IOTRUST

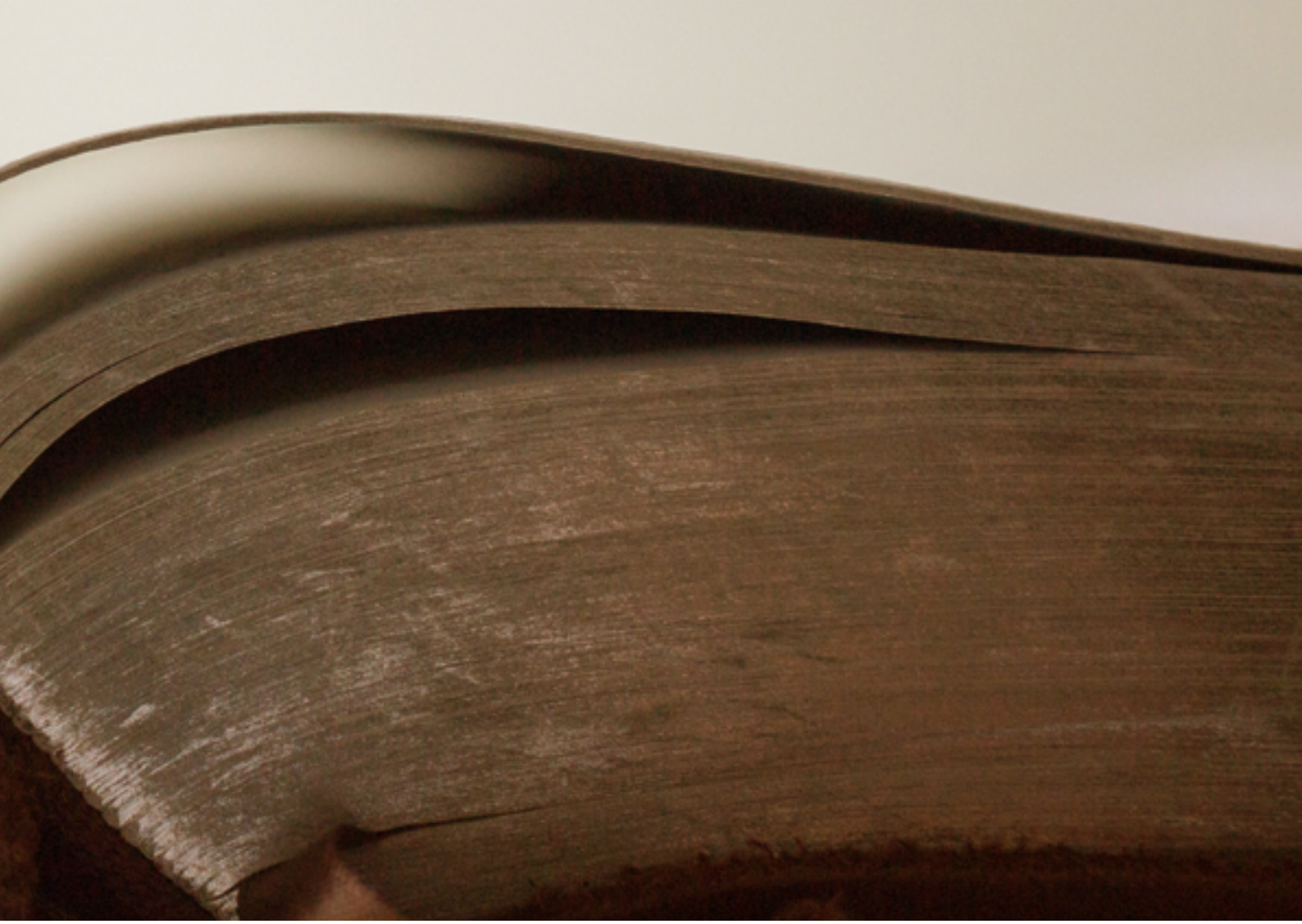
GUIDE DE BONNES PRATIQUES

DÉVELOPPEMENT DE SYSTÈME IOT

SOMMAIRE

1

PRÉSE
DOCU



ENTATION DU
UMENT

INTRODUCTION

POURQUOI AVOIR ÉCRIT CE GUIDE ?

Le marché des objets connectés est en pleine explosion depuis plusieurs décennies. De nos jours, tout doit être connecté et les objets anodins d'hier sont désormais les nœuds d'un vaste réseau, communiquant et partageant des données avec d'autres nœuds. Dans ce contexte, la sécurité joue un rôle primordial pour chacun de ses nœuds, quelle que soit sa nature. Peu importe qu'il s'agisse d'une caméra de sécurité ou d'un simple ventilateur, un nœud mal sécurisé peut être compromis et devenir une menace pour les autres nœuds, pour son utilisateur, ou même pour l'entreprise qui l'a mis au point.

Au-delà des problèmes de mauvais fonctionnement ou d'utilisation frauduleuse auxquels peut mener un manque de sécurité, on s'intéresse ici plus particulièrement au vol de données personnelles. L'utilité d'un objet connecté réside dans sa capacité à capter et à transmettre des informations sur son environnement ou son utilisateur. Il est donc primordial de s'assurer que ces informations ne puissent être ni écoutées, ni détournées, ni modifiées par une personne ou un équipement tiers.

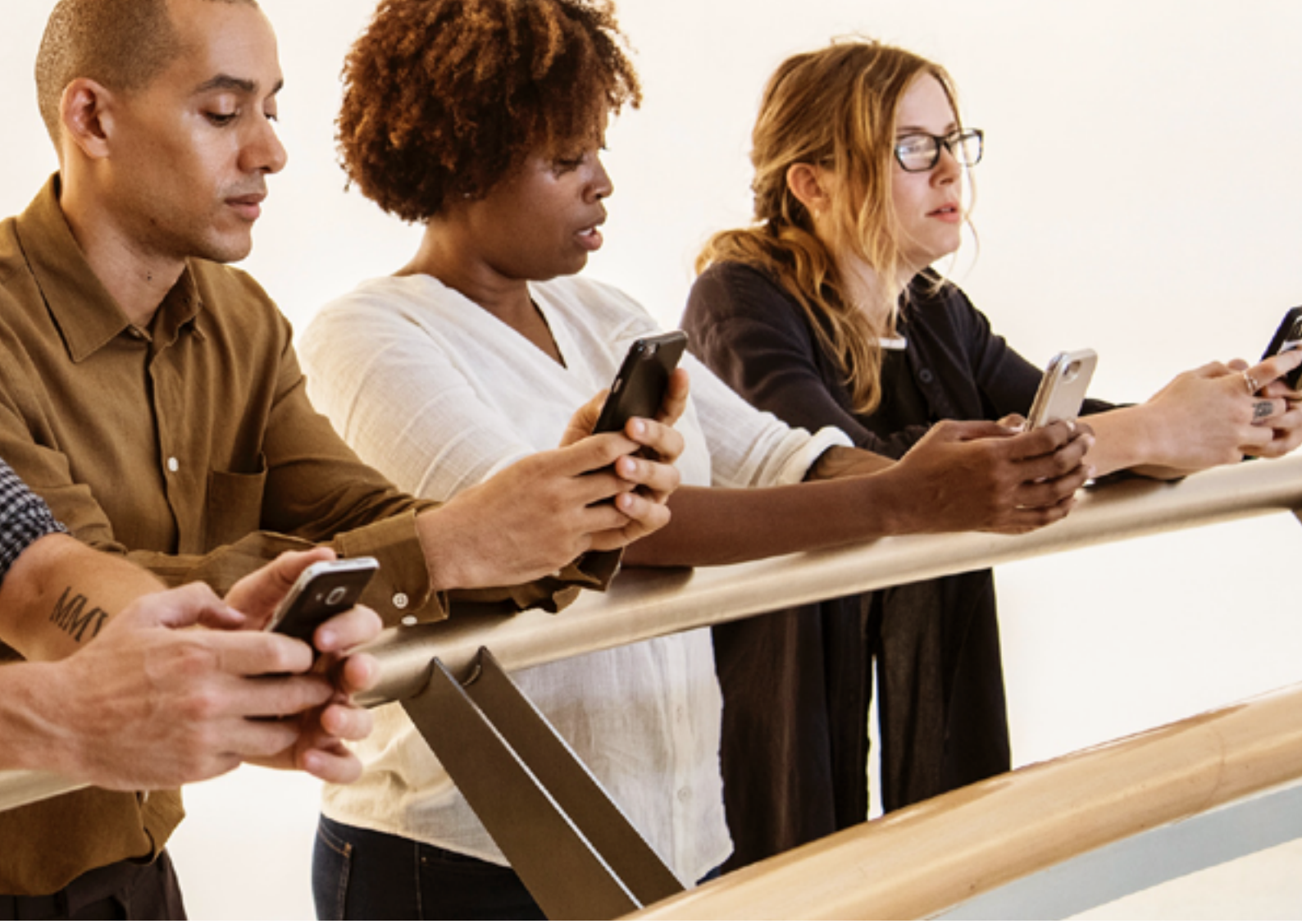
À QUI S'ADRESSE CE GUIDE ?

Ce guide s'adresse à toute personne développant des objets connectés. Avant le commencement du développement d'un projet, il peut servir à définir des spécifications. Pendant le développement d'un produit, il peut servir de guide lors des phases de conception et d'implémentation. Après la mise en production d'un produit, il peut servir à guider la correction d'erreurs non repérées antérieurement.

ATTRIBUTIONS

2

PRÉSE
AUTE



ENTATION DES
URS

LES AUTEURS

ANNE-LISE BOULET

Juriste au sein de la société Digitemis, **Anne-Lise BOULET** conseille et accompagne ses clients dans leur mise en conformité avec le règlement européen sur la protection des données personnelles (RGPD). Cet ouvrage aborde de manière pédagogique les principes juridiques à prendre en compte pour la conception d'objets connectés.

ADRIEN COUERON

Ingénieur en sécurité des systèmes d'information, **Adrien COUERON** a élaboré la structure de ce guide de bonnes pratiques en fonction des principaux manquements de sécurité constatés sur les objets étudiés dans le cadre du projet IoTrust.

ROMAIN GARNIER

Étudiant en Big Data et cloud computing à l'ESIEA, **Romain GARNIER** a rédigé ce guide dans le cadre de son « stage technique » au cours duquel il a travaillé sur une méthodologie d'audit d'objets connectés et particulièrement sur leurs applications Android.

LUDOVIC VALLY

Étudiant en système d'information à l'ESIEA, **Ludovic VALLY** a participé à la rédaction de ce guide en apportant ses réflexions et ses connaissances dans le domaine de l'IoT acquises au cours de son stage au laboratoire de sécurité informatique CNS.

2 PRÉSENTATION DES AUTEURS

SOUS LA SUPERVISION DE : RICHARD REY, DAVID CARNOT ET SLIM TOUHAMI

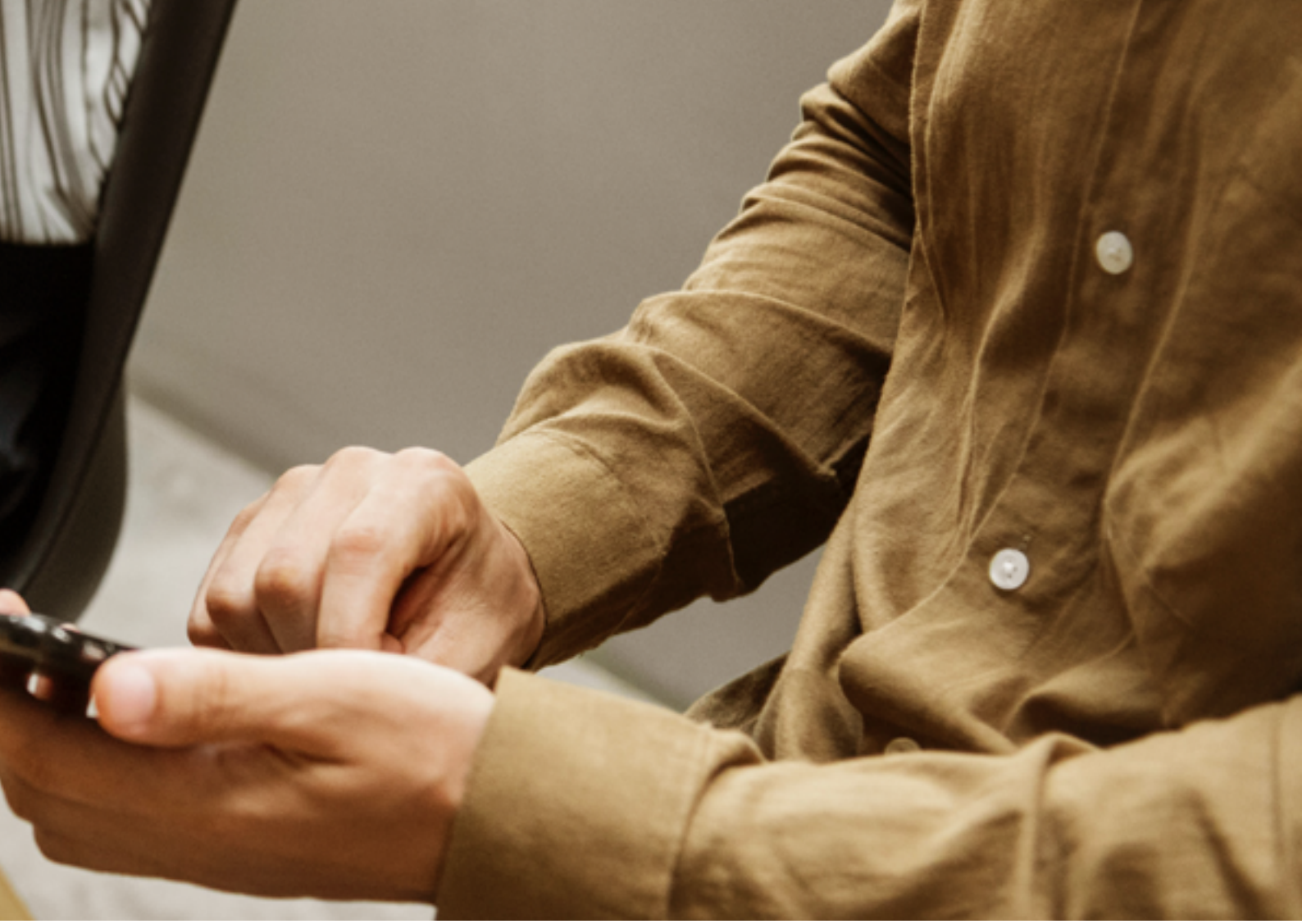
Richard REY : Ingénieur de recherche en sécurité informatique

David CARNOT : Consultant sécurité des systèmes d'information

Slim TOUHAMI : Juriste consultant RGPD / Vie privée

3

PRÉSI



ENTATION DU PROJET

LE PROJET

FINALITÉS DU PROJET

Dans les années soixante-dix, les législations nationales, notamment française, se sont développées afin de limiter les atteintes aux données personnelles et, a fortiori, au respect de la vie privée des personnes. Avec le développement des nouveaux outils de communication et l'arrivée d'Internet, le transfert et l'exploitation des données personnelles ont été facilitées et la protection des données personnelles est devenue d'autant plus sensible.L'adoption, le 14 avril 2016, du règlement général européen sur la protection des données personnelles (RGPD) permet l'adaptation et l'harmonisation des outils juridiques aux nouveaux enjeux et risques de l'économie de la donnée.

Avec l'arrivée du règlement en mai 2018, les risques liés à la vie privée des personnes doivent désormais être pris en compte par le professionnel dès la conception (« privacy by design »), en passant par les phases de développement et de distribution des produits et services. Le principe de responsabilité (« accountability ») prévu par le règlement européen impose de démontrer la mise en place de mesures internes pour assurer la conformité à la législation sur la protection des données personnelles, et ce dès la conception du produit ou service.

Jusqu'à l'adoption du règlement, la labellisation d'un produit ou d'un service devait impérativement passer par la Commission Nationale de l'Informatique et des Libertés. Le législateur européen encourage désormais la certification d'organismes privés chargés de labelliser des procédures, des produits ou des services. Le projet IoTrust vise ainsi la création d'un organisme de certification en charge de vérifier et qualifier le niveau de conformité juridique et technique des objets connectés proposés par les industriels.

MÉTHODOLOGIE ET RÉFÉRENTIELS

Le référentiel comprend l'ensemble des exigences techniques et juridiques que l'objet ou le service doit satisfaire afin d'obtenir le label. Il vise à vérifier la sécurité des objets connectés et des flux de données, la gestion des données personnelles, et le respect de la législation, notamment des droits des utilisateurs.

| 1. LE COMITÉ DE PILOTAGE

Un comité de pilotage a défini un référentiel de labellisation, en prenant en compte les avis du consortium, composé de juristes, d'industriels du secteur de l'internet des objets, d'associations de protection de consommateurs et de spécialistes en sécurité de l'information.

| 2. L'OUTIL DE VALIDATION

Un outil de validation de la sécurité technique des objets connectés a également été développé à partir des référentiels de l'ANSSI, de l'OWASP (Open Web Application Security Project), du CEH (Certified Ethical Hacker) et de l'état de l'art des vulnérabilités. L'outil a vocation à analyser les flux de données transitant par l'objet pour en déterminer le niveau de sécurité.

| 3. LES TESTS PRÉLIMINAIRES

Des tests préliminaires ont ensuite été réalisés sur des objets connectés disponibles sur le marché et couvrant différents domaines de l'internet des objets (domotique, voiture connectée, bien-être…).

Le comité a enfin eu pour mission de rédiger le guide de bonnes pratiques à destination des concepteurs d'objets connectés.

| 4. LA CRÉATION DE L'ORGANISME

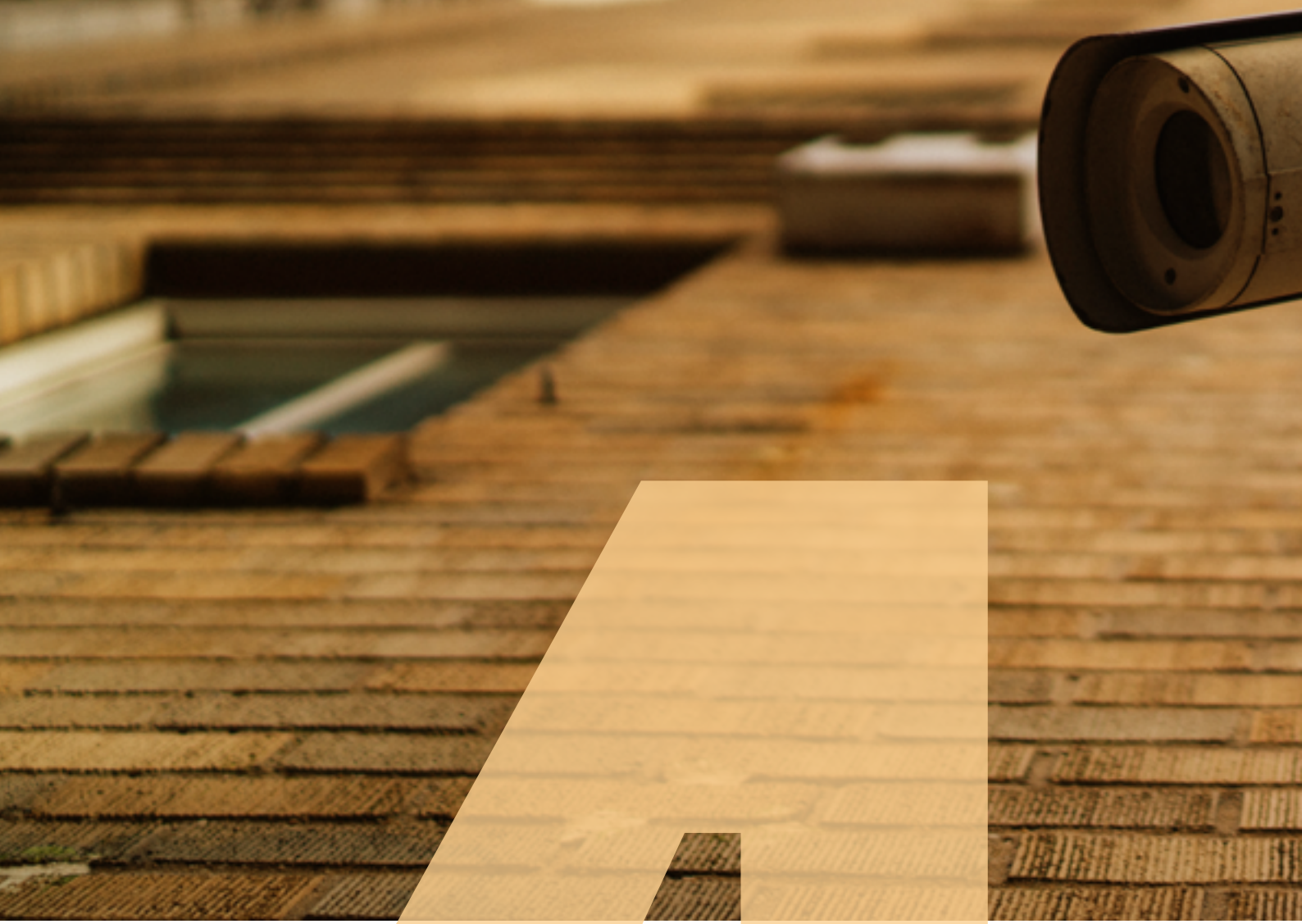
La création de l'organisme de labellisation est intervenue après finalisation du référentiel, de l'outil de validation de la sécurité technique et du guide de bonnes pratiques. Une demande de certification auprès de la CNIL a été déposée, permettant à l'organisme de délivrer un label européen, ayant force légale sur l'ensemble du territoire de l'Union européenne, pour une durée de trois ans.

DIFFÉRENTES PARTIES PRENANTES

La Fondation **MAIF**, reconnue d'utilité publique, finance la recherche dans le domaine de la prévention des risques qui affectent les personnes, les biens et la vie quotidienne. À l'image de sa participation au projet IoTrust, la fondation soutient des projets innovants dans le but de réduire les risques.

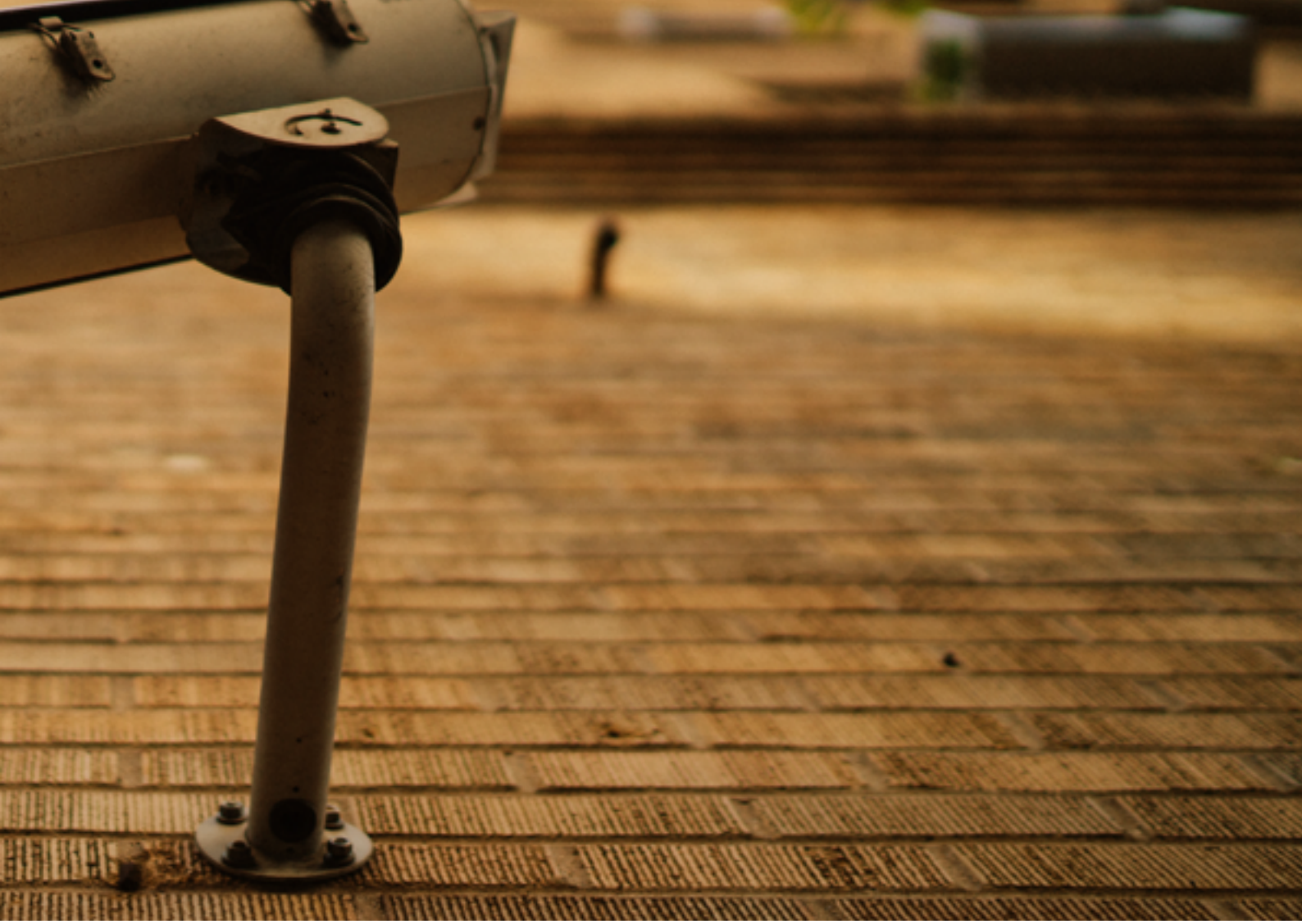
Digitemis accompagne ses clients dans la protection des données personnelles et dans la mise en place de politiques de cybersécurité. Elle propose également des prestations d'audit et de sensibilisation à la sécurisation des données ainsi que des formations et du conseil.

L'**ESIEA** (École supérieure d'informatique, électronique, automatique) forme des ingénieurs dans le domaine des sciences et technologies du numérique. L'ESIEA apporte son expertise dans le mise en place de solutions techniques innovantes pour la sécurisation des objets connectés.



4

LA SÉ
DES C



CURITÉ TECHNIQUE
OBJETS CONNECTÉS

1. CHIFFREMENT DES COMMUNICATIONS

EXEMPLE

Un clavier sans fil est connecté à un ordinateur via le protocole « Bluetooth© ». Les communications sont chiffrées avec un algorithme faible. Un équipement pirate pourra intercepter les communications et retrouver l'ensemble des frappes de l'utilisateur dans un rayon pouvant atteindre plusieurs centaines de mètres. Dans ces conditions, pourquoi prendre le risque de tenter d'introduire physiquement un dispositif USB de captation et d'enregistrement des frappes clavier (« keylogger ») ?

NOS RECOMMANDATIONS

L'ensemble des communications transitant sur un réseau doivent être sécurisées via le protocole TLS avec des suites de chiffrements fiables. N'hésitez pas à consulter le guide de l'ANSSI[1] à ce sujet.

Les clés utilisées dans ces communications doivent être temporaires et générées aléatoirement lors de chaque session. Le partage de clé secrète peut se faire via l'algorithme « Diffie-Hellman ».

Vous pouvez déterminer la longueur des clés utilisées en suivant les recommandations disponibles sur le site Keylength[2].

LES ERREURS À ÉVITER

Évidemment il ne faut jamais envoyer d'informations en clair, ou simplement encodées, sur un réseau. En effet, il peut être utile de rappeler que l'encodage n'apporte aucune sécurité. Ces algorithmes ne doivent servir que pour optimiser ou adapter un flux de données sur un support de transport.

Il faut bien entendu rester méfiant par rapport à la fausse impression de sécurité apportée par l'utilisation d'un algorithme faible. De nombreux anciens standards de chiffrement ne sont plus fiables aujourd'hui (DES, SHA1, etc.).

Un autre risque est l'utilisation d'un algorithme conçu en interne. Les standards de chiffrement ont été mathématiquement éprouvés. Cela est très rarement le cas pour les algorithmes « maison » qui peuvent embarquer des faiblesses ou des vulnérabilités. La création d'algorithmes de chiffrement est une activité scientifique ultra spécialisée, réservée aux mathématiciens.

Dans le même ordre d'idée, il faut absolument éviter d'implémenter soi-même un standard de chiffrement. Ce type de développement sensible et complexe ne peut aboutir

que lorsqu'il est géré par des équipes spécialisées dont les processus d'audit de code sont aboutis. Les algorithmes de chiffrement sont mathématiquement fiables, mais les vulnérabilités associées proviennent bien souvent d'erreurs d'implémentations. Ainsi, dans la plupart des cas, vous pourrez exploiter les bibliothèques des standards chiffrement qui vous apporteront le service dont vous avez besoin. Vous devez bien entendu vous assurer que ces bibliothèques sont incluses dans le processus de mise à jour de votre système.

Différents objets connectés ne doivent pas partager une même clé de chiffrement. Une règle très importante dans le milieu des systèmes IoT est que la compromission d'un produit ne doit pas permettre de les compromettre tous.

Une clé de chiffrement ne doit pas servir à sécuriser les communications avec un objet pendant toute sa durée de vie. Les clés doivent être changées régulièrement.

[1] https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-tls/

[2] https://www.keylength.com/fr/5/

2. AUTHENTIFICATION DES SERVEURS

EXEMPLE

Un système IoT utilise le protocole TLS pour sécuriser les communications entre l'application mobile et les serveurs distants. Mais lors de l'initiation des communications, l'application mobile ne vérifie pas la validité du certificat envoyé par le serveur. Un utilisateur qui utiliserait cette application via le Wi-Fi public d'un l'hôtel où il séjourne peut très facilement être écouté. Le pirate situé dans l'hôtel ou à proximité peut se positionner au milieu de la communication entre l'application et les serveurs distants. Il aura ainsi accès à toutes les informations transmises. Il aura même la possibilité de modifier les données transmises.

NOS RECOMMANDATIONS

Il faut acquérir des certificats officiels (de type « x.509 ») chez une autorité de certification et les déployer sur l'ensemble des serveurs.

Lors des communications TLS, les clients doivent vérifier la validité des certificats transmis par les serveurs. Il faut bannir les certificats autosignés. Il faut vérifier la chaîne de confiance du certificat ainsi que la période de validité et le nom de domaine rattaché.

Dans la mesure du possible et si l'expérience utilisateur n'en est pas trop affectée, il faut privilégier l'exploitation de certificats « client » (à la place du simple mot de passe) sur les équipements IoT et les applications.

LES ERREURS À ÉVITER

Il ne faut jamais installer de certificat autosigné sur les serveurs. Utiliser des certificats autosignés revient à empêcher la discrimination entre certificats légitimes et pirates.

Un effet secondaire constaté par l'utilisation de certificats autosignés est le fait que l'on habitue l'utilisateur à accepter ces « faux » certificats ? Cela laisse penser que ce comportement constitue « la normalité » alors que les navigateurs WEB s'efforcent de présenter des fenêtres d'alerte de plus en plus alarmantes. De nombreuses raisons provoquent l'invalidation d'un certificat. Il ne faut pas les négliger sous prétexte d'assurer la continuité de fonctionnement du système (impossibilité de communiquer si le certificat est invalide).

3. RÉDUCTION DE LA SURFACE D'ATTAQUE LOGICIELLE

EXEMPLE

Des caméras IP disposent d'un service d'administration à distance ouvert sur Internet avec des identifiants par défaut. En fin 2016, un ver s'est propagé à travers toutes ces caméras. Il en a pris le contrôle en profitant de cette faille de sécurité. Le 21 octobre 2016, toutes les caméras compromises ont reçu l'ordre d'effectuer une attaque par saturation sur les serveurs de l'entreprise DynDNS. Cela a donc constitué une attaque distribuée en déni de service (ou « DDOS »). La conséquence a été que certains sites mondialement connus comme Twitter, AirBnB, Spotify, GitHub, Reddit ou encore Netflix ont été rendus indisponibles pendant une grande partie de la journée.

NOS RECOMMANDATIONS

Nous recommandons de fermer tous les services réseau non indispensables au fonctionnement du service IoT. En effet, ceux-ci peuvent comporter des failles logicielles ou de configurations exploitables par des pirates pour prendre le contrôle de l'objet connecté.

Les services nécessitant une authentification ne doivent pas utiliser le mot de passe par défaut défini lors de la conception. Il serait même souhaitable que l'objet ne puisse pas utiliser ses moyens de communication externe avant que ce mot de passe par défaut ait été changé.

La dernière recommandation est de toujours utiliser les versions sécurisées des services réseau. Par exemple utiliser SSH à la place de Telnet, HTTPS à la place de HTTP, etc.

LES ERREURS À ÉVITER

Des services réseau peuvent être nécessaires pendant la phase de développement du produit, ils doivent absolument être supprimés avant la mise en production. Ceux-ci n'apportent aucune fonctionnalité à l'utilisateur, mais pourraient être exploités par un pirate dans le cadre de son scénario d'attaque.

4. RÉDUCTION DE LA SURFACE D'ATTAQUE MATÉRIELLE

EXEMPLE

Un détecteur de fumée dispose d'un port de débogage opérationnel. Un pirate se sert de celui-ci pour extraire le logiciel embarqué et/ou le contenu de mémoire vive du produit. Il pourra utiliser les informations sensibles recueillies pour compromettre les objets et revendre le logiciel embarqué à des concurrents qui pourront créer une copie du produit sans engager de frais en R&D.

NOS RECOMMANDATIONS

La majorité des microcontrôleurs embarquent des systèmes de protection, ils doivent être configurés pour empêcher la récupération des firmwares (micrologiciels) et de la mémoire vive.

L'utilisation de mécanisme d'obfuscation et chiffrement des firmware peut compliquer la tâche d'un pirate souhaitant observer le contenu du de ce dernier.

Pour plus de sécurité, la connexion physique du port JTAG peut être totalement inhibée une fois la phase R&D terminée.

Dans le cas où l'utilisation du port JTAG est indispensable, certains composants peuvent supporter l'utilisation d'un système d'authentification avant d'activer toute interaction.

LES ERREURS À ÉVITER

Les composants de la carte électronique doivent fournir le plus d'informations possible durant la phase de développement. Mais dès lors que les produits sont mis en vente, ces informations peuvent être exploitées par un pirate voulant compromettre le système. Il ne faut pas laisser d'informations concernant le circuit et les composants sur la carte électronique.

5. STOCKAGE LOCAL SÉCURISÉ

EXEMPLE

Une application installée sur un ordinateur permet de visionner les enregistrements d'une caméra connectée pour particuliers. Dix minutes du flux sont sauvegardées sur le PC permettant un visionnage différé. Les communications sont correctement protégées, un pirate ne peut les compromettre. Mais il est possible d'infecter l'ordinateur et de récupérer les données qui ne sont pas chiffrées. Le pirate peut surveiller les habitudes de la famille pour organiser un cambriolage.

NOS RECOMMANDATIONS

Un point essentiel est de qualifier la sensibilité des informations et d'y adapter un niveau de protection correspondant. Toutes les données pouvant aider à compromettre le système et les données personnelles doivent impérativement être au plus haut niveau de sensibilité.

Un moyen efficace de protéger des données est de les chiffrer via l'utilisation d'un algorithme de chiffrement fort de type AES-256

Pour des raisons évidentes, les clés de chiffrement utilisées pour le stockage ne peuvent être sauvegardées sur le même terminal. Nous préconisons de ne sauvegarder que l'empreinte numérique (hash) d'une clé de chiffrement ou d'un mot de passe.

LES ERREURS À ÉVITER

Le premier point est de considérer toutes les informations comme non sensibles et de ne pas les protéger. Il n'y a aucun moyen pour le fabricant de savoir si le terminal est sécurisé ou non.

Le deuxième point à éviter est de stocker les clés de chiffrement directement sur le terminal en clair ou de les coder en dur lors du développement. Cela revient à avoir un niveau de sécurité similaire à un stockage en clair.

Dans l'idéal il est recommandé de définir un mot de passe sur chaque clef de chiffrement. Ce mot de passe doit être déterminer par l'utilisateur afin de s'assurer qu'il soit le seul à pouvoir accéder aux données.

6. ACCÈS AUX INFORMATIONS EXTERNALISÉES

EXEMPLE

Les données récoltées par un GPS connecté sont envoyées sur un serveur distant pour être stockées. L'utilisateur aimerait connaître la nature de ces informations et savoir comment elles sont utilisées, mais ses demandes restent sans réponse. La CNIL peut appliquer des sanctions à l'encontre de l'entreprise pour non-respect du RGPD.

NOS RECOMMANDATIONS

Les serveurs ne doivent être utilisés que pour le stockage de données. La revente ou l'exploitation de ces données à d'autres fins malicieuses constitue un manquement aux droits de la personne concernée si celle-ci n'a pas donné explicitement son consentement.

L'utilisateur possède tous les droits sur les données le concernant, il faut lui fournir un moyen d'accéder à ses données, de les modifier et de les supprimer. Il doit aussi pouvoir supprimer son compte et toutes les données afférentes le cas échéant. Ces demandes d'accès aux données doivent être réalisées via un formulaire simple disponible sur un site web ou directement sur l'application.

POUR ALLER PLUS LOIN

Pour offrir plus de transparence concernant l'utilisation des données personnelles, il est judicieux de permettre à l'utilisateur de choisir le serveur de stockage qu'il souhaite utiliser ce qui lui permettrait, s'il le désire d'utiliser son propre serveur et d'être certain de pouvoir accéder à ses données à tout moment. Le fait d'être complètement transparent par rapport au dispositif de stockage constitue un gage de confiance.

LES ERREURS À ÉVITER

Les données sont la propriété de l'utilisateur, même si elles sont stockées chez un tiers. Elles ne doivent pas être transmises n'importe où. Il est nécessaire de s'assurer de l'identité du demandeur quand quelqu'un souhaite accéder aux données.

7. POLITIQUE DE MOT DE PASSE

EXEMPLE

Un thermostat connecté permet de contrôler le système de chauffage d'un logement à distance. Par défaut il embarque un compte utilisateur dont l'identifiant et le mot de passe sont publics. Un pirate peut nuire à n'importe quel consommateur de ce produit en prenant le contrôle de toute la configuration de son chauffage.

NOS RECOMMANDATIONS

Les attaquants peuvent effectuer des attaques par dictionnaires avec les milliers de mots de passe les plus communs et ainsi compromettre les objets connectés à grandes échelles. Un contrôle de complexité des mots de passe définis par l'utilisateur est ainsi recommandé.

Nous conseillons un minimum de huit caractères de longueur et l'utilisation de trois catégories parmi les quatre suivantes : lettres minuscules, lettres majuscules, chiffres et caractères spéciaux.

Lorsque des mots de passe par défaut sont utilisés, par exemple pour la première connexion, il faut imposer à l'utilisateur de le changer directement. L'utilisation de mots de passe par défaut dans des systèmes est une grande cause de piratage par des attaquants même très peu expérimentés.

L'utilisateur doit aussi savoir qu'il est possible de changer son mot de passe. Une fonctionnalité intuitive dans les paramètres doit permettre de modifier son mot de passe.

POUR ALLER PLUS LOIN

La politique de complexité de mots de passe peut être adaptée suivant les privilèges du compte rattaché. Un compte à privilèges élevés peut devoir respecter une politique plus restrictive. Les comptes privilégiés méritent une protection plus efficace, car ils donnent accès à des données ou des actions plus sensibles.

Pour améliorer encore la sécurité, il est possible de mettre en place une date d'expiration des mots de passe après laquelle il est impératif de les changer. Cela limite le temps d'exposition aux pirates des mots de passe compromis.

LES ERREURS À ÉVITER

Il ne faut surtout pas mettre de mot de passe par défaut sans donner la possibilité de le changer ou même sans inciter l'utilisateur à le changer. Un mot de passe par défaut est

connu et apporte la même sécurité que s'il n'y avait pas d'authentification.

Les mots de passe faibles en longueur ou en complexité ne doivent pas pouvoir être utilisés.

La dernière mauvaise pratique est de fixer un maximum de caractères dans la longueur des mots de passe. Cela peut être mis en place seulement avec une limite suffisamment élevée comme 40 caractères. Mais cela n'apporte pas d'intérêt du point de vue de la sécurité.

8. VERROUILLAGE DE L'APPLICATION MOBILE

EXEMPLE

Une application permet le contrôle à distance du système de sécurité du domicile de l'utilisateur. Cet utilisateur laisse son téléphone déverrouillé et sans surveillance pendant quelques minutes. N'importe qui peut lancer l'application, prendre connaissance de l'état du système de sécurité, le désactiver et potentiellement récupérer l'adresse de l'utilisateur.

NOS RECOMMANDATIONS

Il est possible d'empêcher l'utilisation d'une application par une personne non autorisée en demandant un déverrouillage par schéma, mot de passe ou empreintes digitales. Pour que cette précaution soit efficace, cette commande de déverrouillage doit être stockée de manière sécurisée comme préconisée dans la partie **5. STOCKAGE SÉCURISÉ**.

La demande de déverrouillage de l'application doit être systématiquement effectuée au lancement de celle-ci, après une mise en veille du système ou après une certaine durée d'inactivité.

POUR ALLER PLUS LOIN

Pour augmenter encore la sécurité, il est conseillé d'utiliser un mot de passe et de respecter les préconisations de la partie **7. POLITIQUE DE MOT DE PASSE**.

On peut également exiger un déverrouillage de l'application quand l'utilisateur utilise une commande sensible.

LES ERREURS À ÉVITER

Il ne faut pas négliger d'implémenter un système de verrouillage de l'application et, quand ce système est mis en place, il ne faut pas rendre son utilisation impossible par l'utilisateur.

D'autre part, abuser de ce système, en demandant un déverrouillage à chaque action par exemple, présente deux risques :

- En effectuant régulièrement la commande de déverrouillage, on augmente le risque que celle-ci soit interceptée par quelqu'un
- L'utilisateur risque de favoriser une commande plus simple à utiliser et moins efficace du point de vue de la sécurité

9. REMONTÉE DES FAILLES

EXEMPLE

En utilisant l'application lui permettant de contrôler la caméra de sécurité de son domicile, un utilisateur se rend compte qu'il peut prendre le contrôle de la caméra du même modèle de son voisin. Il tente de contacter l'entreprise qui lui a vendu la caméra pour leur indiquer la faille, mais ne trouve aucune indication concernant le service à contacter et ses messages au service consommateur restent sans réponse. Plus tard, la faille est utilisée par un cambrioleur qui utilise sa caméra et celle de son voisin pour surveiller et pénétrer sans risque dans les deux maisons.

NOS RECOMMANDATIONS

L'utilisation d'un objet connecté ou de son application peut mener à la découverte de failles passées inaperçues durant les phases de test. Ces découvertes pouvant être réalisées par des utilisateurs lambda, il est nécessaire d'être à l'écoute et de prévoir une procédure claire, simple à utiliser et anonyme de remontée de failles de sécurité.

Une fois la faille découverte, un correctif doit être rapidement déployé sur tous les exemplaires de ce produit afin d'en interdire l'exploitation par un pirate.

POUR ALLER PLUS LOIN

En proposant son produit dans des « bug bounty », une entreprise incite les utilisateurs à rechercher les failles et à les rapporter en échange d'une récompense, ce qui permet de les corriger avant que le grand public n'en soit informé. Attention toutefois à bien identifier l'expert sécurité associé au «bug bounty», afin de ne pas donner son secret d'entreprise directement à la concurrence.

LES ERREURS À ÉVITER

Associer systématiquement la communauté des Hackers aux actes de piraterie. Les hackers éthiques se font un devoir de faire évoluer les systèmes qu'ils étudient. Ils contactent systématiquement les éditeurs et les industriels. Encore faut-il avoir prévu un point de contact et une procédure de traitement pour cela.

Enfin, les personnes remontant les failles peuvent vouloir protéger leur anonymat, il ne faut donc pas prévoir une procédure de remontée dont les éléments envoyés seraient rendus publics.

10. MISE À JOUR LOGICIELLE

EXEMPLE

Un système d'ampoules connectées présente une faille permettant à n'importe qui d'empêcher l'utilisateur d'allumer ses lumières. Ces ampoules ne disposent pas de système permettant de les mettre à jour. Après la découverte de la faille, les ampoules en production sont corrigées, mais celles déjà vendues doivent continuer à fonctionner avec une vulnérabilité rendue publique.

NOS RECOMMANDATIONS

Afin d'anticiper la potentielle découverte de failles de sécurité, il est primordial de mettre en place une procédure permettant la mise à jour sécurisée du logiciel embarqué (firmware).

Pour s'assurer qu'une mise à jour soit effective, il est nécessaire de vérifier les deux points suivants :

- La communication lors des mises à jour doit être authentifiée et chiffrée pour s'assurer que l'objet récupère de manière authentique les mises à jour officielles du constructeur
- Les mises à jour de sécurité doivent être imposées à l'utilisateur pour éviter qu'il ne les reporte et finalement oublie de les installer

11. GESTION DE PROJET

EXEMPLE

Une entreprise travaille sur un projet de frigo connecté. Favorisant l'ergonomie et l'expérience utilisateur à la sécurité, elle décide de repousser ce point à la fin du développement, sous réserve qu'il reste suffisamment de temps pour la mettre en place. Quelques semaines avant l'aboutissement du projet, une attaque massive utilisant des objets connectés révèle au grand public la faiblesse de la sécurité de ceux-ci et l'importance de la sécurité. Or l'implémentation des points de sécurité de base dans le projet du frigo connecté nécessite la réécriture d'une énorme partie du code ce qui pousse l'entreprise à reprendre la conception depuis le début.

NOS RECOMMANDATIONS

La sécurité du système doit être prise en compte dès la genèse du projet : elle doit être intégrée dès la phase de définition des besoins. Le choix des technologies utilisées doit se baser en partie sur leurs fiabilités en termes de sécurité. Si la sécurité n'est pas intégrée au projet dès le départ, l'entreprise prend le risque de devoir appliquer des correctifs plus tard.

Les agences gouvernementales comme l'ANSSI ou le NIST proposent des recommandations de sécurité concernant les technologies qu'il faut prendre en compte durant le développement du projet.

Au cours du développement et à la fin de la conception, il faut faire auditer les codes sources par des experts en sécurité internes à l'entreprise, mais également par des entreprises externes et suivre les recommandations qu'ils fournissent.

POUR ALLER PLUS LOIN

Les certifications sont un gage de qualité et de confiance pour les produits et les logiciels. Gérer le projet dans l'optique d'obtenir une certification de sécurité est le meilleur moyen de s'assurer qu'il présente un minimum de faille. Une certification européenne concernant les objets connectés est actuellement à l'étude.

LES ERREURS À ÉVITER

L'erreur principale à ne pas commettre est de considérer la sécurité comme un bonus à apporter au projet : ce n'est pas un élément à prendre en compte à la fin du développement. C'est un élément majeur qui indiquera le niveau de confiance qu'on peut accorder au projet et à l'entreprise.

Il ne faut pas non plus considérer que la sécurité n'est qu'un coût sous prétexte qu'elle n'apporte pas de fonctionnalités au projet : Si une faille est découverte et exploitée, les coûts de remédiation risquent d'affaiblir la structure de l'entreprise (dédommagements, remboursements, rappels de produits, articles de presse, etc.). Sans parler de la perte de confiance des clients, les coûts seront beaucoup plus importants que ce qu'ils auraient été si la sécurité avait été intégrée dès le début de la conception.

12. AUTHENTIFICATION DES UTILISATEURS

EXEMPLE

Le système de chauffage installé dans un domicile permet à son utilisateur de s'y connecter en Bluetooth via une application pour programmer les heures de fonctionnement. L'application se contente de se connecter avec le chauffage, sans chercher à savoir si l'utilisateur est bien le propriétaire. N'importe qui pénétrant dans le domicile avec l'application peut donc contrôler le système.

NOS RECOMMANDATIONS

Le premier point à mettre en place est d'empêcher tout utilisateur non autorisé de prendre le contrôle d'un objet : l'application doit se lancer directement sur un écran de connexion ou d'inscription.

Pour définir les utilisateurs pouvant accéder à un objet, on peut penser à lier l'objet à un ou plusieurs comptes utilisateurs.

L'utilisateur doit alors se connecter à son compte pour avoir accès à l'objet. La connexion doit inclure une bonne politique de mot de passe, comme préconisé dans la partie **7. POLITIQUE DE MOT DE PASSE**, et un mécanisme contre les attaques par force brute, en désactivant temporairement le compte après un certain nombre de tentatives de connexions échouées par exemple.

POUR ALLER PLUS LOIN

Si l'objet est destiné à n'être utilisé que par une seule personne, il est conseillé de limiter le nombre d'utilisateurs à cette seule personne pour éviter que quelqu'un d'autre ne se lie également à l'objet. Si l'objet est destiné à être utilisé par un groupe d'individu, on peut définir un utilisateur propriétaire qui pourra être en charge d'en ajouter ou supprimer d'autres.

Pour augmenter la sécurité de l'authentification, on peut également envisager une authentification à deux facteurs, en demandant une confirmation par courriel ou SMS par exemple et en envoyant un courriel au propriétaire quand un utilisateur tente de se connecter depuis un nouvel appareil.

LES ERREURS À ÉVITER

Négliger la sécurité au niveau de l'authentification, si quelqu'un parvient à accéder au compte du propriétaire, il aura accès à toutes ses informations et au contrôle du système.

Partir du principe que l'utilisateur comprend les problématiques de sécurité, surtout dans le cas d'une application grand public. Il faut lui imposer, et si possible lui faire comprendre, les règles minimales de sécurité pour qu'il les respecte.

3

LA CO

JURID

CONN

ONFORMITÉ

DIQUE DES OBJETS

NECTÉS

INTRODUCTION

Les objets connectés peuvent collecter de nombreuses données personnelles, et notamment des informations sur la santé ou les habitudes de vie. Il est donc nécessaire de s'assurer que ces objets soient développés dans le respect de la vie privée des utilisateurs et conformément aux dispositions du règlement général sur la protection des données (RGPD).

1. ASSURER LA PROTECTION DES DONNÉES PERSONNELLES DÈS LA CONCEPTION DE L'OBJET

PRINCIPE

Le RGPD impose au responsable de traitement l'obligation d'intégrer la protection des données personnelles dès la phase d'élaboration et de conception d'un produit. On parle de *privacy by design*.

Le responsable de traitement doit également mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données personnelles qui sont nécessaires au regard des finalités du traitement sont traitées. Il s'agit du principe de *privacy by default*.

NOS RECOMMANDATIONS

Avant chaque lancement de nouveau projet, la personne en charge de la conformité au RGPD au sein de l'organisme du fabricant devrait être consultée. En cas d'incidence sur des données à caractère personnel, ce référent en matière de protection des données pourra s'intégrer tout au long du projet.

Il est préférable de réaliser une analyse d'impact relative à la protection des données (ou PIA, *Privacy Impact Assessment* en anglais) avant le lancement de toute nouvelle application liée à un objet connecté. Celle-ci permettra d'anticiper le plus tôt possible les risques qui peuvent peser sur la vie privée des utilisateurs de l'objet. La méthodologie à suivre est précisée par la CNIL sur son site internet, qui met également à disposition des responsables de traitement un logiciel dédié[1]. Lorsque cela est approprié et réalisable, le fabricant peut envisager de mettre l'analyse à la disposition du grand public

LES ERREURS À ÉVITER

La prise en compte de la protection des données personnelles ne doit pas intervenir seulement à la fin du développement de l'application.

[1] *Pour télécharger l'outil PIA de la CNIL :*
https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

2. INFORMER LES UTILISATEURS

PRINCIPE

Pour être loyale et licite, la collecte de données personnelles doit s'accompagner d'une information claire et précise. Cette obligation de transparence impose au responsable de traitement de prendre des mesures appropriées pour fournir toutes les informations concernant le traitement de leurs données aux utilisateurs, et ce de façon concise, transparente, compréhensible et aisément accessible.

L'information à transmettre concerne l'identité et les coordonnées du responsable de traitement, les coordonnées du délégué à la protection des données le cas échéant, les finalités du traitement, la base légale du traitement, les destinataires des données, les transferts de données hors UE, les durées de conservation des données, et les droits des personnes.

NOS RECOMMANDATIONS

Il est nécessaire de veiller à ce que l'information soit préalable à la collecte des données, mais également que l'utilisateur de l'objet connecté garde la maîtrise de ses données tout au long du traitement. Pour cela, une politique relative aux données personnelles devrait être transmise au moment de l'installation de l'application mobile liée à l'objet connecté, et ensuite être accessible à tout moment directement sur l'application.

L'information doit être rendue la plus conviviale possible pour les utilisateurs de l'objet connecté. Les politiques de confidentialité doivent se concentrer sur des informations claires et compréhensibles pour l'utilisateur.

Si les utilisateurs visés par l'objet connecté sont des enfants, le fabricant doit transmettre l'information de la manière la plus ludique possible, notamment par le biais d'infographies imagées et de termes accessibles aux plus jeunes.

LES ERREURS À ÉVITER

L'information ne doit pas se limiter à une politique générale relative au respect de la vie privée sur le site internet du responsable de traitement. L'information donnée doit être suffisamment spécifique à l'objet utilisé, et ne doit pas porter sur l'ensemble de la gamme des produits du fournisseur.

3. PERMETTRE L'EXERCICE DES DROITS DES PERSONNES

PRINCIPE

Les personnes concernées disposent de droits afin de garder la maîtrise de leurs données. Le RGPD consacre ainsi un droit d'accès, de rectification et de suppression des données, un droit à la portabilité de celles-ci, ainsi qu'un droit d'opposition, un droit à la limitation du traitement et le droit de retirer son consentement à tout moment.

NOS RECOMMANDATIONS

Les utilisateurs doivent pouvoir avoir le contrôle de leurs données. Les droits d'accès, de rectification et de suppression dont ils disposent devraient pouvoir s'exercer directement par le biais de l'application, sans qu'il soit nécessaire de se tourner vers le responsable de traitement pour les exercer. De la même manière, les utilisateurs devraient pouvoir exercer le droit à la portabilité en exportant l'ensemble de leurs données depuis l'application dans un format structuré, courant et lisible par machine.

Si besoin, les utilisateurs doivent néanmoins pouvoir entrer en contact, directement via l'application mobile de l'objet par exemple, avec le délégué à la protection des données ou le service référent en matière de données personnelles au sein de l'organisme.

Pour formaliser le droit de retirer son consentement ou le droit d'opposition au traitement de ses données, le responsable de traitement devrait proposer une option pour désactiver la fonction « connectée » de l'objet et lui permettre de fonctionner en mode déconnecté (par exemple, désactiver la fonctionnalité connectée sur une montre ou des lunettes intelligentes)[2].

LES ERREURS À ÉVITER

Les utilisateurs ne doivent pas être obligés d'arrêter d'utiliser le service fourni pour retirer leur consentement ou s'opposer au traitement de leurs données[3].

[2] *Avis 8/2014 du G29 du 16 septembre 2014 sur les récentes évolutions relatives à l'internet des objets.*

[3] *Décision n°MED-2017-075 du 27 novembre 2017 : « un mécanisme d'opposition reposant sur la suppression définitive d'un compte ne permet pas d'assurer un juste équilibre entre l'intérêt de la société et l'intérêt des personnes concernées en ce qu'il a pour conséquence de priver la personne de l'utilisation d'un service ».*

4. DISPOSER D'UNE BASE LÉGALE POUR METTRE EN ŒUVRE LE TRAITEMENT

PRINCIPE

Un traitement de données personnelles n'est licite que dans la mesure où il repose sur une base légale définie. Le règlement prévoit six bases légales. Dans le contexte des objets connectés, trois bases légales sont pertinentes : le consentement des personnes concernées, l'exécution d'un contrat, et l'intérêt légitime du responsable de traitement.

NOS RECOMMANDATIONS

Il est nécessaire de veiller à ce que le recueil du consentement soit valable. Pour cela, la manifestation de volonté de la personne concernée doit être libre, spécifique et éclairée. L'application doit permettre à l'utilisateur de donner un consentement sur les différents aspects, clairement définis, d'un traitement spécifique. Une mention d'information près d'une case à cocher pour donner son consentement doit préciser à l'utilisateur pour quelle finalité il donne exactement son consentement.

Lorsque la base légale est l'intérêt légitime du responsable de traitement, cet intérêt doit être mis en balance avec l'intérêt et les libertés et droits fondamentaux de la personne concernée, auxquels il ne peut porter atteinte.

LES ERREURS À ÉVITER

Pour que le recueil de son consentement soit libre, l'utilisateur doit pouvoir exercer un choix, sans que celui-ci ait une conséquence négative sur l'utilisation de l'objet . L'utilisateur ne doit pas être obligé de désinstaller l'application pour s'opposer au traitement de ses données pour une finalité accessoire à celle pour laquelle il donnait son consentement.

L'utilisateur ne doit pas avoir l'impression de donner un consentement général couvrant toutes les finalités légitimes poursuivies par le responsable de traitement.

[4] *Avis n°15/2011 du G29 du 13 juillet 2011 : « le consentement ne peut être valable que si la personne concernée est véritablement en mesure d'exercer un choix et s'il n'y a pas de risque de tromperie, d'intimidation, de coercition ou de conséquences négatives importantes si elle ne donne pas son consentement. Si les conséquences du consentement sapent la liberté de choix des personnes, le consentement n'est pas libre ».*

5. DÉTERMINER DES FINALITÉS

PRINCIPE

Le principe de limitation des finalités implique que les données ne peuvent être collectées que pour des finalités déterminées, explicites et légitimes. Les données collectées ne doivent pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

NOS RECOMMANDATIONS

Les finalités doivent être définies avant que le traitement des données ne soit mis en œuvre. Le responsable de traitement doit donc avoir une vue d'ensemble du projet avant de commencer à collecter des données personnelles. Le fabricant doit se demander quel objectif il souhaite atteindre grâce à la mise en place de ce fichier de données et si ce but est légitime au regard de son intérêt, mais également des droits et libertés des utilisateurs.

LES ERREURS À ÉVITER

La finalité doit être respectée. Le responsable de traitement ne peut pas modifier librement la finalité du traitement et utiliser les données collectées pour de nouveaux besoins. Concrètement, un fichier de données révélant les caractéristiques physiques des utilisateurs (poids, taille …) collectées par un objet de bien-être afin de suivre leur activité physique ne peut pas être utilisé pour proposer des offres commerciales pour des produits de régime.

6. MINIMISER LA COLLECTE DE DONNÉES PERSONNELLES

PRINCIPE

Les données collectées sur la personne concernée doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard de la finalité spécifique précédemment déterminée par le responsable du traitement.

NOS RECOMMANDATIONS

En cas de réutilisation des données collectées pour une finalité autre, qui ne serait pas la réalisation du service proposé par l'objet, le consentement de l'utilisateur devra être recueilli. Le responsable de traitement peut également choisir d'anonymiser les données avant de les utiliser pour d'autres finalités ou de les partager à des tiers.

La collecte de certaines données, en apparence nécessaire, peut également être adaptée afin de protéger plus efficacement la vie privée des utilisateurs. Par exemple, le responsable de traitement peut prévoir l'utilisation d'un pseudonyme plutôt que le nom et le prénom des utilisateurs. De la même manière, si l'âge est nécessaire pour la fourniture du service, la collecte de l'année de naissance peut être suffisante, à la place de la date de naissance complète.

LES ERREURS À ÉVITER

Les données qui ne sont pas nécessaires à cette fin ne doivent pas être collectées et stockées « au cas où » ou parce qu'elles pourraient « être utiles plus tard ».

7. LIMITER LA CONSERVATION DES DONNÉES COLLECTÉES

PRINCIPE

Le RGPD prévoit que les données collectées doivent être conservées sous une forme permettant l'identification des personnes pendant une durée n'excédant pas celle nécessaire au regard des finalités déterminées par le responsable de traitement.

NOS RECOMMANDATIONS

Pour chaque traitement, il est nécessaire pour le responsable de traitement de définir la durée nécessaire à la réalisation de la finalité. Ainsi, les données personnelles communiquées par un utilisateur lorsqu'il s'abonne à un service doivent être supprimées dès que l'utilisateur met un terme à son abonnement. Les durées de conservation peuvent également prendre en compte les durées relatives aux prescriptions légales en cas de contentieux.

L'application liée à l'objet connecté doit prévoir la possibilité pour l'utilisateur de supprimer lui-même les informations enregistrées (que ce soit les informations qu'il a communiquées au moment de son inscription ou celles collectées au fur et à mesure de l'utilisation de l'objet) à tout moment. Les informations supprimées par l'utilisateur sur son compte ne doivent pas être conservées.

Il est essentiel pour le responsable de traitement de prévoir une limitation de la conservation en mettant en place une purge automatique ou manuelle des données, et de définir des durées de conservation qui ne soient pas excessives. Les données pourront être conservées pour une durée plus longue, à des fins de statistiques notamment, toutefois elles devront faire l'objet d'une anonymisation.

LES ERREURS À ÉVITER

Le responsable de traitement ne devrait pas conserver les données de manière infinie sous prétexte que l'utilisateur n'a pas supprimé son compte, alors même qu'il n'utilise pas le service ou l'application pendant une certaine période. Dans un premier temps, le profil de l'utilisateur devrait être paramétré comme étant inactif. Après une autre période, les données devraient être définitivement supprimées . L'utilisateur devra être informé avant que ces mesures ne soient prises.

[5] *Avis 8/2014 du G29 du 16 septembre 2014 sur les récentes évolutions relatives à l'internet des objets.*

8. ENCADRER LES TRANSFERTS DE DONNÉES HORS UE

PRINCIPE

Par principe, le RGPD interdit les transferts de données en dehors de l'Union européenne. Néanmoins, les responsables de traitement et les sous-traitants peuvent réaliser ces transferts internationaux à condition d'assurer un niveau de protection des données suffisant et approprié.

Le RGPD encadre ces transferts et complète les outils existants afin de répondre aux différentes situations rencontrées par les responsables de traitements et leurs sous-traitants.

NOS RECOMMANDATIONS

Pour ce qui est des relations avec des prestataires, il est recommandé au fabricant de privilégier au maximum les prestataires établis dans l'Union européenne.

En cas de transferts en dehors de l'Union, il est essentiel pour le fabricant de se renseigner sur le type de mécanisme lui permettant de les encadrer au mieux. Ainsi, s'il s'agit de transferts vers des filiales basées à l'international, des règles internes d'entreprises (BCR) pourront être la solution la plus adaptée. Dans le cas d'un transfert vers un prestataire, le fabricant pourra vérifier que le pays dans lequel il est établi a fait l'objet d'une décision d'adéquation, ou bien, s'il se trouve aux Etats-Unis, si l'entreprise adhère au Privacy Shield. A défaut, des clauses contractuelles types pourront être signées entre le fabricant et son prestataire.

Les utilisateurs doivent être informés précisément de l'existence d'un transfert de leurs données en dehors de l'Union européenne, de l'identité et de la localisation du destinataire, des modalités permettant de sécuriser le transfert de données, etc.

LES ERREURS À ÉVITER

Le fabricant ne devra pas délaisser cet aspect de la protection des données personnelles, en choisissant un prestataire sans se renseigner préalablement sur sa localisation ou sans étudier le contrat conclu pour la prestation de service.

9. TRAITER DES DONNÉES SENSIBLES

PRINCIPE

Certaines catégories de données personnelles sont considérées comme des données sensibles au sens du RGPD (des données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, mais également des données génétiques, biométriques, ou concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne).

Certains objets connectés dédiés au bien-être, tels que des bracelets, des thermomètres ou encore des électrocardiographes connectés, peuvent être amenés à traiter des données sensibles. Il s'agit essentiellement de données pouvant révéler l'état de santé de l'utilisateur.

NOS RECOMMANDATIONS

Le fabricant pourra traiter des données sensibles dès lors que les utilisateurs ont donné leur consentement explicite au traitement de ces données pour une ou plusieurs finalités spécifiques. Le consentement doit donc être un acte positif. Pour cela, l'application devrait mettre à disposition des utilisateurs une case à cocher décochée par défaut ou un bouton cliquable.

L'utilisateur devrait ensuite pouvoir retirer son consentement à tout moment, directement sur l'application, à l'aide d'une case à décocher par exemple.

LES ERREURS À ÉVITER

La frontière est parfois mince entre les simples données personnelles et les données sensibles, et le fabricant de l'objet connecté doit prévoir un changement possible de qualification. En effet, certaines données collectées par des objets dédiés au bien-être (bracelets ou montres, thermomètres, etc.) sont à première vue des données personnelles sans caractère de sensibilité particulier puisqu'elles ne révèlent pas en tant que tel l'état de santé de l'utilisateur. Néanmoins, le fait que ces données personnelles soient enregistrées dans le temps et permettent de tirer des conclusions sur l'état de santé au bout d'une certaine durée peut engendrer une modification de qualification. Ces données de bien-être deviendraient dès lors des données de santé, et revêtiraient un caractère sensible.

SE FA

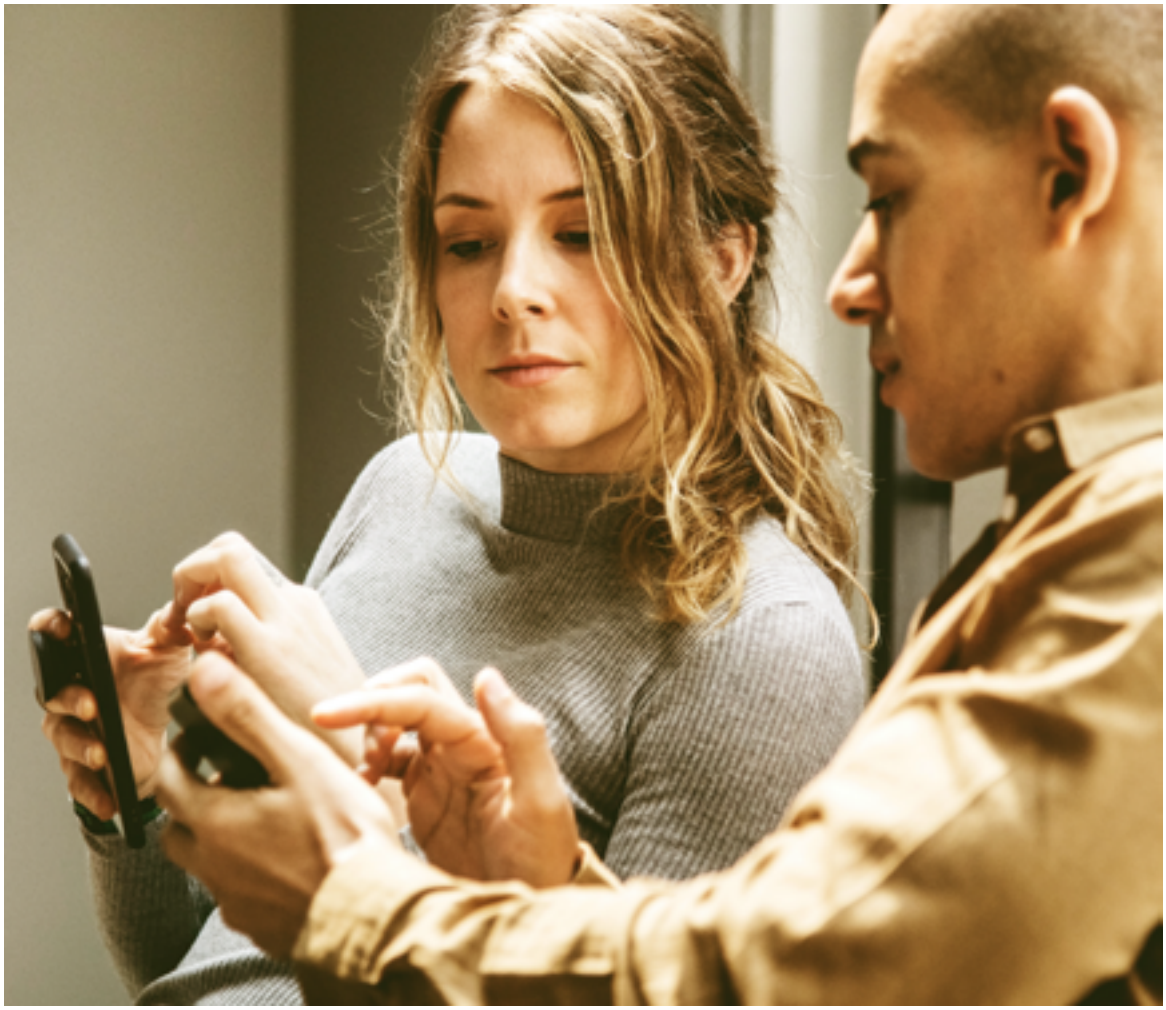
IRE LABELLISER

1. GUIDE DE BONNES PRATIQUES

Dans le cadre du projet IoTrust, un guide de bonnes pratiques est mis à disposition des professionnels. Clair et accessible, il peut être mis en œuvre aussi bien par une entreprise mature qu'une jeune société en cours de développement.

Ce guide comprend les règles et les conseils qui vous permettront de vous conformer à la législation sur la protection des données personnelles.

Il a pour vocation d'être un outil documentaire afin d'accompagner les industriels du secteur de l'internet des objets dans leur démarche de labellisation.



2. AVANTAGES DE LA LABELLISATION

Les industriels du secteur des objets connectés peuvent, dès l'obtention du label IoTrust, faire valoir cette marque de confiance sur les produits et services mis en vente. Le label IoTrust constitue un gage de confiance et d'indépendance pour le grand public en lui permettant de choisir des solutions respectueuses de sa vie privée.

Sur le plan commercial, le label est un véritable avantage concurrentiel vis-à-vis des autres acteurs du secteur, une manière de se distinguer sur le marché des objets connectés.

3. COMMENT SE FAIRE LABELLISER

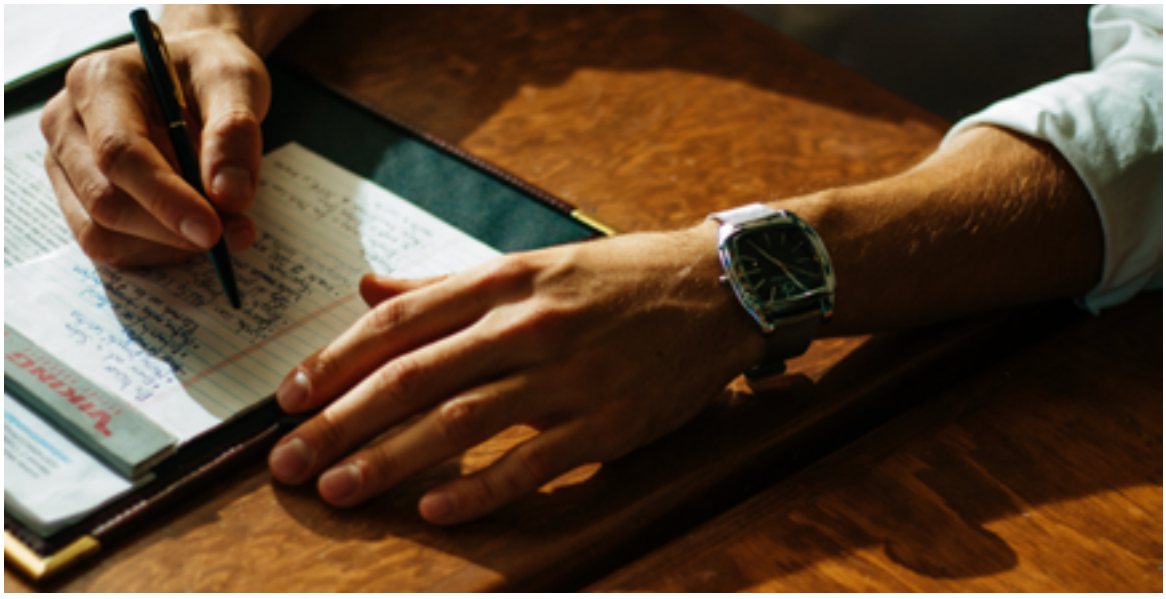
En tant que concepteurs d'objets connectés ou prestataires de services, vous pouvez nous contacter et nous proposer de tester votre objet connecté.

Suite à cette demande, une première phase de discussion est prévue, dans le but de préciser les conditions pratiques de réalisation de la prestation. Elle permet de déterminer le périmètre d'intervention et les restrictions éventuelles, ainsi que le planning des tests et de la remise du rapport.

Lorsque, à l'issue de ces négociations, l'autorisation de débuter les tests est obtenue, les consultants Digitemis étudient la conformité de l'objet à la législation sur la protection des données personnelles, grâce au référentiel juridique et technique. L'outil de validation de la sécurité technique permet quant à lui d'identifier les potentielles vulnérabilités de l'objet connecté.

Une fois la prestation terminée, un rapport vous est remis, contenant les résultats des tests ainsi que des recommandations et des axes d'amélioration.

La labellisation est également délivrée en fonction des résultats et du barème.



4. NIVEAUX DE LABELLISATION

Le fonctionnement de l'objet connecté permet de garantir une protection optimale des données personnelles de ses utilisateurs et assure une conformité avec l'ensemble des exigences de la réglementation sur la protection des données.

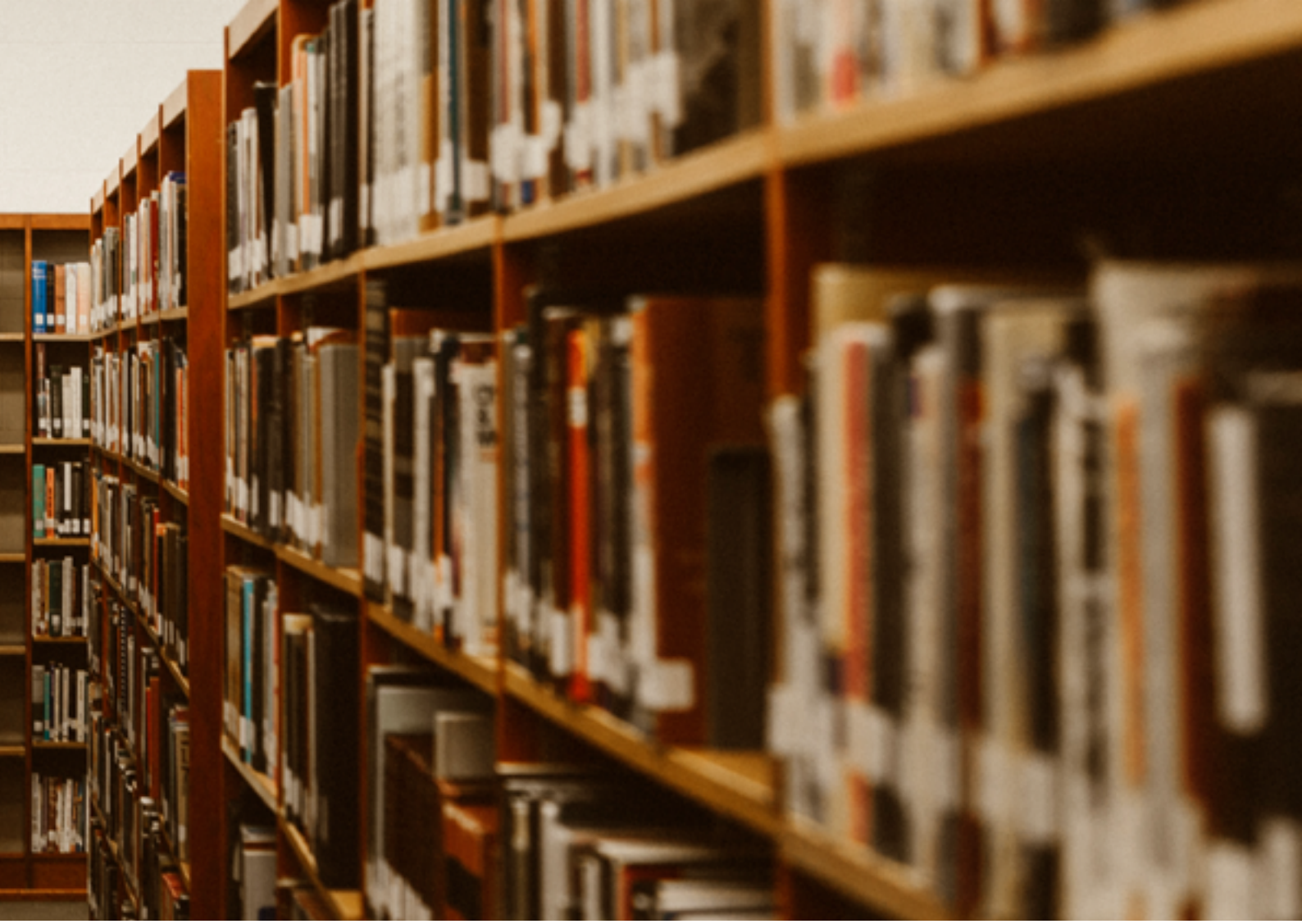
Le fonctionnement de l'objet connecté permet de garantir une protection renforcée des données personnelles de ses utilisateurs.

Le fonctionnement de l'objet connecté permet de garantir une protection adéquate des données personnelles de ses utilisateurs.

Le fonctionnement de l'objet connecté répond aux principales obligations réglementaires en matière de protection des données personnelles.

Le fonctionnement de l'objet connecté ne permet pas de répondre aux exigences essentielles en matière de protection des données personnelles et de respect de la législation s'y référant.

ANNE



EXES

ANNEXES

GLOSSAIRE

Ce glossaire a pour objectif de faciliter la compréhension du guide de bonnes pratiques. Le lecteur peut s'y référer pour éclaircir un concept qui lui semble obscur ou à titre culturel, mais les définitions présentées ne peuvent pas être considérées comme des définitions absolues.

AES : L'AES (pour Advanced Encryption Standard) est l'algorithme de chiffrement utilisé par les organisations gouvernementales aux États-Unis depuis 2000. À ce jour, aucune faille concernant cet algorithme n'a été découverte et il est considéré comme l'algorithme de chiffrement le plus sûr.

ANSSI : L'Agence Nationale de la Sécurité des Systèmes d'Information est un service national français rattaché au secrétaire général de la défense et de la sécurité nationale. Son rôle est d'établir des règles de protection des systèmes d'information, mais également de détecter et réagir aux attaques informatiques. *https://www.ssi.gouv.fr/*

APPAREIL : Le mot appareil est ici utilisé pour désigner indistinctement tout téléphone, tablette ou ordinateur communiquant avec un objet connecté à travers une application.

AUTHENTICITÉ : L'authenticité est un des 4 principes de base de la sécurité de l'information, elle garantit que l'information provient bien de la source qui prétend l'avoir émis. Une information dont l'authenticité n'est pas vérifiée peut provenir d'un pirate qui essaie de se faire passer pour quelqu'un d'autre.

AUTHENTIFICATION : Une authentification est un procédé permettant de s'assurer de l'identité de l'entité avec laquelle on communique. Cela revient dans le monde réel à vérifier la carte d'identité d'une personne.

BUG BOUNTY : Les «bug bounty» sont des programmes de compensation de report de failles. Ces programmes permettent de récompenser les utilisateurs qui indiquent les failles qu'ils découvrent.

CERTIFICAT : Un certificat peut être vu comme une carte d'identité numérique, c'est un ensemble de données (nom, adresse électronique, signature numérique ...) servant à prouver l'identité de l'entité qui le présente.

CERTIFICAT AUTOSIGNÉ : Un certificat autosigné est un certificat dont la signature numérique provient de l'entité qui le présente. Accepter un certificat autosigné comme pièce d'identité numérique revient donc à accepter un bout de papier avec une signature comme une carte d'identité.

CERTIFICAT X.509 : x.509 est une norme indiquant le format que doivent avoir les certificats. Les certificats x.509 doivent impérativement être signés par une autorité de certification ce qui leur procure un important degré de confiance.

CERTIFICATION : Une certification est un gage de qualité obtenue en remplissant un certain nombre de critère. Obtenir une certification de respect de la vie privée pour un produit indique par exemple au consommateur que ses données ne seront pas utilisées à des fins commerciales ou malicieuses.

CHIFFREMENT : Le chiffrement est un procédé permettant de rendre illisible des données aux personnes non autorisées à les consulter (les personnes ne possédant pas la clé de déchiffrement). Il permet d'assurer la confidentialité et l'intégrité des communications.

CLÉ DE CHIFFREMENT : La clé est le paramètre utilisé dans un algorithme de chiffrement permettant de rendre les données illisibles. Dans le cas d'un algorithme de chiffrement symétrique, la clé de chiffrement fait aussi office de clé de déchiffrement et doit donc rester secrète, alors que dans le cas d'un algorithme asymétrique la clé de chiffrement est publique tandis que la clé de déchiffrement ne doit être connue que du destinataire. La robustesse d'un chiffrement repose en grande partie sur la longueur de ses clés.

CNIL : La Commission Nationale de l'Informatique et des Libertés est une autorité française chargée de s'assurer que l'informatique ne porte pas atteinte aux libertés individuelles, à la vie privée ou encore aux droits de l'Homme. *https://www.cnil.fr/*

COMPROMISSION : On parle ici de compromission d'un système lorsqu'une personne non autorisée parvient à en prendre le contrôle ou à récupérer les données qu'il contient. Un système compromis n'est pas digne de confiance.

CONFIDENTIALITÉ : La confidentialité est un des 4 principes de base de la sécurité de l'information, elle assure qu'une information communiquée n'est accessible qu'aux personnes autorisées.

CRYPTOGRAPHIE : La cryptographie est la discipline consistant à chiffrer des messages, c'est-à-dire les rendre illisibles. Elle n'empêche pas d'intercepter les messages, mais ceux-ci sont totalement incompréhensibles tant qu'ils n'ont pas été déchiffrés.

DDOS : Le DDoS (pour Distributed Deny of Service) est un type d'attaque consistant généralement à saturer la bande passante de la cible. Le DDoS ne permet pas de voler d'informations, son objectif est uniquement de bloquer l'accès aux services offerts par la cible.

DES : Le DES (pour Data Encryption Standard) est le prédécesseur de l'AES. Il a été utilisé comme algorithme de chiffrement standard des organisations gouvernementales aux États unis à partir de 1976 jusqu'à son obsolescence en 1999. Il ne doit plus être utilisé pour protéger des informations.

DIFFIE-HELLMAN : L'échange de clé de Diffie-Hellman est une méthode permettant à deux communicants de se mettre d'accord sur un nombre secret sans risquer que celui-ci ne soit intercepté. Il permet ainsi d'échanger une clé de chiffrement sans risque.

ENCODAGE : L'encodage consiste à représenter une donnée dans un format particulier. Il ne faut pas confondre l'encodage avec le chiffrement puisque l'encodage n'a pas pour objectif de rendre la donnée illisible et n'apporte aucune sécurité.

FAILLE : Une faille ou vulnérabilité est une faiblesse dans la conception d'un système qui permet à un assaillant d'exploiter des fonctionnalités pour lesquelles il n'a théoriquement pas l'accès.

FORCE BRUTE : L'attaque par force brute est le type d'attaque le plus basique pour trouver un mot de passe ou une clé, il consiste simplement à tester toutes les possibilités jusqu'à trouver la bonne. Utiliser une clé suffisamment longue permet d'allonger le temps nécessaire pour trouver la bonne, mais il existe des techniques pour accélérer l'attaque, il est donc judicieux de toujours mettre en place des mécanismes contre les attaques par force brute.

HACKER : Un hacker est une personne cherchant à connaître les mécanismes et le fonctionnement des systèmes qu'il utilise. Le terme tel qu'il est utilisé dans ce guide désigne un « grey hat », c'est-à-dire une personne qui recherche des failles sans en avoir l'autorisation et donc généralement illégalement, mais sans pour autant chercher à les exploiter. Le terme hacker ne doit pas être confondu avec pirate.

HASH : Un hash, ou empreinte est le résultat obtenu par une fonction de hachage. Le principe est le suivant : on passe une donnée en paramètre et on obtient son hash, une chaîne de caractère qui lui est théoriquement unique. La moindre modification de la donnée initiale entraîne une modification radicale de son hash et il est impossible de retrouver une donnée à partir de son hash. En pratique, on stocke le hash d'un mot de passe à la place du mot de passe lui-même dans la base de données et quand l'utilisateur tente de se connecter, il suffit de comparer le hash du mot de passe qu'il rentre avec celui déjà présent dans la base de données pour l'identifier. Connaître le hash d'un document permet également de s'assurer de son intégrité puisque seuls deux documents strictement identiques auront le même hash, ainsi si une communication est interceptée et modifiée, son hash le sera aussi. Les fonctions de hachage de la famille des SHA-2 comme SHA-256 et SHA-512 sont préconisées dans le cadre d'un stockage sécurisé.

JTAG : Le sigle JTAG (pour Joint Test Action Group) est abusivement utilisé pour désigner le TAP (pour Test Access Port), un port universellement utilisé pour le débogage des logiciels embarqués dans les cartes électroniques. Accéder au JTAG offre la possibilité de modifier le firmware ou d'accéder aux données qu'il contient.

KEYLOGGER : Un keylogger est un outil ou un logiciel espion donc l'objectif est d'enregistrer les touches tapées au clavier par l'utilisateur. En récupérant ces informations, on peut très simplement retrouver les mots de passe de l'utilisateur par exemple.

NIST : Le National Institute of Standards and Technology est une agence du département du commerce des États unis dont le rôle est d'élaborer et promouvoir des standards et de nouvelles technologies. *https://www.nist.gov/*

OBJET CONNECTÉ : Un objet est dit connecté si sa fonction première ne nécessite aucune interaction avec son environnement, mais que l'ajout d'une connexion internet lui apporte une valeur ajoutée. Dans ce guide, on désigne par objet connecté, ou simplement objet, le produit qui est ciblé par une attaque ou qui présente une faille.

OWASP : L'Open Web Application Security Project est une organisation à but non lucratif dont l'objectif est de développer la sécurité des applications web en offrant des conseils aux entreprises et internautes. *https://www.owasp.org/*

PIRATE : Pirate est le terme populairement utilisé pour désigner un hacker « black hat », c'est-à-dire un hacker qui cherche à s'introduire dans un système à des fins malveillantes. Dans ce guide, le terme pirate est utilisé pour désigner un attaquant qui cherche à nuire à l'entreprise.

POLITIQUE DE COMPLEXITÉ DE MOTS DE PASSE : Une politique de complexité de mots de passe permet d'imposer aux utilisateurs l'adoption de mots de passe suffisamment sécurisés, par exemple en interdisant l'utilisation de mots de passe trop courts ou trop communs comme « azerty ».

RGPD : Applicable depuis le 25 mai 2018, le RGPD (pour Règlement Général sur la Protection des Données) est le règlement européen de référence concernant le traitement des données personnelles et la responsabilisation des acteurs au cours de ce traitement.

SENSIBILITÉ DES DONNÉES : La sensibilité d'une donnée correspond au niveau de préjudice qu'elle pourrait porter à l'entité concernée et le degré de confidentialité qu'on souhaite lui apporter. Un pseudonyme est une donnée peu sensible puisqu'il est toujours public, contrairement à un mot de passe qui doit à tout prix être gardé secret et est donc une donnée très sensible. Les informations personnelles comme l'origine, la santé, l'opinion politique et l'orientation sexuelle (entre autres) sont des données sensibles.

SESSION : La session est l'ensemble des actions qu'effectue l'utilisateur sur une application entre le moment où il se connecte et celui où il se déconnecte de l'application.

SSH : Le SSH (pour Secure SHell) est le protocole de référence permettant de se connecter à un ordinateur distant. Il est utilisé pour contrôler et utiliser les ressources d'un ordinateur ou d'un serveur à distance en démarrant une session en toute sécurité grâce à un échange de clé

SURFACE D'ATTAQUE : La surface d'attaque est l'ensemble des vulnérabilités pouvant être exploitées par un pirate pour attaquer un équipement informatique. Pour pouvoir lancer une attaque, il est au préalable nécessaire d'étudier la surface d'attaque pour trouver des failles exploitables.

TELNET : Telnet est le prédécesseur de SSH en ce qui concerne la connexion à distance. Il est tombé en désuétude à cause de son absence totale de sécurité, les messages étant envoyés en clair.

TLS : Le TLS (pour Transport Layer Security) est un protocole de sécurisation des communications sur Internet. Il permet d'authentifier le système avec lequel on tente de communiquer en vérifiant la validité de son certificat avant d'échanger des données chiffrées avec lui.

BIBLIOGRAPHIE

RÉGLEMENTATIONS

Règlement (UE) 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD), 27 avril 2016.

OUVRAGES

WINKLER Vic. La sécurité dans le cloud. Pearson, 2011.

ELENKOV Nikolay. Android security internals. No stratch press, 2015.

PAAR Christof. Understanding cryptography. Springer, 2010.

RAPPORTS ET AVIS

https://www.wavestone.com/app/uploads/2016/09/Objects-connectes-Securite-4D_FR_publi.pdf

https://www.entreprises.gouv.fr/files/files/directions_services/etudes-et-statistiques/prospective/Numerique/2018-05-24-Etude-objets-connectes.pdf

CNIL, Pack de conformité véhicules connectés et données personnelles, octobre 2017.

Groupe de travail « Article 29 » sur la protection des données, *Avis 8/2014 sur les récentes évolutions relatives à l'internet des objets*, 16 septembre 2014.

ARTICLES

PEPIN Guénaël. Dyn : on fait le point sur l'attaque DDoS qui a touché de nombreux sites [en ligne].(publié le 24 octobre 2016) https://www.nextinpact.com/news/101871-dyn-on-fait-point-sur-attaque-ddos-qui-a-impactee-nombreux-sites.htm (Consulté le 01/06/2018)

SEARS Alec. A Beginner's Guide to Securing Your IoT Devices [en ligne].(publié le 1er juin 2018) https://www.iotforall.com/how-to-secure-iot-devices/ (Consulté le 01/06/2018)

MERKI Mathieu. Bug Bounty : Google récompense un adolescent péruvien avec 31 000 euros [en ligne].(publié le 29 mai 2018) https://www.generation-nt.com/bug-bounty-google-recompense-adolescent-peruvien-31000-euros-actualite-1954199.html (Consulté le 01/06/2018)

SITE INTERNET

Commission Nationale de l'Informatique et des Libertés (CNIL) [en ligne]. [Consulté le 07/06/2018]. Disponible à l'adresse : https://www.cnil.fr/

Un projet soutenu par la fondation MAIF.

Graphiste : Betty Bulleux
Responsable Projet : Slim Touhami
Responsable Communication : François Guibert

Réalisé en **Juin 2018**

DIGITEMIS
CYBERSECURITY & PRIVACY

IOTRUST