CAP'TRONIC
Systèmes électroniques et logiciel embarqué

PME : COMMENT MAÎTRISER LA CYBERSÉCURITÉ DE VOS OBJETS ET SYSTÈMES CONNECTÉS.

DGE
DIRECTION GÉNÉRALE DES ENTREPRISES

NANOELEC.

Guide sous la direction éditoriale de Jean-François Baillette,
dirigeant de G-Echo et Claude Vittoria, ingénieur conseil
CAP'TRONIC.

Recueil et rédaction des témoignages : Jean-François Baillette,
Vincent Lagnier et Claude Vittoria.

Nous remercions l'ensemble des personnes interviewées pour
leurs disponibilités et leurs avis éclairés.

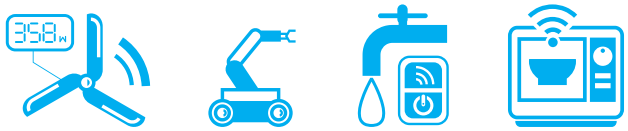
Rédactions des chapitres : Jean-François Baillette (G-Echo),
Alain Briton (CAP'TRONIC), Yohann Desiles (CAP'TRONIC),
Saghar Estehghari (Cybersecura), Joël Heslaut (Cabinet Nemezys),
Jean-Philippe Malicet (CAP'TRONIC), Laurent Meyer (Digitam),
Gérard Péliks (CyberEdu), Bernard Roussely (Cyberens),
Sébastien Salas (CAP'TRONIC), Richard Salvetat (CAP'TRONIC),
Assia Tria (CEA-Tech), Claude Vittoria (CAP'TRONIC).

Imprimé en décembre 2017 par Aprime Act à Villeurbanne.
Conception graphique Violaine Cleyet-Marrel.

Crédits photos : Thales, CyberEdu,
Picturetank - Gaillardin, G-ECHO, DRUST, Cyberens, Bretagne
Développement Innovation, Préfecture de Police de Paris, NeoTech
Assurance, Gendarmerie Nationale, Nemezys, CEA-TECH, Cybersecura, CEA,
SERMA safety&security, Oppida, Digitam, CAP'TRONIC, Shutterstock.

Contact et questions à guide@captronic.fr

SOMMAIRE



PRÉAMBULE

Les avancées technologiques dans le monde de la microélectronique ont donné lieu à des systèmes embarqués de plus en plus intelligents, pouvant prendre des décisions critiques, et ce tout en devenant de plus en plus connectés sur des réseaux ouverts sur le monde.

L'émergence et la croissance de l'Internet des Objets deviennent ainsi un vecteur puissant de création de valeur pour les entreprises. De nouveaux services sont inventés et proposés chaque jour en B2C et B2B. Les prévisionnistes annoncent que ces centaines de milliers de services nécessiteront de connecter des milliards d'équipements entre eux d'ici 10 ans !

Pour tenir cette promesse et se déployer massivement, cette formidable vague devra s'appuyer sur des systèmes sécurisés.
Cette thématique étant vaste, nous nous concentrons ici, volontairement, sur la protection de la chaîne de valeurs déployée sur le terrain ; objets connectés et passerelles de communication, matériels, applications, supports et protocoles de communication.

Après les guides ***"Prendre le virage des objets connectés"***, ***"Ils ont pris le virage des objets connectés / 10 retours d'expérience en B to B"*** et ***"Quelle méthodologie pour réussir votre projet électronique",*** ce guide a pour objectif de vous présenter les bonnes pratiques à mettre en œuvre pour assurer la sécurité de vos produits connectés. Il vous permettra de structurer votre démarche cybersécurité en vous posant les bonnes questions, de comprendre toutes les dimensions à considérer en matière de sécurité, de vous donner un panorama des solutions existantes et des différents référentiels normatifs et juridiques ainsi que de vous informer sur les partenaires qui pourraient vous aider.

Il vous fournira plus particulièrement les clés de la stratégie à adopter sur les questions suivantes :

- **Garantie de confidentialité :** comment garantir le caractère confidentiel (voir privé) des données émanant de ces objets et transitant sur les réseaux de communication ?
- **Garantie d'authenticité :** pour le récepteur des données, comment être sûr de la non modification des données depuis l'appareil émetteur ?
- **Garantie d'intégrité :** comment garantir qu'un appareil reste dans une configuration contrôlée tout au long de son cycle de vie ?
- **Comment communiquer sur les garanties** offertes par ces systèmes pour obtenir la confiance des clients & utilisateurs ?

AVANT-PROPOS

INTERVIEW

Stanislas de Maupeou
VP Strategy & Marketing
THALES

Pourquoi la cybersécurité est-elle une problématique stratégique pour les grandes comme pour les petites entreprises ?

Il n'y a pas de petite ou grande entreprise face à la cybercriminalité : tout le monde est concerné car nous sommes dans un monde en réseau. Aujourd'hui, sous l'impulsion des réglementations et des attaques, tous les acteurs économiques prennent conscience des risques du tout numérique lorsqu'ils ne sont pas maîtrisés. La cybersécurité doit devenir une activité stratégique pour toute entreprise qui trouvera son intérêt à traiter de cette problématique.

D'un point de vue légal tout d'abord, avec l'entrée en vigueur, en mai 2018, du Règlement Général Européen sur la Protection des Données (RGPD), qui prévoit de fortes amendes en cas de non-conformité. Mais on peut aussi citer bien entendu la Loi de Programmation Militaire qui impose des règles particulières pour les Opérateurs d'Importance Vitale, qui ne sont pas tous des grandes entreprises.

Commercialement ensuite, un produit analysé ou sécurisé par un tiers peut constituer un vrai différentiateur business car cela apporte l'indispensable confiance, qui peut se voir concrétisée par exemple par l'obtention d'une certification de type CSPN (Certification de premier Niveau). La sécurité informatique des produits, solutions et développements réalisés par les PME tout comme la sécurité de leurs propres systèmes d'information vont devenir des prérequis à leur développement, souvent directement lié à la transformation numérique de notre société.

La cybersécurité nécessite-t-elle un investissement important pour des PME ?

Le monde numérique évolue rapidement mais la sécurité n'est un défi inatteignable pour les PME, ni économiquement, ni techniquement! Appliquons les bonnes pratiques maintenant plutôt que d'avoir à le faire dans l'urgence en cas d'attaque. Attendre augmente toujours le coût et les attaques ne concernent pas que les autres..... Un certain nombre des attaques récentes aurait pu être stoppé en respectant des fondamentaux qui sont une première marche accessible à tous y compris aux PME. Prendre connaissance des guides de l'ANSSI et appliquer notamment les règles d'hygiène essentielles sont à la portée de tous : mettre systématiquement à jour ses applications ; avoir une politique de mot de passe ; sensibiliser les collaborateurs ; réaliser des sauvegardes régulières. Autant de règles simples, efficaces et peu couteuses, qui garantissent un premier niveau de sécurité qui peut faire la différence.

Avec l'avènement de l'Internet des objets (IoT), les attaques ne viennent plus seulement des systèmes informatiques traditionnels mais aussi des objets connectés, pour lesquels les règles d'hygiène doivent s'appliquer également en fonction des risques identifiés. Comme par exemple :

- La réalisation d'une analyse de risques en amont pour identifier les menaces et pouvoir y répondre correctement (fixer une feuille de route sur les points essentiels des données à protéger et des attaques à prévenir afin de prendre au plus tôt les décisions structurantes pour le produit tel que les mécanismes de cybersécurité à mettre en œuvre);

- Le contrôle de l'intégrité des firmwares pour en détecter toute modification (le maintien des conditions de sécurité d'un produit qui nécessite de réaliser des actions de veille régulière est un vrai challenge émergent);

Le chiffrement des données stockées et celles échangées pour garantir leur confidentialité. Et il existe des solutions accessibles, efficaces et performantes! On peut citer, en particulier, Vormetric, solution proposée par Thales, qui permet aisément de protéger la donnée

- Des processus doivent être mis en place au sein de l'entreprise pour garantir des environnements de confiance et assurer une traçabilité du développement (ne pas négliger de réguliers audits de code).

Quelles sont les attaques qui peuvent viser les PME ?

L'erreur serait de ne considérer que des attaques cyber de type gouvernemental comme Snowden tout en se disant : « cela ne me concerne pas ». Les attaques « communes » auxquelles tout le monde est confronté sont le vol de données personnelles, l'installation de Ransomware afin de faire chanter les victimes en leur extorquant de l'argent pour qu'elles accèdent à nouveau à leurs données (cas par exemple du récent malware Wannacry). Les attaques peuvent aussi viser à provoquer des dysfonctionnements. Dans un monde en réseau et massivement interconnecté, vos systèmes peuvent se retrouver victimes d'attaques sans avoir été directement visés (exemple des défigurations de sites internet).

J'encourage les chefs d'entreprise à penser qu'en investissant dans la cybersécurité, ils protègent la valeur de leur entreprise et garantissent de bonnes conditions à son développement. La cybersécurité n'est certes pas une fin en soi, mais viendrait-il à l'idée d'un dirigeant de ne pas investir pour protéger ses locaux ? La cybersécurité c'est notamment la protection de la donnée qui est « l'or noir » du 21e siècle !

La protection parfaite n'existe pas, quelle que soit la taille de l'entreprise et les moyens mis en œuvre. Toutefois, des mécanismes de défense efficaces créant de la résilience peuvent permettre de décourager ou de ralentir un attaquant potentiel... de manière suffisante pour protéger correctement l'entreprise.

1

CONTEXTE.

LA SÉCURITÉ, CRÉATRICE DE VALEUR !

1.1 TOUT LE MONDE EST POTENTIELLEMENT CONCERNÉ, N'AYEZ PAS PEUR, POSEZ-VOUS LES BONNES QUESTIONS

1

La totalité des marchés impactés

Tous les marchés sont potentiellement impactés par les cyberattaques.

Fonctionner en réseau fermé et isolé ou avec des protocoles propriétaires n'est pas un gage d'invulnérabilité.

Ce n'est pas parce qu'on n'a rien vu se passer sur un marché donné qu'aucune attaque notable n'a véritablement eu lieu. Pour des questions d'image, des acteurs agissant sur vos marchés, des concurrents proches ont pu choisir d'étouffer d'éventuelles failles, attaques et/ou fuites de données. Parfois même, suite à des transactions ou au paiement de rançons auprès des attaquants.

Des profils d'attaquants multiples

Les hackers ne sont que la partie immergée et médiatique de l'iceberg.

Dans beaucoup de cas les cyberattaques proviennent d'employés en interne ou de concurrents directs dans le cadre d'espionnage industriel ou de velléité de nuire.

Des mobiles d'attaques nombreux

Peu importe votre marché, les ressorts qui poussent un agresseur à lancer une attaque sont nombreux.

Les mobiles peuvent être d'ordres commerciaux : il s'agit d'attenter à la réputation sur le marché d'une société que l'on souhaite voir décrédibilisée ou affaiblie. Exemple de l'attaque boursière de la société San-Jude Medical[1].

Toujours dans une perspective de visée économique et financière, l'espionnage de la concurrence, l'appât du gain, une demande de rançon, la revente de données personnelles sur un marché noir ou encore la mise à l'arrêt temporaire des capacités de travail d'un concurrent sont des mobiles couramment observés[2].

La sécurité, un standard bientôt demandé

Que cela soit par les autorités compétentes ou directement par vos clients, la cybersécurité de vos objets ou systèmes connectés deviendra très rapidement un standard à adopter sous peine de se voir éjecté du marché visé. C'est déjà une obligation sur certains marchés auprès de grands comptes d'obtenir des certifications comme la certification ISO27001[3].

En parallèle, le législateur semble aujourd'hui montrer une vraie volonté pour être moteur sur ces sujets.

Des coûts associés à une cyberattaque non négligeables

L'entreprise est responsable des données qu'elle détient qu'elle en soit propriétaire ou non.

En dehors des données personnelles (dont l'usage est encadré par la CNIL en France), les données médicales sont certainement les informations les plus sensibles. La législation est très stricte à ce sujet, en Europe, mais également à l'international. Les sanctions en cas de diffusion peuvent s'avérer très lourdes.

En ce qui concerne les objets connectés qui inondent désormais tous les marchés, il va s'agir de ne pas être le premier à défrayer la chronique ni de constituer un cas d'école[4].

(1) https://www.g-echo.fr/20161005-iNovia-Slides.html

(2) http://www.lavoixdunord.fr/130177/article/2017-03-10/l-usine-renault-l-arret-lundi-mardi-et-peut-etre-mercredi

(3) https://www.nolimitsecu.fr/methodologie-d-evaluation-du-niveau-de-securite-des-prestataires-de-services-it/

(4) https://www.g-echo.fr/20161117-Slides.html

1.2 LA SENSIBILISATION À LA SÉCURITÉ DES DONNÉES NUMÉRIQUES, UNE ACTION POUR TOUS

La sécurité est l'affaire de tous et de chacun a-t-on l'habitude d'entendre. C'est particulièrement vrai pour la sécurité de l'Information et des systèmes d'Information, car qui accède à l'information numérique détient une parcelle de pouvoir sur cette information et les éléments matériels qui la contiennent sont très souvent reliés entre eux par un ou plusieurs réseaux, avec ou sans fils.

Les objets connectés, qui se chiffrent déjà par milliards dans le monde et dont le nombre va encore exploser ces prochaines années, peuvent constituer des vecteurs d'attaque foudroyants, d'autant plus si ces objets connectés ne sont pas conçus avec une « security by design » ou « by default ».

Mais dans la chaîne de sécurité que doit présenter tout système de données numériques, le point le plus faible, et qui constitue, bien souvent, le point d'entrée le plus utilisé par les attaquants, reste encore l'utilisateur. Il convient donc de sensibiliser cet utilisateur aux dangers du cybermonde et lui faire comprendre que ce n'est pas parce qu'un objet qu'il détient lui est familier, comme par exemple sa montre connectée, son bracelet qui détecte ses paramètres biologiques, son téléviseur intelligent..., que cet objet si familier ne présente aucun danger, pour lui et pour les autres.

Et bien entendu, la sensibilisation à la sécurité des données numériques remontées par les capteurs, utilisées par les actionneurs, stockées dans des lacs de données d'où elles peuvent être corrélées pour fournir des éléments exploitables, doit être, comme nous l'avons écrit, l'affaire de tous et de chacun. La sensibilisation doit donc être suivie par tous à tous les niveaux de la hiérarchie d'une organisation.

Toutes sortes de sensibilisations existent pour adresser l'ensemble d'une organisation. Le secret de l'efficacité de ces sensibilisations réside dans l'implication de ceux qui les suivent, car il est à redouter, surtout pour les sensibilisations imposées, que les participants les ressentent comme une action inutile et donc comme une perte de temps.

« Dis-le-moi et je l'oublie ; montre-le-moi et je le retiens; implique-moi et je le comprends » dit un proverbe. C'est particulièrement vrai pour les sensibilisations aux dangers que présentent les objets connectés, qui sont en général d'autant moins redoutés qu'ils sont familiers. Donc, dans les sensibilisations, il faut prévoir des démonstrations qui percutent, et si possible certaines avec les propres objets des participants.

1.2 LA SENSIBILISATION À LA SÉCURITÉ DES DONNÉES NUMÉRIQUES, UNE ACTION POUR TOUS

1

INTERVIEW

Gerard Peliks
Président

CyberEdu

Les attaques récentes font prendre conscience que les données numériques sont exposées aux plus grands dangers, et les PME ont compris que si l'on ne peut complètement éliminer le risque, on peut le réduire...et même l'assurer. Des experts mutualisés ou des solutions tierces peuvent être accessibles pour les PME, par exemple en confiant sa sécurité à un Security Operation Center (SOC) externe. Il faut à minima avoir en interne des personnes au moins capables de discuter avec ces experts sécurité.

Au sein d'une PME, la meilleure place du responsable de la sécurité du numérique (RSSI) est au plus près de la direction générale. La cybersécurité est un métier à part entière. Si on n'a pas les moyens d'employer une compétence en interne, c'est une bonne idée de s'attacher une compétence externe sur le sujet en bordant en particulier la confidentialité et l'intégrité des données sensibles, mais également la réversibilité avec un contrat à regarder de très près.

Une entreprise a été inquiétée suite à un vol de données ensuite vendues sur internet après une cyberattaque.Le PDG et la moitié du Conseil d'Administration ont été remerciés. La direction assume la responsabilité en cas de fuites de données personnelles par exemple et cela sera encore plus grave quand le RGPD sera mis en application.

L'importance de la formation doit être soulignée. Les conférences sont indispensables mais n'ont pas autant d'impact que si l'on arrive à montrer les dégâts potentiels, voire à « impliquer » les employés en interne. Une fois qu'on a subi une cyberattaque comme des infections par vers/virus, on vit différemment la gestion du risque. Aujourd'hui il y a pénurie d'experts dans le domaine. Les enseignements existent mais en trop petit nombre. La cybersécurité ne devrait pourtant pas être que l'affaire de spécialistes mais bien de toutes les formations supérieures. L'ANSSI édite un guide d'hygiène qui permet de contrer 80% des menaces...Pour les 20% qui restent, c'est l'affaire d'un expert.

Le label CyberEdu a pour objectif de référencer les formations non spécialisées en sécurité du numérique qui intègrent à leur cursus des éléments de sensibilisation à la sécurité fournis par l'association CyberEdu.

L'association CyberEdu propose une labellisation des formations de l'enseignement supérieur mettant en œuvre les principes de sa démarche pédagogique de la sécurité du numérique.

1

1.2 LA SENSIBILISATION À LA SÉCURITÉ DES DONNÉES NUMÉRIQUES, UNE ACTION POUR TOUS

© Picturetank - Gaillardin

Vincent Strubel
Sous-directeur Expertise

INTERVIEW

Qu'est que l'ANSSI ?

L'ANSSI, l'Agence Nationale de la Sécurité des Systèmes d'Information, est une agence rattachée aux services du Premier ministre employant un peu plus de 500 personnes. En tant qu'autorité nationale en matière de cybersécurité et de cyberdéfense, elle assure plusieurs missions à destination en priorité de l'Etat et ses administrations mais aussi envers les Opérateurs d'Importance Vitale (OIV). Ses actions couvrent la prévention, la détection et la réaction. Il est bon de rappeler que la mission de prévention de l'ANSSI est composée de recommandations applicables à tout acteur du numérique.

Votre rôle au sein de l'ANSSI ?

J'assume le pilotage de la sous-direction Expertise qui a pour mission d'identifier des solutions de sécurité répondant aux besoins de l'Etat et des entreprises. Pour se faire, la sous-direction labellise des produits, forme et conseille les administrations et les OIV. Notre objectif est également de diffuser l'information sur les bonnes pratiques (promotion des technologies, des produits et services de confiance, des systèmes et des savoir-faire nationaux).

Une mission importante de la sous-direction Expertise consiste à assurer un travail de recherche et de veille avec des laboratoires internes qui publient régulièrement des articles sur les challenges à venir face à l'évolution de l'état de la menace.

Quels conseils donner aujourd'hui aux PME ?

Ne pas faire l'impasse sur le numérique et la cybersécurité. Les PME peuvent être, à divers titres (par exemple pour la protection des données personnelles), soumises à des contraintes réglementaires en matière de cybersécurité. Au-delà de ces contraintes, la bonne prise en compte des menaces informatiques peut être une question de survie pour une PME, une attaque sur son système d'information ou son produit phare pouvant avoir des conséquences catastrophiques.

Tout le monde est une cible pour la cybercriminalité : tout moyen informatique peut faire l'objet de vols de données ou être un vecteur d'attaque informatique. La sécurité des systèmes d'information et des produits est un enjeu déterminant.

Un guide pratique à destination des entreprises, réalisé en partenariat avec la CGPME, donne un certain nombre de recommandations et de conseils pratiques à mettre en œuvre : chiffrer les flux, ne pas utiliser la même clé, prévoir un mécanisme de mise à jour, tester ses produits...

1.2 LA SENSIBILISATION À LA SÉCURITÉ DES DONNÉES NUMÉRIQUES, UNE ACTION POUR TOUS

1

INTERVIEW / SUITE

Il faut bien comprendre que la sécurité d'un produit ne concerne pas que le développeur. Un dirigeant d'entreprise n'est pas un juriste, ni un économiste et pourtant dans son quotidien il conclut des contrats ou gère les ressources de sa société. Les dirigeants doivent se préoccuper de la sécurité informatique et comprendre les risques et enjeux associés, car il sera nécessaire d'arbitrer la conception d'un produit et de le faire en comprenant les risques, leurs sévérités et leurs occurrences. Un dirigeant peut se faire accompagner par des compétences externes, l'ANSSI labellise d'ailleurs des solutions techniques, des acteurs et des prestataires qualifiés pour avancer sur les sujets de la cybersécurité.

De plus, l'entreprise devrait faire auditer régulièrement son système informatique ou son produit afin d'entamer et de faire perdurer un processus d'amélioration continue. L'évaluation des processus internes ou des produits vis-à-vis de référentiels établis est un plus et une différentiation qui prend de plus en plus d'importance sur les marchés. La certification est obligatoire dans certains secteurs (par exemple pour les cartes bancaires) mais les acteurs agissant sur des secteurs où aucune certification n'est obligatoire devraient aussi passer des certifications afin de connaître les manques et failles de sécurité de leurs produits. Cela afin de décider avec tous les éléments en main des actions à mener pour établir un cercle vertueux d'amélioration.

Dans quelques mois, l'ANSSI va qualifier des prestataires de cloud ce qui permettra aux sociétés offrant des services connectés avec leur produit de sélectionner des prestataires offrant des infrastructures avec des garanties de sécurité.

Que faire si un produit ou son système d'information est victime d'une attaque ?

L'ANSSI assure avant tout un service de veille, de détection, d'alerte et de réaction aux attaques informatiques, au service de l'État et de ses réseaux avec une mission renforcée au profit des opérateurs d'importance vitale (OIV). Néanmoins plusieurs outils sont développés et mis à disposition pour tous les acteurs du monde de l'entreprise et du numérique. Ainsi, la plateforme « Cybermalveillance.gouv.fr », pilotée par le GIP ACYMA, un groupement d'intérêt public incluant des entreprises du numérique, propose un guichet d'orientation pour les PME rencontrant des problèmes de cybercriminalité et les aide à trouver des prestataires pour les assister. Lorsqu'une attaque massive sur un produit à lieu, la signalisation de l'attaque se fait depuis le site de l'ANSSI afin que le CERTFR la recense et diffuse les risques encourus aux utilisateurs ainsi que des recommandations actualisées régulièrement.

Par ailleurs, l'ANSSI est présente en région grâce à ses référents territoriaux qui ont pour mission de sensibiliser les acteurs territoriaux et acteurs économiques locaux. Comme ils ne peuvent pas répondre à toutes les PME en direct, l'approche choisie est de mener des actions avec les syndicats et associations professionnelles pour porter les bonnes pratiques auprès des membres.

1.3 LA FORMATION DE RÉFÉRENTS INTERNES, UNE NÉCESSITÉ POUR PROTÉGER SES DONNÉES NUMÉRIQUES ET SON SYSTÈME D'INFORMATION

INTERVIEW

Jean-François Baillette

G·ECHO
sécurité des systèmes d'information

www.g-echo.fr

La sécurité, ce n'est pas compliqué, il vous suffit de retenir 3+1 lettres:

- D pour Disponibilité,
- I pour Intégrité,
- C pour Confidentialité,

Et P/T/A pour Preuve, Traçabilité ou Auditabilité selon les auteurs.

Tout commence dans la recherche de la Disponibilité du service. Les industriels souhaitent que leurs systèmes ne « tombent pas en marche », mais fonctionnent correctement, incluant des modes dégradés lors d'évènements particuliers qui peuvent être ... des attaques. Il faut donc travailler dans une démarche systémique à laquelle collaborent toutes les forces vives de l'Entreprise. La prise de conscience doit se faire au niveau de la direction générale et impliquer toutes les parties prenantes avec une forme d'humilité et de bienveillance qui mène à une chaîne de confiance dans l'Entreprise.

La mise en sécurité d'une Entreprise et de ses produits passe par une écoute de l'environnement et de ses bruits faibles, un apprentissage des bonnes pratiques, métiers, techniques indispensables à la mise en œuvre d'une posture adaptée à un développement durable et sans risque de l'activité.

Les formations en sécurité des systèmes d'information concernent tous les postes et peuvent être renforcées également par des jeux sérieux, des audits réels ou encore des entraînements : sensibilisation aux risques pour les directions générales, démonstrations d'attaque type "Arnaque au président" pour les équipes financières et administratives, test d'intrusion pour les équipes réseau, téléphonie, métier,... Dans tous les cas, des tests « grandeur réelle » sont également à prévoir comme des simulations de crise et de mise en œuvre de plans de continuité ou de reprise d'activité. Ces entraînements permettent de mettre tout le monde en situation et d'être prêts le jour où un sinistre se produit. Et ce n'est pas accessoire ... ces entraînements permettent également de créer une cohésion dans les équipes tout en optimisant les processus en place.

Difficile de trouver les bonnes solutions en cybersécurité : À travers des questionnaires ciblés, G-echo propose du support à ses clients pour leur faire accéder aux offres adaptées du marché : audit/conseil/expertise, sensibilisations/formations/aide au recrutement, solutions de cybersécurité.

De la TPE au grand groupe, G-echo propose une approche unique pour améliorer le niveau global de cybersécurité de chaque entreprise.

Mais la sensibilisation de tous n'est qu'une partie du problème. A moins d'externaliser la sécurité de son information vers des prestataires de service, ce qui peut poser des problèmes techniques et juridiques qu'il faut maîtriser et qu'il faut établir clairement sur un contrat, il convient de s'attacher des personnes ayant l'expertise en sécurité des données numériques, dans le domaine de l'Internet des Objets. Ces experts doivent maîtriser le volet technique de la sécurité, mais également les implications juridiques. Le règlement européen RGPD (ou GDPR en anglais), par exemple, nous rappelle les règles quant à la protection des données personnelles qu'une organisation détient, manipule ou transmet. Quand ce règlement sera appliqué à tous les pays d'Europe, en mai 2018, une perte de données personnelles sera punie de lourdes sanctions.

Il est donc plus que temps de s'attacher un responsable des données personnelles (un DPO) pour se mettre en conformité, le plus tôt possible et avant le 25 mai 2018, d'autant plus que dans le secteur des objets connectés, la fuite ou le vol des données personnelles est un risque très réel.

1.3 LA FORMATION DE RÉFÉRENTS INTERNES, UNE NÉCESSITÉ POUR PROTÉGER SES DONNÉES NUMÉRIQUES ET SON SYSTÈME D'INFORMATION

1

PAROLE DE PME

Nous sommes venus à ces thématiques de la cybersécurité car nous visions un produit dans un contexte d'usage comportant un certain nombre de risques : données personnelles collectées, protection du conducteur en jeu (ne pas modifier le comportement du véhicule, le boitier doit rester un observateur) et possibilité qu'une personne malveillante puisse prendre le contrôle du véhicule. Une dégradation de la sécurité du client peut définitivement empoisonner l'image de marque. Etre innovateur dans le domaine est un gros plus sur beaucoup d'aspects.

En effet, en B2B, la prise en compte du risque cyber tire le business, les partenaires sont rassurés et cela est même devenu une condition nécessaire, notamment pour les assureurs, d'intégrer les technologies à l' « état de l'art» contre la cybercriminalité. Concernant spécifiquement les investisseurs, il n'y a pas non plus d'intransigeance absolue sur la partie cybersécurité de leur part. Les investisseurs challengent plutôt sur le délai de mise sur le marché du produit et les fonctions nouvelles apportées. La cybersécurité devient un challenge car sa prise en considération allonge indéniablement le temps et les efforts de développement. C'est un passage obligé pour mettre un produit sécurisé sur le marché.

La première étape de notre démarche a consisté en un audit pour savoir où on en était. Il faut prendre conscience (prise de conscience dans les équipes notamment) que des défauts entrainent souvent un redesign. Oui c'est lourd, oui ça ralentit la conception, mais ça permet d'avoir un produit de haute qualité et sécurisé, cela doit être compris par tous au quotidien.

Le pentesting doit devenir une étape de la conception produit. Chez Drust, une personne a été dédiée au pentesting (nous avons mis en place un véritable processus là dessus). Au passage, nous avons aussi une personne à temps plein pour gérer la problématique du traitement des données personnelles en relation avec la CNIL (les clients sont sensibles sur l'aspect des données personnelles).

La cybersécurité est un travail de fourmi, il ne faut pas de temps mort ou d'arrêt dans un cycle, il est en effet primordial d'arbitrer très régulièrement entre les priorités (en regard de la faisabilité, des délais, des coûts,...) voire reporter au conseil d'administration les plans d'actions. L'audit de sécurité - à considérer très tôt dans le processus - a permis d'établir une feuille de route des choix structurants pour le produit.

drust
Be a superdriver

AKOLYT
Your personal co-driver

Fabriqué en France, la solution de DRUST consiste en un boîtier connecté ainsi qu'une application mobile ludique permettant de maîtriser sa conduite et la maintenance de sa voiture. Une fois branché sur le port diagnostic dit « OBD » (On-Board Diagnosis) de la voiture, le boîtier se synchronise en Bluetooth avec l'application communautaire.

PAROLE D'EXPERT

L'avantage de travailler avec une startup comme Drust c'est la relation simple des séances de travail, les conseils n'interfèrent pas avec des procédures existantes. Mes interlocuteurs étaient disponibles et impliqués avec l'envie de comprendre et d'aller au résultat.

Grande implication, volonté d'exposer, de faire, de vérifier, ce sont les clés du succès.

L'expert doit avoir un rôle rassurant durant l'accompagnement, essayant de toujours expliquer la démarche, même si les problèmes sont profonds et complexes à résoudre.

Quelques milliers d'euros pour un diagnostic représente un réel investissement pour une PME qui a la volonté de réussir l'essai. En terme de démarche, il est nécessaire de hiérarchiser la menace, à savoir à un niveau de menace associer le coût de la contre mesure. Cette classification fait partie du devoir de conseil, on ne peut pas cacher les choses et il est nécessaire de rester conscient des coûts.

La cybersécurité ce sont aussi les risques organisationnels à aborder et les politiques à mettre en place. La structuration est importante surtout pour une entreprise qui est amenée à grossir. Les mises à jour OTA sont aujourd'hui primordiales.

Mon dernier conseil à donner à une PME pour adresser les alertes de sécurité ? Effectuer des mises à jour transparentes pour l'utilisateur en employant l'état de l'art actuel.

Bernard Roussely

Cyberens
Technologies & Services

1.4 S'INFORMER, SE FORMER ... QUELQUES RESSOURCES

Des formations de tous niveaux sont proposées, allant d'une sensibilisation générale d'une journée à des cours particularisés de plusieurs jours, par exemple dans le domaine de la e-santé, de la ville intelligente, de la distribution d'électricité ou de la domotique. Il existe également des cursus de plusieurs mois dans le cas de formations diplômantes. Les formations généralistes ont pour principal but de faire comprendre en quoi les objets connectés vont révolutionner les technologies et les marchés d'un point de vue marketing et socio-économique, alors que des formations plus techniques s'attacheront au design des objets et à la conception de solutions mettant en œuvre les protocoles réseaux et les algorithmes de chiffrement et d'échanges des clés ainsi qu'aux standards les plus courants.

Le Big Data, partie intégrante du concept des réseaux d'objets connectés, pour stocker, corréler et visualiser les données remontées par les objets devra également faire partie de ces formations, ainsi que les notions de base sur les Blockchains qui pourraient devenir incontournables pour établir une confiance distribuée sur les transactions sur l'Internet. L'aspect juridique, en particulier celui posé par l'accumulation des données à caractère personnel, confronté au règlement européen (RGPD) qui va être mis en application en mai 2018, devra également être inclus dans les formations.

Ce guide se limite à mentionner, sans émettre de conseils particuliers ni d'appréciations, quelques formations sur les objets connectés. On trouve dans les offres publiques et privées des parcours de formation et des outils complets de renforcer ses compétences :

- De nombreux guides sont proposés par l'ANSSI sur son site web (règles d'hygiène, guide PME, guide export, ...),
- L'association CyberEdu met à disposition des supports de cours pour les formateurs - ces supports sont accessibles pour tout un chacun qui a des compétences en informatique, réseau et télécom, emparez-vous en ![(1)]
- Des ressources gratuites (MOOC, vidéos en ligne, outils de test d'intrusion comme Kali Linux, ...) permettent de renforcer vos nouvelles connaissances par la pratique,
- Des clubs et associations (CLUSIF et CLUSIR, OSSIR/Resist, Club 27001, Club EBIOS, ...) permettent de participer à des retours d'expérience et de rencontrer les experts du secteur,
- Le CERT-FR lance des alertes et des bulletins de sécurité, des veilleurs et des blogueurs diffusent également de l'information gratuitement sur les réseaux sociaux, abonnez-vous !
- Des podcasts dédiés existent (exemple : NoLimitSecu, LeComptoirSecu, ...),
- Enfin, tournez-vous vers des formations certifiantes pour obtenir le "plus" qui renforcera votre crédibilité sur vos marchés.

Parmi ces formations, citons le Certificat d'Enseignement Supérieur "Internet des objets (IoT), conception de solutions" délivré par Télécom Evolution, à Télécom ParisSud, Evry pour se former aux technologies des objets connectés, en incluant bien sûr leur sécurité. L'Ecole polytechnique propose une formation certifiante en ligne "Internet of Things / Objets connectés". Des écoles d'ingénieurs, de plus en plus nombreuses ont ajouté des formations sur les objets connectés dans leur enseignement initial comme, sans être exhaustif, l'ECE (Paris), l'ENSIM (Le Mans), l'ENSIMAG (Grenoble), l'INP Esisar (Valence), l'ESEO (Anger), l'ESIEA à Ivry, l'ISEP (Paris), EMSE CMP (Gardanne) ...

Pour les formations initiales, le label SecNumedu permet de repérer les formations labellisées par l'ANSSI [(2)]. A noter en particulier la matrice de compétences pour les niveaux de formation licence et maîtrise[(3)]. La liste des établissements est disponible sur le site de l'ANSSI[(4)].

(1) https://www.ssi.gouv.fr/administration/formations/cyberedu/contenu-pedagogique-cyberedu/

(2) https://www.ssi.gouv.fr/entreprise/formations/secnumedu/

(3) https://www.ssi.gouv.fr/uploads/2016/05/anssi-secnumedu_f-02_v1-matrice_competences_metiers.xlsx

(4) https://www.ssi.gouv.fr/particulier/formations/formation-et-cybersecurite-en-france

1.4 S'INFORMER, SE FORMER ... QUELQUES RESSOURCES

Pour les formations non spécifiques en sécurité, le label CyberEdu permet de repérer celles qui ont introduit dans leur cursus une composante Cybersécurité[1].

Et comme dans une stratégie d'Entreprise, il peut être nécessaire d'acquérir de nouvelles sociétés pour accélérer son développement, il peut être utile ou nécessaire de faire l'acquisition de nouvelles compétences pour intégrer la fonction sécurité dans votre organisation. Une politique de sourcing (externalisation de certaines fonctions) ou de recrutement adaptée vient ensuite renforcer la GPEC (Gestion Prévisionnelle de l'Evolution des Compétences) que vous aurez planifiée pour prendre la vague de la cyber-sécurité ...

Exemples de parcours de formation pour les SI et l'embarqué :

- ***Pour devenir Ingénieur en sécurité/implémentation*** vous pouvez suivre un parcours sur les fondamentaux techniques de la SSI, la surveillance, la détection, la réponse aux incidents, et traiter l'aspect organisationnel (implémentation de l'ISO27001, gestion des risques avec ISO27005, environ 130 heures au total sur un an),
- ***Pour devenir auditeur sécurité,*** il vous faut découvrir les fondamentaux techniques de la SSI, savoir réaliser des tests d'intrusion et également les aspects sécurité offensive, et intégrer les aspects gouvernance de la SSI (avec l'ISO 27001 pour la partie processus, l'ISO27005 Risk pour l'analyse de risques, environ 130 heures au total sur un an),
- ***Si vous souhaitez devenir Responsable sécurité*** commencez par les fondamentaux techniques, sachez implémenter la norme du secteur (ISO27001), gérer les risques (ISO27005), intégrer les obligations et risques liés au droit de la Sécurité Informatique, et éventuellement ... la mise en œuvre de tableaux de bord (ISO 27004) ou encore le pilotage et la gestion des incidents de sécurité (au total environ 150 heures sur un an et demi),
- ***Pour devenir analyste sécurité*** apprenez les fondamentaux techniques, intégrez les dimensions du droit de la Sécurité Informatique, et les modalités pratiques pour la surveillance et la réponse à incidents + la gestion de crises en SSI (une centaine d'heures pour ce parcours).

Au-delà des formations classiques en SSI qui permettront de renforcer les compétences de chacun en fonction de sa mission dans l'organigramme, pour le sujet des systèmes embarqués et des systèmes communicants il est impératif de participer à des colloques, à la vie de clubs et associations spécialisés, ainsi qu'à des formations techniques pointues ou demander du support avec transfert de compétences de la part de professionnels reconnus.

Il faut vous intéresser à la protection de votre organisation (au sens juridique, brevets, commercial du terme), à la protection de votre système d'information (on parle souvent d'IT), à la protection de votre chaîne de production (que ce soit un processus de tests continus ou de la programmation in-situ / est-ce que quelqu'un peut l'attaquer ?), aux tests et validation en sécurité de vos produits, au maintien en condition de sécurité de vos produits ... Si je suis client de vos produits, je suis intéressé par recevoir des bulletins d'alerte si jamais on y trouvait une faille ...

(1) *https://www.cyberedu.fr/billets/2016/12/principe-de-la-labellisation-cyberedu/*

(2) *http://www.nanoelec-formations.fr/formations-en-management-mecatronique-cyber-securite*

Soyez également curieux : de nombreuses ressources et outils sont librement disponibles sur internet, des vidéos dans divers domaines et des MOOCs (cours en ligne) sont également disponibles pour comprendre certains aspects comme la gestion des risques au niveau de l'Entreprise et de son système d'information, la production de systèmes tolérants aux attaques, la protection des composants, le chiffrement hardware, le stockage sécurisé, l'attaque/défense des systèmes, ... A noter aussi les formations mises en place dans le cadre de l'IRT Nanoelec par Grenoble INP, EPITA ou Grenoble Ecole de Management dans ce domaine[2]. Sans oublier les formations que le programme CAP'TRONIC propose en ciblant spécifiquement l'IoT, l'embarqué critique ou l'électronique!

Webographie

Les formations proposées sur l'IoT sont nombreuses, en voici quelques unes :

- Telecom Evolution : Certificat d'Etudes Spécialisées «Internet des objets (IoT), conception de solutions ***http://www.telecom-evolution.fr/fr/domaines/internet-des-objets***
- Ecole Polytechnique : Usages, opportunités, contraintes et limites de l'IoT ***http://www.objetconnecte.com/lecole-polytechnique-lance-une-formation-sur-les-objets-connectes/***
- Institut Cap Gemini : Objets connectés et Internet des objets ***http://www.institut.capgemini.fr/formation-objets-connectes-capgemini-institut_p216***
- CAP'TRONIC : Comprendre l'Internet des objets ***http://www.captronic.fr/FORMATION-Comprendre-l-Internet-des-objets.html***

1.5 FOCUS SUR LA FILIÈRE : PRESTATAIRES PUBLICS ET PRIVÉS PERTINENTS, STRUCTURES & AIDES MOBILISABLES

Au-delà du confort de la vie quotidienne et de la disponibilité de ces applications devenues parties intégrantes de nos vies, l'enjeu est économique. Il est désormais vital pour préserver les compétences, savoir-faire et avantages concurrentiels, en un mot la compétitivité et donc l'emploi, que les entreprises se protègent des attaques informatiques. L'impératif de cybersécurité concerne le parc informatique dans son ensemble, depuis le développement de la bureautique jusqu'à la conception du système industriel intégré à la chaîne de production. L'ANSSI accompagne les entreprises en fonction de leur profil par des actions de conseil, de politique industrielle et de réglementation afin de rendre disponibles des produits de sécurité et des services de confiance.

L'ANSSI offre de nombreuses ressources pour permettre aux sociétés de se sensibiliser à l'importance de la sécurité informatique et de trouver les prestataires qui leur permettront d'acquérir rapidement la compétence nécessaire à leur domaine. La publication essentielle, et qui fait référence dans le monde de la cybersécurité, est le guide d'hygiène informatique[1]. Ce guide présente les 42 mesures d'hygiène informatique essentielles pour assurer la sécurité de votre système d'information et les moyens de les mettre en œuvre, outils pratiques à l'appui.

L'ANSSI adresse également la sécurité des TPE/PME de manière pratique. En partenariat avec la CGPME, l'ANSSI a édité le « Guide des bonnes pratiques de l'informatique »[2]. Ce guide présente douze recommandations à destination des non-spécialistes, issues de l'analyse d'attaques réussies et de leurs causes.

La cybersécurité doit se fondre dans la vie de l'entreprise, la cybersécurité doit faire partie des projets de l'entreprise et des processus qui les dirigent. Le guide « Intégrer la sécurité numérique dans une démarche Agile » a pour objectif d'aider les organismes publics et privés à intégrer la sécurité numérique dans un projet Agile[3].

L'un des rôles de l'ANSSI est aussi de qualifier pour les administrations françaises des prestataires de confiance répondant à de hauts niveaux d'exigence[4]. Ces prestataires peuvent être sollicités par les entreprises françaises pour les accompagner dans leur projet et ainsi assurer que la cybersécurité répondra à des critères de qualité définis et audités régulièrement par l'ANSSI[5].

Ces prestataires certifiés agissent dans de nombreux domaines des systèmes informatiques, des services d'hébergement certifiés à l'audit des systèmes et produits informatiques d'une entreprise[6].

(1) https://www.ssi.gouv.fr/entreprise/guide/guide-dhygiene-informatique/

(2) https://www.ssi.gouv.fr/entreprise/guide/guide-des-bonnes-pratiques-de-linformatique/

(3) https://www.ssi.gouv.fr/entreprise/guide/integrer-la-securite-numerique-dans-une-demarche-agile/

(4) https://www.ssi.gouv.fr/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/

(5) https://www.ssi.gouv.fr/entreprise/qualifications/

(6) https://www.ssi.gouv.fr/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/

1.5 FOCUS SUR LA FILIÈRE : PRESTATAIRES PUBLICS ET PRIVÉS PERTINENTS, STRUCTURES & AIDES MOBILISABLES

1

INTERVIEW

Rémy DAUDIGNY
Directeur du Centre d'Évaluation de la Sécurité des Technologies de l'Information (CESTI)

THALES

Leader européen de la cybersécurité, Thales emploie environ 2000 spécialistes dans ce domaine et sécurise les systèmes informatiques critiques de plus de 130 clients. Parmi ses nombreuses activités de cybersécurité, Thales dispose d'une équipe de 40 personnes dédiée à l'expertise et l'évaluation de sécurité.

Cette équipe accueille depuis 1999 le CESTI Thales (Centre d'Evaluation en Sécurité des Technologies de l'Information), agréé par l'ANSSI pour la réalisation d'évaluations de sécurité matérielle selon les Critères Communs, jusqu'au niveau maximum (EAL7). Le CESTI Thales est agréé CSPN logiciel (Certificat de Sécurité de Premier Niveau) en 2007, ce qui lui permet alors de devenir le seul laboratoire à double compétence en France.

La CSPN peut être nécessaire pour obtenir la qualification ANSSI d'un produit, étape préalable à la mise au catalogue de certains types de produits au profit de l'administration française. Il s'agit également d'une certification très intéressante pour les PME.

Pour conserver son accréditation, le CESTI est audité par l'ANSSI tous les 2 ans, ce qui nécessite un effort constant de formation de ses équipes.

Le service réalise à la fois des expertises et des évaluations, ce qui constitue deux profils de missions bien différents. La mission d'expertise permet de tester la résistance aux cyberattaques de certains produits pour le compte du vendeur. L'évaluation vise quant à elle l'obtention d'une certification et est donc tripartite :

- le commanditaire qui fait évaluer le produit,
- l'évaluateur au travers d'un CESTI
- le certificateur qui éventuellement certifie le produit au vu des éléments fournis par le rapport technique d'évaluation (par exemple l'ANSSI dans le cadre des Critères Communs).

Il existe d'autres schémas d'évaluation que les Critères Communs, par exemple dans le monde des applications bancaires (internationales ou domestiques), ou encore de schémas spécialisés tel celui de GlobalPlatform qui permet la promotion de solutions de sécurisation de plateformes permettant par exemple le développement du paiement mobile.

Le rôle du CESTI est l'évaluation de la robustesse des fonctions de sécurité vis-à-vis des référentiels techniques promus par les différents schémas. Des experts internationaux établissent des grilles de cotations permettant de « noter objectivement » la complexité d'une attaque. L'évaluation permet donc d'apprécier la résistance d'un produit en fonction de la menace auquel il est confronté en phase opérationnelle. Un schéma définit une note minimale à atteindre en fonction d'un niveau de risque. Le CESTI cherche donc à trouver des failles dans le logiciel et le matériel, et à évaluer l'effort nécessaire pour mettre en défaut un mécanisme de sécurité du produit.

Evidemment quand les enjeux sont à la hauteur de la souveraineté d'un état, les moyens mis en œuvre pour découvrir des failles sont plus poussés : on peut ainsi procéder à l'amincissement du silicium d'une puce afin d'effectuer des micro tirs laser permettant de provoquer des erreurs pour obtenir une augmentation de privilège sur le composant ou créer une erreur cryptographique permettant de révéler des éléments secrets enfouis dans la puce.

En ce qui concerne les PME, il est possible d'être accompagné pour obtenir une certification CSPN sur ses produits. Cette certification, parfaitement adaptée aux PME, à la fois en matière de coûts et de délais de réalisation, permet d'obtenir une reconnaissance étatique ce qui constitue un différentiateur notable sur le marché de la sécurité.

Le CESTI de Thales propose d'accompagner les candidats à la CSPN par :

- Une aide à l'analyse de risque sur le produit (contexte d'utilisation, menaces sur le produits, hypothèses d'utilisations, obligations règlementaires, etc.)
- Une aide à la rédaction de la Cible de Sécurité, le « cahier des charges sécuritaire », qui synthétise l'analyse de risque et qui est un préalable à l'entrée en évaluation.
- Un accompagnement dans les démarches administratives.

Il est parfois difficile, notamment pour les PME, de définir précisément ce qui doit être protégé, et quels sont les évènements à redouter. D'où l'importance d'un accompagnement solide, dès la conception du produit. Un produit franchira le CSPN plus facilement si les développeurs ont du recul sur la problématique sécurité et s'ils consacrent un effort à la réflexion amont sur l'environnement du produit et la gestion des risques.

1.5 FOCUS SUR LA FILIÈRE : PRESTATAIRES PUBLICS ET PRIVÉS PERTINENTS, STRUCTURES & AIDES MOBILISABLES

INTERVIEW

Tiphaine Leduc
Chef de mission
Cybersécurité – BDI

BRETAGNE DÉVELOPPEMENT INNOVATION

Avec 130 entreprises cyber, 8000 emplois, 3000 étudiants formés et 200 chercheurs, la Bretagne s'impose comme une région de référence en cybersécurité. L'Ouest est particulièrement positionné sur des domaines d'expertise en cryptologie, microélectronique, architectures d'équipements de sécurité et de systèmes informatiques et industriels, analyse de composants logiciels et matériels, coopération matérielle / logicielle.

Une Cyber Valley ancrée en Bretagne

La Région Bretagne s'est dotée de moyens spécifiques visant à construire une véritable filière cyber autour de la recherche, de la formation et de l'innovation. Bretagne Développement Innovation (BDI) participe au développement du volet industriel de la cybersécurité, et en particulier de son tissu PME.

L'enjeu est de faciliter l'accès des PME de l'Ouest aux marchés de la cyber sécurité en France et à l'international et de diffuser la cyber sécurité dans des filières applicatives telles que les objets connectés, l'industrie, l'usine du futur, les smart grid, la santé, le véhicule.

Les actions menées portent sur un accompagnement global des entreprises, en visant :

- Le recensement des acteurs à travers un observatoire, annuaire accessible en ligne
- La promotion des entreprises dans les salons emblématiques du domaine
- Le soutien à l'innovation par l'émergence de projets collaboratifs nationaux ou européens
- L'animation de la communauté, avec des réunions mensuelles et des conférences
- La mise en relation qualifiée avec les grands industriels

L'Ouest au cœur de la dynamique nationale

L'ensemble des actions mises en place se fait en parfaite coordination avec les instances nationales, et tout particulièrement l'ANSSI.

En Bretagne, un chef de projet est dédié à cette filière. N'hésitez pas à contacter Tiphaine Leduc pour toute recherche et toute question.

Tiphaine Leduc

Chef de mission Cybersécurité – BDI

t.leduc@bdi.fr

Deux illustrations concrètes

Les cyber breakfast mensuels :

l'occasion pour la communauté des PME cyber de se retrouver pendant 2h autour de 3 volets :

- Prendre connaissance de l'actualité nationale (AAP nationaux), mise en place de la filière nationale et de l'observatoire
- L'actualité technique : comprendre les événements de sécurité apparus dans la presse
- L'ouverture sur un sujet connexe à la cyber : par exemple l'enjeu juridique de la cybersécurité, la mise en place d'assurance de cyber risques ou l'émergence de l'intelligence artificielle dans le processus de détection des incidents de sécurité

Les appels à projets dédiés à l'expérimentation

l'occasion pour une PME cyber de tester son développement avec un intégrateur / utilisateur et d'avoir des feed-back terrain de sa solution pour une mise sur le marché rapide.

SERMA Safety & Security et particulièrement l'entité OPALE SECURITY a bénéficié de ce soutien pour mettre au point sa **plateforme Hardsploit** d'évaluation de la sécurité d'un objet connecté.

1.5 FOCUS SUR LA FILIÈRE : PRESTATAIRES PUBLICS ET PRIVÉS PERTINENTS, STRUCTURES & AIDES MOBILISABLES

Le programme CAP'TRONIC et ses actions en cybersécurité pour les PME

Fondée par le CEA et Bpifrance, et financée par le ministère de l'Économie et des Finances, l'association JESSICA France est chargée de la mise en œuvre du **programme CAP'TRONIC**. Celui-ci a pour objectif d'**aider les PME françaises, quel que soit leur secteur d'activité, à améliorer leur compétitivité** grâce à l'intégration de solutions électroniques et de logiciel embarqué dans leurs produits.

Spécialistes en électronique et en logiciel embarqué, les 24 ingénieurs CAP'TRONIC sont présents sur l'ensemble de la France, **au plus proche des entreprises** et des défis qu'elles doivent relever au quotidien. Ils mettent en place, en toute neutralité, les expertises adaptées au projet, à l'entreprise et au marché, afin de parvenir rapidement à une **solution réaliste en termes de choix technologique, de délai et de coût.**

Les interventions prennent la forme de séminaires techniques et marché, de formations et de conseils. L'aide de CAP'TRONIC peut prendre ensuite la forme d'expertises cofinancées par le programme (choix technologiques, finalisation du cahier des charges…) et d'accompagnement du projet.

CAP'TRONIC mobilise de nombreux experts venant de centres de compétences publics et privés en électronique et en logiciel embarqué. Ces centres sont des laboratoires universitaires, des écoles d'ingénieurs, des sociétés d'études électroniques du secteur privé.

CAP'TRONIC se mobilise pour mettre en place un accompagnement très pragmatique des PME, start-up & ETI dans la gestion de la sécurité de leurs systèmes & objets connectés, en l'intégrant dans la démarche globale de conception de ces systèmes, dès l'amont des projets jusqu'à leur industrialisation.

CAP'TRONIC
Systèmes électroniques et logiciel embarqué

SÉMINAIRES TECHNIQUES

Journées ouvertes de sensibilisation

ATELIERS & FORMATIONS

Transfert de savoir-faire sur 2 à 3 jours

CONSEIL

Aide à l'identification de points critiques, au choix de solutions et à la mise en œuvre de solutions techniques

APPUI TECHNIQUE : EXPERTISE CAP'TRONIC

Intervention cofinancée d'un ou plusieurs experts identifiés en fonction de chaque problématique

SUIVI DE PROJET

Appui d'un expert cofinancé pour assurer le suivi technique et la bonne exécution du projet

IDÉES BESOINS → **ACCOMPAGNEMENT CAP'TRONIC** → **PRODUIT**

1.5 FOCUS SUR LA FILIÈRE : PRESTATAIRES PUBLICS ET PRIVÉS PERTINENTS, STRUCTURES & AIDES MOBILISABLES

L'ENTRETIEN CONSEIL CAP'TRONIC

L'introduction de technologies électroniques et logicielles dans un produit peut répondre à de multiples motivations :

- **moderniser un produit existant** pour prendre de l'avance sur la concurrence aux niveaux des performances, du prix, du design,
- **créer un produit nouveau** (pour l'entreprise) pour **développer un marché**,
- **créer un produit nouveau** (pour le marché) pour **concurrencer un ou des produits existants**.

Dans tous les cas une réflexion initiale s'impose avant tout investissement :

- **définir les objectifs de développement** par rapport à l'entreprise et à ses produits,
- **préciser les objectifs** techniques et commerciaux,
- **évaluer les moyens** humains, techniques et financiers nécessaires et disponibles,
- **établir un planning,**
- **et évaluer le bénéfice** apporté au produit et à l'entreprise par l'introduction d'une technologie électronique.

Dans de nombreuses PME, l'apport de l'électronique et du logiciel embarqué a marqué le début d'une nouvelle croissance en France comme à l'international.

Pour d'autres, ces technologies ont été une nécessité pour faire face à la concurrence au niveau des performances et des coûts. Il est souvent difficile de séparer les deux aspects dans la mesure où ces technologies entrainent souvent une re-conception du produit, de ses méthodes de production, voire une évolution de sa commercialisation et du service après-vente associé.

Aujourd'hui, quels que soient les objectifs recherchés : amélioration des performances, réduction des coûts, petite ou grande série, réduction de l'encombrement, protection contre les contrefaçons, il existe une ou plusieurs solutions techniques. Le rôle des ingénieurs CAP'TRONIC est d'accompagner l'entreprise dans le choix des solutions les plus adaptées, et dans le choix des meilleures méthodes pour les mettre en œuvre. L'industriel qui envisage l'introduction d'une technologie électronique et/ou logiciel embarqué dans ses produits se pose la question suivante : quel bénéfice pour mon produit et mon entreprise ?

Une bonne part de la réussite de son projet dépend de la qualité des réponses à ces questions. C'est le rôle des ingénieurs CAP'TRONIC d'aider l'industriel dans cette démarche. Son conseil concerne donc aussi bien les aspects technologiques et économiques que la construction même du projet (coûts, délais, méthodologie...). Il permet d'envisager des solutions techniques et de préparer, si nécessaire, l'intervention d'un expert. Ce conseil est gratuit.

Les ingénieurs CAP'TRONIC accompagnent les PME dans leur démarche de conception produit au travers d'étapes structurantes pour prendre en compte le risque Cyber et améliorer la résistance aux attaques. La démarche est différente si le produit est encore au stade d'idée ou si le produit est déjà commercialisé.

Nous allons expliciter les accompagnements en fonction des phases de votre projet et de vos besoins.

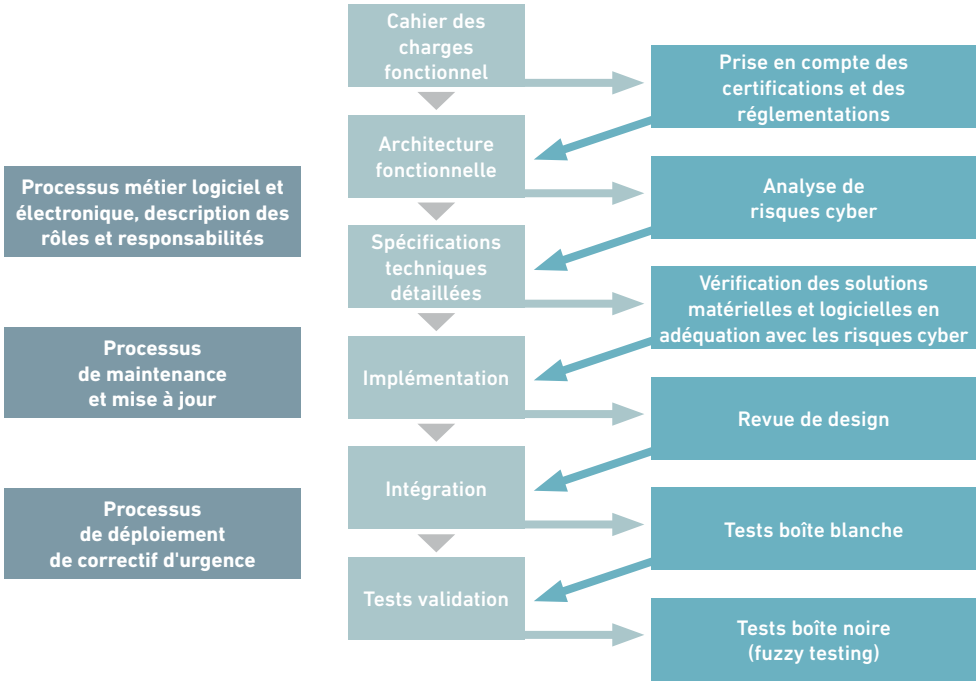
1.5 FOCUS SUR LA FILIÈRE : PRESTATAIRES PUBLICS ET PRIVÉS PERTINENTS, STRUCTURES & AIDES MOBILISABLES

1

Parcours CAP'TRONIC pour la conception de produits avec prise en compte du risque Cyber

Au stade de l'idée, CAP'TRONIC intervient pour que vous puissiez, au travers d'un cahier des charges, obtenir des spécifications qui permettront de consulter des bureaux d'études dans le but d'assurer la réalisation d'un démonstrateur et aussi l'industrialisation du produit. Dans le cadre d'un produit connecté, ce guide liste l'ensemble des bonnes pratiques Cyber à mettre en place.

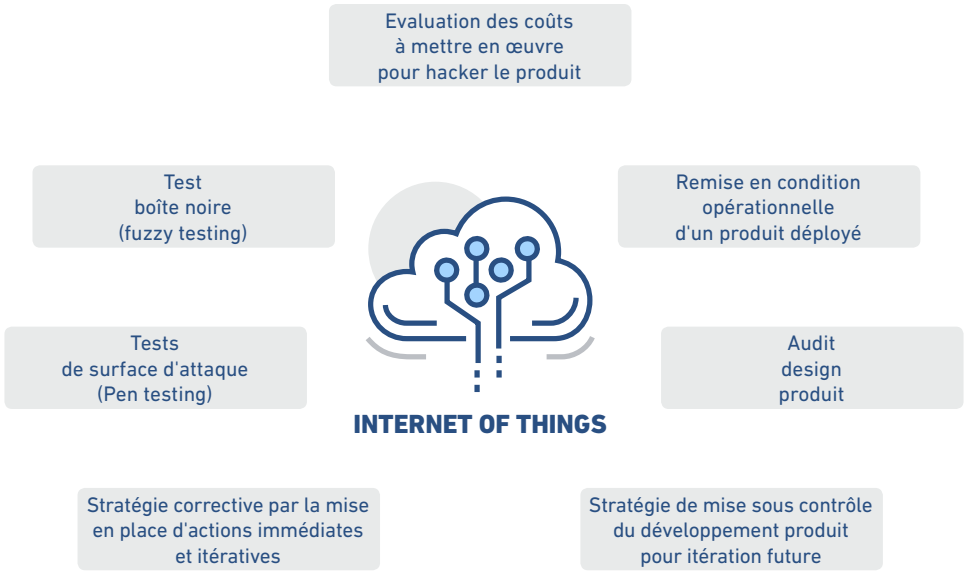
Nous présentons ci-dessous la prise en compte du risque cyber pour chaque étape d'un projet.



Toutes les étapes peuvent faire appel à du conseil de la part d'un ingénieur CAP'TRONIC. En fonction de la complexité et des compétences internes de la PME, nous pourrons vous conseiller une formation, une réalisation externe ou un suivi technique afin de mener à bien votre projet.

Parcours CAP'TRONIC pour évaluer la surface d'attaque Cyber d'un produit déjà réalisé

Nous intervenons également sur des produits déjà conçus et déployés. Dans ce cas, notre accompagnement porte sur les audits possibles avec différentes approches en fonction des buts recherchés.



1.6 PROTECTION CIVILE – LE CITOYEN AU CŒUR DES PRÉOCCUPATIONS DE LA CYBER-PRÉFECTURE

INTERVIEW

Anne Souvira
Commissaire
Divisionnaire & Chargé de
mission Cybercriminalité,
Cabinet du Préfet de
Police de Paris

PREFECTURE DE POLICE

La préfecture de Police prend en compte la cybersécurité par rapport à ses réseaux, infrastructures et autres moyens qu'elle utilise pour ses missions. Aussi, sensibiliser les fonctionnaires et hauts responsables est une partie essentielle de ma mission. Les particuliers, les entreprises et les collectivités ne sont pas oubliés par nos services; ils disposent sur **www.prefecturedepolice.paris.fr** de "votre espace cybersécurité", avec nombre de conseils et documentations, tels comment réagir en cas d'attaque et déposer plainte et où ?

Concernant les attaques qui remontent à nos services ce sont principalement celles du rançonnage par crypto-virus, ou par déni de service. Lors de chiffrement de données, il est important de collaborer avec des spécialistes et les services de police car, même si l'entreprise paye, imaginant que cela lui coûtera moins cher, il est très rare de récupérer toutes les données. Il est donc impératif d'effectuer des sauvegardes pour éviter la disparition de l'entreprise parfois. Pour les objets connectés tels des systèmes embarqués, ceux de la domotique ou des compteurs intelligents peu de remontées existent, mais le développement de leur usage verra vraisemblablement s'accroitre la menace, d'où la nécessité de leur excellente cybersécurité.

Quelques bonnes pratiques ? S'attacher à développer du code sécurisé (les écoles d'informatique professent des cours de sécurité de code), sensibiliser le personnel sur les principaux modes opératoires (la fraude dite « au Président »), réaliser des analyses de risque, établir des contrats adaptés entre fabricant/vendeur et usager (si c'est un bracelet qui compte vos pas, ou un objet qui relève votre taux de diabète, le risque est bien différent). Face à l'usager béotien, le fabricant devrait assumer la responsabilité de mettre sur le marché des systèmes de traitement de données sensibles, adaptés, avec le bon niveau de sécurité et cela devient désormais un élément marketing « discriminant » même pour des objets de faible valeur.

Les actions en cybersécurité comprennent des conseils aux particuliers et aux entreprises (le dépôt de plainte en cas de cyber-attaque) et la lutte contre la cybercriminalité à travers des services d'enquête de police judiciaire notamment via la brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI).

Riche de quelque 46 000 femmes et hommes, dont près de 30 000 policiers et 8 500 sapeurs-pompiers, la préfecture de police de Paris s'engage au quotidien pour garantir la sécurité et l'exercice des libertés de tous ceux qui vivent, travaillent ou visitent Paris et son agglomération.

2

Les objets connectés en réseau avec ou sans fils, qui se comptent déjà par milliards, et dont le nombre sera en très forte augmentation dans les années qui viennent, nous environnent et font désormais partie de notre vécu quotidien.

Au niveau de la cité, au niveau des transports, au niveau des usines, les objets connectés deviennent incontournables car ils rendent et rendront de plus en plus de services dont on ne pourra plus se passer.

Nos modes de vie seront transformés. Le problème est que ces objets connectés n'ont pas souvent été conçus sécurisés et, par conséquent, ils présentent d'importants dangers pour la sécurité des données numériques qu'ils créent, stockent et manipulent.

POURQUOI.

QUELLES SONT LES ATTAQUES ET RISQUES POTENTIELS ?

2

2.1 TYPOLOGIE DES ATTAQUES, QUELQUES GRANDS SCÉNARIOS (QUELQUES EXEMPLES ORIGINAUX ET RÉCENTS)

Les objets connectés en réseau et non sécurisés constituent autant de points d'entrée dans un système d'information.

Ils peuvent se transformer, infectés par un maliciel, en un vecteur d'attaque, ou même être détournés de leurs fonctionnalités, en devenant ainsi un danger pour qui les possède.

Citons, pour illustrer le propos, quelques attaques très médiatisées réelles ou simulées de divers types.

L'attaque en déni de service distribuée (DDoS), le 26 septembre 2016, au cours de laquelle 425 000 caméras de surveillance mal sécurisées se sont tournées vers l'infrastructure de l'hébergeur OVH, causant un débit de 1200 milliards de bits par seconde, accaparant un septième des capacités réseau d'OVH, donc ralentissant grandement les performances utiles du réseau. Tentative d'attaque pour prouver la faisabilité d'une attaque encore plus violente ? En tout cas elle souligne la faiblesse des caméras de surveillance qui ont pour certaines d'entre elles des mots de passe par défaut.

L'attaque sur les infrastructures informatiques de la société DYN, le 21 octobre 2016, par une variante du Virus Mirai (dont les sources sont publiées), qui a contaminé des réseaux d'objets connectés, établissant un botnet de dizaines de millions d'objets connectés pour mener l'attaque qui a rendu inopérants, pendant plusieurs heures, des services tels que Amazon, Twitter, PayPal, ...

La démonstration, faite en octobre 2012, qu'il est possible, à 10 mètres de distance, de provoquer une **décharge de 830 volts sur un Pacemaker,** pouvant causer la mort par crise cardiaque d'un patient qui le porterait. Crime parfait car difficilement attribuable ?

La démonstration durant l'été 2015, qui a **conduit dans un fossé une Jeep Cherokee** après avoir actionné à distance sa radio, ses essuie-glaces et finalement avoir bloqué son volant et désactivé ses freins.

2.2 CONSÉQUENCES ASSOCIÉES DE CES ATTAQUES (FINANCIÈRES, JURIDIQUES, IMAGE...)

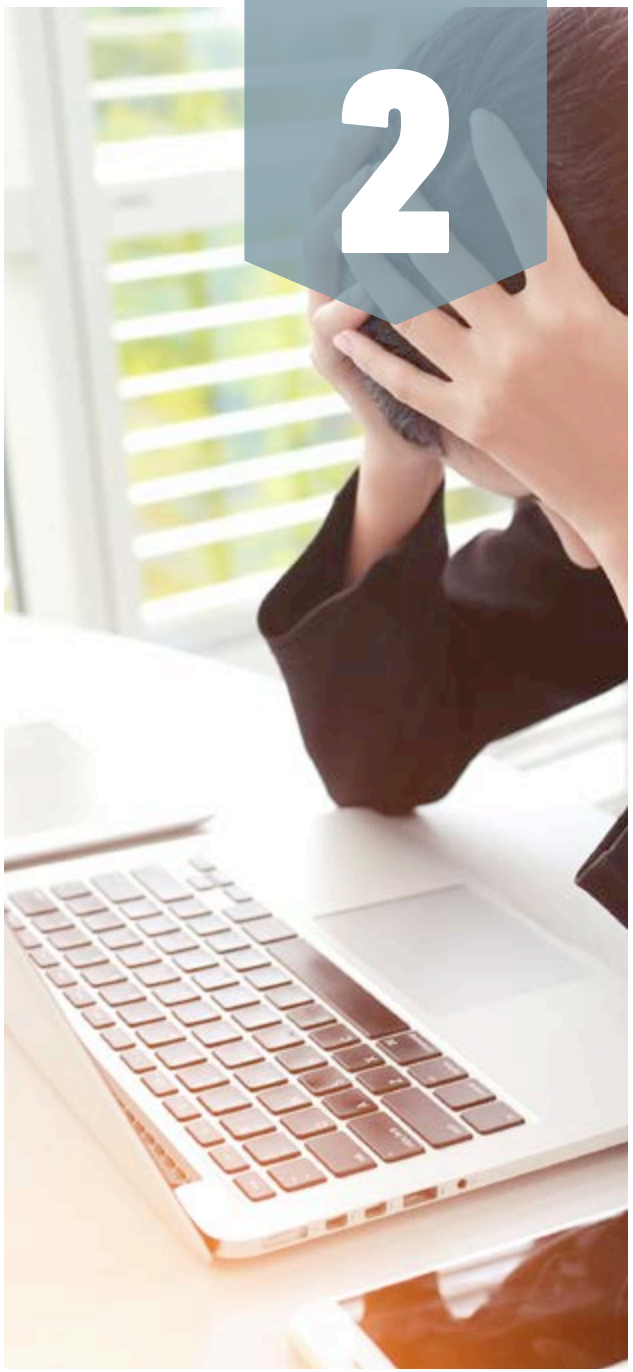
Les rapports annuels (Internet Security Threat Report) publiés par Symantec insistent régulièrement sur l'énorme manque de mesures cybersécurité dans les objets connectés conçus ces dernières années. Le problème est que ces vulnérabilités sont très évidentes et faciles à exploiter.

Par conséquence, les objets connectés seront fortement ciblés par les cybercriminels dans les prochaines années, ce qui entraînera une augmentation du nombre de cyberattaques réussies.

Les cyberattaques peuvent également avoir des conséquences pour les clients. Une attaque, qui cause une perte de données de santé ou bancaires des clients, peut sérieusement impacter leur vie privée ou peut être financièrement préjudiciable pour eux. Elle peut également entraîner des rappels massifs de produits.

Les conséquences pour les entreprises peuvent être catégorisées en trois types :

- **Financières :** Les vols de données peuvent représenter pour les entreprises un coût colossal. Ces données peuvent par exemple être de type économique, contractuel, etc. Selon l'étude IBM/Ponemon Institute réalisée auprès de 350 entreprises dans 11 pays, le coût total consolidé moyen d'une violation de données peut s'élever jusqu'à 3,8 millions de dollars.
- **Juridiques :** Si une cyberattaque cause une perte des données confidentielles ou personnelles, l'entreprise en charge peut être tenue de payer des amendes ou d'assumer des sanctions règlementaires.
- **Préjudice à l'image :** Une cyberattaque peut abimer l'image de l'entreprise. Elle peut aussi retirer la confiance que des clients avaient dans l'entreprise ce qui peut entraîner une perte importante de clients et de chiffre d'affaires.



2.3 SAVOIR ÉVALUER LES ENJEUX POUR VOTRE PRODUIT (EN FONCTION DES CARACTÉRISTIQUES OBJET ET DES DONNÉES MANIPULÉES) ET VOUS SITUER

L'importance de la cybersécurité

La cybersécurité est l'ensemble des méthodes, pratiques et mécanismes pour protéger un système informatique et garantir la résilience des données collectées et sauvegardées contre les cyberattaques. Le but final de la cybersécurité est d'assurer le respect de la vie privée des utilisateurs et la protection du fonctionnement et des affaires des entreprises concernées.

La cybersécurité est trop souvent vue, à tort, comme une étape supplémentaire au projet technologique et numérique, et qui peut être appliquée à la fin de la conception d'un produit. Comme exposé précédemment, les conséquences des cyberattaques sont importantes et le manque de stratégie en cybersécurité peut irrémédiablement impacter la croissance et le développement d'une entreprise.

Par conséquence, la cybersécurité doit avoir sa place au cœur du développement des produits et systèmes numériques afin qu'elle soit pris en compte dès le début d'un projet pour être vérifiée et suivie régulièrement.

La cybersécurité doit être intégrée parmi les bonnes pratiques d'une équipe de développement. Le design d'un projet numérique consiste non seulement au développement d'une idée innovante, mais consiste aussi à envisager les volets cybersécurité au travers de la sensibilisation, la formation et le recrutement en compétence en cybersécurité.

Une méthodologie telle que la ***« cybersécurité par design »*** garantit l'intégration des stratégies cybersécurisées dès la phase de conception d'un produit ou d'un système. Ce type de méthodologie s'attache à réduire les menaces et vulnérabilités ainsi que de minimiser les impacts d'une cyberattaque.

2.3 SAVOIR ÉVALUER LES ENJEUX POUR VOTRE PRODUIT (EN FONCTION DES CARACTÉRISTIQUES OBJET ET DES DONNÉES MANIPULÉES) ET VOUS SITUER

2

Une conception sécurisée est garantie par l'intégration des trois piliers principaux de la cybersécurité :

- **Confidentialité :** l'objectif est de s'assurer que seules les personnes autorisées ont accès aux ressources échangées;
- **Intégrité :** l'objectif est de garantir que les données sont bien telles qu'on les attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante;
- **Disponibilité :** l'objectif est de garantir un accès constant aux services et ressources installés et le bon fonctionnement global du système.

Dans une conception sécurisée, ces principes sont priorisés en fonction de la sensibilité des données à collecter, l'environnement, l'architecture, les risques, etc.

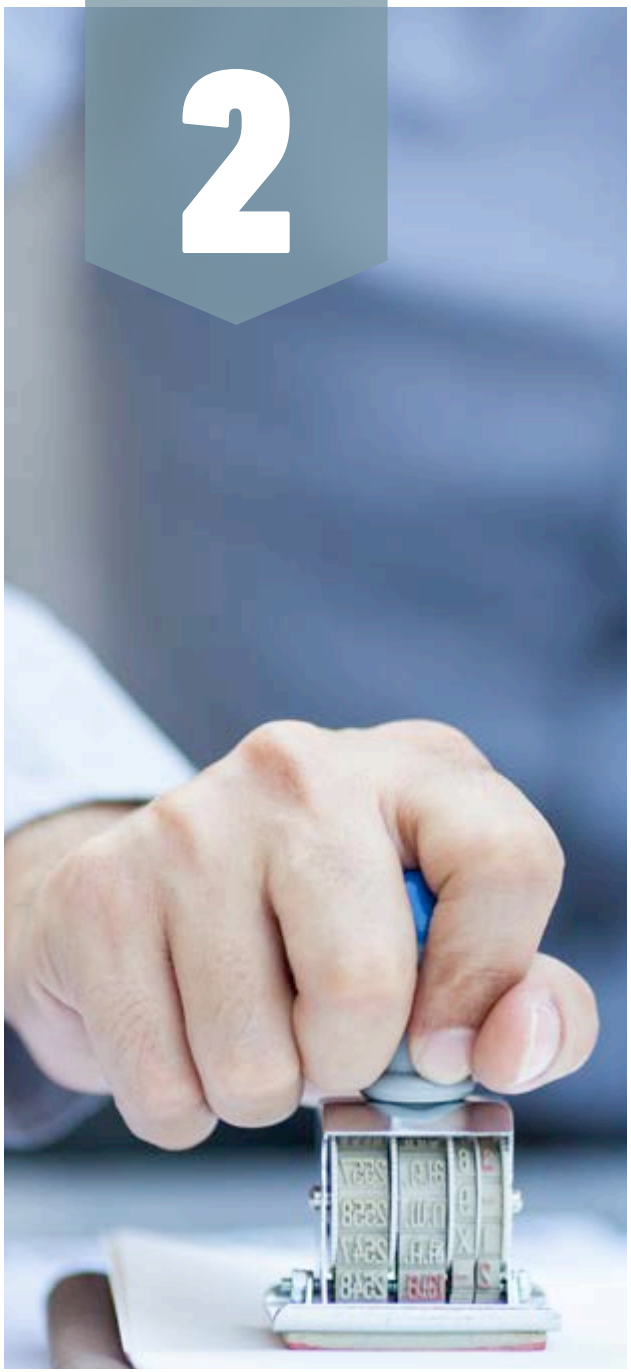
Par conséquent, il est nécessaire de bien définir les principaux cas d'utilisation d'un produit qui détermineront ensuite la priorité d'implémentation de ces principes. Par exemple, pour un objet connecté de santé qui collecte les données des patients, il faut s'attacher particulièrement aux aspects de confidentialité alors qu'un outil industriel connecté devra proposer un haut niveau de disponibilité pour assurer le bon fonctionnement du système.

Ces principes peuvent être garantis par l'implémentation des méthodes principales de la cybersécurité. Ces méthodes sont :

- **Authentification :** l'objectif est de s'assurer que seuls les utilisateurs légitimes ont accès au système et aux ressources.
- **Autorisation :** Cela permet de déterminer qu'un utilisateur a les permissions suffisantes pour accéder aux ressources. Dans une conception sécurisée, il faut toujours garantir **le principe de moindre privilège**. Cela veut dire que les utilisateurs ne doivent se voir accordés uniquement les privilèges nécessaires et essentiels.
- **Audit (traçabilité) :** l'objectif est d'enregistrer les traces des actions effectuées par les utilisateurs. Par exemple, des connexions/déconnexions, changement du mot de passe, changements des configurations d'un objet ou système.
- **Protection des données :** les données stockées ou en transit doivent être protégées contre les accès ou altérations malicieux. Cela est garanti par les technologies cryptographiques pour fournir la **communication sécurisée** entre des objets connectés et le **stockage sécurisé** des données sensibles (par ex. le mot de passe) sur un objet.
- **Contrôle des entrées et sorties :** Cela vérifie que toutes les entrées faites par les utilisateurs correspondent bien aux règles du système. Il garantit aussi que les sorties contiennent seulement les données demandées et qu'il n'y a aucune fuite d'informations.
- **Mise à jour du fimware :** le composant logiciel d'un objet connecté doit être itérativement testé contre des failles de sécurité et, en conséquent, doit évoluer pour la mise en place des contre-mesures de cybersécurité. Ces contre-mesures doivent être distribuées aux utilisateurs de manière sécurisée et sous-forme d'une mise à jour du logiciel.

Ces méthodes peuvent être implémentées en trois niveaux de sécurité : Bas, Modéré et Élevé.

Le niveau de sécurité d'un produit intelligent est identifié en phase de design et, comme déjà mentionné, dépend fortement des cas d'usages.



2.3 SAVOIR ÉVALUER LES ENJEUX POUR VOTRE PRODUIT (EN FONCTION DES CARACTÉRISTIQUES OBJET ET DES DONNÉES MANIPULÉES) ET VOUS SITUER

Les normes à suivre et les bonnes pratiques

Les normes sont essentielles pour garantir que les méthodes de la cybersécurité sont bien implémentées et que les objets, conformant à ces normes, peuvent être facilement intégrés dans un système connecté et en communication avec d'autres objets.

Aujourd'hui, les instituts de standardisation sont un peu en retard pour fournir les normes pertinentes pour la cybersécurité des produits connectés. Toutefois des standards internationaux existent pour l'industrie tel que **ISA/IEC 62443 et ISA/IEC 62351, ISO 15408 (Critères Communs)**. Il est crucial de les prendre en compte dès lors que l'usine devient connectée (Industrie 4.0) avec les problématiques de circulation de la donnée dans un contexte d'interopérabilité des machines et des supervisions.

Pour améliorer la qualité d'objets ou de systèmes connectés, leur développement doit non seulement suivre les normes de la cybersécurité spécifiées mais également celles liées à la sécurité des systèmes d'information en général tels que l'ISO 27001 et l'ISO 27002 (au niveau international) ou les recommandations de l'**ANSSI** (au niveau national).

Comme exposé dans les sections précédentes, la disponibilité des objets connectés dans un système IoT est primordiale. Les entreprises doivent fortement considérer pour leurs produits intelligents l'obtention de **certifications** de type **EDSA[1] ou CSPN[2]**. A minima aujourd'hui, le développement d'un produit intelligent doit prévoir dans sa conception une confrontation à des étapes de tests d'intrusion ou aux cas de tests définis par EDSA de ISA Secure.

En plus des normes, il existe également des **bonnes pratiques** à suivre, comme celles de **NIST[3]** ou d'**OWASP[4]**. Ces « bonnes pratiques » peuvent être utilisées comme des guides qui contiennent des informations et techniques à jour et qui garantissent la bonne application des règles de la cybersécurité.

(1) http://www.isasecure.org/en-US/Certification/IEC-62443-EDSA-Certification

(2) https://www.ssi.gouv.fr/administration/produits-certifies/cspn/les-procedures-formulaires-et-methodologies/

(3) https://www.nist.gov/publications/search?term_node_tid_depth%5B%5D=248731

(4) https://www.owasp.org

2.4 OBLIGATIONS RÉGLEMENTAIRES EN FONCTION DES DOMAINES APPLICATIFS DE VOTRE PRODUIT IOT

2

INTERVIEW

Nicolas Hélenon
Directeur Associé

NeoTech ASSURANCES
LE COURTIER DES SOCIÉTÉS INNOVANTES

Pour les PME éditrices de logiciel en mode SaaS, les risques de dépendance de leur fournisseur, à savoir les risques opérationnels, peuvent être couverts avec des garanties de pertes de marge brute d'exploitation (PE). Une attention toute particulière doit être portée sur les causes et les évènements couverts et surtout sur la définition de la PE : en effet, certains contrats d'assurances ne couvrent pas la perte de marge brute d'exploitation mais la perte de résultat. Par conséquent, si celui-ci est négatif, il n'y aura pas d'indemnisation. Les contrats ne peuvent souvent également que couvrir les pertes d'exploitation si les serveurs se situent dans les locaux de l'assuré; en cas de malveillance informatique chez votre hébergeur/fournisseur, serez-vous indemnisé ?

Une bonne assurance cybersécurité peut néanmoins couvrir un bon nombre d'atteintes aux données ou aux systèmes. On observe 3 grandes catégories de risque :

- **Risque de responsabilité civile**, divulgation, altération des données, suppression, déni de service, ... Cela couvre les pertes pécuniaires dont l'assuré serait responsable.
- **Risque de dommages** liés à l'assuré lui-même qui peut avoir des frais à engager pour restaurer & reconstituer ses données (frais supplémentaires d'exploitation, perte de marge brute d'exploitation...). A noter que dans ce cadre, on regarde avant l'incident, on calcule un coefficient de baisse auquel on applique la marge brute d'exploitation pour l'indemnisation.
- **Risque de crise**, parfois des incidents de sécurité ne créent pas de dégâts ou n'engagent pas la Responsabilité Civile de l'assuré. Néanmoins, une intervention d'un expert informatique pour savoir ce qu'il se passe (instruire), et des frais pour décontaminer sont souvent quand même nécessaires. L'assuré peut avoir besoin des conseils d'un expert en communication ou être convoqué par la CNIL, être sanctionné au paiement d'une sanction pécuniaire administrative ou devoir notifier. Ces 3 volets peuvent être assurés.

A titre d'exemple, dernièrement des pirates avaient hébergé des sites de fishing sur le réseau d'une PME, qui a été ensuite attaquée en contrefaçon de logiciels. L'assureur a pu rapidement prendre en charge 20 à 30 000 euros pour des interventions d'experts et le problème a été désamorcé très vite. De manière générale, nous conseillons de lancer le chantier de conformité au règlement européen. Par ailleurs, plus qu'avoir des outils de sécurité, nous pensons qu'il est pertinent d'avoir une "maturité" de la sécurité (gouvernance). Enfin, suivre les règles d'hygiène de l'ANSSI ainsi que relire vos contrats et demander confirmation à votre courtier par écrit que les 3 volets sont couverts (RC, Dommages aux biens, gestion de crise) constituent quelques grands préalables importants.

NeoTech Assurances est une société de courtage en assurance dédiée aux sociétés de nouvelles technologies et aux entreprises de services du numérique : SSII, ESN, Editeur, Conseil en Technologie, Web Agency, Site marchand, e-commerce, hébergeur et data center.

2

2.4 OBLIGATIONS RÉGLEMENTAIRES EN FONCTION DES DOMAINES APPLICATIFS DE VOTRE PRODUIT IOT

INTERVIEW

Major Fabrice CRASNIER
Commandant de la division analyse criminelle et investigations spécialisées à la section d'appui judiciaire de Toulouse

L'une de nos missions au sein de la division est d'appréhender les auteurs des infractions pénales qui se commettent dans le cyberespace, l'objectif étant d'éviter que le risque se propage et ne devienne pandémique. Toutefois, cela ne peut se faire sans élément de preuve, je vous rappelle que **la cybercriminalité est une activité de police judiciaire** soumise aux règles juridiques. Ainsi, nous conseillons et aidons les victimes avant un dépôt de plainte à relever les éléments matériels qui constitueront l'infraction pénale qui sera relevée et poursuivie. Suivant le type d'enquête qui sera alors pris, après autorisation de M. le procureur de la République, nous recherchons les preuves numériques de l'infraction. Encore faut-il que les acteurs techniques qui ont été appelés en premier recours n'aient pas détruit toutes les preuves (après un dépôt de plainte, la destruction de preuves est une infraction pénale si cette dernière a été commise en pleine conscience). La gendarmerie depuis plus de 15 ans est également engagée dans le volet prévention et sensibilisation pour informer le public sur les menaces que nous enregistrons ou observons au travers de manifestations comme le Forum Internationale de la Cybersécurité (FIC). Parallèlement à mon activité judiciaire, je suis coordinateur du relais Occitanie de la Réserve Citoyenne Cyberdéfense.

La RCC est constituée de bénévoles et a pour objectif de sensibiliser la Nation aux enjeux de la cybersécurité au travers de conférences, d'informer les sociétés demanderesses sur les évolutions de la maturité des systèmes d'informations et enfin de réaliser des démonstrations à l'aide d'objets du quotidien détournés de leur objet initial (par exemple concevoir des objets de démonstration qui montrent les compromissions de capteurs ou d'effecteurs dans l'IOT). A ne pas confondre avec la réserve opérationnelle de cyberdéfense qui est un réservoir de forces mobilisables en cas de crise majeure sur le territoire national.

Au cœur de l'IoT, les menaces en cybersécurité sont décuplées compte tenu du nombre d'objets connectés et de la faible capacité des systèmes IoT à enregistrer des traces. D'autant qu'aujourd'hui la miniaturisation progresse aussi sur les composants de collecte utilisés par les attaquants (caméra de la taille d'une tête d'épingle,...). Dans Industrie 4.0, nous sommes confrontés à des problématiques d'objets ou de systèmes qui ont des failles de sécurité connues, les températures mesurées des machines-outils peuvent par exemple être délibérément altérées pour mener à un arrêt de production. Sur les Smart-cities, la menace serait de faire face à une « liquidation numérique ».

Il faut apprendre à utiliser les outils informatiques, dans l'industrie comme à la maison, et pratiquer en premier lieu le cloisonnement. Le réseau de l'IoT doit être disjoint du système central. Un bon modèle d'architecture évite qu'une compromission dans un réseau faible comme celui des objets connectés ne compromette votre réseau d'Entreprise. **Il est indispensable de se faire accompagner par des professionnels qualifiés sur ces sujets et d'avoir soi-même une culture de sécurité des SI. Il est donc indispensable de former à la cybersécurité toutes les acteurs de l'entreprise.**

La division analyses criminelles et investigations regroupe une cellule **Cybercrimes,** *une cellule* **Coordination criminalistique et imagerie** *(scènes de crimes, vidéos), une cellule dédiée aux* **Avoirs criminels** *et une cellule* **Analyses criminelles** *qui cartographie le spectre d'une attaque ou d'un phénomène en cours.*

3

Joël Heslaut
Cabinet Nemezys

Avocat titulaire des mentions de spécialisation en Droit de l'Informatique et en Droit de la Propriété Intellectuelle, Joël Heslaut a exercé auparavant dans plusieurs grands cabinets internationaux français, tels qu'Alérion, Ernst & Young et Salans.

DONNÉES PERSONNELLES ET RGPD :
LES NOUVEAUX ENJEUX

3

DONNÉES PERSONNELLES ET RGPD : LES NOUVEAUX ENJEUX

Termes et définitions

Certification : c'est un instrument qui permet, en répondant à des exigences normatives (voir plus loin), de démontrer que les produits ou services opérés par une entreprise répondent aux attentes de ses clients, de renforcer la crédibilité de celle-ci, et de garantir un certain niveau de protection des données.

Destinataire des données : « toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données » (Art. 3 loi Informatique et libertés).

Donnée à caractère personnel : « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne » (Art. 2 loi Informatique et libertés).

Données sensibles : « données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci » (Art. 8 loi Informatique et libertés).

Responsable de traitement : « la personne, l'autorité publique, le service ou l'organisme qui détermine les finalités et les moyens dudit traitement, sauf désignation expresse par des dispositions législatives ou réglementaires relatives à ce traitement » (Art. 3 loi Informatique et libertés).

Traitement de données à caractère personnel : « toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction » (Art. 2 loi Informatique et libertés).

Avocats : leur activité et leur rôle

Les enjeux relatifs à la protection des données étant primordiaux pour la pérennité d'une entreprise, leur rôle est de vous avertir et de vous prémunir contre les risques éventuels en matière de gestion des données, notamment à l'aune du Règlement général européen sur la protection des données personnelles (RGPD), lequel concerne tous les acteurs et constitue un véritable changement de culture d'entreprise en matière de données personnelles.

A défaut de disposer d'un service juridique étoffé et compétent dans ces domaines, les entreprises auront intérêt à consulter des avocats spécialisés qui pourront, en s'adjoignant au besoin des experts d'autres domaines connexes, les conseiller et les assister pour :

- identifier les risques liés aux traitements mis en œuvre ou aux technologies opérées,
- élaborer des schémas contractuels cohérents permettant à l'entreprise de poursuivre ses activités dans des conditions de sécurité juridiques acceptables,
- construire un référentiel légal interne pour s'assurer de la cohérence et de l'applicabilité des process internes avec les obligations légales ou normatives,
- négocier les contrats avec les clients, fournisseurs ou sous-traitants afin de s'assurer que leurs intérêts sont protégés et que chaque risque identifié y soit adressé et si possible maîtrisé,
- participer à la mise en place des obligations en assurant le rôle de DPO pour le compte de l'entreprise,
- les défendre auprès des autorités de contrôle ou des instances judiciaires,

DONNÉES PERSONNELLES ET RGPD : LES NOUVEAUX ENJEUX

3

La problématique du point de vue d'un cabinet d'avocats

À l'heure où la place de l'informatique dans toutes les sphères de notre société ne cesse de grandir, l'ère étant à l'Open data, au Big Data (traitement massif des données) voire au Data Lake (centraliser toutes les données de l'entreprise afin de pouvoir à tout moment construire de nouveaux traitements pour les exploiter), de nouvelles menaces pèsent nécessairement sur les réseaux et systèmes d'information (perte de données, détournement de finalité, piratage).

Si les citoyens sont davantage sensibilisés à l'utilisation faite de leurs données personnelles, parallèlement, de nouveaux outils produisant et exploitant des données voient le jour.

Or, la cybersécurité, qui désigne l'ensemble des règles visant à protéger les personnes et les biens contre les atteintes portées au moyen de technologies, en particulier aux données personnelles, concerne tous les acteurs de l'économie : entités publiques ou privées, grandes entreprises ou PME.

Aussi, une des difficultés est celle de la mise en œuvre des règles édictées par le RGPD et notamment la mise en conformité au Règlement européen avant le 25 mai 2018.

Ce vade-mecum a pour but de répondre à vos principales interrogations :- Quels changements pour les entreprises avec le RGPD ?- Comment se mettre en conformité ?- Comment réagir en cas de problème ?

Le Règlement général européen sur la protection des données personnelles : quels changements pour votre entreprise ?

Directement applicable dans chaque État membre de l'Union européenne à compter du 25 mai 2018, le Règlement a pour finalités d'harmoniser les législations européennes en matière de sécurité et de gestion des données personnelles, d'encourager l'innovation au sein du marché unique du numérique et d'assurer un niveau de protection élevé des citoyens.

Que prévoit le GDPR ?

Les PME doivent d'ores déjà s'interroger sur leur mise en conformité aux principes édictés par le Règlement (principe d'Accountability et de coresponsabilité, règle du Privacy by Design), et pour ce faire revoir non seulement leur organisation interne afin de placer la sécurité au cœur de leur activité, mais également réfléchir à l'opportunité de faire appel à des fournisseurs certifiés.

Le principe d'« Accountability »

Tandis que les obligations des responsables de traitement prévues par la loi Informatique et libertés visent des formalités préalables (système de déclaration et d'autorisation auprès de la CNIL), le Règlement privilégie quant à lui une logique de responsabilisation et de transparence.

Ce principe d'« Accountability » signifie que l'entreprise est responsable du respect des obligations posées par le Règlement, mais également qu'elle doit pouvoir prouver qu'elle les respecte en ayant mis en place des mesures appropriées.

Il est donc exigé du responsable de traitement de :

- prendre des mesures efficaces et appropriées pour se conformer au Règlement
- adopter des règles et des outils internes garantissant une protection élevée des données traitées
- conserver un registre décrivant les traitements effectués sous la responsabilité du responsable du traitement ou du sous-traitant
- réaliser une analyse des risques en matière de traitements des données à caractère personnel
- respecter la règle du « Privacy by design » (exige que tout traitement mis en œuvre par l'entreprise doit dès le départ être conçu pour protéger les données personnelles)
- désigner un délégué à la protection des données (DPO).

3

DONNÉES PERSONNELLES ET RGPD : LES NOUVEAUX ENJEUX

La règle du « Privacy by Design » (PbD)

Il s'agit de répondre au problème lié à la multiplication des traitements de données personnelles par le biais de technologies et d'objets interconnectés.

En vertu de cette règle, les entreprises doivent garantir dès leur conception et lors de chaque utilisation de nouvelles technologies de traitement le plus haut niveau possible de protection des données.

L'objectif est le respect de la vie privée de manière préventive, dès la conception, c'est-à-dire en prenant en compte les exigences en matière de protection de la sphère privée avant qu'une nouvelle technologie puisse créer un risque de violation de protection des données.

Le PbD s'articule autour de 7 principes :

- des mesures proactives et préventives
- une protection implicite et automatique
- une intégration de la vie privée dans la conception des systèmes et au cœur des pratiques
- une protection intégrale
- une sécurité durant toute la durée de conservation des données
- de la visibilité et de la transparence
- respecter la vie privée des utilisateurs

Négliger les problématiques en lien avec la vie privée est susceptible d'engendrer des conséquences graves pour les entreprises :

- poursuites judiciaires
- vols de données
- dégâts en termes d'image de marque

Le principe de « coresponsabilité »

Alors qu'auparavant seul le responsable du traitement était responsable en cas de faille (et non le sous-traitant), le Règlement prévoit une coresponsabilité : est responsable la personne dès lors qu'elle participe au traitement de données. Cette coresponsabilité aggrave donc le sort des sous-traitants.

De facto, de nombreux sous-traitants deviendront coresponsables, ce qui est d'ailleurs plus conforme à la réalité, c'est-à-dire à l'hypothèse de délégation par une entreprise à des tiers d'une partie de ses activités de traitements relatifs à des données personnelles.

Rappelons qu'en cas de faille dans la chaîne de contrats, n'importe lequel des acteurs risque une sanction. Cette coresponsabilité va donc conduire les entreprises à faire beaucoup plus attention à leur politique de sécurité des données :

- soit en s'autocontrôlant de manière poussée
- soit en contrôlant les autres acteurs (sous-traitants) de la chaîne. Dans ce cas de figure, l'entreprise concernée aura le choix entre soit intégrer dans les contrats avec ses sous-traitants les règles de sécurité imposées par le Règlement (travailler en PbD), soit se réserver une possibilité de contrôler le sous-traitant en question par le biais d'un audit.

La certification

L'organisation internationale de normalisation (ISO) joue un rôle déterminant dans la création de normes de protection des données personnelles.

À titre d'exemple :

- la norme ISO/IEC 27001 définit les exigences concernant les systèmes de management de la sécurité des informations (SMSI).
- la norme ISO/IEC 29134 *(Privacy impact assessment — Guidelines)* fournit un cadre pour analyser les impacts sur la vie privée, conformément au RGPD.
- la norme ISO/IEC 27018 *(Code of practice for protection of personally identifiable information (PII) in public clouds)* en matière de Cloud Computing, concerne quant à elle les sous-traitants chargés des traitements de données personnelles pour le compte d'un responsable de traitements.

En pratique, la certification permet de répondre facilement à l'exigence de contrôle ou d'autocontrôle.

DONNÉES PERSONNELLES ET RGPD : LES NOUVEAUX ENJEUX

3

Comment vous mettre en conformité avec le RGPD ?

En tant que PME, vous devez vous poser les bonnes questions pour identifier les risques et utiliser les données de manière conforme. Une analyse des risques en interne est donc indispensable afin d'évaluer le niveau de sécurité des données personnelles. Cette analyse doit être structurée et adaptée au contexte, à la finalité du traitement, au volume et à la sensibilité des données, ainsi qu'à la quantité et à la vulnérabilité des personnes concernées.

Exemples de risques redoutés:

- coordonnées récupérées et utilisées à l'insu des intéressés à des fins commerciales;
- identités usurpées à des fins d'activités illégales (risque de poursuites pénales des personnes concernées) ;
- dommages liés à l'e-réputation ;
- vol par une entreprise concurrente d'un disque dur portable ;

Mener un PIA (Privacy Impact Assessment)

C'est un outil d'évaluation d'impact sur la vie privée qui s'adresse aux responsables de traitement afin de justifier la mise en œuvre des principes de protection de la vie privée et qui se déroule en quatre étapes :

- analyse du contexte : délimiter et décrire les traitements, leur contexte et leurs enjeux ;
- analyse des mesures : identifier les mesures existantes ou prévues ;
- analyse des risques : étudier les risques liés à la sécurité des données susceptibles d'avoir un impact sur la vie privée des personnes faisant l'objet du traitement de données ;
- validation : confirmer (ou infirmer) les mesures envisagées pour respecter les exigences légales et traiter les risques identifiés ;

Désigner un Délégué à la Protection des Données (Data Protection Officer)

Le Règlement prévoit trois cas dans lesquels la désignation d'un délégué est obligatoire :

- lorsque le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;
- lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ;
- lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 (données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses, philosophiques, l'appartenance syndicale, les données génétiques, biométriques, de santé, relatives à la vie sexuelle ou l'orientation sexuelle d'une personne physique) et de données à caractère personnel relatives à des condamnations et infractions pénales ;

Le Règlement prévoit également qu'un groupe d'entreprises peut nommer un délégué unique. La notion de « groupe d'entreprises » doit être entendue comme « une entreprise qui exerce le contrôle et les entreprises qu'elle contrôle ».

Le délégué doit disposer de certaines qualités :

- être doté de connaissances spécialisées du droit et des pratiques professionnelles en matière de protection des données ;
- être capable d'accomplir les missions visées à l'article 39 (notamment l'information et la sensibilisation des employés à la protection des données, le contrôle de la conformité du traitement, la coopération avec l'autorité de contrôle) ;

Le délégué devra être associé à toutes les questions relatives à la protection des données personnelles et aura pour mission d'informer et de conseiller l'entreprise et les employés dans le cadre de la mise en œuvre des traitements de données, de contrôler le respect du Règlement, de vérifier l'exécution de l'analyse des risques, et de coopérer avec l'autorité de contrôle.

3

DONNÉES PERSONNELLES ET RGPD : LES NOUVEAUX ENJEUX

Réglementer le BYOD

L'abréviation de l'expression anglaise *« Bring Your Own Device »* (« Apportez Votre Equipement personnel de Communication »), désigne l'emploi d'équipements informatiques personnels dans le cadre professionnel (par exemple un salarié qui utilise son ordinateur personnel pour se connecter au réseau de l'entreprise).

Si la législation en droit du travail impose à l'employeur de fournir aux employés les moyens nécessaires à l'exécution des tâches professionnelles, l'entrée du BYOD au sein de l'entreprise efface les frontières entre vie professionnelle et vie personnelle. Or, le responsable du traitement est responsable de la sécurité des données personnelles traitées au sein de son entreprise, y compris celles stockées sur des terminaux dont il n'a pas la maîtrise, mais dont il a autorisé l'utilisation pour accéder aux ressources informatiques de l'entreprise.

S'il ne lui est pas possible, au regard du respect de la vie privée, d'empêcher l'utilisation par les salariés de leurs outils personnels (par exemple interdire l'accès à internet depuis leur smartphone), l'employeur doit néanmoins limiter les risques pour la sécurité des données.

Il lui est donc conseillé d'informer et de sensibiliser ses employés sur ces risques et les précautions à prendre, ainsi que de les avertir sur leur responsabilité par le biais d'une charte informatique annexée au règlement intérieur de l'entreprise et ayant valeur contraignante.

D'autres solutions sont également envisageables :

- le CYOD (*« Choose Your Own Device »* / « Choisissez Votre Équipement personnel de Communication ») : l'entreprise propose aux employés d'acheter leur équipement parmi des appareils certifiés répondant aux normes de sécurité de l'entreprise ;
- le COPE (*« Corporate Owned, Personally Enabled »* / « Propriété de l'entreprise avec accès privé ») : les outils de communication sont détenus par l'entreprise et configurés selon sa politique de protection des données ;

DONNÉES PERSONNELLES ET RGPD : LES NOUVEAUX ENJEUX

3

Les aspects normatifs & réglementaires et les conséquences en cas de problème

Si l'arsenal juridique européen dans le domaine du numérique ne cesse de se développer (directive européenne NIS, RGPD), il durcit également les sanctions en cas de non-respect des obligations imposées aux responsables de traitement en matière de protection des données (amendes financières).

La directive NIS (Network and Information Security)

La directive NIS 2016/1148 du 6 juillet 2016 (relative aux mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union) oblige nombre d'entreprises à se conformer et respecter de nouvelles obligations en matière de sécurité et de signalement d'incidents.

La directive, qui devra être transposée en droit interne par les États membres avant le 9 mai 2018, prévoit notamment :

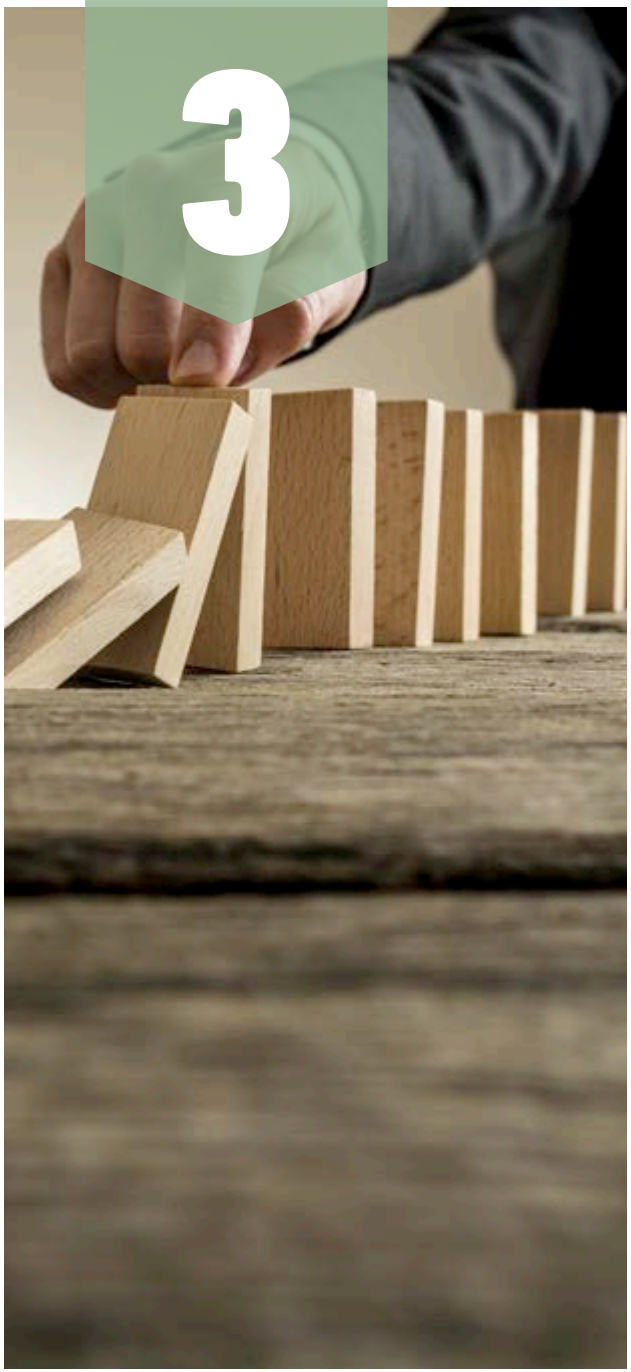
- pour chaque État membre de l'Union de désigner une autorité nationale compétente en matière de cybersécurité (Agence Nationale de la Sécurité des Systèmes d'Information/ ANSSI en France) ainsi que des centres de réponse aux incidents de sécurité informatique (CSIRT) ou des centres de réponse aux urgences informatiques (CERT) afin d'alerter et analyser les incidents ;
- la création d'un « *groupe de coopération* » en matière de politiques de cybersécurité entre États membres, composé des représentants des États membres, de la Commission européenne et de l'Agence européenne de la sécurité des réseaux et de l'information (ENISA / European Union Agency for Network and Information Security) ;
- le renforcement par les États membres de la cybersécurité concernant les « opérateurs de services essentiels » (opérateurs présents dans les secteurs de l'énergie, des transports, des banques de la santé, des marchés financiers…), d'une part par l'instauration de règles qu'ils devront respecter, d'autre part par l'obligation de signaler les incidents ;
- l'adoption de règles européennes communes en matière de cybersécurité des fournisseurs de services numériques, des places de marché en ligne, des fournisseurs de services de Cloud et des moteurs de recherche, et notamment des mesures pour assurer la sécurité de leur infrastructure et signaler les incidents majeurs aux autorités nationales ;

S'agissant des PME, la directive prévoit de les dispenser des exigences prévues par la législation européenne : *« pour éviter que la charge financière et administrative imposée aux opérateurs de services essentiels et aux fournisseurs de service numérique ne soit excessive, il convient que les exigences soient proportionnées aux risques que présentent le réseau et le système d'information concernés, compte tenu de l'état le plus avancé de la technique en ce qui concerne ces mesures. Dans le cas des fournisseurs de service numérique, ces exigences ne devraient pas être applicables aux microentreprises et aux petites entreprises ».*

Des amendes dissuasives

Le RGPD prévoit un système gradué de sanctions en cas de violation des règles édictées :

- Amende d'un montant de 10 000 000 d'euros maximum ou 2% du chiffre d'affaires annuel mondial total de l'exercice précédent (absence de protection des données dès la conception et par défaut, défaut de sécurité des données, absence de notification des violations de données, absence de registre des traitements ou encore non-respect des règles de désignation du DPO).
- Amende d'un montant de 20 000 000 d'euros ou 4% du chiffre d'affaires annuel mondial total de l'exercice précédent (non-respect des principes de la protection des données personnelles, infraction aux règles applicables au consentement ou encore infractions aux dispositions relatives aux transferts de données personnelles hors de l'EEE).



3

DONNÉES PERSONNELLES ET RGPD : LES NOUVEAUX ENJEUX

Quelle couverture du risque cybersécurité par les assureurs ?

Est-il possible de s'assurer contre les sanctions administratives et notamment contre les sanctions prévues par le RGPD ?

Aucune disposition du code des assurances ne prévoit formellement l'interdiction de l'assurabilité des sanctions administratives. Toutefois, en droit français l'interdiction (d'ordre public) de s'assurer pour des amendes prononcées par des juridictions pénales reste le principe (en raison du caractère personnel de la peine). Dès lors, si les sanctions administratives revêtent un caractère pénal, elles ne pourront pas être prises en charge par les assureurs.

Cependant, ne serait-il pas possible d'envisager leur assurabilité en démontrant le caractère non pénal des sanctions administratives ? Avec quelques réserves toutefois, ne conviendrait-il pas dès lors en matière de cybersécurité pour les entreprises de se rapprocher non seulement de fournisseurs certifiés, mais également d'envisager la piste de l'assurance ?

En France, l'assurance RCMS (Responsabilité Civile des Mandataires Sociaux) est une assurance qui garantit la responsabilité des dirigeants (on parle également d'assureurs de Responsabilité Des Dirigeants/RDD).

Dans les pays anglo-saxons, il est autorisé pour les entreprises de s'assurer pour la prise en charge des condamnations prononcées contre leurs dirigeants pour des faits commis dans le cadre de leurs fonctions (on parle d'assurances D&O/ « Directors and Officers »).

Si la question de cette assurabilité en France n'a pas été tranchée jusqu'à présent, l'arrêt de la Cour de cassation (Civ 2e 14 juin 2012, Marionnaud, n°11-17367) semble ouvrir le débat et pourrait entamer une évolution en matière d'assurabilité des sanctions pécuniaires infligées par certaines autorités administratives, les juges ne visant pas le fondement de l'ordre public, mais celui du caractère intentionnel des faits. En l'espèce, l'assuré avait eu la volonté de mettre les conséquences financières qui résulteraient de ses fautes à la charge de son assureur. La Cour de cassation approuve les juges du fond d'avoir considéré que le dirigeant avait commis une faute intentionnelle incompatible avec l'aléa, excluant ainsi la garantie de l'assureur.

À l'heure actuelle, on ne peut affirmer avec certitude l'abandon par la haute juridiction du fondement sur l'ordre public, et subséquemment la reconnaissance de l'assurabilité des sanctions administratives.

Si le débat judiciaire reste ouvert, la pratique incite à la mise en œuvre de telles assurances, à l'instar de nos voisins anglo-saxons, lesquelles permettraient aux dirigeants d'exercer leurs fonctions plus sereinement.

DONNÉES PERSONNELLES ET RGPD : LES NOUVEAUX ENJEUX

3

Nemezys est un Cabinet orienté vers les entreprises technologiques (ESN, éditeurs, industries technologiques avancées, mais aussi start-up ou investisseurs) qui accompagne ses clients tout au long de leurs projets. À l'écoute, son équipe aide les entreprises à se développer et à innover, à résoudre les différends de ses clients et à leur délivrer des conseils avisés.

Dans un monde en mutation constante, Nemezys offre bien plus que des services juridiques et met à disposition son exigence et sa créativité. Fondé en août 2013 par Joël Heslaut, avocat titulaire des mentions de spécialisation en Droit de l'Informatique et en Droit de la Propriété Intellectuelle, ayant exercé auparavant dans plusieurs grands cabinets internationaux français, tels qu'Alérion, Ernst & Young et Salans, Nemezys réunit une équipe pluridisciplinaire en mesure de couvrir les principaux besoins juridiques des entreprises (contrats, droit de l'informatique, droit d'auteur, marques et brevets, droit des sociétés, droit social).

Nemezys : Déesse grecque, exécutrice de la justice des dieux, du grec **νέμειν** « répartir équitablement, distribuer ce qui est dû ».

Pour résumer

Les échéances du printemps 2018 sont comme un mur vers lequel une voiture se dirige à grande vitesse, il est encore temps d'éviter la collision mais il ne faudra pas attendre le dernier moment pour freiner ou changer de route.

Toutes les entreprises, y compris les plus petites doivent se préparer.

En premier lieu, elles doivent prendre conscience de l'impact économique du RGPD, le principe de Coresponsabilité qu'il édicte sera de loin le plus pénalisant pour les petites entreprises.

Face à des acteurs coresponsables, les victimes de violation de la sécurité des données traitées ou les autorités de contrôle choisiront toujours d'agir contre le coresponsable le plus solvable (les grandes entreprises). Ces dernières vont devoir de facto porter non seulement leurs propres risques mais aussi ceux induits par leurs fournisseurs et ce, peu importent les dispositions contractuelles.

Un tel principe devrait donc conduire leurs clients ou leurs donneurs d'ordre à renforcer leurs contrôles pour limiter leurs risques mais de tels contrôles ont des coûts élevés que ni le client, ni la PME ne vont accepter d'assumer car, soit ils diminueraient la marge de l'une ou soit ils renchériraient le coût pour l'autre.

Pour éviter ces coûts, les grandes entreprises exigeront probablement de leurs fournisseurs qu'ils soient certifiés. La certification permettra en effet au Client d'éviter d'avoir à faire auditer son prestataire pour vérifier la conformité de ses pratiques, mais également de pouvoir limiter son exposition personnelle.

La certification (ISO 27001 et/ou ISO 29134 en particulier), pour une bonne partie des PME agissant dans le domaine, sera donc probablement un passage obligé pour préserver leur compétitivité.

Si la certification est une lourde charge c'est aussi un cercle vertueux qui oblige à identifier et adresser l'ensemble des risques de l'entreprise, élaborer des process de gestion de ces risques, formaliser un cadre contractuel efficient. En cela la certification, conduit les entreprises à plus de maturité industrielle leur permettant d'améliorer leur compétitivité faisant donc finalement de cette charge un investissement rentable

Une certification ne sera sûrement pas obtenue d'ici le printemps prochain, mais mettre le processus en route, c'est déjà prendre le bon chemin pour répondre aux exigences du RGPD et la directive NIS à savoir dès maintenant :

- Désigner un DPO (si l'activité de l'entreprise le nécessite),
- Engager une analyse de risques, définir leur périmètre, les identifier et les évaluer,
- Former ses équipes de développement aux exigences du Privacy by Design,
- Auditer son environnement contractuel et ses règles internes pour en vérifier l'adéquation aux nouvelles exigences légales.

Autre piste à explorer pour les acteurs coresponsables, l'assurance projet.

4

COMMENT .
QUELLE POLITIQUE DE SÉCURITÉ ADOPTER ?

4.1 LE PARCOURS STRUCTURÉ À SUIVRE POUR UN OBJET SÉCURISÉ

4

Il existe différents processus et normes pour l'évaluation des risques cyber lors de la conception d'un produit et ce décliné par secteur d'activité. Dans ce chapitre, nous citons en exemple la méthode élaborée par Microsoft (SDL) car celle-ci est publiée sous la licence Creative Common permettant à tout un chacun de se procurer les documents gratuitement[1].

Security Development Lifecycle (SDL)

Le chapitre 2 a montré que l'absence de prise en compte de la cybersécurité dans les produits connectés peut provoquer des dommages, pour les entreprises et leurs clients, qui ont parfois des conséquences irréversibles. Par conséquent, la cybersécurité a une place incontournable dans la conception des produits connectés et doit être impérativement intégrée dans le cycle de développement de ces produits. Pour atteindre cet objectif, il est recommandé d'adapter le « Security Development Lifecycle (SDL) » qui est spécialement conçu pour garantir la « Cybersecurity by Design ».

Le SDL est un processus qui ajoute des activités supplémentaires, axées sur la cybersécurité, à chaque phase du cycle de développement d'un logiciel, système ou produit sécurisé. En d'autres termes, le SDL modifie le processus classique du développement d'un produit en intégrant certaines pratiques liées à la cybersécurité pour garantir que les principes de la cybersécurité seront bien implémentés dès la phase de conception.

Comment intégrer le SDL dans le cycle de développement d'un produit ?

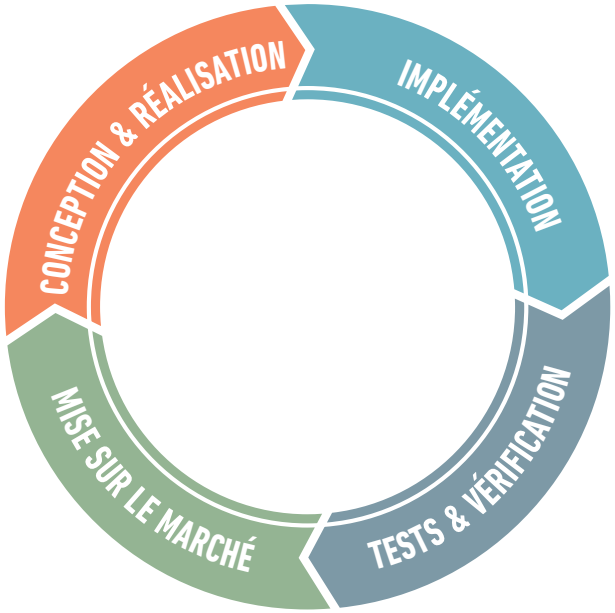
Le SDL assure que les développeurs tiennent compte des enjeux liés à la cybersécurité, en définissant les stratégies de cybersécurité pour réduire les risques et développer des produits ou systèmes cyber-résilients.

La figure ci-dessous montre les étapes du processus SDL :

(1) https://www.microsoft.com/en-us/download/details.aspx?id=29884

4

4.1 LE PARCOURS STRUCTURÉ À SUIVRE POUR UN OBJET SÉCURISÉ



Le SDL insiste sur la formation en cybersécurité, qui est considérée comme un prérequis pour un développement sécurisé. Une équipe de développement se doit donc d'être sensibilisée à la cybersécurité et aux conséquences du manque de mesures adéquates. La formation des équipes passe par la mise en place d'activités liées à la cybersécurité durant le cycle de développement. Ces activités sont :

- **Pendant la conception et la spécification des besoins :** la modélisation des menaces. Elle est au cœur du processus SDL et constitue la base d'une conception sécurisée. La pratique aide les développeurs à identifier les menaces associées au système et à définir la liste des exigences essentielles de cyber-sécurité pour limiter les risques.
- **Pendant l'implémentation :** les développeurs se doivent de déployer les bonnes pratiques et normes pour minimiser les vulnérabilités au maximum. Le recours à l'utilisation d'outils de développement à jour, l'application de règles de codage pour obtenir une programmation sécurisée (par ex. éviter les fonctions obsolètes) et la réalisation d'analyses statiques du code source avant la compilation, sont des étapes essentielles.
- **Pendant les tests et la vérification :** le produit devra être testé pour révéler ses potentielles failles de sécurité afin de garantir que les exigences liées à la cybersécurité, identifiées dans la phase de conception, sont bien satisfaites. Les tests de sécurité à effectuer peuvent être classés par catégorie tels que l'analyse dynamique, le test à données aléatoires (Fuzz testing), le test d'intrusion et le test de robustesse. Aujourd'hui, le développement d'un produit connecté se doit d'intégrer tout ou partie de ces tests.
- **Pendant la mise sur le marché du produit :** Un plan de réponses aux incidents de sécurité doit être constitué afin de déterminer la liste des actions préventives à effectuer et les services de mise en sécurité à proposer aux clients en cas d'attaque ou de découverte de vulnérabilités. Dans le cadre de la cybersécurité, l'entreprise se doit donc d'assurer la continuité entre les développeurs et les opérationnels.

4.1 LE PARCOURS STRUCTURÉ À SUIVRE POUR UN OBJET SÉCURISÉ

INTERVIEW

4

Dr Assia TRIA
Chargé d'affaires
CEA Tech Occitanie
(Montpellier)

L'omniprésence des objets communicants dépourvus de protection physique et de surveillance, les rend une proie facile aux attaques matérielles et logicielles. Ces objets peuvent être volés, corrompus ou contrefaits. Sans mesures particulières, les données stockées sur ces dispositifs sont alors accessibles, y compris des données cryptographiques qui permettent d'accéder à d'autres données ou jouer des rôles sensibles dans les systèmes complexes les hébergeant. Par ailleurs, les transmissions sans fil, sont à leur tour une proie facile à l'écoute et au déni de service. Il existe aujourd'hui des solutions cryptographiques pour assurer des services de confidentialité, de contrôle d'intégrité, d'authentification, de non-répudiation, mais il reste encore beaucoup à faire pour rendre ces algorithmes efficaces et performants sur des dispositifs embarqués de plus en plus miniaturisés. De tels besoins en sécurité imposent la recherche d'algorithmes cryptographiques efficaces et ayant une petite empreinte matérielle.

La prise en compte de la sécurité et du respect des données privées n'est intégrée que très peu ou pas du tout dans la conception des produits. On peut affirmer que la quasi-totalité des objets intelligents sont aujourd'hui vulnérables. Sécuriser un objet est très complexe techniquement car la cible de sécurité et la surface d'attaque sont naturellement plus étendues que pour une application web dont on peut contenir les serveurs par exemple. Dans le cas d'un objet communicant, toutes les attaques imaginables sont quasiment possibles. Les protections passives de type « défense en profondeur » doivent être développées.

Parmi les difficultés d'implémentation des solutions, on retrouve les contraintes propres à l'embarqué telles que la mémoire disponible, la puissance de calcul ou la consommation électrique. En cela, la cryptographie est malheureusement très consommatrice de ces 3 ressources.

La sécurité de la communication nécessite d'assurer la confidentialité, l'authenticité, l'intégrité, la disponibilité et la non répudiation des données sans compter la préservation de la privacy. La plupart de ces aspects reposent sur l'utilisation de la cryptographie. Deux algorithmes s'imposent actuellement dans l'IoT : l'AES pour le chiffrement symétrique et les courbes elliptiques pour le chiffrement asymétrique à clé publique qui a supplanté le RSA à cause de l'utilisation de clefs trop longues et trop encombrantes.

Afin de gérer les différentes contraintes de l'embarqué, des travaux ou de nouvelles normalisations portent actuellement sur une cryptographie allégée (« Ligthweight Cryptography ») qui serait en mesure d'être compatible avec les contraintes d'un objet communicant. La commission européenne, a émis mi-janvier 2015, auprès de ses organisations un mandat sur la privacy. Elle demande à ce que les données produites par les capteurs doivent être accessibles par l'utilisateur qui doit avoir un droit de regard sur ses données personnelles. Il y a aujourd'hui à l'ETSI un groupe qui travaille sur des protocoles de type ABAC (Attribute Based Access Control). Ceux-ci sont capables d'accoler des attributs aux données générées, les algorithmes à mettre en œuvre ne sont cependant pas totalement spécifiés. Ces protocoles, qui datent de 2004, proposent des moyens de verrouiller l'accès aux données personnelles. Le protocole ABAC basé sur l'ABE (Attribut Based Encryption) à base d'algorithmes de Couplages (Pairing Based Cryptography ou PBC) permet de fournir des solutions cryptographiquement sûres.

Le chiffrement homomorphe avec tout l'espoir qu'il porte pour assurer la confidentialité des données tout en permettant leurs manipulations dans le cloud n'en est qu'à ses balbutiements. Il existe à ce jour des outils permettant son utilisation : compilateur spécifique, parallélisation du code, moteur d'optimisation, chiffrement symétrique adapté à une surcouche homomorphe pour s'intégrer à un nœud de capteurs. Ces outils ont montré des performances 5 fois plus rapides que celles de l'état de l'art mais ils restent malgré tout encore insuffisants en termes de performance.

Pour compliquer encore le tout, le développement de la cryptographie quantique dont on sait qu'elle rend très vulnérable les systèmes à base de RSA et divise par 2 la taille des clés AES est un élément à prendre en compte pour des objets intelligents ayant vocation à être présents de nombreuses années dans nos maisons, nos bureaux et nos villes. Il faut donc dès à présent travailler sur des architectures post-quantum cryptography comme l'Europe et l'ETSI ont commencé à aborder. L'anticipation des attaques et des progrès dans la gestion des Qbits des ordinateurs quantiques est une contrainte forte dans le développement technique des futures applications et objets.

Il apparaît aujourd'hui comme un enjeu majeur dans la sécurisation des systèmes de communication, de devoir améliorer drastiquement la résistance des composants et des systèmes à ces techniques d'attaques.

L'expertise du CEA Tech couvre le conseil, l'évaluation sécuritaire, la caractérisation et l'architecture sécurisée de composants et de systèmes, la cryptographie et la sécurisation de protocoles de communication.

Le CEA Tech renforce la résistance des circuits intégrés aux attaques physiques avec des technologies pionnières comme des dispositifs physiques (écrans, capteurs, architectures) pour contrer les attaques comme les canaux auxiliaires ou l'injection de fautes.

Communication sans fil

Nos travaux de R&D comprennent le développement de protections contre les attaques sur les communications comme les attaques relais, « man in the middle », les interceptions, techniques de parage d'attaques de types relais, homme du milieu, écoutes par le biais du développement de protocoles et de composants spécifiques (ex : antennes).

Évaluation de systèmes

Pour les applications systèmes complexes, nous concevons et mettons en place des protocoles de sécurité et des architectures utilisant des noyaux de systèmes ultra-résistants.

L'évaluation et l'assurance du niveau de sécurité sont garanties par des analyses de risques, caractérisation des menaces et évaluations sécuritaires basées sur les normes en vigueur dans un laboratoire accrédité.

4

4.2 TOUT COMMENCE PAR UNE ANALYSE DE RISQUE

Modélisation des Menaces (Threat Modeling)

La modélisation des menaces est un processus de gestion des risques qui permet d'identifier les menaces potentielles pour le système, déterminer les risques découlant de ces menaces et définir les contre-mesures pertinentes. La modélisation des menaces est un outil qui aide les développeurs à évaluer les risques associés aux cas d'utilisation et à mieux appréhender les enjeux de la cybersécurité dans leurs projets de systèmes intelligents.

Cette pratique comporte différentes étapes :

1. Identifier les cas d'utilisations
2. Identifier et lister les menaces associées aux cas d'utilisation
3. Évaluer et classer les menaces selon leurs criticités et priorités
4. Définir les contre-mesures cybersécurité pour atténuer les menaces identifiées

Identifier les cas d'utilisations

L'identification des cas d'utilisation consiste à définir les éléments suivants :

- L'architecture du système (i.e. les points d'entrées, de sorties et les zones/limites de confiance)
- Les actifs du système (par ex. les données confidentielles ou personnelles, etc.)
- Les acteurs et leurs interactions avec le système (par ex. les utilisateurs, etc.)
- Les flux de données entre les éléments du système
- Les technologies utilisées

Tous les éléments mentionnés ci-dessus aident les développeurs à mieux comprendre le fonctionnement de leur système sous l'angle de la cybersécurité.

Identifier et lister les menaces associées aux cas d'utilisation

L'étape suivante est d'identifier et lister les menaces associées au système suivant les grandes catégories de menaces connues sous le nom de **STRIDE** :

- **Spoofing (Falsification) :** lorsqu'un utilisateur illégitime peut s'identifier en tant qu'un utilisateur légitime.
- **Tampering (Altération) :** lorsqu'un utilisateur illégitime parvient à provoquer une altération malicieuse des données du système.
- **Repudiation (Répudiation) :** lorsqu'un utilisateur nie effectuer une action et qu'il est impossible de le prouver.
- **Information disclosure (Divulgation de l'information) :** lorsque les données sont exposées aux utilisateurs illégitimes.
- **Denial of service (Déni de service) :** lorsque le service est indisponible aux utilisateurs légitimes.
- **Elevation of privilege (Élévation de privilèges) :** lorsqu'un utilisateur illégitime obtient un accès privilégié au système, comme celui d'administrateur, pour effectuer les altérations qu'il souhaite.

4.3 CETTE ANALYSE ABOUTIT À DES SUGGESTIONS DE CONCEPTION ET DE BRIQUES TECHNO ASSOCIÉES (CHOIX DES PROTOCOLES, CHOIX DE SECURE ELEMENTS, CRYPTO...)

4

Évaluer et classer les menaces selon leurs criticités et priorités

Les menaces identifiées dans l'étape précédente devront maintenant être classifiées et priorisées. La classification est faite en se basant sur cinq catégories des critères connus sous le nom du DREAD :

- **Damage (Dommage) :** quelle serait la gravité de l'attaque pour le système ?
- **Reproducibility (Reproductibilité) :** quelle est la facilité à reproduire l'attaque ?
- **Exploitability (Exploitabilité) :** quel volume de travail faut-il pour lancer l'attaque ?
- **Affected users (Utilisateurs impactés) :** combien d'utilisateurs seraient impactés ?
- **Discoverability (Accessibilité) :** quelle est l'accessibilité de la menace ?

Pour chaque menace une valeur du DREAD devra être calculée. Cela veut dire que pour chaque menace, les cinq critères de DREAD devront être évalués en donnant une valeur (entre 1 et 10) à chacun d'entre d'eux, puis en prenant la moyenne de ces valeurs pour l'indice final. Enfin, les menaces seront priorisées par rapport à leur valeur du DREAD, du plus élevé au plus faible.

Définir les contre-mesures cybersécurité pour atténuer les menaces identifiées

L'étape finale consiste à définir des contre-mesures de cybersécurité pour les top 10 ou 20 des menaces identifiées. Les contre-mesures proposées devront être basées sur les méthodes principales de cybersécurité présentées dans le chapitre 2.

Les méthodes existantes

Il existe des méthodologies différentes pour réaliser une modélisation de menace pertinente. La méthodologie décrite dans cette section est celle de Microsoft qui est basée sur STRIDE[1]. Les autres méthodologies, notamment TRIKE[2], P.A.S.T.A[3], VAST[4] et EBIOS[5] (d'ANSSI), sont aussi efficaces et performantes que STRIDE.

(1) https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

(2) https://sourceforge.net/projects/trike/

(3) Risk Centric Threat Modeling : Process for Attack Simulation and Threat Analysis, Marco M. Morana et Tony UcedaVelez, ISBN 13: 9780470500965

(4) http://threatmodeler.com/threat-modeling-methodology/

(5) https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

INTERVIEW

Saghar Estehghari

CYBERSECURA

Il est important de ne pas attendre le moment de la mise sur la marché pour faire appel à une expertise en cybersécurité. Dans ce cas, l'architecture choisie peut rendre la sécurisation difficile. Au contraire je conseille à une PME de se faire accompagner dès la conception d'une solution, pour que l'architecture que je propose puisse encore être prise en compte.

Depuis plus de 10 ans maintenant, j'ai toujours travaillé en tant que consultante en cybersécurité et j'ai développé une spécialité en sécurité des objets connectés. Cette spécialisation est peu fréquente, elle comporte des particularités par rapport aux systèmes informatiques classiques. J'effectue les prestations d'accompagnement dans leur totalité, aux côtés de nos clients. Nos clients apprécient de s'adresser à un seul expert.

Les besoins en cybersécurité des PME sont grandissants. Je les conseille notamment au travers d'accompagnement « à temps partagé ». La PME accède ainsi à un accompagnement stable et durable avec une maîtrise complète des coûts associés. Après un temps d'interaction avec le client, j'ai une période d'étude de mon côté, avant de partager mes conclusions avec lui et de l'accompagner dans leur prise en considération.

Nous avons récemment accompagné une TPE, dont la dirigeante était, à juste titre, inquiète. Après un temps d'étude de l'activité, nous avons répondu à leurs interrogations en décrivant les menaces auxquelles ils étaient exposés dans leur domaine d'activité. J'ai conduit alors une étude approfondie des technologies utilisées et scénarios d'interactions possibles sur leur plateforme. Les mesures de sécurité que j'ai proposées ne sont pas forcément coûteuses à mettre en place. Elles incluent de simples mesures empêchant d'être victime d'une attaque de déni de service, protégeant les données privées des clients, ou permettant de détecter l'éventualité d'une intrusion

4

4.3 CETTE ANALYSE ABOUTIT À DES SUGGESTIONS DE CONCEPTION ET DE BRIQUES TECHNO ASSOCIÉES (CHOIX DES PROTOCOLES, CHOIX DE SECURE ELEMENTS, CRYPTO...)

INTERVIEW

Florent Kirchner
Chef du Laboratoire pour la Sûreté et la Sécurité du Logiciel

Les équipes du CEA List s'intéressent à la cybersécurité sur l'ensemble de la chaîne logicielle, jusqu'à l'utilisateur : **les données** (protection, crypto calcul, environnements d'exécution sûrs), **les logiciels qui manipulent ces données** (bugs qui servent de « portes d'entrée » aux attaques, conformité à un cahier des charges de sécurité), **les passerelles et protocoles de communication** entre systèmes (incluant le cloud) et enfin **les systèmes complexes**.

En haut de cette pyramide, l'humain reste l'élément fondamental d'une politique efficace de cybersécurité. Nous mettons l'accent sur la sensibilisation des utilisateurs et la fourniture d'outils pour mieux comprendre et appréhender l'environnement cyber.

Les attaquants ont l'avantage de la rapidité (il est aujourd'hui beaucoup plus lent de sécuriser un système ou de vérifier s'il a été compromis que de le corrompre). Pour faire évoluer ce rapport de force entre l'attaquant et le défenseur, on peut chiffrer les données ou garantir l'absence de vulnérabilités. Sur la partie réseau, le calcul est assez simple : le temps de réaction d'un humain est de quelques mois, celui d'un logiciel de quelques secondes, d'où l'importance des systèmes numériques dans la problématique de la détection et de la réaction à l'attaque. La priorité du CEA LIST est donc d'utiliser au mieux ces systèmes numériques pour inverser le déséquilibre entre attaquants et défenseurs.

Lorsque nous travaillons avec des PME sur ces sujets, notre conseil est d'appréhender la cybersécurité non comme une contrainte, mais comme une réelle opportunité pour protéger leurs systèmes. Un accompagnement et un conseil pertinents peuvent suffire : une demi-journée de workshop permet de circonscrire le besoin de la PME, de diffuser des avis techniques forts via notre connaissance de l'écosystème, et éventuellement de réorienter les entreprises vers des solutions potentiellement existantes.

De manière générale, les experts de la filière restent les interlocuteurs privilégiés. Ce n'est pas tabou ! La France compte de nombreux spécialistes parmi les meilleurs du monde sur la cybersécurité (acteurs de R&D publics ou privés, organismes de certification, autorités nationales type ANSSI,...), et les occasions de rencontres ne manquent pas.

Face aux attaques logicielles ou matérielles qui visent des applications informatiques, des circuits intégrés, des équipements électroniques portables (smartphones...) ou des systèmes embarqués, la plateforme Cyber-sécurité du CEA List mobilise plus de 100 experts pour identifier les vulnérabilités des produits et développer des protections innovantes.

Les études de vulnérabilité s'appuient sur des outils de haut niveau : modèles d'analyse de risque, plateformes d'analyse de logiciel (Frama-C et Binsec), simulateurs de plateformes matérielles, bancs de tests de protocoles de communication, composants de visualisation et d'apprentissage, outils de gestion de fonctions virtuelles de réseaux, compilateurs sécurisants.

4.3 CETTE ANALYSE ABOUTIT À DES SUGGESTIONS DE CONCEPTION ET DE BRIQUES TECHNO ASSOCIÉES

(CHOIX DES PROTOCOLES, CHOIX DE SECURE ELEMENTS, CRYPTO...)

4

INTERVIEW

Notre laboratoire (l'un des 3 CESTI 'matériel' labellisés par l'ANSSI) effectue à ce jour autour de 200 évaluations sécuritaires par an. Les objets connectés revêtent souvent des contraintes de type sûreté (exemple, son impact sur les utilisateurs). L'enjeu est d'arriver à gérer la convergence sûreté et sécurité au travers des analyses de risque. Un des autres enjeux amenés par les objets connectés est d'étendre la menace en cybersécurité non plus seulement au réseau IT/SI de l'entreprise mais également sur ses produits et outils de production. Tous les services de l'entreprise sont impactés et doivent désormais coopérer.

Voici quelques bonnes pratiques que nous recommandons :

- Suivre des formations "pratiques" qui permettent de comprendre les attaques et de prévoir dès le début de la conception les mesures pragmatiques pour limiter les risques,
- Outiller son bureau d'étude pour réaliser des tests d'intrusions ou tests formels
- Réaliser des revues de spécifications afin de vérifier si l'implémentation visée sera conforme à l'état de l'art.

Pour aider pendant le cycle de développement, il est également souhaitable de mesurer la sécurité des objets connectés avec des outils du marché (notre plateforme de test HardSploit par exemple).

Des conférences internationales proposent des formations comme BlackHat, Defcon, HackInTheBox, CanSeqwest, HardWear.io, ou en présentiel via CAP'TRONIC, le Clusif ou le BreitzCTF.

S'informer via ces supports permet de gagner entre 3 et 6 ans face aux menaces à venir.

Suivez nous sur @Serma_S3.

Yann ALLAIN

SERMA SAFETY & SECURITY

Acteur reconnu de la sécurité numérique depuis plus de 15 ans, SERMA Group a créé son CESTI (Centre d'Evaluation de la Sécurité des technologies de l'Information) en 1998.

Parallèlement à cette activité historique d'EVALUATION, SERMA SAFETY AND SECURITY propose ses services de CONSEIL SPECIALISE (expertise conseil en sécurité pour accompagner les concepteurs, intégrateurs et utilisateurs de systèmes dans la maitrise de leur sécurité, tant dans leur fonctionnement que face à des actions de malveillance).

Son offre s'adresse à tous les acteurs industriels dès lors que la confidentialité, la complexité, la connectivité et la numérisation de leurs systèmes requièrent des niveaux élevés de SECURITE et de SURETE, aussi bien pour la SECURITE des PRODUITS que la SECURITE des SYSTEMES d'INFORMATION.

5

Dans une architecture intégrant des objets connectés (OC), il faut distinguer **l'objet lui-même**, **le réseau qui transmet ses données** ou sert à le gérer et **le système de traitement des données** recueillies, qui peut se trouver dans un "nuage" privé, public ou hybride.

Ces trois sous-ensembles constituent un système qui nécessite une sécurisation globale dont le niveau va dépendre des objectifs de sécurité définis par ailleurs et qui vont permettre de déterminer le niveau d'assurance à atteindre ainsi que les fonctionnalités de sécurité du système.

L'ingénierie de sécurité va permettre de décliner les objectifs de sécurité en mesures, techniques ou autres, sur les différents sous-ensembles du système en tenant compte des autres contraintes comme l'utilisabilité, les performances et le coût. Cette ingénierie va devoir appliquer des concepts devenus classiques en cybersécurité, comme la défense en profondeur, la minimalité, la séparation des privilèges, et les traduire en architectures, fonctions, protocoles et mécanismes ainsi qu'en procédures de mise en œuvre et d'exploitation.

PRATIQUE.

RÉALISATION D'OBJETS CONNECTÉS SÉCURISÉS ET BONNES PRATIQUES

5.1 SÉCURISATION DE L'OBJET CONNECTÉ

5

Un objet connecté (OC) est composé d'une logique de traitement, d'un capteur et/ou d'un actionneur, d'une interface de communication et éventuellement d'interfaces physiques comme des connecteurs, des prises et des boutons.

En général un OC recueille des données locales, transmet ces données à un service via un réseau local ou d'infrastructure, reçoit des commandes de la part d'un serveur de gestion et émet des états vers ce même serveur. L'ingénierie de sécurité va permettre de protéger l'OC et ses données contre des actions malveillantes visant à perturber son fonctionnement, falsifier ou voler ses données.

Nous ne développerons pas outre mesure les aspects physiques, non pas parce qu'ils ne sont pas importants mais parce qu'ils nécessitent de comprendre l'environnement de mise en œuvre et d'éventuelles contraintes de design. Il est important de comprendre que si un adversaire a un accès physique et qu'il peut facilement manipuler l'OC et modifier son fonctionnement ou accéder localement à ses données, alors il a atteint son objectif. Il faut donc tenir compte de cette dimension dans la phase d'ingénierie et adapter les protections physiques selon le contexte, l'OC personnel ou professionnel, et la criticité des données ou du service rendu par l'OC.

Sur un plan générique, il faut s'attacher à protéger l'intégrité de l'OC (avec des mesures physiques éventuelles), de son électronique, de son (micro)logiciel, de ses données de configuration, des informations reçues et des informations captées ou recueillies. Si l'objet est complexe, il peut aussi être nécessaire de protéger les données échangées entre les différents modules qui le composent.

Dans une architecture de sécurité, la protection repose le plus souvent sur des mécanismes cryptographiques. Il est donc primordial de pouvoir protéger les différentes clés qui servent à les activer. Cette protection peut s'effectuer de différentes façons mais l'implantation d'un "coffre de clés" est en principe nécessaire. Ce "coffre", généralement une puce spécifique comme celles que l'on trouve sur les cartes bancaires, peut servir aussi à stocker un identifiant unique de l'OC. Différentes fonctions cryptographiques, dont un générateur de nombres aléatoires, peuvent aussi être implantées dans la puce pour préserver leur intégrité. Il sera alors possible de construire une architecture sécurisée sur cette fondation.

En particulier, le coffre contiendra une clé privée, de préférence définie sur une courbe elliptique pour des raisons de performance, qui permettra de vérifier la signature des mises à jour du micro-code et du logiciel d'exploitation de l'OC. Le mode de génération et d'implantation de la paire clé publique / clé privée devra être soigneusement étudié et les certificats, à un standard adapté aux OC, devront être gérés par une Infrastructure de Gestion de Clé (IGC) capable de traiter une configuration avec de très nombreux OC en offrant des services performants (notamment pour gérer les révocations) à travers un réseau dont la bande passante peut être limitée.

Le démarrage, voire l'arrêt, de l'OC devront être contrôlés dans les contextes les plus critiques. Ces actions peuvent être protégées par un mot de passe ou une clé dérivée à partir d'un mot de passe. Cet élément secret devra aussi être protégé. Idéalement l'intégrité du logiciel devrait être vérifiée à chaque (re)démarrage.

Les commandes reçues depuis une console d'administration, ou d'un serveur de contrôle, devront être authentifiées. Les données recueillies devront au moins être envoyées avec un contrôle d'intégrité cryptographique (par exemple un HMAC) et, quand elles sont sensibles, devront être chiffrées de bout en bout ou, si ce n'est pas possible, transiter par un réseau chiffré.

5

5.2 RÉSEAU DE TRANSMISSION

INTERVIEW

Bernard Roussely

Cyberens Technologies & Services

Notre conseil pour une PME qui souhaiterait intégrer la dimension cybersécurité dans son projet serait déjà de respecter quelques principes de bon sens : ne pas donner son mot de passe à un inconnu, avoir un esprit critique sur les solutions proposées par les vendeurs, faire simple (les solutions complexes sont rapidement contournées), maîtriser ses systèmes et son information, ne pas sous-estimer la motivation d'un adversaire et la valeur de son patrimoine informationnel, et pour finir, dans le doute, faire appel à des spécialistes.

Un minimum de notion d'ingénierie de sécurité est souvent nécessaire. Le choix des mesures de sécurité dépend de la menace identifiée, des informations traitées ou stockées et du contexte d'emploi. La difficulté avec les objets connectés est que certaines mesures de sécurité sont difficiles à mettre en œuvre dans des produits à faible coût et de capacités limitées. Il existe maintenant des structures spécialisées pour le développement d'objets connectés prototypes qui permettent de mettre les développeurs avec des professionnels de différents métiers (ex. le CATIE en Nouvelle Aquitaine). Il est recommandé d'utiliser leurs services pour éviter les erreurs de débutant.

Côté Cyberens , nous intervenons en particulier sur l'ingénierie de sécurité d'une solution (de l'analyse de risques dès la conception d'un système en préliminaire à la phase d'ingénierie poussée).

Les activités de Cyberens comportent essentiellement deux volets :

- ***Le conseil avec des audits et des analyses de sécurité dès la phase de conception jusqu'à la mise en service avec des outils d'analyse de risques comme EBIOS, la définition d'architectures de sécurité ou encore la mise en place de services opérationnels de cybersécurité (veille sur les menaces, SOC, CSIRT) ;***
- ***Le développement de logiciels de cybersécurité à base de cryptographie avec une solution de chiffrement de courriels, une application de gestion de licences et une bibliothèque ne contenant que des algorithmes réputés « forts ».***

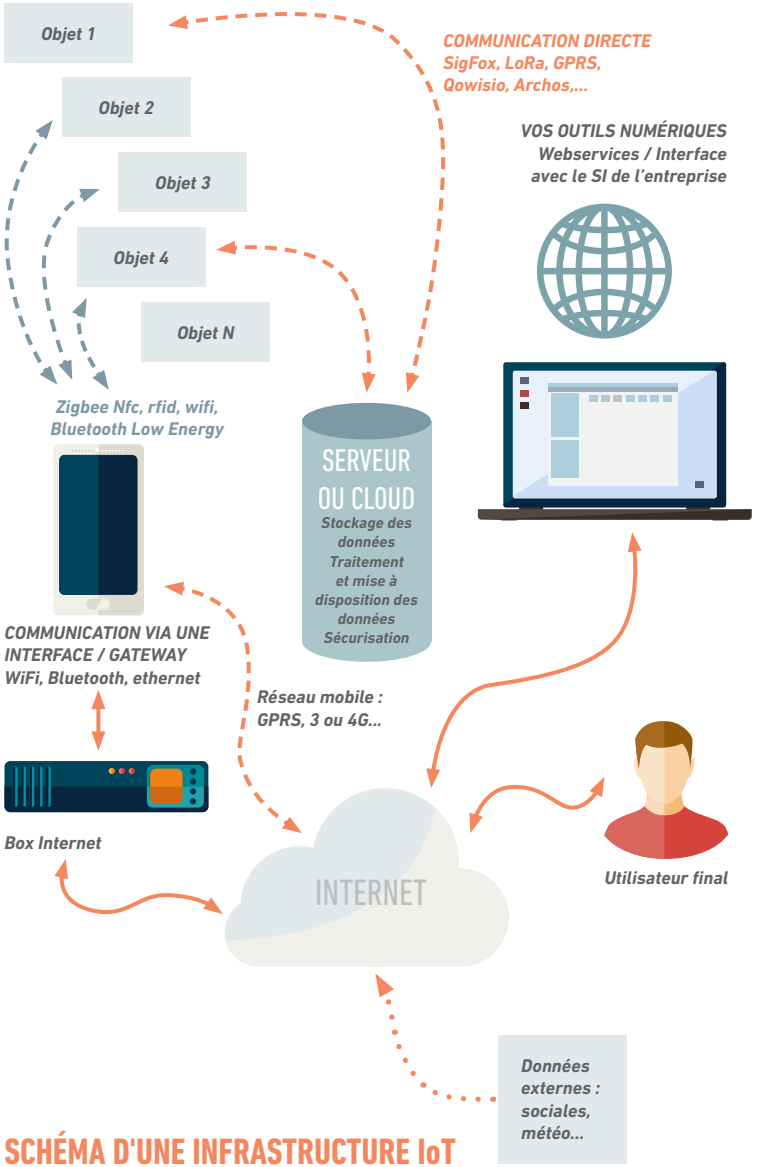


SCHÉMA D'UNE INFRASTRUCTURE IoT

5.2 RÉSEAU DE TRANSMISSION

De nombreux protocoles propres à l'internet des objets (IdO), ou plus anciens, peuvent être utilisés pour que les OC communiquent avec leur base arrière ou leur centre de contrôle. Certains protocoles permettent de communiquer localement avec les OC, d'autres permettent de communiquer à distance via une infrastructure adaptée.

Le choix du type de réseau et du protocole de communication devra se faire en fonction des besoins de disponibilité et de confidentialité. D'autres critères, sans rapport avec la sécurité, peuvent cependant influencer fortement le choix comme l'accès au réseau, sa couverture ou encore le coût de sa mise en œuvre (installation, abonnement, etc.).

L'IdO possède des protocoles d'échange de données spécifiques qui ne sont pas sécurisés. Pour assurer la confidentialité de ces données, il faudra donc soit utiliser un réseau chiffré soit assurer le chiffrement entre les OC et leur serveur de contrôle. Si le réseau n'offre pas de service propre, il faudra alors l'intégrer dans les OC et le serveur de contrôle pour l'assurer de bout en bout. Plusieurs options sont possibles, du développement spécifique à l'utilisation du protocole TLS adapté aux performances des OC.

De nombreuses infrastructures de réseau ont une bande passante assez faible et ce point devra faire l'objet d'une réflexion dans le cas où le système offre un service d'une certaine criticité.

Dans le cas où l'OC à une capacité de traitement très faible, il est probable qu'il doive être relié à un « agrégateur » (ou « passerelle ») qui pourra fournir différents services avant de renvoyer les données vers le centre de contrôle (le terme edge computing est souvent employé). La sécurité de cet agrégateur devra être prise en compte avec un point précis sur sa disponibilité car de nombreux OC en seront potentiellement dépendants.

5

INTERVIEW

Eric Dehais

OPPIDA
EXPERT EN SÉCURITÉ DES SYSTÈMES D'INFORMATION

Une de nos spécificités est d'être un des trois laboratoires agréés en France pour réaliser des évaluations Critères Communs et CSPN. Notre rôle consiste, dans le cadre du schéma français d'évaluation, à réaliser l'ensemble des contrôles et tests techniques permettant à une société de faire certifier et éventuellement qualifier son produit par l'ANSSI .

Ne s'adressant initialement qu'à des produits de sécurité (firewall, outils de chiffrement...), la démarche s'est étendue désormais à tout produit IT. On peut notamment citer des systèmes de contrôle d'accès, des automates industriels, et bien d'autres produits relativement éloignés des produits classiques de cybersécurité.

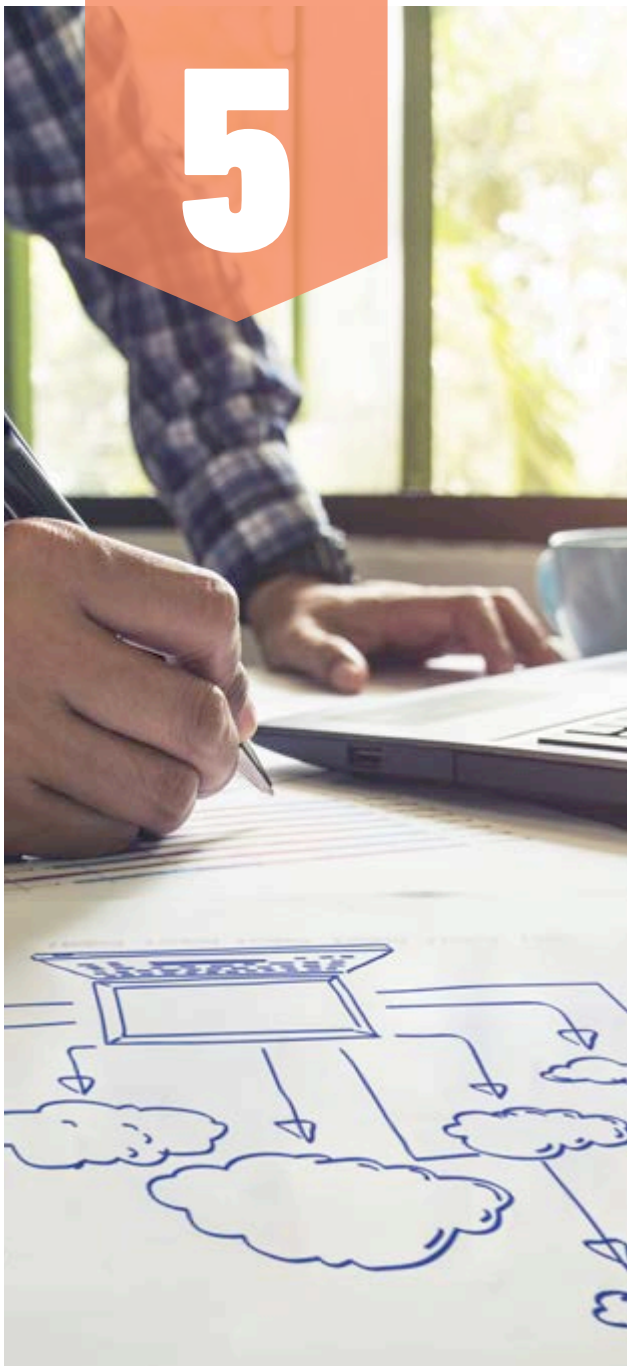
La certification des produits est désormais devenue un point de passage obligé dans de nombreux domaines. Pour les fournisseurs de solutions, les démarches de certifications sont de véritables facteurs de différenciation. Elles sont parfois même obligatoires pour accéder à certains clients et certains marchés. Pour les utilisateurs finaux, c'est un moyen de s'assurer préalablement de la sécurité du produit.

L'évaluation est faite sur la base d'une cible de sécurité (document rédigé par le client décrivant le produit et les fonctions à tester). Il n'existe pas de « check-list » de tests à réaliser.

Une évaluation se prépare. Nous conseillons, quelque soit le type d'évaluation, de faire monter en compétences les équipes de développement sur le domaine de la sécurité ainsi que de réaliser des tests préparatoires.

La préparation du produit et la formation des équipes permettent de limiter les risques d'échec et assurent un véritable transfert de compétences auprès des développeurs.

Acteur historique de la cybersécurité, Oppida a vu le jour en 1998. Avec près de 20 ans d'existence, Oppida est aujourd'hui le plus ancien cabinet de conseil indépendant en Sécurité des Systèmes d'Information. « Pure Player » Oppida réalise des missions d'expertise, d'évaluation et de conseil dans le domaine de la Sécurité des Systèmes d'Information (SSI).
Oppida est agréé en tant que Laboratoire d'Essai (CESTI), qualifié auditeur eIDAS, qualifié PASSI-LPM.



5.3 SERVEURS ET NUAGES

Le troisième sous-ensemble du système à sécuriser est la base arrière qui est composée d'un ou plusieurs serveurs de contrôle et de recueil des données renvoyées par les OC. Ces serveurs peuvent être hébergés sur un site distant (ou plusieurs sites) et la tendance est de les héberger dans un "nuage" mis en œuvre par un opérateur spécialisé.

Plusieurs serveurs avec des finalités différentes peuvent coexister pour, par exemple, assurer la diffusion des mises à jour du micrologiciel des OC, envoyer des commandes de configuration et de contrôle des OC, recueillir et traiter les données collectées ou générées par les OC.

L'accès à ces serveurs devra être sécurisé et, dans la mesure du possible, différents rôles (administrateur, développeur, utilisateur...) définis, avec des privilèges différents et en rapport avec la fonction (par exemple, exploitant, opérateur, administrateur), pour assurer leur fonctionnement et leur exploitation.

La disponibilité de ces serveurs devra faire l'objet d'une étude en fonction de la solution retenue (hébergement interne ou externe) et des mesures de sécurité éventuellement déjà en place par ailleurs.

Si des mises à jour des OC sont faites depuis un serveur de contrôle, une fonction d'authentification devra être implémentée pour éviter la prise de contrôle des OC par un tiers malveillant à l'aide d'une mise à jour factice.

La confidentialité et l'intégrité des données envoyées et recueillies seront aussi étudiées et mises en œuvre avec des protocoles et mécanismes supportés par les OC, sauf si les services (de confidentialité et l'intégrité) offerts par le réseau d'infrastructure sont acceptables.

La propriété des données hébergées devra être étudiée en fonction du type de service de "nuage" retenu. Dans certains cas, les données recueillies seront la propriété de l'opérateur du service et leur récupération éventuelle en cas de changement d'opérateur devra aussi être étudiée.

FOCUS

5

Présentation de la structure

Dans le cadre du Programme Investissements d'Avenir (PIA), la France s'est dotée de nouveaux outils d'innovation, les instituts de recherche technologique (IRT), réunissant recherche publique et recherche privée. L'enjeu était renforcer la compétitivité dans des filières technologiques stratégiques et la structuration d'écosystèmes puissants et performants d'innovation et de croissance. Les IRT mènent des activités qui couvrent l'ensemble du processus d'innovation en se déployant à la fois sur la R&D, la formation et la valorisation économique des résultats.

L'IRT Nanoelec a démarré en 2012 et ses activités se concentrent sur les technologies qui permettent d'améliorer les performances des circuits intégrés et d'offrir de nouvelles fonctionnalités (intégration 3D, photonique sur silicium). L'IRT travaille sur la diffusion des technologies par le développement de nouveaux produits ou services qui s'appuie sur la connectivité entre les objets et en liaison avec des travaux menés sur les usages.

La Cybersécurité est une thématique transverse dans Nanoelec avec des actions conduites dans trois de ses programmes : PULSE, FORMATION et EASYTECH. Le programme PULSE, fondé par des leaders industriels comme ST Microelectronics, Schneider Electric et Bouygues, ainsi que des laboratoires (CEA-Léti, Inria, Université Grenoble Alpes, Grenoble-INP) réalise chaque année des démonstrateurs de nouveaux services innovants et évalue leur performance et leur résistance aux attaques (physiques et logiciel). Le programme FORMATION conçoit les formations nécessaires à la bonne prise en compte de la Cybersécurité dans les entreprises. Deux premières formations (Préventeur Cybersécurité(1) et Manager de la sécurité(2) et des risques de l'information) ont ainsi été imaginées, respectivement par Grenoble-INP et Grenoble Ecole Management, ainsi que plusieurs modules pour enrichir des parcours de formations déjà existants.

Comment vous pouvez interagir avec les PME et ce que vous pouvez leur apporter

Le programme EASYTECH, dirigé par le pôle de compétitivité Minalogic est un programme à destination des PME souhaitant intégrer de l'intelligence dans leurs produits. Ce dispositif agile permet de mener à bien des projets innovants intégrant des technologies issues des organismes de recherche membres de l'IRT Nanoelec. A ce jour plus de 180 projets ont été réalisés pour des entreprises réparties sur plus de 30 départements.

Lors de rendez-vous conseils organisés 2 fois par mois, les PME peuvent échanger avec des experts pour mieux définir le besoin et les opportunités à saisir aussi bien sur des problématiques business que techniques. Ces accompagnements personnalisés permettent d'identifier des pistes d'innovation et de pouvoir accéder à de nouvelles sources de financement.

Pour aider les PME souhaitant améliorer la sécurité de leurs produits, ce type de dispositif est essentiel. Selon une étude récente de l'alliance ALLISTENE, la région Auvergne Rhône Alpes est le second vivier en compétences Cybersécurité, avec plus de 20% des chercheurs français. Nanoelec est un bon tiers de confiance pour aider les PME à identifier le bon partenaire pour renforcer la sécurité de leurs produits.

Les quick win essentiels en cybersécurité que doit appliquer une PME.

Renforcer la sécurité de leurs produits est désormais indispensable pour les PME. Une approche globale et systémique est vraiment nécessaire pour éviter le syndrome de la porte « blindée sur un mur de balsa » que l'on rencontre parfois. Le désarroi des entrepreneurs est grand, quand après une validation sécuritaire, ils réalisent qu'ils vont devoir redévelopper tout ou partie de leur produit et retarder la commercialisation de leurs innovations.

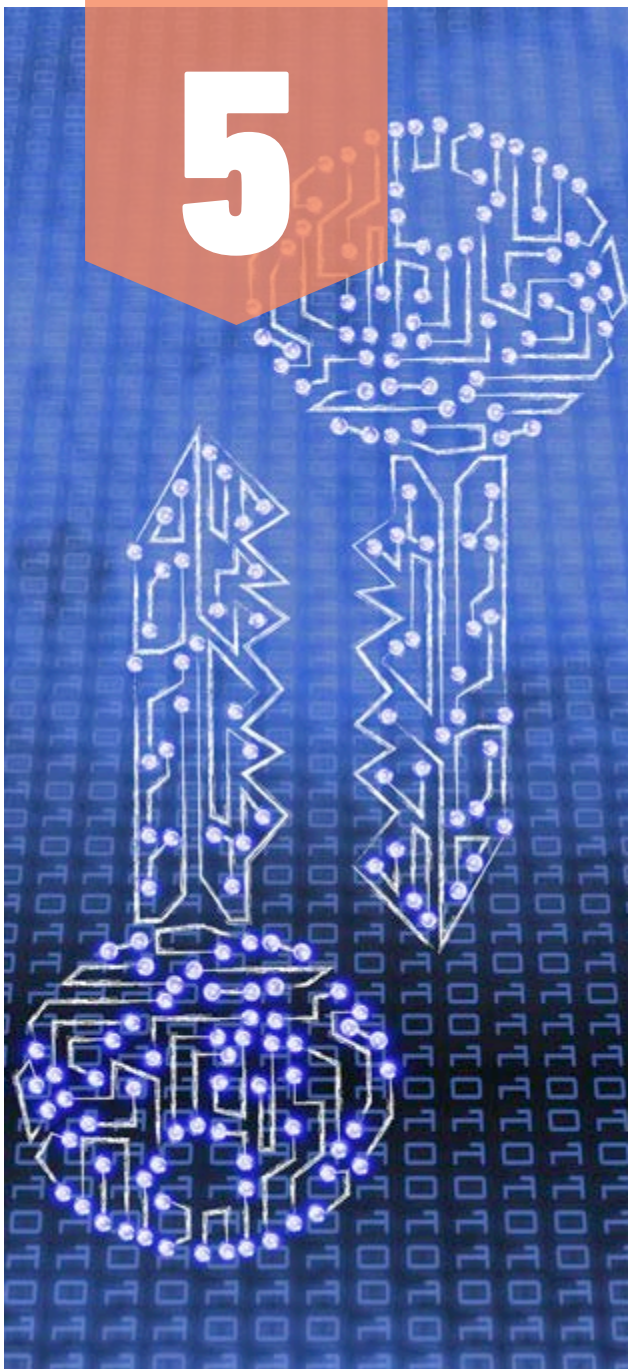
Une première recommandation est de conduire une analyse de risque et une caractérisation de la menace à laquelle leurs produits et services pourraient être confrontés. Avoir une idée claire des biens à protéger et de la nature des attaquants et des évènements à redouter est désormais essentiel. L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a développé de très bons outils pour les aider, comme par exemple la méthodologie d'analyse de risques EBIOS. Mais il est souvent utile pour les PME d'être aidées d'experts pour les mettre en œuvre.

La sécurité tout au long du cycle de vie de leurs futurs produits doit également être prise en compte. Cela nécessite de réfléchir aux futures mises à jour des logiciels embarqués, aux réparations et changements de sous-systèmes associés. Tous ces points dimensionnent l'architecture (électronique, logiciel) à mettre en place pour vérifier l'intégrité des systèmes, gérer et assurer la traçabilité des modifications, et bien sûr protéger la propriété intellectuelle des PME contre la copie et la contrefaçon. Il y a encore trop d'exemples de PME qui sous-estiment cela et se retrouvent avec leurs innovations contrefaites rapidement, faute de protection adéquate de leurs systèmes embarqués.

Enfin, une validation sécuritaire menée par des laboratoires indépendants dont la compétence est vérifiée (par des accréditations) est souvent un plus significatif. Cela peut éviter, au mieux, les mauvais buzz sur Internet et dans les cas les plus graves des actions en justice pour ne pas voir suffisamment pris en compte les risques de détournement de leurs produits. Aux Etats-Unis, la Commission fédérale du commerce (FTC) a déposé plainte en 2017 contre un fabricant d'objets connectés en lui reprochant de mettre en danger des milliers de clients en ne sécurisant pas ses caméras IP et ses routeurs.

Sur chacune de ces étapes l'IRT Nanoelec peut assurer l'interface entre les PMEs et les interlocuteurs régionaux membres de Nanoelec. Les PME ont la possibilité de collaborer plus facilement avec le vivier d'experts et de chercheurs ayant un rayonnement international dans le domaine de la cybersécurité et capables de les conseiller sur les choix technologiques de la sécurisation.

Bruno Charrat
Directeur du Programme
PULSE, IRT Nanoelec



5.4 IMPLÉMENTATION ET MISE EN ŒUVRE DE LA CRYPTOGRAPHIE ET DU CHIFFREMENT

Ce chapitre aborde quelques pratiques techniques relatives à la cybersécurité à mettre en œuvre lors de la conception d'un produit connecté. Ce chapitre n'est pas exhaustif dans les moyens techniques et ne se veut pas être un guide de conception garantissant une inviolabilité du produit, mais il expose les fondamentaux actuels.

De nombreux services de sécurité reposent sur des fonctions et des mécanismes cryptographiques et plusieurs options s'offrent aux fabricants et développeurs d'OC pour les implanter :

- réaliser des développements spécifiques
- utiliser du logiciel en source ouverte
- utiliser des fonctions implantées dans des composants sur étagère

Dans le premier cas, les développements devront être confiés à (ou encadrés par) des personnes expérimentées en cryptographie pour éviter des erreurs basiques de codage et de mise en œuvre.

Dans le second cas, il est recommandé de faire examiner le code par des personnes expérimentées et sans doute de le limiter aux services strictement nécessaires (règle de minimalité) à l'atteinte des objectifs.

En effet, si les logiciels en source ouverte sont riches et permettent d'accélérer les développements, ils ne sont pas exempts de problèmes et de vulnérabilités et sont parfois fournis sans support technique.

Dans le troisième et dernier cas, il convient de vérifier au moins les versions des protocoles et mécanismes implantés car elles sont souvent en décalage par rapport aux versions intégrant des correctifs de sécurité. Les fonctions cryptographiques devront être testées. De préférence, des composants ou briques logicielles certifiés devront être choisis en priorité.

Les différents services cryptographiques, dans la mesure du possible, et la conformité aux standards nécessitent plusieurs types de clés pour fonctionner. L'IGC (Infrastructure de Gestion de Clé) sera donc sans doute un service critique pour le fonctionnement du système. Sa mise en œuvre et son exploitation devront être particulièrement soignées, en particulier lors de la génération et la distribution des clés privées et secrètes.

De même, selon le contexte, l'enregistrement d'un nouvel OC dans le système ainsi que son retrait (ou sa destruction ou sa perte) devront sans doute être correctement appréhendés au sein de l'IGC pour éviter une possible fuite d'éléments secrets.

5.4 IMPLÉMENTATION ET MISE EN ŒUVRE DE LA CRYPTOGRAPHIE ET DU CHIFFREMENT

5

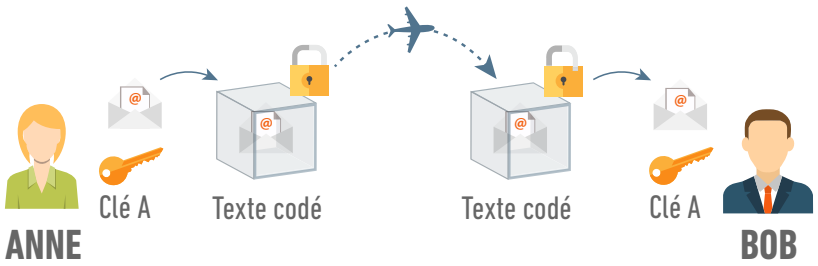
Méthodes de chiffrement

Avant d'aborder le processus de conception, abordons les 3 grands principes de chiffrements et de signature de la donnée afin de comprendre les mécanismes et bonnes pratiques décrits plus loin. Le but est de chiffrer un message afin de garantir la confidentialité de la donnée transmise et si possible de l'identité de l'expéditeur lors du déchiffrement. En fonction de la méthode choisie, l'attaque que devra réaliser un tiers pour déchiffrer sera plus ou moins complexe.

Chiffrement symétrique

L'algorithme de chiffrement symétrique est basé sur la confidentialité d'un mot de passe, appelé la clé de chiffrement/déchiffrement. Toute personne possédant la clé peut chiffrer et déchiffrer les messages émis entre les tiers utilisant la même clé. Il est impossible de distinguer qui est l'émetteur d'un message si la clé est partagée entre plusieurs produits diffusant de la donnée.

Si la clé est compromise, il devient possible à un attaquant de décoder l'ensemble des messages échangés et de falsifier des messages à injecter sur le réseau.



INTERVIEW

Laurent Meyer

Digitam

Intervenant dans différents domaines de l'industrie, nous sommes souvent sollicités par des entreprises mises en difficulté suite à un produit introduit sur le marché bien que présentant des défauts électroniques et/ou logiciels. Nous expertisons le produit afin de le remettre sur le marché le plus tôt possible et aidons l'entreprise à ne pas reproduire le problème. Bien entendu, il est préférable de prendre ces aspects bien plus en amont (en investissant par exemple dans un banc de test approprié) car une fois l'objet connecté dans la nature et en grande quantité, les erreurs et bugs seront difficiles et couteux à corriger. Anticiper doit en effet être le maitre mot. La faille la moins chère à corriger est celle qu'on ne produit pas. Avoir des équipes formées, appliquer les bonnes pratiques dès le départ impactera bien moins le projet et l'entreprise qu'une expertise pour régler le problème a posteriori.

Nous recommandons d'avoir une vision système / architecturée de son objet dès la conception (dans le but d'intégrer les exigences de testabilité et de sécurité dès le début) et de ne pas négliger les compétences télécoms, la partie connectée de l'objet. Une indisponibilité du serveur ou du canal de communication ne doit pas empêcher l'objet de fonctionner.

Enfin les équipes techniques du projet doivent être formées aux concepts de la cybersécurité, (a minima comprendre les attaques et les principes du chiffrement).

DIGITAM est un centre d'expertise en systèmes embarqués et objets connectés.

Nous aidons nos clients à concevoir des systèmes IOT (électronique et micro-logiciel) surs et sécurisés. Ceci à travers nos formations, nos expertises et notre bureau d'étude. La cybersécurité prend une place toujours croissante dans nos activités, et nous développons une méthodologie pour aider nos clients à la mettre en place dans leurs cycles de développement logiciel.

5 5.4 IMPLÉMENTATION ET MISE EN ŒUVRE DE LA CRYPTOGRAPHIE ET DU CHIFFREMENT

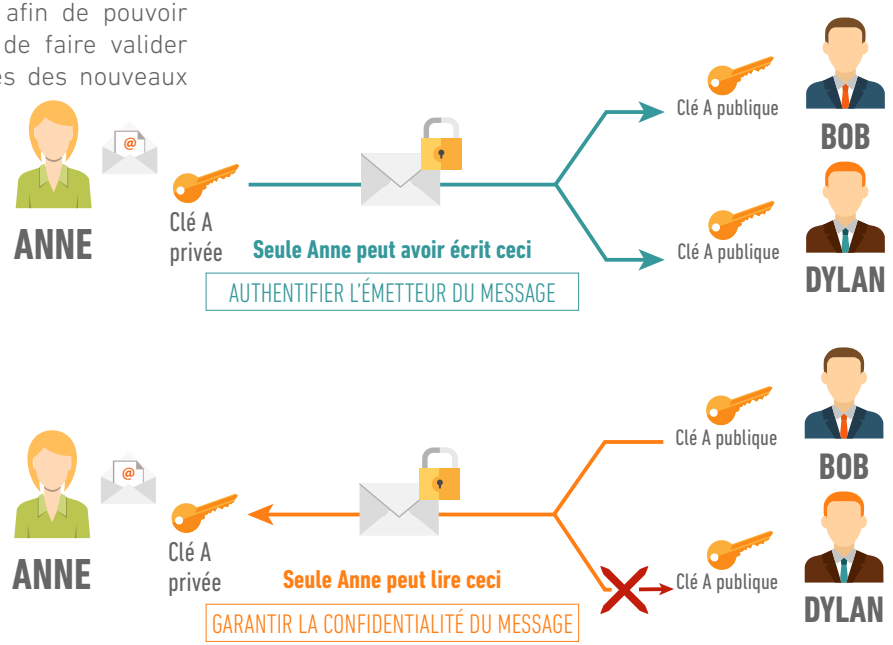
Chiffrement asymétrique

L'algorithme de chiffrement asymétrique est basé sur un couple de clés que possède chaque personne ou entité voulant échanger des messages. Chaque produit possède une clé dite publique qui est communiquée à toute entité devant échanger de la donnée et une clé privée qui n'est connue que du produit. Pour échanger des données, un produit émetteur chiffre la donnée avec la clé publique du produit destinataire. Le destinataire déchiffrera la donnée avec sa clé privée. La méthode est donc asymétrique, chiffrement avec la clé publique, déchiffrement avec la clé privée. Il apparait que seul le destinataire peut décoder le message qui lui est destiné car il est le seul à connaître sa clé privée. Si une clé privée est compromise, seul un produit est compromis sur le réseau, à condition de respecter une clé privée par produit. De plus, ce mécanisme permet également de signer les messages par l'émetteur afin d'authentifier la provenance. Dans ce cas, l'émetteur chiffre une seconde fois le message préalablement chiffré avec la clé publique du destinataire. Cette fois pour ce second chiffrement, l'émetteur utilise sa propre clé privée. La première action faite par le destinataire sera alors de déchiffrer le message reçu avec la clé publique de l'émetteur afin de s'assurer de la provenance du message. Dans la pratique, pour des raisons de temps de calcul, seule une partie du message expédié est chiffrée pour authentifier l'expéditeur et non sa totalité.

Clés publiques et certificats

Afin de prendre en compte l'augmentation d'un parc de produits et de se faciliter l'intégration des produits futurs, il peut être nécessaire de privilégier une architecture avec une autorité centrale pour permettre la diffusion des clés publiques des produits. Dans ce cas, il convient de mettre en œuvre un serveur qui fournira les clés publiques à l'ensemble des produits afin de leur permettre de communiquer entre eux. Ce serveur sécurisé a un rôle central, et chaque produit contient un certificat de ce serveur afin de pouvoir communiquer avec lui, dans le but de faire valider les clés publiques existantes et celles des nouveaux produits apparaissant sur le réseau.

Le certificat contient les données de l'identité numérique du serveur (Nom, Adresse, Clé publique). Si une clé privée est compromise, ce mécanisme a pour avantage de pouvoir invalider une clé publique facilement sur l'ensemble des produits utilisant ce serveur. Dès lors qu'un produit interroge un serveur sur l'authenticité d'une clé publique, le serveur informe le produit sur la qualité fallacieuse ou non de cette clé.



5.4 IMPLÉMENTATION ET MISE EN ŒUVRE DE LA CRYPTOGRAPHIE ET DU CHIFFREMENT

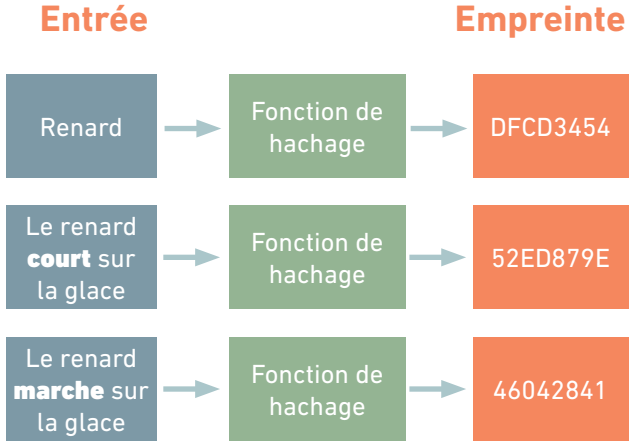
5

Hash

Le hash d'un message sert à valider la non-détérioration d'un message lors de sa transmission. Ce mécanisme est pratique dès lors qu'on utilise des connexions sans code correcteur pour vérifier à réception du message son intégrité ou pour associer un message à une signature électronique. Ce principe n'a pas vocation à garantir la confidentialité de la donnée échangée. Une fonction de hash répond à une définition stricte, cette fonction est injective. Il est donc impossible d'obtenir la même valeur de sortie pour des entrées différentes de la fonction. Quand un message est transmis, le résultat de la fonction de hash est également fourni, afin que le produit puisse vérifier qu'il obtient le même résultat de la fonction de hash que la valeur transmise afin de valider l'intégrité du message transmis.

Quel mot de passe, quel algorithme de chiffrement, quelle infrastructure de certificats ?

Afin de préserver la sécurité informatique, les chercheurs travaillent en continu à trouver des failles dans les algorithmes de chiffrement et définir des bonnes pratiques pour les longueurs de clé. En France, l'ANSSI publie un guide, [Mécanismes cryptographiques - Règles et recommandations, Rev. 2.03, ANSSI, 02/2014], mis à jour régulièrement sur les dernières avancées en matière de chiffrement afin de conseiller les algorithmes à utiliser et ceux à bannir car des vulnérabilités ont été découvertes. Une entreprise doit être responsable de l'efficacité des moyens de chiffrement mis en œuvre et se doit, si nécessaire, de faire appel à une expertise afin de confirmer ses choix et de s'assurer de leur bonne mise en œuvre. Avec la RGPD, la confidentialité des données personnelles devient obligatoire ce qui en fait un pilier stratégique pour l'entreprise



Une fonction de hachage garantit l'unicité de l'empreinte.

5

5.4 IMPLÉMENTATION ET MISE EN ŒUVRE DE LA CRYPTOGRAPHIE ET DU CHIFFREMENT

INTERVIEW

Philippe Wolf
Chef de projet

SYSTEMX

L'IRT SystemX est une fondation de coopération scientifique pour faire travailler des partenaires de recherches et des industriels, dans le domaine de l'ingénierie numérique des systèmes du futur. L'IRT SystemX répond aux défis technologiques d'aujourd'hui au moyen d'une innovation flexible, ouverte et collective. L'IRT travaille sur les cas d'usage de la transformation numérique et offre aux industriels des recherches finalisées.

Mon groupe de travail EIC (Environnement pour l'Interopérabilité et l'Intégration en Cybersécurité) au sein de l'IRT, et en collaboration avec l'ANSSI, a pour but de réaliser un environnement pour détecter les failles de sécurité dans les réseaux et les éléments qui les composent au travers de technologies innovantes et de recherches sur la simulation hybride. Cette nouvelle approche de simulation interface des équipements réels (de réseaux, serveurs, objets connectés) avec des équipements virtuels. Ces recherches ont pour objectif de répondre à ***"comment sécuriser des systèmes complexes ?"*** que sont les Smart Grids, le transport d'énergie intelligent, l'usine connectée ou encore les Smart Cities. Ce projet de recherches construit une plateforme CHESS (Cybersecurity Hardening System of Systems) qui permet, par exemple, de trouver les équipements à durcir dans un Smart Grids pour éviter des effets en cascade depuis la fuite de données jusqu'au blocage de la distribution énergétique. Ces travaux de recherches sont menés conjointement avec des industriels tels que Airbus, Engie, Bertin, Gemalto, Prove&Run et Thales, et ils ont montré l'importance de sécuriser les concentrateurs de quartier afin d'éviter toute intrusion. Ces collaborations de recherches permettent, également, de créer des liens économiques entre des grands groupes et des PME. Un autre travail réalisé a été d'étudier une usine de traitement des eaux afin de détecter les faiblesses des automates pilotant l'usine pour définir une stratégie de protection et de ségrégation des réseaux critiques et le déploiement sur l'infrastructure numérique de solutions de sondes réseaux pour détecter les comportements anormaux le plus tôt possible. Les solutions du futur pour la protection des réseaux seront basées sur l'apprentissage comportemental afin de détecter les intrusions et les anomalies de fonctionnement des services. Un axe important de recherches, mené conjointement avec le CEA, est de démontrer des applications du chiffrement homomorphe à des applications industrielles *(https://hal.archives-ouvertes.fr/hal-01435505).*

Un autre axe de travail[1] pour le groupe EIC est la protection des PME contre les ransomwares ou rançongiciels et l'assurabilité face aux risques cyber. En allant à la rencontre des dirigeants de PME, nous nous sommes rendu compte de l'importance de former ces dirigeants aux risques Cyber et du manque d'offres à destination des PME. Ces travaux ont aussi démontré que les offres des assureurs proposées aujourd'hui ne sont pas adaptées à tous les risques Cyber, ce qui pousse les assureurs à réfléchir à de nouvelles offres. De ces travaux, nous en avons déduit 5 thématiques :

1. Information vers les dirigeants sur le risque Cyber et,
2. sur les prestataires pouvant former le personnel,
3. Urbanisation des infrastructures de l'entreprise avec des moyens de défense appropriés aux menaces actuelles telle que la sauvegarde hors ligne pour se prévenir des crypto-virus,
4. diffusion de prestataires de confiance pour les services d'hébergement et de stockages de données,
5. entraînement des ressources de l'entreprise à réagir correctement en cas d'attaque cyber touchant la PME.

Au-delà des travaux de recherches techniques, l'IRT SystemX travaille également à proposer des stratégies et solutions juridiques et réglementaires en cybersécurité.

L'IRT SystemX réalise un appel[2] aux Start-Ups, proposant des solutions en cybersécurité, afin d'accueillir les lauréats à travailler pendant 6 mois sur la plateforme CHESS afin de confronter leur solution à des cas d'usage.

(1)http://www.irt-systemx.fr/wp-content/uploads/2017/10/ISX-IC-Cyber-Risque.pdf

(2) http://www.irt-systemx.fr/valorisation/startsystemx/les-thematiques/

5.5 QUELQUES RECETTES PRATIQUES

5

Quelques recettes pratiques

Ce document a exposé l'importance de l'analyse des risques et de l'adéquation de la sécurité face aux risques encourus et non face à la valeur du produit. La cybersécurité peut être comparée à une chaine qui a la force de son maillon le plus faible, il est donc important d'être cohérent sur l'ensemble des moyens mis en œuvre pendant le cycle de conception et de la vie du produit. Il a été exposé qu'il existe trois interfaces d'attaques pour un hacker :

- Depuis le réseau, soit directement par les connexions réseaux du produit ou l'application fournie pour utiliser le produit
- Depuis le produit en s'introduisant sur l'électronique pour récupérer des informations, par exemple, sur le bus mémoire
- Depuis les composants qui permettent une retro engineering du produit, par exemple, lecture de la mémoire de stockage du firmware

Les attaques les plus classiques restent :

- l'exploitation d'une faille dans le protocole de communication entre le produit et un serveur ou un smartphone. Cette attaque permet de passer outre les mécanismes de sécurité pour récupérer les données utilisateur, le firmware ou permettre l'exécution de code malveillant
- depuis l'électronique en obtenant la mise en mode de test de production du produit pour en prendre le contrôle
- la mise en défaut d'un composant électronique réalisant le générateur aléatoire de nombres, pilier des mécanismes de cryptographie afin de réduire le niveau de protection du système.

Comme évoqué dans ce document, un produit connecté sûr repose sur 4 étapes majeures de conception :

- Authentification du produit
- Protection des données échangées par le produit
- Protection des données manipulées par le produit
- Protection des données stockées par le produit

Authentification du produit

Le but est d'assurer l'identité des produits sur le réseau, ce qui est primordial quand le réseau est ouvert à tous et peut posséder des millions de produits générant des flux importants de données personnelles. Il serait donc catastrophique pour l'entreprise qu'un produit espion puisse accéder à ces informations. Nous avons vu précédemment les différentes méthodes pour chiffrer les messages afin de permettre l'échange de données et simultanément authentifier le produit émetteur. Un chiffrement asymétrique de la donnée, associé à une infrastructure de serveurs de certificats est aujourd'hui le plus adapté au monde des produits connectés. Cet ensemble technique représente l'état de l'art à mettre en œuvre dans de nouveaux produits vis-à-vis de la cybersécurité. Il est tout aussi primordial de garantir l'intégrité d'une clé publique générée et stockée dans un produit que de garantir l'intégrité de la clé privée.

5

5.5 QUELQUES RECETTES PRATIQUES

En effet, si une clé publique peut être changée, alors un appareil espion sur le réseau pourra émettre des messages à destination de l'ensemble des produits. Dans le cas d'utilisation d'une infrastructure avec serveur de certificats, il est également plus difficile de corrompre une clé publique, car les produits voulant échanger des données avec un tiers doivent faire valider la clé publique de ce tiers par ce serveur.

Idéalement, l'environnement matériel du produit doit contenir un générateur de clés, un coffre-fort pour stocker les clés et une unité matérielle d'exécution cryptographique pour réaliser les opérations de dé/chiffrement. Le but est de s'assurer de l'unicité des clés par produit et garantir que celles-ci ne seront pas dévoilées facilement par rétro-ingénierie. Les microprocesseurs et microcontrôleurs modernes proposent ces fonctionnalités : lors de la conception du produit, il convient donc de se former à leur utilisation afin de réaliser un pas important vers la sécurisation du nouveau produit connecté.

Lors de la fabrication, la génération des clés et leur chargement dans les produits est une étape critique car faite le plus souvent en dehors des murs de l'entreprise par des sociétés sous-traitantes, il convient donc de mettre en place les procédures garantissant la confidentialité de ces données.

Il convient, comme évoqué avec les fonctions de Hash, d'avoir un mécanisme pour authentifier le firmware exécuté par le produit. Là encore le matériel récent permet de s'assurer de l'intégrité du firmware et de garantir que le produit n'a pas été corrompu. Idéalement, ce firmware doit pouvoir se mettre à jour au travers du réseau et nécessite des fonctions de boot avancées. Le plus simple au vu de la technicité spécifique d'un logiciel de boot est de faire appel à un éditeur spécialisé ou choisir un équipementier électronique proposant ce type de solution avec son processeur.

Protection des données échangées par le produit

Comme évoqué, le chiffrement des messages échangés par un produit connecté avec un tiers est devenu la « base » pour la cybersécurité. Aujourd'hui les systèmes d'exploitation du commerce ou opensource fournissent des bibliothèques pour gérer ces communications chiffrées. Pour certains produits, où l'autonomie est un enjeu important, le chiffrement de messages peut être vu comme un handicap. Là encore, disposer d'un composant matériel spécialisé permettra d'être plus rapide et plus efficient énergétiquement qu'une solution uniquement logicielle. L'importance du choix d'un matériel adapté et de sa maitrise est un enjeu majeur dans la conception d'un produit connecté.

5.5 QUELQUES RECETTES PRATIQUES

5

Protection des données manipulées par le produit

Sur le produit, le code qui s'exécute et les données manipulées sont des données sensibles qu'il convient également de protéger contre les attaques physiques, modification, corruption ou vol. Il convient d'empêcher l'accès aux clés de chiffrement durant le fonctionnement du produit ce qui serait une conséquence catastrophique pour la sécurité du produit.

La protection des informations peut se faire directement par le processeur qui contient des éléments matériels sécurisés nécessaires tel qu'un « secure element » ou une plateforme d'exécution sécurisée. Un secure element a pour but de fournir un coffre-fort pour le stockage de données confidentielles et les fonctions de cryptographie.

Une plateforme d'exécution sécurisée est désignée pour répondre à des critères d'intégrité d'exécution élevés, par exemple les microprocesseurs spécifiques utilisés dans les cartes bancaires, cartes SIM...

Il est possible d'ajouter ces composants matériels externes au processeur principal du produit pour réaliser ces fonctions de sécurité. Toutefois, il convient d'établir un bus de communication enfoui et sécurisé entre le processeur et l'élément de sécurité.

Il est possible de mettre en œuvre des mesures purement logicielles tel que l'offuscation de code qui est un premier niveau de sécurisation et qui permet d'augmenter l'effort à fournir par un attaquant pour faire de la retro-ingénierie sur le produit.

L'autre point important est de s'assurer que le produit n'exécute que le code du produit et non un code tiers comme expliqué précédemment. Le mécanisme dit de « secure boot » est un bootloader (logiciel réalisant le chargement du code) qui autorise uniquement l'exécution d'un firmawre signé par le fabricant.

Ce type de logiciel s'appuie sur les fonctionnalités fournies par le processeur pour stocker et vérifier une fonction de hash pour permettre ou non l'exécution du programme.

Il est aussi important de prendre en compte les mises à jour futures d'un produit en intégrant un bootloader pouvant mettre à jour par les réseaux disponibles les firmwares du produit tout en utilisant des méthodes de chiffrement afin de vérifier leur intégrité et leur provenance.

Protection des données stockées par le produit

Les données recueillies et stockées doivent également être protégées. Nous avons vu que les secure elements permettent de fournir un coffre-fort pour stocker des données tels que les clés de chiffrement et les certificats. Ces composants ne sont pas faits pour stocker de grandes quantités de données. Il existe des mémoires (ROM, RAM, FLASH) intégrant des mécanismes de chiffrement et/ou anti-intrusion qui rendent difficile les attaques contre les données stockées par le produit.

5

5.5 QUELQUES RECETTES PRATIQUES

INTERVIEW

Jean-Philippe MALICET
Directeur national du
Programme CAP'TRONIC

CAP'TRONIC
Systèmes électroniques et logiciel embarqué

Pourquoi faire de la cybersécurité un axe fort de la mission de CAP'TRONIC ?

CAP'TRONIC a pour but d'accompagner les PME dans leurs défis technologiques et de les sensibiliser aux nouveaux enjeux créateur de valeur. Ces 5 dernières années le programme a mis l'accent sur l'IoT et les nouveaux usages associés aussi bien en B2B qu'en B2C, ainsi que sur l'organisation des projets pour réussir au mieux l'industrialisation des produits.

Nous conseillons les start-up, PME & ETI sur les technologies associées à l'IoT telle que la connectivité sans fils, les capteurs, l'électronique numérique intégrée, l'autonomie énergétique, l'architecture logicielle, la sureté de fonctionnement... pour tous les secteurs d'activité (industrie, santé, bâtiment) avec des fonctions des plus simples aux plus complexes.

Aujourd'hui, face à la généralisation des systèmes connectés et interconnectés, il devient primordial de protéger les données collectées et échangées pour garantir le bon fonctionnement des services proposés, la confidentialité des données mais aussi l'intégrité et l'authenticité de ces données qui sont un élément essentiel des services proposés.

La cybersécurité est une science jeune en évolution permanente, quelle légitimité de traiter de cette thématique pour un programme tourné vers l'électronique ?

Les 24 ingénieurs CAP'TRONIC, présents sur toute la France, conseillent chaque année plus de 700 PME avec pour objectif principal de réussir leurs projets en mettant sur le marché des produits intégrant de l'électronique qui fonctionne, en retenant les meilleures solutions techniques, en optimisant les coûts et en respectant les délais. Ils s'appuient pour cela sur un réseau de plus de 300 centres de compétences publics et privés en électronique et en logiciel embarqué. Ces centres sont des laboratoires universitaires, des écoles d'ingénieurs ou des sociétés d'études électroniques du secteur privé.

Le rôle d'un ingénieur conseil CAP'TRONIC est en perpétuelle évolution, et les séminaires & formations que nous organisons en sont les meilleures preuves car ils sont là pour aider les PME à bénéficier de toutes les technologies actuelles et de demain.

La cybersécurité est une thématique récurrente depuis 3 ans. Nous avons mis en place un programme de formation des ingénieurs CAP'TRONIC afin de leur apporter des bases solides pour leur permettre de conseiller aussi bien les Start-up que les TPE/PME et de faire intervenir les experts les plus adaptés.

Vous sensibilisez habituellement à l'importance de penser un projet électronique dans son ensemble de la maquette à l'industrialisation, conseillez-vous également de considérer la cybersécurité en amont et dans sa globalité ?

En effet, s'il y a deux bonnes pratiques à retenir de ce guide, ce serait, d'une part d'être cohérent sur la valeur du service proposé et la protection de la donnée associée (quel usage, quelle valeur, quel danger & pour quel coût) afin de définir les moyens de sécurité pertinents et adaptés à déployer, et d'autre part d'être évolutif sur le logiciel, afin de corriger les vulnérabilités à venir. Il sera plus facile, plus rapide et moins couteux de prendre en compte la gestion de la cybersécurité le plus en amont possible dans son projet, au même titre que les fonctions du produit et les exigences réglementaires et d'utilisation.

5.6 LEXIQUE

5

AES : Advanced Encryption Standard, soit « standard de chiffrement avancé » en français est un algorithme de chiffrement symétrique.

Agile : une méthode Agile est une approche itérative et collaborative, capable de prendre en compte les besoins initiaux du client et ceux liés aux évolutions.

B2B ou Business to Business : Modèle d'affaire d'une entreprise visant une clientèle d'entreprises.

B2C ou Business to Consumer : Modèle d'affaire d'une entreprise visant une clientèle de particuliers.

Blockchain : est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle

CCRT : Centre de Calcul Recherche et Technologie est une des composantes du complexe de calcul scientifique du CEA .

Certificat : un certificat électronique (aussi appelé certificat numérique ou certificat de clé publique) peut être vu comme une carte d'identité numérique. Il est utilisé principalement pour identifier et authentifier une personne physique ou morale, mais aussi pour chiffrer des échanges.

Chiffrement : est une opération qui consiste à transformer un message à transmettre, dit « message clair », en un autre message, inintelligible pour un tiers, dit « message chiffré », en vue d'assurer le secret de sa transmission. (Application d'un codage pour le traitement des questionnaires d'une enquête statistique.)

Chiffrement asymétrique : cryptographie dans laquelle on utilise une paire de clés asymétriques, une clé publique et la clé privée correspondante, pour chiffrer et déchiffrer les données. La cryptographie asymétrique rend aussi possible l'utilisation de la signature numérique qui permet de corroborer l'origine d'un message.

Chiffrement homomorphe : chiffrement qui possède certaines caractéristiques algébriques qui le font commuter avec une opération mathématique, c'est-à-dire que le déchiffrement du résultat de cette opération sur des données chiffrées donne le même résultat que cette opération

Chiffrement symétrique : cryptographie également dite à clé secrète (par opposition à la cryptographie asymétrique), est la plus ancienne forme de chiffrement. Elle permet à la fois de chiffrer et de déchiffrer des messages à l'aide d'un même mot clé.

Clé : est un paramètre utilisé en entrée d'une opération cryptographique (chiffrement, déchiffrement, scellement, signature numérique, vérification de signature). Une clé peut se présenter sous plusieurs formes : mots ou phrases, procédure pour préparer une machine de chiffrement (connexions, câblage, etc.)

5

5.6 LEXIQUE

Cloud : connu sous le terme français de « Nuage » est l'exploitation de la puissance de calcul ou de stockage de serveurs distants par l'intermédiaire d'un réseau, généralement l'internet.

Cryptovirus : est un virus de type cheval de Troie, et plus précisément un ransomware. Son fonctionnement est basé sur le chiffrement de données personnelles, et ces données ne pourront être décryptées qu'au paiement d'une rançon permettant de recevoir une "clé de décryptage".

CSIRT : Computer Security Incident Response Team est un centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises ou aux administrations, mais dont les informations sont généralement accessibles à tous.

EBIOS : est une méthode d'évaluation des risques en informatique par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

eIDAS : electronic IDentification, Authentication and trust Services est une norme européenne autour des transactions électroniques.

Firmware : est un programme intégré dans un matériel informatique (ordinateur, photocopieur, automate (API, APS), disque dur, routeur, appareil photo numérique, etc.) pour qu'il puisse fonctionner.

FTPS : File Transfert Protocol Secure - recouvre les différentes manières d'envoyer de manière sécurisée des données par FTP. Les informations transmises sont cryptées, afin d'en garantir la confidentialité.

Hacker : personne qui, par jeu, goût du défi ou souci de notoriété, cherche à contourner les protections d'un logiciel, à s'introduire frauduleusement dans un système ou un réseau informatique.

Hash : séquence de caractères alphanumériques de longueur fixe, qui représente le contenu d'un message, sans le révéler, dont la valeur unique est produite par un algorithme de hachage, et qu'on utilise pour créer une signature numérique.

HMAC : de l'anglais keyed - Hash Message Authentication Code (code d'authentification d'une empreinte cryptographique de message avec clé), est un type de code d'authentification de message (CAM), ou MAC en anglais (Message Authentication Code), calculé en utilisant une fonction de hachage cryptographique.

HTTPS : HyperText Transfert Protocol Secure est un mode de sécurisation technique des données échangées entre le serveur visité et les internautes.

Injective : une fonction est dite injective si deux éléments distincts de son ensemble de départ ont deux images distinctes par cette fonction.

Malware : est un terme anglais signifiant nuisible/malveillant, un "malware" est un logiciel pouvant être un virus, vers, spywares, keyloggers, chevaux de Troie, backdoors.

MISRA C : est une norme de programmation en langage C créée en 1998 par la Motor Industry Software Reliability Association.

5.6 LEXIQUE

OWASP : Open Web Application Security Project est un guide de sécurisation des applications web, c'est un « ouvrage » de référence des bonnes/mauvaises pratiques de développement, d'une base sérieuse en termes de statistiques, et d'un ensemble de ressources amenant à une base de réflexion sur la sécurité.

Passerelle de communication ou Gateway : désigne un dispositif permettant de relier deux réseaux distincts présentant une topologie différente.

PASSI-LPM : est un prestataire d'audit de la sécurité des systèmes d'information qualifié pour les besoins de sécurité nationale. La mention PASSI LPM porte sur les catégories de prestations d'audit pour lesquelles le prestataire est qualifié.

Pen Testing : une méthode d'évaluation de la sécurité d'un système.

Ransomware : est un logiciel informatique malveillant, prenant en otage les données, il chiffre et bloque les fichiers contenus sur votre ordinateur et demande une rançon en échange d'une clé permettant de les déchiffrer.

RGPD : est l'initiale de Réglement Général pour la Protection des Données et désigne la dernière directive européenne concernant les données personnelles, publiée en 2016 et devant entrer en application dans les états membres le 25 mai 2018.

RSA : est un algorithme de cryptographie asymétrique, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet.

Sécurité de fonctionnement : est l'aptitude d'un système à remplir une ou plusieurs fonctions requises dans des conditions données ; elle englobe principalement quatre composantes : la fiabilité, la maintenabilité, la disponibilité et la sécurité

SoC : System On a Chip est un système complet embarqué sur une seule puce, pouvant comprendre de la mémoire, un ou plusieurs microprocesseurs, des périphériques d'interface, ou tout autre composant nécessaire à la réalisation de la fonction attendue.

SSH : Secure Shell (SSH) est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les échanges sont authentifiés et chiffrés.

SSL : Security Socket Layer est un protocole de communication sécurisé qui supporte plusieurs services de sécurité. C'est un protocole utilisé par les systèmes de paiement et de transaction en ligne se situant entre le protocole d'application HTTP pour le Web et le protocole TCP/IP.

Système complexe : est un ensemble constitué d'un grand nombre d'entités en interaction qui empêche l'observateur de prévoir sa rétroaction, son comportement ou évolution par le calcul.

TLS : norme de sécurisation par chiffrement du transport de l'information au sein des réseaux informatiques.

5.7 LA CYBERSÉCURITÉ PAR L'EXEMPLE

Nous traitons, en exemple, dans ce chapitre, la conception fonctionnelle d'une serrure de porte connectée pour espace public (hôtel, centre d'affaire bureaux...). Le but est de montrer qu'une démarche de conception produit intégrant la Cyber-sécurité n'est pas plus complexe et que cette démarche est naturellement structurante pour la conception, ce qui réduit les oublis techniques et produira généralement un prototype mieux abouti et proche d'un produit de pré-série qu'en l'absence de méthode. L'exercice fait ici, est bien incomplet pour arriver à un produit, tant sur le plan fonctionnel que dans les réponses apportées mais le but est de montrer les étapes et de discuter sur la structuration

Définissons le fonctionnel

Le schéma ci-après montre les fonctionnalités de la serrure et son interaction avec son environnement, composé d'une connexion sans fil moyenne portée, ex. technologie Zigbee, pour être accessible depuis un serveur, et une connexion sans fil courte portée pour un badge, ex. technologie NFC.

Quels risques pour ce produit

Le risque le plus redouté est l'ouverture de la serrure par un tiers malveillant. La cause peut être: reprogrammation du code, création d'une clé, mise en mode maintenance de la serrure, envoi d'un ordre d'ouverture urgence. Si nous appliquons la méthode DREAD, expliquée plus tôt dans le guide, nous nous apercevons que chacun des évènements redoutés à un indice différent en fonction du moyen utilisé.

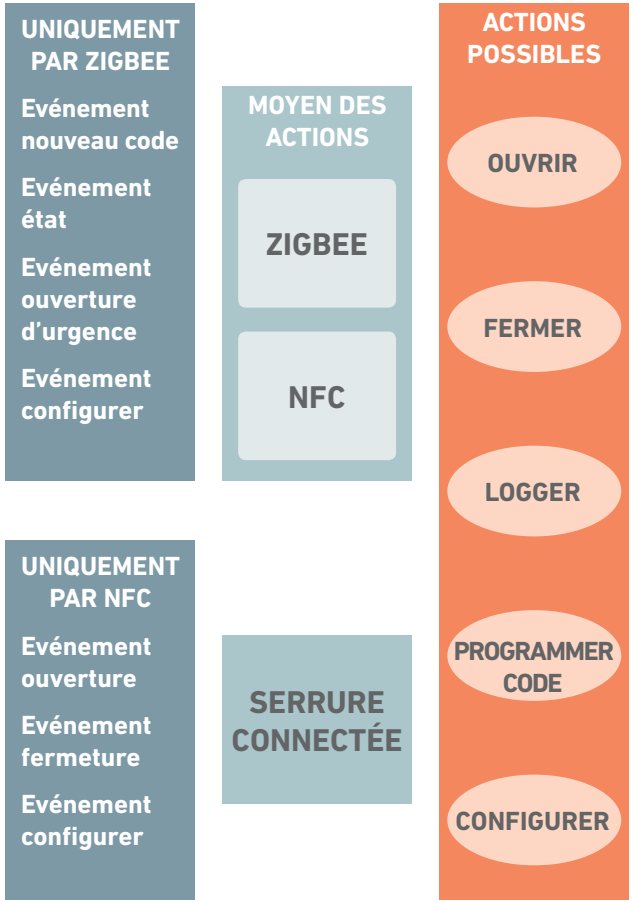
Prenons l'évènement « envoi d'un ordre d'ouverture urgence », à travers divers scénarios d'attaques :

(1) l'attaque est faite depuis un moyen Zigbee tiers développé pour l'attaque ou si l'attaque est fait depuis l'accès au PC de gestion en

(2) volant les identifiants d'un employé ou

(3) un acte malveillant d'un employé.

	SCÉNARIO 1	SCÉNARIO 2	SCÉNARIO 3
DOMMAGE	10	10	10
REPRODUCTIBILITÉ	7	3	1
EXPLOITABILITÉ	1	5	10
UTILISATEURS	10	10	10
ACCESSIBILITÉ	1	3	1
TOTAL	4,8	5,1	5,3



SERRURE CONNECTÉE, ACTIONS ET MOYENS D'INTERACTION

5.7 LA CYBERSÉCURITÉ PAR L'EXEMPLE

Le scénario 3 « acte malveillant d'un employé » est l'attaque avec le plus de risques. Nous avons fait quelques hypothèses pour arriver à ces résultats. Une analyse de risques a toujours une part subjective et est liée au métier ciblé. L'hypothèse majeure est qu'un employé mécontent prenne ce risque en sachant que la conséquence sera probablement la perte de son emploi. Si on estime que ce degré de mécontentement est plus qu'excessif dans toute relation sociale alors ce type d'attaque n'est plus que coté 3,7 et devient donc le scénario le moins probable. Le scénario 2 est par contre plus sournois car il y a tromperie d'identité et rappelle l'importance de la règle d'hygiène sur la politique des mots de passe pour s'en prémunir. Le meilleur moyen pour dissuader cette attaque est de tracer les accès au système et demander l'authentification d'un supérieur pour les accès aux fonctions critiques, d'où l'importance d'établir les rôles et les droits pour chaque personne accédant au système ce qui est également une règle d'hygiène.

Nous allons traiter le scénario 1 plus en détails afin de lister les contremesures techniques à mettre en œuvre.

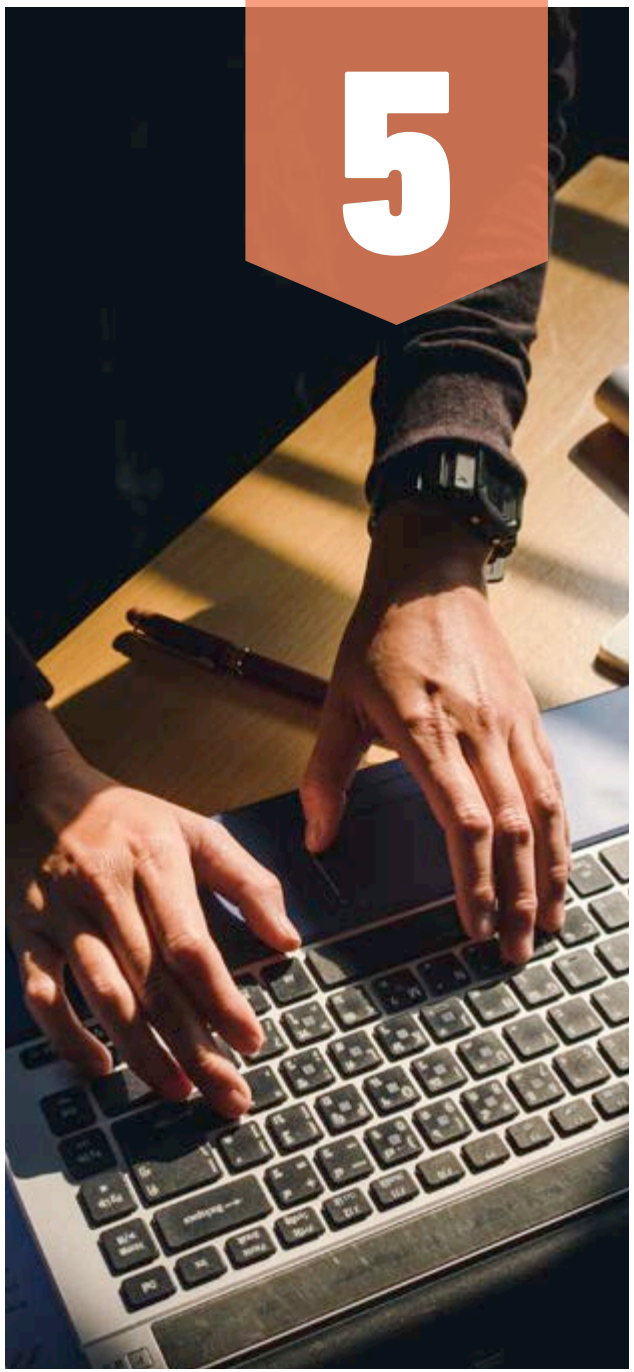
Analyse approfondie du scénario 1

Ce scénario est d'autant plus problématique qu'il est difficilement repérable et compréhensible, sans une analyse poussée de l'attaque. Aucun ordre n'est émis par le serveur mais les serrures se déverrouillent. Une fois le hack mis en œuvre, il est répétable indéfiniment, le détecter devient un enjeu majeur.

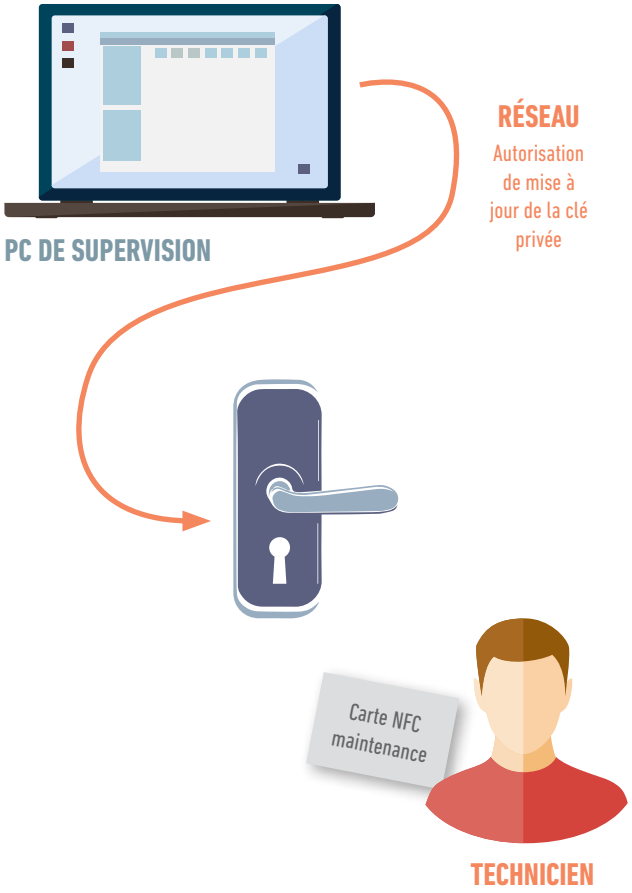
Il convient de raffiner les causes probables et vecteurs probables pour ce scénario. Si une attaque est possible depuis un équipement Zigbee, c'est que celui-ci sait s'identifier sur le réseau, que le message était chiffré correctement pour être compris par l'équipement et que la syntaxe du protocole était connue.

Quelles causes pour le scénario 1

Quels sont les causes de ces failles: un firmware rétro-analysé directement sur l'équipement, un ré-émission du message, un défaut de chiffrement de la radio ou du protocole. Le chiffrement est basé sur des clés, le vol de celles-ci peuvent se faire à différents endroits : production, configuration ou en attaquant le matériel. Il convient de sécuriser l'ensemble de ces phases. Les clés privées utilisées en production doivent être changées lors de la première mise en service ou les clés privées doivent être inaccessibles et sans possibilité de modification par un tiers de la chaîne de fabrication du produit. Dans ce cas, un mécanisme doit être prévu pour répudier un produit corrompu.



5 5.7 LA CYBERSÉCURITÉ PAR L'EXEMPLE



Réfléchir à sa protection

Il est difficile de changer une clé privée sur un équipement corrompu par liaison sans fil si l'environnement n'est pas un environnement de confiance. Cette opération reviendrait à rendre publique la nouvelle clé à garder secrète!

Si la clé privée est protégée lors de la production, il convient d'offrir un service pour que les équipements puissent récupérer les certificats afin de communiquer. Cette solution très sûre impose au client d'ouvrir son réseau vers l'extérieur ce qui n'est pas toujours possible.

La solution intermédiaire est de changer les clés privées uniquement quand l'équipement est en maintenance, maintenance provoquée depuis le serveur de gestion du parc de serrures et est lu depuis une puce NFC. Nous utilisons ici une double authentification, seul le gérant du bâtiment peut passer en maintenance une ou un ensemble de serrures et seul un technicien avec un équipement approprié pourra changer la clé privée lors de l'installation de la serrure. Le but ici est de décourager une attaque en incluant 2 rôles à usurper.

Les modules sans fil offre la possibilité de chiffrer la communication, il convient de prendre des modules dont le firmware peut être mis à jour en cas de faille détectée dans sa fonction de chiffrement et ce afin de ne pas devoir changer l'ensemble du parc produit. Evidemment le choix d'une puce avec un certificat de sécurité reconnu est un gage de bon niveau de cyber-sécurité. Il est également nécessaire de respecter les préconisations du fabricant de la puce afin de ne pas dégrader la sécurité lors des phases de conception. Ce chiffrement de communication peut également se faire par le processeur de l'objet si celui-ci en a les capacités afin de relâcher les contraintes sur le composant radio.

Logiciel et son processeur

Il convient de regarder la sécurité du logiciel qui devra subir des batteries de tests allant de l'analyse statique de code aux tests boîte noire aléatoires. Il convient de durcir le développement avec un processus rigoureux afin de ne pas offrir un bug trivial exploitable dès le premier jour. Il est aussi nécessaire de soumettre les briques logicielles achetées aux mêmes traitements afin de ne pas s'exposer inutilement. Enfin un mode debug est à proscrire sur l'objet en production.

(1) Texas instruments https://www.ti.com/seclit/ml/swpb020a/swpb020a.pdf
(2) STMicroelectronics http://www.st.com/en/secure-mcus.html
(3) NXP : https://www.nxp.com/applications/solutions/internet-of-things/secure-things:Secure-Things
(4) Atmel : http://www.atmel.com/applications/iot/aws-zero-touch-secure-provisioning-platform/default.aspx

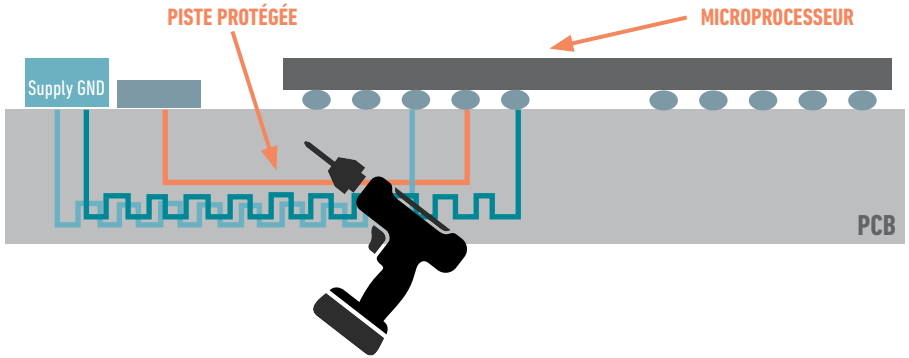
5.7 LA CYBERSÉCURITÉ PAR L'EXEMPLE

5

La recommandation d'avoir un mode de mise à jour par les airs du firmware du produit avec de l'authentification et du contrôle d'intégrité est devenue une nécessité forte aujourd'hui. Ces mécanismes ne sont possibles que si la cible d'exécution le permet et si les prérequis du logiciel sont implémentés. Le choix est important en terme de coût, de délais d'implémentation et de formation des ressources. Aujourd'hui tous les fabricants de microcontrôleurs offrent des solutions[1][2][3][4] à leur catalogue pour embarquer de la protection des données et permettre de développer des produits offrant un bon niveau de résistance face à des attaques directes sur matériel tel que le remplacement du firmware ou l'accès aux registres du processeur depuis un bus externe.

Composants pour renforcer la sécurité de l'objet

Les éléments de sécurité pour faire du chiffrement peuvent être internes ou externes au micro-contrôleur[5][6][7][8]. Il n'y a pas de bonne ou mauvaise solution, mais des compromis de coûts et de rapidité de mise en œuvre. En fonction de l'application, la protection de l'horloge du système[9][10] servant à cadencer le processeur et/ou gérant le temps et la date est nécessaire. Le but est d'éviter une attaque par l'accélération du temps afin par exemple de rechercher un moment de la journée pour ouvrir la porte automatiquement (nettoyage de la pièce à heure fixe).



Des pistes sensibles peuvent être protégées par un mécanisme anti-intrusion peu coûteux qui effacera la RAM et la FLASH si une piste est coupée. Le type d'attaque illustré sert à venir espionner des bus de communication. Dans le cas ci-dessous, le processeur mesure une alimentation et si ces valeurs deviennent aberrantes, le processeur efface les données stockées.

Les éléments indiqués précédemment s'accompagnent souvent d'un mécanisme anti effraction qui peut être une piste parcourant la carte électronique afin de détecter l'accès à une pin du composant pour faire de la rétro-conception (lire le firmware ou mettre la puce en mode debug de production) ou fil autour du boitier pour détecter l'ouverture du boîtier. Dans ces 2 cas, l'action doit être l'effacement des mémoires firmware et des clés de chiffrement. Il existe des méthodes plus sophistiquées de protection tel que faire un boîtier étanche sur pression avec un capteur de pression qui détectera une ouverture du boîtier car la pression descendra en cas d'effraction ou bien avec une led émettrice et une led réceptrice qui détectera des variations de luminosité et réfléchissement sur le boîtier en cas d'effraction. Ces systèmes ne sont pas infaillibles mais ils sont suffisamment contraignants pour dissuader la majorité des attaquants.

(5) http://www.st.com/en/secure-mcus/authentication-secure-iot.html

(6) http://www.microchip.com/wwwproducts/en/ATECC508A

(7) https://www.nxp.com/products/identification-and-security/authentication/secure-authentication-microcontroller:A700X_FAMILY

(8) http://www.microchip.com/design-centers/security-ics/cryptoauthentication/overview

(9) http://www.st.com/en/clocks-and-timers/m41st87w.html

(10) https://www.nxp.com/products/analog/signal-chain/real-time-clocks:MC_71246

5

5.7 LA CYBERSÉCURITÉ PAR L'EXEMPLE

Synthèse

Dans ce petit exemple, nous avons vu comment l'évaluation d'un risque peut être subjectif et versatile en fonction de la perception de l'environnement et de l'attaquant. Les moyens techniques listés avec les exemples de solutions techniques ne sont pas exhaustifs et les catalogues de composants sont pleins de solutions dont il est nécessaire d'arbitrer la pertinence en fonction de la décomposition technique de l'attaque envisagée. L'idéal est de recenser l'ensemble des vecteurs techniques d'attaque afin de trouver la réponse globale adaptée. En dernier ressort, le coût d'une solution face à son enjeu sera l'argument décisionnel majeur.

Au travers des différents liens illustrant l'exemple, vous pouvez voir qu'aujourd'hui les livres blancs et des solutions techniques clés en main existent sur lesquels il est primordial de s 'appuyer, mais il est encore plus primordial de respecter leurs mises en œuvre en respectant un processus de conception rigoureux et structurer.

Les documents d'exigences, de conception et de tests restent le premier rempart face à la survenue d'un bug ayant une portée catastrophique en termes de fonctionnalités et de cybersécurité. L'idéal est de confronter aussi bien son produit que sa méthode de développement à un audit externe. L'audit peut être ciblé et limité en moyens afin d'être abordable mais également répondre à l'attrait du produit pour subir une attaque. Un processus de développement en place et respecté garantit une valeur pour l'entreprise qui se mesure en efficacité et transparaîtra donc sur le gain de productivité. Enfin la sensibilisation et la formation restent les piliers forts d'un produit bien conçu, empiler des solutions techniques sans appréhender les risques, la mise en œuvre ou le déploiement ne mène pas vers un produit plus sur et de qualité. Veuillez aussi noter que vous pouvez être accompagné dans vos démarches par des prestataires certifiés par l'ANSSI. Vous pouvez également bénéficier de subventions et les jeunes entreprises de bourses pour vous aider techniquement et pour monter en compétence sur les thématiques de la cybersécurité et de la protection des données qui seront les enjeux des années à venir.

5.8 CHECKLIST

- [ ] Nommer un responsable sécurité, qui définit et est garant des bonnes pratiques de conception ainsi que du maintien en sécurité du produit
- [ ] Choisir et appliquer un standard pour la cybersécurité
- [ ] Réaliser une analyse des risques cyber du produit et définir les mitigations associées (à savoir les mesures de précaution pour en atténuer les dommages)
- [ ] Un démarrage sécurisé du produit par secure boot activé
- [ ] Interfaces de debug (JTAG) désactivées
- [ ] Les mémoires de stockage ou volatiles intègrent un mécanisme contre le reverse engineering et la falsification
- [ ] Les bus et ports réseaux non utilisés sont désactivés
- [ ] Les noms des points de tests sur la carte du produit final sont non significatifs
- [ ] Les composants servant à la cybersécurité du produit ne peuvent être substitués lors de l'assemblage
- [ ] Les clés de chiffrement asymétrique sont uniques pour chaque produit
- [ ] Les personnes ayant accès aux clés de chiffrement et au firmware sont clairement identifiées lors de la production
- [ ] Le produit possède un mécanisme de mise à jour sécurisé
- [ ] Le produit ne peut exécuter que des firmwares signés numériquement
- [ ] Périodiquement le logiciel vérifie son intégrité
- [ ] Toutes les fonctions de debug sont retirées du firmware de production
- [ ] Le logiciel utilise le secure element pour stocker les clés de chiffrement
- [ ] Le logiciel utilise les fonctions matérielles pour le chiffrement des données
- [ ] Un identifiant unique non modifiable par le logiciel est à disposition du logiciel pour assurer l'identification du produit
- [ ] Si un système d'exploitation est utilisé, les mécanismes d'isolation mémoire et de privilège d'exécution sont employés
- [ ] Si un système d'exploitation est utilisé, et que celui-ci permet l'utilisation de comptes privilégiés, ces comptes sont utilisés uniquement par le firmware, sans accès distant possible
- [ ] Si un système d'exploitation est utilisé, seuls les services utilisés sont actifs
- [ ] Tous les protocoles réseaux utilisent un chiffrement (HTTPS, FTPS, SSH)
- [ ] Le mot de passe utilisateur par défaut est obligatoirement changé à la première utilisation de l'objet
- [ ] En cas de connexion distante possible, en cas d'échec de la saisie d'un mot de passe un délai d'attente avant un nouvel essai existe
- [ ] Aucun protocole réseau chiffré ou algorithme de chiffrement avec une faille connue n'est utilisé
- [ ] Le code source est soumis à des règles de codage et elles sont vérifiées par un logiciel tiers
- [ ] Les fonctions liées aux mitigations de l'analyse des risques de cybersécurité subissent des tests unitaires
- [ ] Les bulletins de sécurité de l'ensemble des logiciels tiers utilisés pour la réalisation du firmware (environnement de développement et librairies utilisées) sont suivis pendant la conception et la durée de vie du produit afin de réagir à l'identification d'une faille
- [ ] Le firmware est vérifié par une série d'antivirus avant son envoi en production
- [ ] Chaque nouvelle version du produit est éprouvée par un Pen Testing
- [ ] En cas de données non anonymes, une politique sur la gestion des données est mise en œuvre afin de garantir l'intégrité et la sécurité de celles-ci

5

5.9 TEST

Pré-évaluez la sécurité de votre produit connecté!

Quand les questions de sécurité ont été traitées pour votre objet connecté :

Au début du projet, lors de la phase de spécifications ★★★★★
En fin de projet, avant la mise sur le marché ★★★
La sécurité n'est pas prise en compte dans la conception, nous corrigeons à distance avec des patchs. ★

Faites-vous une évaluation des risques en termes de sécurité dans la conception de votre objet connecté ?

Oui ★★
Non ★

Quelles normes de codage sont utilisées par les développeurs logiciels de votre objet connecté ?

Les normes de l'OWASP, le standard CCERT ★★★
Les normes MISRA ★★
Vos propres normes ★★
Aucunes ★

Les développeurs de votre objet connecté ont-ils bénéficiés de formation sur la cybersécurité ?

Oui ★★★
Oui, en autoformation ★★
Non ★

Faites-vous des revues de code ?

Oui, axées qualité et règles de sécurité ★★★★
Oui, pour respect de la norme de codage ★★★
Oui, mais c'est informel ★★
Non ★

Votre objet connecté dispose-t-il d'un dispositif de mise à jour à distance ?

Oui ★★★
Non ★

Le firmware de votre objet connecté est-il signé pour éviter l'installation de firmwares pirates par un tiers ?

Oui ★★★
Non ★

Utilisez-vous des outils de fuzzing pour vérifier la robustesse de votre objet connecté ?

Oui ★★★
Non ★

Utilisez-vous des outils pour vous prémunir des attaques par déni de service (DOS) ?

Oui ★★★
Non ★

Avez-vous prévu de faire des tests d'intrusions sur votre objet connecté ?

Oui, avant la mise sur le marché ★★
Oui, le plus tôt possible ★★★
Non ★

La communication entre votre objet connecté et Internet (ou toute autre entité centrale) est elle chiffrée ?

Oui ★★★
Non ★

Le protocole de communication entre votre objet connecté et l'extérieur est-il protégé par un système d'anti rejeu ? (possibilité d'un attaquant de copier/coller des trames dans une communication entre l'objet et une autre entité)

Oui ★★★
Non ★

Votre objet connecté dispose-t-il d'un mot de passe par défaut ?

Oui ★
Oui, mais c'est en fonction de son numéro de série (ou toute autre numéro propre de l'objet) ★★
Non ★★★

Stockez-vous des données captées par l'objet connecté dans sa mémoire RAM/FLASH/SSD/HD?

Oui en clair ★
Oui, en crypté ★★★
Non ★★★

Est-il possible de réinitialiser l'objet connecté afin qu'il supprime toute donnée captée ou appartenant à l'utilisateur (factory reset) ?

Oui ★★★
Non ★

Les fonctionnalités de debug du processeur sont-elles accessibles depuis le PCB de l'objet connecté ?

Oui ★
Oui, les pistes sont tirées, mais il n'y a pas de broches ★★
Non ★★★

L'objet connecté dispose-t-il d'un système d'effacement mémoire en cas d'ouverture du boitier ?

Oui ★★★
Non ★

L'objet connecté peut-il remonter des statistiques d'utilisation permettant de détecter un comportement non autorisé ?

Oui ★★★
Non ★

Peut-on facilement voler l'objet connecté (à proximité de la voie publique par exemple) ?

Oui ★
Non ★★★

L'objet connecté vérifie-t-il l'identité du serveur avec lequel il communique ?

Oui via des certificats SSL/TLS par exemple ★★★
Oui, via un système de mots de passe ou équivalent ★★
Non ★
Sans objet ★★★

Inférieur à 30 ★
La sécurité n'est clairement pas prise en compte dans votre produit. Ce qui peut être acceptable dans le cas d'un prototype. En revanche si une industrialisation est envisagée, il faudra impérativement mener une étude approfondie.

Entre 30 et 50 ★
Bien que prise en compte, le niveau de votre objet connecté en sécurité est très probablement insuffisant, et il convient de faire une étude pour combler les probables lacunes.

Entre 50 et 62 ★
Votre prise en compte de la sécurité semble mature, restez cependant à jour par rapport aux nouvelles menaces et intégrez la sécurité dès les premières phases du projet.

63 ★ et plus : La sécurité est une priorité dans votre produit, bravo.

NOTES

A PROPOS DE CEA TECH

CEA Tech est le pôle « recherche technologique » du CEA, constitué des trois instituts Leti, Liten, List et de l'Institut CEA Tech en région, qui lui permettent de disposer d'un portefeuille de technologies complet dans les domaines de l'information et de la communication, de l'énergie et de la santé.

Bénéficiant d'un savoir-faire unique issu d'une culture de l'innovation, CEA Tech a pour mission de produire et diffuser des technologies pour en faire bénéficier l'industrie, en assurant un « pont » entre le monde scientifique et le monde économique. Alors que le risque « cyber » se renforce avec la transition numérique, les instituts de CEA Tech proposent des briques technologiques innovantes pour assurer l'intégrité et la sécurité des données, depuis leur captation jusqu'à la production du service à l'utilisateur final.

www.cea-tech.fr

A PROPOS DE CYBEREDU

L'association CyberEdu propose une labellisation des formations de l'enseignement supérieur mettant en œuvre les principes de sa démarche pédagogique de la sécurité du numérique.

Le label CyberEdu a pour objectif de référencer les formations non spécialisées en sécurité du numérique qui intègrent à leur cursus des éléments de sensibilisation à la sécurité fournis par l'association CyberEdu.

www.cyberedu.fr

A PROPOS DE CYBERENS

Les activités de Cyberens comportent essentiellement deux volets :

- Le conseil avec des audits et des analyses de sécurité dès la phase de conception jusqu'à la mise en service avec des outils d'analyse de risque comme EBIOS, la définition d'architectures de sécurité ou encore la mise en place de services opérationnels de cybersécurité (veille sur les menaces, SOC, CSIRT) ;
- Le développement de logiciels de cybersécurité à base de cryptographie avec une solution de chiffrement de courriels, une application de gestion de licences et une bibliothèque ne contenant que des algorithmes réputés « forts ».

www.cyberens.fr

A PROPOS DE CYBERSECURA

CyberSecura conseille et accompagne ses clients dans leur gestion de la cybersécurité des objets ou applications communicantes qu'ils conçoivent ou utilisent. Cet accompagnement peut prendre la forme de formation, audit, tests, aide à la conception, accompagnement de l'implémentation et gestion des risques et attaques au quotidien. En mode projet ou en accompagnement « à temps partagé » la spécialisation en objets connectés de CyberSecura permet notamment à des PME d'accéder à un accompagnement stable et durable avec une maîtrise complète des coûts. Architecte en sécurité des systèmes, Saghar Estehghari, formée à University College London, cumule plus de 10 ans d'expérience de projets en cybersécurité pour de petites entreprises et de grands comptes. Elle est accompagnée de David Rozier, docteur en intelligence artificielle, 20 ans d'expérience industrielle.

www.cybersecura.com

A PROPOS DE G-ECHO

Difficile de trouver les bonnes solutions en cybersécurité :

A travers des questionnaires ciblés, G-echo propose du support à ses clients pour leur faire accéder aux offres adaptées du marché : audit / conseil / expertise, sensibilisations / formations / aide au recrutement, solutions de cybersécurité.

De la TPE au grand groupe, une approche unique pour améliorer le niveau global de cybersécurité de votre Entreprise.

www.g-echo.fr

A PROPOS DE NEMEZYS

Nemezys est un Cabinet orienté vers les entreprises technologiques (ESN, éditeurs, industries technologiques avancées, mais aussi start-up ou investisseurs) qui accompagne ses clients tout au long de leurs projets. À l'écoute, son équipe aide les entreprises à se développer et à innover, à résoudre les différends de ses clients et à leur délivrer des conseils avisés.

Dans un monde en mutation constante, Nemezys offre bien plus que des services juridiques et met à disposition son exigence et sa créativité. Fondé en août 2013 par Joël Heslaut, avocat titulaire des mentions de spécialisation en Droit de l'Informatique et en Droit de la Propriété Intellectuelle, Nemezys réunit une équipe pluridisciplinaire en mesure de couvrir les principaux besoins juridiques des entreprises (contrats, droit de l'informatique, droit d'auteur, marques et brevets, droit des sociétés, droit social).

A PROPOS DE CAP'TRONIC

Fondée par le CEA et Bpifrance, et financée par le ministère de l'Economie et des Finances, l'association JESSICA France est chargée de la mise en œuvre du programme **CAP'TRONIC.** Celui-ci a pour objectif d'**aider les PME françaises**, quel que soit leur secteur d'activité, à **améliorer leur compétitivité grâce à l'intégration de solutions électroniques et de logiciel embarqué dans leurs produits**. Chaque année, **CAP'TRONIC aide plus de 3500 PME,** tous secteurs confondus, à conquérir de nouvelles parts de marché en faisant de l'électronique et du logiciel le levier concurrentiel indispensable à leur croissance.

Pour plus d'informations:
www.captronic.fr

A PROPOS DE L'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée le 7 juillet 2009 sous la forme d'un service à compétence nationale.

En vertu du décret n° 2009-834 du 7 juillet 2009 modifié par le décret n° 2011-170 du 11 février 2011, l'agence assure la mission d'autorité nationale en matière de défense et sécurité des systèmes d'information. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

Pour en savoir plus sur l'ANSSI et ses missions, rendez-vous sur www.ssi.gouv.fr.

Ce travail a bénéficié d'une aide de l'Etat Français au titre du programme d'Investissements d'Avenir, IRT Nanoelec, portant la référence ANR-10-AIRT-05

Dans le cadre du Programme d'Investissements d'Avenir, **l'Institut de Recherche Technologique Nanoelec** (IRT Nanoelec) réunit des partenaires privés et publics pour conduire un programme de développement et de diffusion technologique dans le domaine des NTIC au bénéfice des entreprises de tous secteurs. L'IRT Nanoelec vise deux objectifs : hisser la R&D au meilleur niveau mondial pour développer les technologies d'intégration 3D et de photonique sur silicium ; développer de nouveaux produits ou applications s'appuyant sur la connectivité entre les objets. Un programme spécifique est destiné aux PME/ETI et leur permet d'accéder à des modules de formation ainsi qu'à des briques technologiques pour enrichir leurs produits ou en développer de nouveaux.