Code de bonnes pratiques pour la sécurité de l'IdO grand public

Titre

Code de bonnes pratiques pour la sécurité de l'IdO grand public

Date

Octobre 2018

Synthèse

À mesure que nous connectons davantage d'appareils de notre domicile à Internet, les produits et dispositifs qui étaient traditionnellement hors ligne font de plus en plus partie de l'Internet des objets (IdO).

L'IdO représente une nouvelle étape de l'intégration de la technologie à nos foyers, pour nous simplifier la vie et la rendre plus agréable. Puisque les consommateurs confient une quantité croissante de données personnelles à des appareils et services en ligne, la cybersécurité de ces produits revêt aujourd'hui une importance aussi cruciale que la sécurité physique de nos domiciles.

L'objectif du présent Code de bonnes pratiques est de soutenir toutes les parties impliquées dans le développement, la fabrication et la vente dans le domaine de l'IdO grand public via un ensemble de lignes directrices visant à garantir que les produits sont sécurisé de par leur conception, afin de favoriser la sécurité des consommateurs dans un monde numérique.

Ce Code de bonnes pratiques largement reconnues en matière de sécurité de l'IdO comporte treize lignes directrices axées sur les résultats. Il a été développé par le DCMS (Ministère britannique du numérique, de la culture, des médias et du sport), en collaboration avec le NCSC (Centre national de cybersécurité au Royaume-Uni), et fait suite à un engagement avec l'industrie, les associations de consommateurs et les universités. Ce Code a été publié pour la première fois en tant qu'ébauche en mars 2018 dans le cadre du rapport Secure by Design (Sécurisation par la conception).[1]

Introduction

L'Internet des objets (IdO) offre de grandes possibilités aux consommateurs. Cependant, il s'avère que beaucoup des appareils qui sont aujourd'hui sur le marché n'intègrent pas les mesures de sécurité de base. Les consommateurs devraient pouvoir bénéficier des technologies connectées en toute sécurité, en étant assurés que des mesures de sécurité et de confidentialité adéquates sont en place pour protéger leurs activités en ligne.

[1] DCMS, 2018, « Secure by Design: Improving the cyber security of consumer Internet of Things: Report », (Rapport sur la sécurisation par la conception : amélioration de la cybersécurité de l'Internet des objets grand public), https://www.gov.uk/government/publications/secure-by-design.

Le présent Code de bonnes pratiques énonce les mesures concrètes que les fabricants et les autres intervenants du secteur de l'IdO doivent prendre pour améliorer la sécurité des produits et des services liés à l'IdO grand public. La mise en œuvre de ses treize lignes directrices contribuera à la protection de la vie privée et de la sécurité des consommateurs, tout en leur permettant d'utiliser plus facilement leurs produits sans risque. Il permettra également d'atténuer la menace d'attaques par déni de service distribué (DDoS) lancées à partir d'appareils et de services IdO mal sécurisés.

Les lignes directrices réunissent de bonnes pratiques largement reconnues en matière de sécurité de l'IdO. Elles sont axées sur les résultats plutôt que sur des normes, ce qui donne aux entreprises la souplesse nécessaire pour innover et mettre en œuvre des solutions de sécurité adaptées à leurs produits.

Ce Code de bonnes pratiques n'est pas une panacée pour résoudre tous les problèmes de sécurité. Ce n'est qu'en adoptant une mentalité axée sur la sécurité et en investissant dans un cycle de développement sûr qu'une entreprise peut réussir à créer un IdO sécurisé. Les produits et les services doivent être conçus en gardant la sécurité à l'esprit, à partir du développement des produits et tout au long de leur cycle de vie. Les organisations doivent également évaluer régulièrement les risques de cybersécurité liés à leurs produits et services et mettre en œuvre des mesures appropriées pour y faire face.

Les chaînes d'approvisionnement des produits IdO peuvent être complexes et internationales, et impliquent souvent de nombreux fabricants de composants et fournisseurs de services. L'objectif de ce Code est d'initier et de faciliter des changements positifs en matière de sécurité tout au long de la chaîne d'approvisionnement.

Un certain nombre d'organismes de l'industrie et de forums internationaux élaborent des recommandations et des normes de sécurité pour l'IdO.[2] Le présent Code de bonnes pratiques est conçu pour compléter et soutenir ces efforts et les normes pertinentes publiées en matière de cybersécurité. Il a été créé directement avec l'industrie dans l'espoir que les futurs systèmes d'assurance et de label de confiance relatifs à l'IdO grand public s'aligneront avec lui.

La mise en œuvre du Code de bonnes pratiques peut aider les entreprises à se conformer aux lois applicables en matière de protection des données. Par exemple, le Règlement général de l'UE sur la protection des données (RGPD) exige que les données à caractère personnel soient traitées de manière sécurisée.[3]

Mise en œuvre

Le Code de bonnes pratiques s'appuie sur un document qui établit un lien entre chacune de ses lignes directrices et les principales normes, recommandations et directives de

[2] PETRAS, 2018, « Summary literature review of industry recommendations and international developments on IoT security » (Résumé de l'analyse documentaire des recommandations de l'industrie et des développements internationaux en matière de sécurité de l'IdO), https://www.gov.uk/government/publications/secure-by-design.

[3] L'article 5, paragraphe 1, point f), du RGPD concerne « l'intégrité et la confidentialité » des données à caractère personnel.

l'industrie.[4] Ce document fournit un contexte supplémentaire aux treize lignes directrices du Code et aide l'industrie à les mettre en œuvre. Il montre également la relation entre le Code et les travaux sur la sécurité de l'IdO qui sont menés par un large éventail d'organisations mondiales.

Hiérarchisation et structure

Les trois premières lignes directrices sont prioritaires car les mesures relatives aux mots de passe par défaut, à la divulgation des vulnérabilités et aux mises à jour de sécurité sont celles qui apporteront les plus grands avantages sur le plan de la sécurité à court terme.

Chacune des lignes directrices est expliquée et détaillée. À la fin du document, des notes explicatives supplémentaires répondent aux questions fréquentes.

Public

Les principaux responsables de la mise en œuvre de chacune des lignes directrices sont indiqués. Ces intervenants sont définis comme suit :

Fabricant d'appareils	L'entité qui crée et assemble un produit final connecté à Internet. Un produit final peut contenir les produits de nombreux autres fabricants.
Fournisseurs de services IdO	Les entreprises qui fournissent des services tels que les réseaux, le stockage dans le Cloud et le transfert de données qui sont intégrés aux solutions IdO. Des appareils connectés à Internet peuvent être proposés dans le cadre de ces services.
Développeurs d'applications mobiles	Entités qui développent et fournissent des applications fonctionnant sur les appareils mobiles. Celles-ci sont souvent proposées comme un moyen d'interagir avec les appareils dans le cadre d'une solution IdO.
Détaillants	Ceux qui vendent aux consommateurs des produits connectés à Internet et des services associés.

Terminologie

L'utilisation de l'expression « données sensibles en matière de sécurité » vise à établir une distinction avec d'autres types de données sensibles, par exemple les données de catégorie spéciale (officiellement dénommées « données personnelles sensibles »), selon la définition du RGPD. Les données sensibles en matière de sécurité peuvent inclure, par exemple, des vecteurs d'initialisation cryptographiques.

[4] DCMS, 2018, « Mapping of IoT Security Recommendations, Guidance and Standards to the Code of Practice for Consumer IoT Security » (Mise en correspondance des recommandations, directives et normes relatives à la sécurité de l'IdO avec le Code de bonnes pratiques pour la sécurité de l'IdO grand public), https://www.gov.uk/government/publications/secure-by-design.

Les termes « grand public » et « consommateur » sont utilisés dans l'ensemble du texte pour des raisons de cohérence ; les consommateurs peuvent généralement être considérés comme les utilisateurs finaux des produits et services IdO.

Champ d'application

Le présent Code de bonnes pratiques s'applique aux produits IdO grand public qui sont connectés à Internet et/ou à un réseau domestique et aux services associés. En voici une liste non exhaustive :

- Jouets pour enfants et moniteurs de bébé connectés,
- Produits de sécurité connectés, tels que les détecteurs de fumée et les serrures de porte,
- Caméras, enceintes et téléviseurs intelligents,
- Dispositifs portables de suivi de la santé,
- Systèmes domotiques et d'alarme connectés,
- Appareils électroménagers connectés (par exemple, machines à laver ou réfrigérateurs),
- Assistants à domicile intelligents.

Les services associés sont ici considérés comme des services numériques qui sont liés aux appareils IdO, par exemple des applications mobiles, de cloud computing / stockage et des interfaces de programmation d'applications (API) de tiers pour des services tels que la messagerie.

Révision

Le DCMS examinera périodiquement le Code et publiera des mises à jour, au minimum tous les deux ans. Veuillez contacter securebydesign@culture.gov.uk pour être tenu informé.

Lignes directrices

1) Aucun mot de passe par défaut

Tous les mots de passe des appareils IdO doivent être uniques et ne peuvent pas être réinitialisés à une valeur universelle par défaut.

De nombreux appareils IdO sont vendus avec des noms d'utilisateur et des mots de passe universels par défaut (tels que « admin, admin ») qui sont censés être modifiés par le consommateur. C'est une source de nombreux problèmes de sécurité en matière d'IdO, et cette pratique doit être éliminée. Les meilleures pratiques en matière de mots de passe et autres méthodes d'authentification doivent être suivies.[5]

S'applique principalement aux : fabricants d'appareils

2) Mise en œuvre d'une politique de divulgation des vulnérabilités

Toutes les entreprises qui fournissent des appareils et des services connectés à Internet doivent offrir un point de contact public dans le cadre d'une politique de divulgation des vulnérabilités afin que les chercheurs dans le domaine de la sécurité et d'autres personnes puissent signaler des problèmes. Les vulnérabilités révélées doivent être traitées dans un délai raisonnable.

La connaissance d'une vulnérabilité en matière de sécurité permet aux entreprises de réagir. Les entreprises doivent également surveiller continuellement, identifier et corriger les vulnérabilités de sécurité dans leurs propres produits et services, dans le cadre du cycle de vie de la sécurité du produit. Les vulnérabilités doivent d'abord être signalées directement aux parties prenantes concernées. Si ce n'est pas possible, les vulnérabilités peuvent être signalées aux autorités nationales.[6] Les notes explicatives fournissent de plus amples détails sur les différentes approches à adopter selon les circonstances. Les entreprises sont également encouragées à partager des informations avec les organismes compétents de l'industrie.[7]

---

[5] Pour en savoir plus, consultez par exemple : NCSC, 2016, « Password Guidance: Simplifying Your Approach » (Conseils en matière de mots de passe : simplification de votre approche), https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach. Voir également : NIST, 2017, « NIST Special Publication 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management » (Publication spéciale 800-63B du NIST : Lignes directrices sur l'identité numérique - Authentification et gestion du cycle de vie), https://pages.nist.gov/800-63-3/sp800-63b.html#sec5.

[6] Au Royaume-Uni, les rapports relatifs aux vulnérabilités peuvent être envoyés à https://www.ncsc.gov.uk/contact.

[7] Les organismes compétents de l'industrie comprennent la GSMA et l'IoT Security Foundation. Des conseils sur la divulgation coordonnée des vulnérabilités (Guidance on Coordinated Vulnerability Disclosure) sont disponibles auprès de l'IoT Security Foundation, en référence à la norme ISO/CEI 29147 sur la divulgation des vulnérabilités. Le programme de la GSMA relatif à la divulgation coordonnée des vulnérabilités au niveau de l'industrie est disponible à l'adresse https://www.gsma.com/cvd.

S'applique principalement aux : fabricants d'appareils, fournisseurs de services et développeurs d'applications mobiles IdO

3) Maintien des logiciels à jour

La mise à jour des composants logiciels des appareils connectés à Internet doit être possible en toute sécurité. Les mises à jour doivent être effectuées en temps opportun, sans incidence sur le fonctionnement de l'appareil. Une politique de fin de vie doit être publiée pour les appareils terminaux, indiquant explicitement la durée minimale pendant laquelle un appareil recevra des mises à jour de logiciels et les motifs de la durée de la période de support. La nécessité de chaque mise à jour doit être indiquée clairement aux consommateurs et la mise en œuvre d'une mise à jour doit être facile. Dans le cas des dispositifs restreints qui ne peuvent pas être mis à jour physiquement, le produit doit pouvoir être isolé et remplacé.

La provenance des correctifs de sécurité doit également être assurée et ils doivent être livrés par un moyen sécurisé. Les fonctions de base d'un appareil doivent continuer à être assurées pendant une mise à jour dans la mesure du possible. Par exemple, une montre doit continuer à indiquer l'heure, un thermostat domestique doit toujours fonctionner et il doit être possible d'activer et désactiver un verrou. Même si cela peut sembler principalement une question de conception, il peut en résulter un problème de sécurité critique pour certains types de dispositifs et de systèmes en l'absence de prise en compte ou de gestion correcte.

Des mises à jour de logiciels doivent être fournies après la vente d'un appareil et disponibles pendant la période appropriée. Cette période de mise à jour des logiciels doit être indiquée clairement à un consommateur lors de l'achat du produit. Le détaillant et/ou les fabricants doivent informer le consommateur qu'une mise à jour est nécessaire. Dans le cas des dispositifs restreints, sans possibilité de mise à jour des logiciels, les conditions et la durée de la prise en charge du remplacement doivent être claires.

S'applique principalement aux : fabricants d'appareils, fournisseurs de services et développeurs d'applications mobiles IdO

4) Stockage sécurisé des informations d'identification et des données sensibles en matière de sécurité

Les informations d'identification doivent être stockées en toute sécurité au sein des services et sur les appareils. Les informations d'identification codées en dur dans le logiciel de l'appareil ne sont pas acceptables.

Le rétroingénierie des appareils et des applications permet de découvrir facilement les informations d'identification telles que les noms d'utilisateur et les mots de passe codés en dur dans les logiciels. Il est également facile de décrypter ces informations codées en dur lorsque des méthodes simples d'obscurcissement ont été utilisées pour les masquer ou les chiffrer. Les données sensibles en matière de sécurité qui doivent être particulièrement sécurisées lors de leur stockage comprennent, par exemple, les clés cryptographiques, les identificateurs d'appareils et les vecteurs d'initialisation. Des mécanismes de stockage

sécurisé et fiable doivent être utilisés, comme ceux fournis par un environnement d'exécution de confiance associé à un stockage fiable et sécurisé.

S'applique principalement aux : fabricants d'appareils, fournisseurs de services et développeurs d'applications mobiles IdO

5) Communication en toute sécurité

Les données sensibles en matière de sécurité, y compris la gestion et le contrôle à distance, doivent être chiffrées en cours de transfert, selon les propriétés de la technologie et de l'utilisation. Toutes les clés doivent être gérées de manière sécurisée.

L'utilisation de normes Internet ouvertes et évaluées par des pairs est fortement encouragée.

S'applique principalement aux : fabricants d'appareils, fournisseurs de services et développeurs d'applications mobiles IdO

6) Limitation des surfaces exposées aux attaques

Tous les appareils et les services doivent fonctionner sur le « principe du moindre privilège » ; les ports non utilisés doivent être fermés, le matériel ne doit pas exposer inutilement l'accès, les services ne doivent pas être disponibles s'ils ne sont pas utilisés et le code doit être réduit au minimum pour assurer la fonctionnalité nécessaire afin que le service fonctionne. Le logiciel doit fonctionner avec les privilèges appropriés, en tenant compte de la sécurité et de la fonctionnalité.

Le principe du moindre privilège est la pierre angulaire d'une bonne ingénierie de la sécurité, applicable à l'IdO comme dans tout autre domaine d'application.

S'applique principalement aux : fabricants d'appareils et fournisseurs de services IdO

7) Assurance de l'intégrité des logiciels

Les logiciels installés sur les appareils IdO doivent être vérifiés à l'aide de mécanismes de démarrage sécurisés. En cas de détection d'un changement non autorisé, l'appareil doit avertir le consommateur/l'administrateur d'un problème et ne doit pas se connecter à des réseaux plus étendus que ceux nécessaires pour effectuer la fonction d'alerte.

La possibilité d'une récupération à distance dans ces situations doit reposer sur un bon état connu, comme le stockage local d'une bonne version connue pour permettre une récupération et une mise à jour fiables de l'appareil. Il sera ainsi possible d'éviter un déni de service et des rappels coûteux ou des visites de maintenance, tout en gérant le risque potentiel de prise de contrôle de l'appareil par un pirate informatique essayant de détourner les mises à jour ou d'autres mécanismes de communication réseau.

S'applique principalement aux : fabricants d'appareils

8) Garantie de la protection des données personnelles

Lorsque des appareils et/ou des services traitent des données à caractère personnel, ils doivent le faire conformément à la législation applicable en matière de protection des données, notamment le Règlement général sur la protection des données (RGPD) et la loi de 2018 relative à la protection des données. Les fabricants d'appareils et les fournisseurs de services IdO procurent aux consommateurs des informations claires et transparentes sur la façon dont leurs données sont utilisées, par qui, et à quelles fins, pour chaque appareil et service. Cela s'applique également à tout tiers pouvant être impliqué (y compris les annonceurs). Lorsque les données personnelles sont traitées sur la base du consentement des consommateurs, elles seront obtenues de façon valide et légale, les consommateurs concernés ayant la possibilité de se rétracter à tout moment.

La présente ligne directrice garantit que :
i) Les fabricants, fournisseurs de services et développeurs d'applications mobiles IdO, les fournisseurs de services et les développeurs d'applications adhèrent aux obligations de protection des données lors de l'élaboration et de la prestation de produits et services ;
Ii) Les données personnelles sont traitées conformément à la loi sur la protection des données ;
Iii) Les utilisateurs bénéficient d'une assistance pour assurer que les opérations de traitement des données de leurs produits sont conformes et qu'ils fonctionnent selon les spécifications ;
Iv) Les utilisateurs disposent de moyens de préserver leur vie privée en configurant l'appareil et les fonctionnalités des services de manière appropriée.

S'applique principalement aux : fabricants d'appareils, fournisseurs de services, développeurs d'applications mobiles et détaillants IdO

9) Résilience aux pannes des systèmes

La résilience doit être intégrée aux appareils et services IdO lorsque leur utilisation ou celle d'autres systèmes dépendants l'exige, en tenant compte de la possibilité de pannes des réseaux de données et de l'alimentation. Dans la mesure du possible, les services IdO doivent rester fonctionnels au niveau local en cas de perte du réseau et se réinitialiser correctement en cas de restauration d'une perte d'alimentation. Les appareils doivent pouvoir se reconnecter à un réseau dans un état raisonnable et de manière ordonnée, plutôt qu'à grande échelle.

Les systèmes et appareils IdO sont utilisés par les consommateurs dans des situations qui pourraient avoir une incidence majeure sur leur sécurité et sur leur vie. Le maintien de l'exécution locale des services en cas de perte de réseau est l'une des mesures qui peuvent être prises pour augmenter la résilience. D'autres actions peuvent inclure la redondance des services ainsi que les mesures d'atténuation contre les attaques DDoS. Le niveau de résilience nécessaire doit être proportionné et déterminé par l'utilisation, mais il faut tenir compte des autres utilisateurs qui peuvent dépendre du système, de services ou d'appareils, car l'impact pourrait être plus important que prévu.

S'applique principalement aux : fabricants d'appareils et fournisseurs de services IdO

10) surveillance des données de télémétrie du système

Si les données de télémétrie sont recueillies à partir d'appareils et de services IdO, notamment les données d'utilisation et de mesure, elles doivent être surveillées pour détecter les anomalies de sécurité.

La surveillance de la télémétrie, y compris les données de journal, est utile pour l'évaluation de la sécurité et permet d'identifier et de traiter rapidement les circonstances inhabituelles, de limiter les risques de sécurité et d'atténuer rapidement les problèmes. Toutefois, conformément à la ligne directrice 8, le traitement des données à caractère personnel doit être réduit au minimum et les consommateurs doivent être informés des données collectées et des raisons pour lesquelles elles le sont.

S'applique principalement aux : Fournisseurs de services IdO

11) Simplification de la suppression des données personnelles par les consommateurs

Les appareils et services doivent être configurés de manière à ce que les données à caractère personnel puissent être facilement supprimées en cas de transfert de propriété, lorsque le consommateur souhaite les supprimer et/ou lorsqu'il souhaite mettre l'appareil au rebut. Les consommateurs doivent disposer d'instructions claires sur la façon de supprimer leurs données personnelles.

Les appareils IdO peuvent changer de propriétaire et peuvent être recyclés ou mis au rebut. Les mécanismes fournis peuvent permettre au consommateur de conserver le contrôle et de supprimer des données personnelles de services, d'appareils et d'applications.

S'applique principalement aux : fabricants d'appareils, fournisseurs de services et développeurs d'applications mobiles IdO

12) Simplification de l'installation et de la maintenance des appareils

L'installation et l'entretien des appareils IdO doivent comporter un minimum d'étapes et suivre les meilleures pratiques de sécurité en matière de convivialité. Les consommateurs devraient également recevoir des conseils sur la façon d'installer leur appareil de façon sécurisée.

Les problèmes de sécurité causés par la confusion ou la mauvaise configuration des consommateurs peuvent être réduits et parfois éliminés en traitant correctement la complexité et la mauvaise conception des interfaces utilisateur. Des conseils clairs aux utilisateurs sur la façon de configurer les appareils en toute sécurité peuvent également réduire leur exposition aux menaces.

S'applique principalement aux : fabricants d'appareils, fournisseurs de services et développeurs d'applications mobiles IdO

13) Validation des données saisies

Il est nécessaire de valider la saisie des données par le biais d'interfaces utilisateur et leur transfert via des interfaces de programmation d'application (API) ou entre réseaux au sein des services et des appareils.

Les systèmes peuvent être corrompus par des données ou du code incorrectement formatés transférés à travers différents types d'interface. Des outils automatisés sont souvent employés par les pirates informatiques afin d'exploiter des lacunes et des faiblesses potentielles qui émergent en raison de la non-validation des données. Les exemples incluent, entre autres, les données qui sont :
i) différentes du type attendu, par exemple du code exécutable plutôt que du texte saisi par l'utilisateur.
ii) hors plage, par exemple une valeur de température qui dépasse les limites d'un capteur.

S'applique principalement aux : fabricants d'appareils, fournisseurs de services et développeurs d'applications mobiles IdO

Notes explicatives supplémentaires

Ligne directrice 1, Aucun mot de passe par défaut : Bien que beaucoup d'efforts aient été consacrés à l'élimination de la dépendance vis-à-vis des mots de passe et à d'autres méthodes d'authentification des utilisateurs et des systèmes, certains produits IdO sont encore commercialisés avec des noms d'utilisateur et des mots de passe par défaut, des interfaces utilisateur aux protocoles réseau. Ce n'est pas une pratique acceptable et elle devrait être abandonnée. La sécurité des appareils peut encore être renforcée par une identité unique et immuable.

Ligne directrice 2, Divulgation coordonnée des vulnérabilités : La divulgation coordonnée des vulnérabilités est normalisée par l'Organisation internationale de normalisation (ISO). Elle est simple à mettre en œuvre et s'est avérée efficace dans certaines grandes sociétés de logiciels du monde entier.[8] La divulgation coordonnée des vulnérabilités n'est cependant pas encore établie dans l'industrie de l'IdO et certaines entreprises peuvent être réticentes vis-à-vis des chercheurs dans le domaine de la sécurité. La divulgation coordonnée des vulnérabilités offre aux chercheurs dans le domaine de la sécurité un moyen de communiquer avec les entreprises pour les informer des problèmes de sécurité afin de prévenir toute exploitation malveillante et de leur donner l'occasion de résoudre les vulnérabilités avant qu'elles ne soient rendues publiques.

Les entreprises qui fournissent des appareils et des services connectés à Internet ont un devoir de diligence à l'égard des tiers qui risquent d'être lésés par leur incapacité à mettre en place un programme de divulgation coordonnée des vulnérabilités. En outre, les

[8] Organisation internationale de normalisation, 2014, « ISO//CEI 29147 - Divulgation de vulnérabilité », https://www.iso.org/standard/45170.html.

entreprises qui partagent ces informations via des organismes de l'industrie peuvent aider d'autres personnes pouvant être confrontées au même problème.

Les divulgations peuvent exiger des approches différentes selon les circonstances : Vulnérabilités liées à des produits ou services uniques : le problème doit être signalé directement à l'intervenant concerné (par exemple, fabricant d'appareils, fournisseur de services IdO ou développeur d'applications mobiles). Des chercheurs dans le domaine de la sécurité ou des pairs de l'industrie peuvent être à la base de ces rapports. Si, après la prise de contact avec le fabricant de l'appareil ou d'autres intervenants concernés, ceux-ci ne répondent pas de façon opportune, il est possible de signaler un problème directement au NCSC.

Vulnérabilités systémiques : il peut arriver qu'un intervenant, tel qu'un fabricant d'appareils, découvre un problème potentiellement systémique. Bien qu'il soit crucial de le corriger dans le produit du fabricant de l'appareil, le partage de ces informations présente des avantages considérables pour l'industrie et les consommateurs. De même, les chercheurs dans le domaine de la sécurité peuvent également signaler ce type de vulnérabilités systémiques. Dans ce cas, un organe compétent de l'industrie pertinente peut coordonner une réponse plus large. Le NCSC peut fournir des conseils et une orientation à l'organisme de l'industrie pertinente afin d'offrir une réponse coordonnée.

La « rapidité d'exécution »" des mesures à prendre pour remédier aux vulnérabilités varie considérablement et dépend de l'incident ; toutefois, la norme de facto pour que le processus de vulnérabilité soit mené à terme ne doit pas dépasser 90 jours. Un correctif matériel peut prendre beaucoup plus de temps à traiter qu'un correctif logiciel. En outre, le déploiement d'un correctif devant être déployé sur les appareils peut nécessiter plus de temps qu'un correctif logiciel du serveur.

Ligne directrice 3 sur le maintien des logiciels à jour : Les mises à jour de sécurité logicielles sont l'une des choses les plus importantes qu'une entreprise peut faire pour protéger ses clients et l'ensemble de l'écosystème technique. Les vulnérabilités découlent souvent de composants logiciels qui ne sont pas considérés comme liés à la sécurité. Par conséquent, il est essentiel que tous les logiciels soient à jour et bien gérés. Des correctifs peuvent être envoyés aux appareils de manière préventive, souvent dans le cadre de mises à jour automatiques, qui peuvent supprimer des vulnérabilités de sécurité avant qu'elles soient exploitées. La gestion peut être complexe, surtout s'il y a des mises à jour du Cloud, d'appareils et d'autres services à traiter. Par conséquent, un plan de gestion et de déploiement clair est essentiel, tout comme la transparence vis-à-vis des consommateurs au sujet de l'état actuel de la prise en charge de la mise à jour.

Dans de nombreux cas, les mises à jour du logiciel de publication dépendent de plusieurs autres organisations, comme les fabricants de sous-composants. Ce n'est pas une raison pour retarder les mises à jour - L'objectif du Code de bonnes pratiques est d'encourager des changements positifs en matière de sécurité tout au long de la chaîne d'approvisionnement de logiciel. Dans certaines situations, l'application de correctifs aux appareils n'est pas possible. Certains appareils ultra-limités peuvent entrer dans cette catégorie et, pour ceux-ci, un plan de remplacement doit être en place et clairement communiqué au consommateur. Ce plan doit préciser un calendrier indiquant à quel moment les

technologies devront être remplacées et, le cas échéant, la fin de la prise en charge du matériel et des logiciels.

Il peut être essentiel pour les consommateurs qu'un appareil continue de fonctionner. C'est pourquoi une mise à jour ne doit pas avoir d'incidence sur le fonctionnement d'un appareil, dans la mesure du possible. En particulier, les appareils qui remplissent une fonction de sécurité ne doivent pas être complètement éteints dans le cadre d'une mise à jour ; une fonctionnalité minimale du système doit être disponible, par exemple le maintien d'un système de chauffage ou d'une alarme antivol. Les fabricants de ces types d'appareils doivent également envisager d'adopter une architecture plus résiliente.

Il est important d'être conscient que les mécanismes de mise à jour de logiciels sont un vecteur d'attaque, et il faut s'assurer de leur sécurisation.

Ligne 5 sur la communication sécurisée : La pertinence des contrôles de sécurité et de l'utilisation du chiffrement dépend de nombreux facteurs, y compris le contexte d'utilisation.[9] Comme la sécurité est en constante évolution, il est difficile de donner des conseils normatifs sur les mesures de chiffrement sans risquer que ces conseils deviennent rapidement obsolètes. Les responsables de la mise en œuvre doivent s'assurer que leur produit peut répondre aux besoins des utilisateurs tout en restant résilient aux attaques portant sur le chiffrement.

Ligne directrice 7 sur l'assurance de l'intégrité des logiciels : Si un appareil IdO détecte que quelque chose d'inhabituel s'est produit concernant son logiciel, il doit être en mesure d'informer la bonne personne. Dans certains cas, les appareils peuvent avoir la capacité d'être en mode d'administration - par exemple, il peut y avoir un mode utilisateur pour un thermostat dans une chambre qui empêche les autres réglages d'être modifiés. Dans ces cas, une alerte à l'administrateur est appropriée car cette personne a la capacité de réagir à l'alerte.

Ligne directrice 9 sur la résilience aux pannes des systèmes : L'objectif de cette ligne directrice est d'assurer le maintien et l'exécution des services IdO, car les appareils IdO font de plus en plus partie de la vie quotidienne des consommateurs, y compris dans le cadre de fonctions concernant la sécurité personnelle. L'impact sur la vie des consommateurs peut être primordial si, par exemple, une connexion Internet est perdue pour une porte connectée et que quelqu'un reste bloqué à l'extérieur. Un autre exemple est un système de chauffage domestique qui s'éteint à cause d'une attaque DDoS contre un service Cloud. Il est important de noter que d'autres règlements liés à la sécurité peuvent s'appliquer, mais l'essentiel est d'éviter que des pannes soient à l'origine de ces [problèmes]

[9] Des conseils sont disponibles, notamment ceux du NCSC à l'adresse https://www.ncsc.gov.uk/guidance/tls-external-facing-services.