabricant.

(31:44) Nicolas : Ok, après... Encore un déni de services. En gros ça c'est juste pour embêter si j'ai bien compris. L'autre après...

(32:14) Pentester : Voilà c'est du flux vidéo sur la sonnette, donc il pourra voir...

(32:20) Nicolas : Ce qu'il se passe à partir du port 80 comme tu disais.

(32:23) Pentester : Ouais, port 80... En gros là il va accéder au flux caméra de ta sonnette extérieure.

(32:35) Nicolas : En gros dès qu'on a accès au wifi, on peut avoir accès à la caméra qui est sur la sonnette. Ça ensuite c'était l'application qui n'était pas chiffrée avec HTTP. Du coup ça double l'authentification aussi pour la protéger. Et ensuite du coup ça c'est le même cas que pour la sonnette, non pas la sonnette, la serrure. Du coup c'est toujours ça. Après il y avait aussi un problème, c'était une faiblesse qui porte sur un QR code qu'on peut utiliser pour lier l'aspirateur.

(33:28) Pentester : En gros c'est que le QR code, son modèle il est prédictible. Ça veut dire qu'en gros c'est possible de deviner... Attends je vais regarder...

(33:42) Nicolas : Les tests ont démontré l'absence de chiffrement de communication du modèle prédictible.

(33:44) Pentester : En gros c'est que tu peux deviner comment il agit le QR code et ainsi tu peux le déchiffrer. C'est le QR code de l'aspirateur robot ?

(33:57) Nicolas : Ouais.

(34:00) Pentester : C'est quoi l'authentification ? Attends, t'as qu'à deviner l'ID de l'appareil et d'en prendre le contrôle. Ah c'est qu'il doit pouvoir se connecter au robot à partir d'un QR code. Et en fait le QR code est mal codé.

(34:22) Nicolas : Et du coup même pour le QR code c'est le fabricant aussi qui fait des erreurs. Ok. Parce que du coup je pense que là je vais faire... Après ça je vais regarder pour faire une petite partie de comment protéger entre guillemets les 10 objets connectés de la meilleure des façons. Parce que du coup je vais expliquer qu'un déni de services, malgré que ce soit une vulnérabilité, pour que les gens le fassent il faut vraiment qu'ils aient un besoin de nuire. Et par contre aussi il y avait...

(34:55) Pentester : Ce qui peut être intéressant c'est le manuel de middle comme il a expliqué au début. Ça les gens ils se rendent un peu compte de...

(35:03) Nicolas : Je pense que je vais essayer d'un peu plus se développer avec ça. Je ne pensais pas que c'était aussi... Enfin je sais qu'on peut arriver sur des pages web qui sont fausses ou on tape nos codes, id et après les gens peuvent se connecter.

(35:17) Pentester : Après tu combines plusieurs techniques et ça donne une technique évoluée mais après de base c'est... Le truc de base c'est vraiment juste t'écoutes et tu regardes quoi. Mais après tu peux vraiment... En fait ça dépend où t'es au niveau de l'écoute quoi. Parce que là si c'est juste une serrure ok t'as le code PIN mais il n'y aura

rien d'autre qui va transiter. Par exemple si c'est le code PIN de ta maison c'est un peu problématique.

(35:40) Nicolas : S'il n'y a pas la double vérification on peut rentrer juste chez la personne.

(35:44) Pentester : C'est ça.

(35:46) Nicolas : Et aussi du coup tous les numéros de CVE. J'avais parlé avec Omar où il m'avait dit qu'en gros du coup il y avait des... Il y a des risques. Enfin des... Comment est-ce qu'on appelle ça déjà ? Ouais c'est les... CVSS...

(36:15) Pentester : Ça c'est une méthodologie pour calculer le score. En fait c'est l'impact. L'impact, la probabilité que ça se passe et le moyen pour l'être en place par exemple. Si t'as pas besoin de t'authentifier ça augmente considérablement le score. Si tu peux accéder à des données confidentielles ça augmente le score. Plus elle est proche de 10 plus son impact est fort. En fait c'est une base métrique.

(36:44) Nicolas : Parce que ça peut-être que ça serait intéressant pour chaque objet connecté que je parle quand même peut-être du risque.

(36:46) Pentester : Je pense que si tu leur... Ouais tu peux te présenter... Je sais pas si t'as des gros... Des gros risques sur les CVE, je me rappelle plus.

(36:56) Nicolas : Je crois qu'il y en a quand même certains qui sont élevé.

(36:58) Pentester : Mais ouais tu peux te présenter un peu le... Enfin une petite brève introduction sur le système métrique et tu dis que 10 est le plus élevé etc. Comme ça ils peuvent comprendre un peu.

(37:14) Nicolas : Ça c'est le CVSS.

(37:16) Pentester : oui tu mets le CVSS et ça t'expliquera...

(37:19) Nicolas : Ouais parce que justement j'avais discuté de ça avec Omar. Je crois que c'était la toute première fois où je l'avais vu et puis j'avais noté. Mais je n'étais pas sûr si...

(37:27) Pentester : Ouais tu fais juste une petite explication. Un petit paragraphe juste pour...

(37:32) Nicolas : oui parce que de toute façon après je me suis dit c'est comme pour chaque objet connecté. De toute façon je reprends à chaque fois les mêmes mots. Le deuxième objet connecté c'est ça et après il y a le CVE. Et du coup je pourrais mettre avec un risque de...

(37:41) Pentester : Comme ça ils comprennent bien le risque. Ils ne se disent pas c'est un truc lambda.

(37:47) Nicolas : Et du coup... Or du coup le cas pratique etc. Mais pour des... Pour un foyer. La double authentification c'est ce qu'il peut... C'est une des protections les plus importante. Mettre à jour. Les dispositifs. Avoir des mots de passe robustes. Après je sais plus s'il y a d'autres trucs qui font que j'y pense. Ouais le fait de pouvoir couper le réseau.

(38:18) Pentester : Segmenter oui, comme il disait Omar. Maintenant sur les box t'as de plus en plus de... Tu peux proposer un wifi invité. Du coup après ça faut aller dans les paramètres d'administration. Mais comme tu proposes un wifi invité. Comme ça si

quelqu'un vient chez toi. Juste une fois il a besoin du wifi. Tu le mets sur le wifi invité. Et il ne va pas pouvoir rentrer sur le principal quoi.

(38:47) Nicolas : Bon il y a le plug and play. Est-ce qu'il y a d'autres choses auxquelles il faudrait que je pense. Et qui ne sont pas trop compliquées à mettre en place. Pour protéger des objets connectés. Les déconnectés quand on ne les utilise pas aussi.

(39:05) Expert en objet connecté : oui typiquement ouais.

(39:07) Nicolas : Après j'avais vu aussi. Si jamais on se fait....

(39:12) Expert en objet connecté : Ah accessoirement. L'histoire du DDoS. Le DDoS ce n'est pas tant qu'on est en tant que personne à la maison. Je me fais DDoSer. Mais qu'on va utiliser mon matériel pour DDoSer les autres.

(39:25) Pentester : Ah oui l'histoire des brosses à dents zombie dont tu m'avais parler.

(39:31) Nicolas : Mais à chaque fois qu'on peut DDoS un appareil on peut l'utiliser après pour DDoS ?

(39:35) Expert en objet connecté : Alors si on arrive à prendre la main sur l'appareil potentiellement il peut devenir un zombie. Ça peut être quelqu'un qui tout à coup on lui donne l'ordre d'envoyer des requêtes sur une cible particulière. Si toutes les caméras vidéo du monde vont envoyer des requêtes sur un serveur web celui-là il va tomber.

(39:53) Pentester : Mais théoriquement s'il y a une vulnérabilité de DoS tu peux pas l'utiliser pour DoS quelqu'un. C'est juste qu'il y a une fonctionnalité qui est vulnérable et que tu vas pouvoir... Mais par exemple je sais pas si il y a un mec qui a 50 zombies pour DDoS et que ton appareil a une vulnérabilité de DDoS, bah il pourra le DDoS avec ces

zombie. Le fait que tes objets soient vulnérables ça peut avoir des conséquences si ton objet attaque quelqu'un d'autre.

(40:30) Nicolas : Parce que là du coup pour toujours l'aspirateur avec le QR code du coup on pouvait deviner l'ID et en prendre le contrôle. Si on en prend le contrôle on peut faire... Si on arrive à prendre le contrôle de l'objet je peux dire qu'il peut être utilisé pour... Parce qu'après du coup je vais remonter aussi à ce que j'avais dit plus tôt où je vous avais demandé si du coup on était coupable.

(40:53) Pentester : Après tu peux avoir des conséquences juridiquement après je ne connais pas trop les textes mais...

(40:58) Encore une fois c'est de définir, de segmenter soit physiquement soit logiquement c'est de dire... Bon l'aspirateur il a un rôle d'aspirateur et il va devoir communiquer avec le site web du fabricant pour faire sa mise à jour. Et là à la place de rien faire et laisser comme ça par défaut tu peux mettre une règle dans ton pare-feu qui dit... Ben lui je l'autorise à faire de l'HTTP, HTTPS tant que j'ai le site web à destination de son fabricant à lui. Comme ça si quelqu'un prend la main et qui essaie de balancer des requêtes ailleurs que là où il est censé aller, ça passe pas. Et là tu te protèges contre toi qui fait des ddos aux autres.

(41:46) Nicolas : Ok et ça c'est avec le pare-feu ?

(41:49) Expert en objet connecté : C'est avec le pare-feu oui.

(41:51) Nicolas : Et le pare-feu on peut le mettre pour chaque objet ?

(41:53) Expert en objet connecté : Le pare-feu c'est à l'entrée de ton internet, tu peux définir plein de règles d'accès, ça j'autorise, ça je n'autorise pas.

(41:59) Nicolas : Et ça c'est toujours du coup sur notre Wi-Fi ?

(42:02) Expert en objet connecté : Il va être applicable pour tous tes réseaux à toi.

(42:06) Nicolas : Ok. Et du coup si on fait un segment pour les objets connectés on peut dire que chaque objet connecté va faire seulement ça, ça et ça. Et comme ça on peut éviter justement l'utilisation pour...

(42:15) Expert en objet connecté : C'est pour ça que tu dis, par exemple tu fais un segment que pour les caméras vidéo et puis comme tu sais que tous ces caméras vidéo là c'est la même fabrique qui les fait, tu peux faire une règle générale pour ce segment là en disant mais lui il peut sortir mais que pour aller ici. Tu fais pas une règle pour chaque appareil. Tandis que ton... Ta domotique à la maison où tu vas avoir ton frigo, tes laves vaisselle ou tes laves linge comme ça. Donc ils sont tous chez toi parce que toi tu veux les commander avec la même application. Et potentiellement ils sont des marques différentes. Là tu vas faire une règle par fabricant. Donc mon frigo, mon lave-linge c'est du Samsung. Je l'autorise à aller chez Samsung. Ou Philips pour les lampes je les autorise à faire ci, à faire ça. Tu vas un peu plus granulaire. Tu fais vraiment des règles qui sont les plus précises possibles. Puis là tu blindes en même temps parce que tu empêches de faire autre chose. Le mot hacking signifie justement faire faire autre chose que ce pour quoi tu es prévu. Là tu évites que ton service, ton objet, ta solution soit détourné par autre chose.

(43:31) Nicolas : Ok, ça je peux moi le faire tout seul ou c'est...

(43:34) Expert en objet connecté : Oui mais c'est pas super compliqué.

(43:37) Nicolas : Donc un petit peu de renseignements externes on peut réussir à... Ok. Ça c'est bien. Ouais et ça c'était plus pour toi. Du coup regarder pour... Voilà. Parce qu'après ici je parlais d'avoir accès au Wifi domestique. C'est par là que j'ai commencé mon cas pratique. Avec du coup... Moi je me suis basé sur le fait qu'il était en protocole

de sécurité WPA2. Après il faut que... j'ai un contact chez Swisscom. Il faut que je lui demande ce qui est le plus présent en suisse mais j'imagine que ça va être peut-être le 3 vu que le 3 ça fait quand même pas mal de temps qu'il est là. Je crois que c'est 2018. Le 3 c'est le meilleur et le 2 c'est celui avant. Et WPA c'est mauvais.

(44:43) Pentester : En fait c'est différents protocoles de chiffrement. Et justement... Justement tu as des protocoles plus ou moins vulnérables. Les anciens protocoles maintenant ils se cassent d'un rien. Mais en fait c'est que tu vas pouvoir capturer... Tu vas pouvoir capturer la clé de chiffrement. Et comme c'est un modèle prédictible un peu comme le QR code. Tu vas pouvoir deviner et retrouver la clé. Tu vas pouvoir te connecter facilement. En fait maintenant tu as des protocoles plus ou moins... Faciles à casser. Le WPA3 normalement c'est le dernier.

(45:21) Nicolas : Ouais le dernier du coup c'était WPA3. Et le seul truc que j'avais trouvé... Du coup c'était ça. C'était une attaque de confusion SSID. Ça venait de sortir... Je crois que c'était en juin 2023 ou 2024. J'ai trouvé ça tout récemment. Il y avait même un numéro de CVE. Du coup vu que je suppose que je rentrez dans wifi, je peux pas juste que je rentre dedans par magie. Parce qu'après ça parlait du standard 802.11. Qui n'exige pas d'authentification au nom de réseau. Et du coup faire croire qu'il se connecte au bon wifi.

(46:35) Pentester : Ouais c'est le Wi-Fi le 802.11. Il n'exige pas d'authentification au nom de réseau. C'est justement ce que je disais. chaque réseau Wi-Fi possède son identifiant unique qui est le SSID. Et c'est qu'en fait tu vas pouvoir faire un faux point d'accès Wi-Fi. Justement en mettant à ce faux point d'accès le SSID du réseau ici. Donc quelqu'un quand il va vouloir se connecter il va croire que c'est son réseau à lui. Et du coup il va t'envoyer une demande d'authentification. Avec justement ces informations de connexion au réseau Wi-Fi. Et c'est à ce moment là que tu vas pouvoir le capturer. Et du coup en fait là tu vas venir faire une... Pour contrer ça tu vas venir d'abord authentifier le SSID. Et après le client va envoyer ses informations d'authentification au Wi-Fi. C'est que ça va passer en... Ça va faire deux systèmes d'authentification. Ça va pas envoyer tout d'un coup. Ça va pas juste se fier au SSID. Ça va d'abord le vérifier. Et après ça va envoyer les informations de connexion. Et justement du coup quand ils vont se connecter

à ce réseau ils vont envoyer les informations en clair. Et tu auras les informations pour te connecter.

(48:09) Nicolas : Parce qu'en fait c'est un peu la même chose que... que quand on parle du... Quand il expliquait du coup le man in the middle où on essaye de mettre les informations dans un site qui est un fake site et qu'après on a le vrai site. Là c'est un peu la même chose mais avec un Wi-Fi. C'est on fait un fake Wi-Fi un peu.

(48:25) Pentester : Ouais c'est un peu pareil. Tu fais un fake Wi-Fi comme ça il te donne ses informations d'authentification. Bon lui il croit que ça n'a pas marché, le Wi-Fi déconne. Toi t'as tout capturé. Lui après tu enlèves ton faux point. Lui il se connecte à son Wi-Fi normal. Mais toi t'as ses informations d'accès quoi. Et après tu vas dans le Wi-Fi et tu es dans le réseau.

(48:44) Nicolas : Et parce que là par exemple si je clique dans mes Wi-Fi etc. Je ne vais pas du coup avoir deux fois par exemple mon Eyra Guest ou quelque chose comme ça ?

(48:57) Pentester : Bah tu peux... Enfin le nom du point d'accès tu peux le... Tu peux mettre le même nom x100. Ça change rien. C'est justement le SSID qui est un identifiant unique au point Wi-Fi qui compte. Donc tu peux l'appeler Eyra Guest ou ils peuvent tous s'appeler Eyra Guest. Ça change rien. Pour toi tu te connecteras sur Eyra Guest et...

(49:18) Nicolas : Donc normalement si le pirate il est pas bête il va mettre le même nom que celui que l'on a. Et comme ça nous on va essayer de se connecter à celui-là.

(49:27) Pentester : C'est ça. Justement il n'est même pas... Par exemple si t'as la fonction connexion automatique. Tu arrives chez toi, t'as ton Wi-Fi, t'as pas besoin de cliquer à chaque fois. En fait justement le fait d'avoir le SSID pareil. Bah lui il va croire que c'est le vrai Wi-Fi d'origine et il va tenter une connexion par lui-même. T'as pas

forcément besoin de cliquer dessus. C'est qu'il ne va pas comprendre en fait. Il va se dire bon je vais me connecter à celui-là et...

(49:56) Nicolas : En fait il a deux choix de SSID qui sont les mêmes et il va...

(49:59) Pentester : Il va envoyer les deux.

(50:01) Nicolas : Ok, ah ok. Non parce que ça il fallait quand même que je sache un peu l'expliquer vu que j'étais complètement perdu. Bon bah ouais mais du coup ça va. Ok. Puis ouais du coup de toute façon tout reste j'avais l'impression que ça allait. Là j'avais trouvé une faille pour WPA2 mais... Faut que je regarde en gros lequel des deux entre WPA3 et 2 est le plus présent en suisse pour mon travail. Et... Ouais là j'avais fait du coup comme t'avais fait un peu la dernière fois. C'est à dire que j'ai essayé de trouver une caméra D-Link sur Shodan en Suisse. Je l'ai trouvée à Bernex où j'avais un peu toutes les informations. Donc de réseau, de détails de serveur web etc. Ouais. Et en gros c'est juste pour expliquer les informations qu'on peut retrouver. Donc les détails qu'on peut retrouver etc. Comme on est sur un réseau local avec une adresse IP, l'adresse MAC, la version du firmware etc. En gros qu'on peut tout trouver. Et même qu'on peut trouver en gros quelle authentification, est-ce que le serveur il a HTTPS ou HTTP etc.

(51:20) Pentester : Ouais tu ne vois rien que l'information de l'authentification bah des fois quand tu rentre dans un wifi tu sais pas vraiment quel protocole de chiffrement il utilise donc tu dois tester plusieurs options et en fonction de comment il réagit à ce que tu testes, tu vas pouvoir en déduire qu'il utilise ce protocole. Donc après tu vas te concentrer sur ce protocole et voir s'il est vulnérable.

(51:49) Nicolas : Parce qu'en gros ça du coup c'est le système d'authentification. L'authentification qu'il utilise c'est Digest, c'est un peu la même chose que le SSID mais c'est un autre ?

(52:04) Pentester : C'est peut-être une authentification propre au caméras D-link. C'est un système d'authentification mais il y a des vulnérabilités dessus. C'est une authentification web.

(53:25) Nicolas : Là du coup c'est un peu ce que tu m'avais montré la dernière fois j'imagine. C'est que c'est encore une fois une caméra et que si on regarde en bas on peut voir en gros ce que la caméra voit. Parce que là du coup c'est toujours une D-link. Bon ça doit être une des extérieures du coup.

(53:45) Pentester : Oui.

(53:46) Nicolas : En gros on peut voir... Après je sais pas, ça c'est par exemple... C'est à un moment pris ça s'actualise avec Shodan automatiquement ou on peut justement accéder à cette caméra ?

(53:59) Pentester : Ça je pourrais pas te dire, ça dépend des... Si tu cliques là. Bon c'était peut-être un moment qui s'est capturé. En fait Shodan ils vont énumérer les informations et après tout ce qui est vulnérable ils vont le lister ici. Donc en fait comme typiquement tu vois... Vas-y monte un peu. Tu vois en fait ça c'est des... C'est comme s'ils avaient... Ils utilisent l'outil nmap et en gros ça va te ressortir toutes les informations. Ça c'est la version du certificat donc c'est pas hyper important mais... En fait t'as plein d'infos quoi. Des fois quand ils y accèdent bah... Ils mettent le lien pour y accéder.

(54:48) Nicolas : Ouais parce que j'avais vu que bah elle était de jour. Là maintenant elle est de nuit.

(54:53) Pentester : Ouais je pense qu'il fait des petites captures. En tout cas la caméra est pas accessible.

(55:01) Nicolas : Ok. parce que je pense que du coup je vais quand même peut-être faire un screen de ça juste pour montrer qu'on peut avoir accès à des caméras sur shodan. Et me renseigner encore plus sur les attaques de wifi.

(55:25) Pentester : Après aussi tu peux regarder les techniques d'attaque sur le wifi. Après t'as plein d'outils pour le tout faire à ta place c'est très intéressant.

(55:55) Nicolas : d'accord, bah merci beaucoup pour votre temps je vous écris si j'ai une demande précise sur un point dont on a discuté aujourd'hui.

FIN de la discussion concernant la partie pratique de ce travail.