LA CYBERSÉCURITÉ APPLIQUÉE AUX PROJETS DE TERRITOIRES CONNECTÉS ET DURABLES

Les projets de territoires de connectés durables sont des solutions numériques **au service de la transition écologique,** avec la spécificité d'intégrer des **objets connectés** sur le territoire. Dans les faits, **ces solutions permettent effectivement d'optimiser les flux et les ressources, d'observer un territoire en pleine mutation pour mieux le comprendre** et adapter des politiques publiques, en communiquer les résultats. Une infrastructure pérenne doit alors être mise en place intégrant objet connecté, réseau de connectivité, serveurs, algorithmes et visualisation des résultats.

Les actes malveillants (vol, sabotage, rançon…) existent dans le monde physique aussi bien que dans le monde numérique. Pour autant, le numérique ouvre de nouvelles portes d'entrée pour les attaquants, dont la variété dépend de leur imagination. Des prérequis doivent ainsi être mis en oeuvre dès la conception de la solution pour se prémunir des attaques les plus évidentes, les usagers de la solution doivent être formés car le facteur humain reste très souvent à l'origine d'une intrusion, une politique de surveillance doit être définie sur le temps long.

Les objets connectés, et l'architecture associée, peuvent être des cibles d'attaque et amènent de nouvelles craintes. L'objectif de cette fiche est de **comprendre ce qui change vraiment par rapport à un projet numérique classique** et quelles seraient les préconisations essentielles.

QUELS RISQUES ?

Les risques sont transverses à tous les éléments de l'architecture, de gravité différente, de probabilité d'occurrence différente :

Sur les données sensibles	Sur les données non sensibles	Pour tout équipe-	Pour tout logiciel	Cas particulier des actionneurs*
• Intercepter : usurpation d'identité, rançon...	• Biaiser : remonter de fausses informations, en supprimer et fausser les calculs des logiciels (fausses alertes, actions déclenchées)	• Perturber le taux de disponibilité ou mettre hors service	Accès et contrôle : - des droits d'accès - des actionneurs* : Envoi de commandes, actions à distance Perturber le taux de disponibilité ou mettre hors service	Prise de contrôle: **Direct :** par l'envoi de commandes directement **Indirect** : Cf données non sensibles Perturber le taux de disponibilité ou mettre hors service

** un actionneur est un objet connecté qui ne se contente pas de remonter des données mais qui réalise des actions à distance (ex : feux tricolore)*

>> Ce qui est nouveau par rapport à un projet numérique classique ?

La crainte par rapport à l'arrivée des objets connectés porte particulièrement sur les actionneurs, ces objets connectés qui réalisent des actions par exemple pour optimiser les feux de circulation en fonction du trafic. En ce qui concerne les données sensibles, très peu d'objets connectés en collectent actuellement : niveau de remplissage des poubelles, détection de fuites d'eau ou encore consommation énergétique d'un bâtiment… Les données sensibles sont plutôt échangées sur des interfaces numériques classiques pour souscrire à un nouveau service et se retrouvent ensuite sur les plateformes, mais pas au niveau des objets connectés qui auront une clé d'authentification.

COMMENT ?

La nature des attaques peut être très variée et il n'est pas possible d'en établir une liste exhaustive. En revanche, il est intéressant d'observer les zones potentielles d'attaque par élément d'architecture.

Liste des principales attaques possibles par élément d'architecture :

Objets connectés

A la réception de l'objet :

- Récupération des clés transmises sur papier ;
- Interception au moment de l'initialisation

En fonctionnement :

- Ouverture mannuelle de l'objet / *facilement détectable*

En détournant d'autres élements de la chaine : Cf réseau, plateforme de données, autres sources de données

Réseau

Radio

Fibre

A l'initialisation :

- Envoi/gestion des clés de chiffrement

En fonctionnement :

Réseau mobile : intercepter les données, envoyer des données / *peu détectable*
Réseau fixe : couper la fibre et intercepter les données / *facilement détectable.*

Il faut ensuite être capable de pirater le chiffrement, recomposer le message, savoir d'où il vient > *peut être très complexe* !

Serveurs et plateforme de données

Accès physique au serveur :

- Branchement et récupération de données ou virus ;

Accès logiciel :

- Faille logiciel ;
- Récupération de mot de passe ;

Par l'usager lui-même :

- Clé usb non sécurisée ;
- Mot de passe accessible…

Les méthodes sont exactement les mêmes entre la plateforme de données et les autres logiciels, si ce n'est qu'il y a une profusion de nouveaux acteurs, dont des startups, qui n'intègrent pas la sécurité « by design » par défaut.

Autres sources de données

>> Ce qui est nouveau par rapport à un projet numérique classique ?

La nature des attaques ne change pas fondamentalement par rapport à un projet numérique classique. Ce qui change :

- **C'est le champ d'application** et notamment à travers la famille des objets connectés qui réalise des actions physiques sur l'espace public (ex : feux tricolore). Deux principaux modes d'attaque sont alors possibles : l'envoi de commandes (depuis l'interface radio ou plus vraisemblablement depuis les logiciels) ou la manipulation des données qui indirectement impactera les algorithmes et créera de « faux évènements » (par exemple, des données de trafic surestimées manipuleront le fonctionnement des feux tricolores).

- **C'est la profusion de solutions** sur la partie logicielle qui pour certaines n'ont pas intégré dès la conception des règles de sécurité ;

- **C'est le nombre d'acteurs** qui accèdent aux différentes parties de l'architecture et qui, si les process et règles de contrôle d'accès ne sont pas parfaitement clairs, risquent de créer des brèches physiques ou logicielles assez faciles pour un hacker.

RÉGLEMENTATION

- Directive NIS2 et la loi attendue du Cyber Resilience Act

RECOMMANDATIONS

Tous les projets ne contiennent pas des données sensibles, tous les projets n'intègrent pas des objets connectés dits actionneurs. En amont de chaque projet, il s'agit de réaliser un audit de l'existant et une matrice de risques (niveau de risque x probabilité d'occurence) puis de mettre en place une politique adaptée. Liste des principales recommandations identifiées par acteur :

	Collectivité	AMO	Équipementier Objet connecté	Fournisseur d'accès réseau	Éditeur de logiciel	Prestataires
A la conception	Réalisation de la matrice de risques Politique de protection de bout en bout Politique de gestion des droits d'accès Intégration de clauses dans le cahier des charges Choix des équipements, logiciels, prestataires en fonction des clauses *> Il est recommandé de passer par un AMO pour un premier projet*		Réglementation Modalités d'accès physique à la partie logiciel Authentification de l'objet, chiffrement du signal, processus d'activation Mécanismes de défense en cas de comportement inhabituel (demande une identification préalable de ce qui peut être inhabituel)	Réglementation Modalités d'accès physique au coeur de réseau Modalités d'authentification, de chiffrement, de protection de l'antenne au coeur de réseau Mécanismes de défense en cas de comportement inhabituel	Réglementation Gestion des droits d'accès Mécanismes de défense en cas de comportement inhabituel	Sensibilisation aux bonnes pratiques Certification de l'entreprise (iso27001, 27005, Apsad cyber ..)
Sur le temps	Formation Gestion des droits d'accès Surveillance continue, contrôle des prestataires Réactivité (MCO, MCS)		Surveillance continue, retours utilisateurs Mise à jour logicielle	Gestion des droits d'accès Surveillance continue Réactivité (MCO, MCS)	Surveillance continue, retours utilisateurs Mise à jour logicielle	Recyclage régulier (piqure de rappel)

>> Ce qui est nouveau par rapport à un projet numérique classique ?

- **La diversité des acteurs** qu'il va falloir coordonner avec de nouveaux processus, notamment à l'installation des objets ;
- **L'arrivée de nouveaux équipements et logiciels** qui n'ont pas tous la maturité des équipements numériques classiques tels que les ordinateurs ou les serveurs ;
- **L'arrivée des réseaux privés** et la nécessité de sécuriser physiquement et logiciellement le coeur de réseau ;
- **Le manque de réglementation** qui permettrait de s'assurer que tous les acteurs intègrent des règles de sécurité dès la conception. Cette réglementation va être amenée à évoluer prochainement, Cf la « Cyber Resilience Act » pour les équipements et la directive européenne NIS2 pour la gestion des risques par typologie d'acteurs.

DOCUMENTATION DE RÉFÉRENCE :

- Guide ANSSI « Recommandations relatives à la sécurité des (systèmes d') objets connectés », 08/2021

Référent du GT : R. Martinez, Eryma

Contributeurs : J. Araujo, Orange — S. Fiquet, Artelia — P. Ducloy, XpFibre — R. Martinez, Eryma

Conception : A. Le Meil, InfraNum

Les fiches InfraNum ont pour objectif de donner des clés pour décliner opérationnellement les thématiques qu'il faut prendre en compte dans le déploiement d'un projet de territoire connecté et durable. Elles sont aussi bien à destination des collectivités que des industriels. Elles donnent un état des lieux à date, issu de la mise en commun des connaissances et des retours d'expériences des membres de la fédération. Cet état des lieux fera ensuite l'objet d'échanges et de dialogue avec le reste de l'écosystème pour en améliorer le contenu dans le temps.