Sécurité, bâtiments et objets connectés

Laurent Signac – CC-BY-SA – 10-02-21 0925 c486a6fb494db0ddb47d

1 Notion de risque

Vulnérabilité : Ça peut être du code mal écrit, une installation système incorrecte, des mots de passe non fiables, ou codés en dur… La vulnérabilité peut être connue, ou non, il peut exister un patch de sécurité ou non.

Impact : c'est ce qui est affecté par l'attaque. Ça peut être un bâtiment, son contrôle d'accès, le centre de contrôle d'une entreprise. Des personnes peuvent être physiquement affectées (blessures etc…).

Menace : Ça peut être des nations, des groupes d'activistes, des professionnels de la cybermalveillance, des amateurs.

Le **risque** est le «produit» de ces trois valeurs. S'il l'une des trois est nulle, alors le risque est nul.

2 Sécurité dans les smart[building|city|object]

SmartCity, le carrefour des innovations, Techniques de l'ingénieur, oct. 2019 :

> On ne va pas énumérer ce qui fait de la sécurisation des données un enjeu fondamental pour l'avènement des smart city : smart buildings, véhicule autonome, internet des objets, gestion des machines dans une usine connectée, santé connectée… toutes ces innovations technologiques ne sont implémentables que si et seulement si la problématique de sécurisation des données relatives à ces usages est assurée.

3 IT /OT

L'IT (*Information Technology*) regroupe les matériels et réseaux habituellement gérés par les service informatiques (ordinateurs, mobiles etc..) alors que l'OT (*Operational Technology*) contient les systèmes industriels, gérés par les responsables du pôle industriel. L'OT s'est particulièrement développé, avec des produits de plus en plus complexes (connectés), offrant donc une surface d'attaque plus grande, sans que les réflexes difficilement acquis par l'IT (mise à jour régulière du système etc..) ne l'accompagne.

L'OT contient donc une flotte importante de matériels vulnérables, qui ne sont pas mis à jour, soit par méconnaissance, soit parce que l'opération est particulièrement complexe (nécessitant un arrêt de production etc.)

4 Faits divers marquants

4.1 Impacts sur le particulier

4.1.1 Camera Ring

La société Ring, filiale d'Amazon équipe des maisons en sonnettes et caméras connectées. En décembre 2019, des pirates ont pris le contrôle des caméras, pour s'adresser directement aux habitants et diffuser le flux vidéo sur Discord.

- Source[1]
- Video Youtube[2]

[1] https://www.lebigdata.fr/hackers-cameras-ring
[2] https://www.youtube.com/watch?start=32&v=GnlIEQt_QFo

4.1.2 Prise de contrôle d'une Jeep

En 2015, deux chercheurs en sécurité montrent comment il est possible de prendre le contrôle d'une Jeep Cherokee :

- Prise de contrôle du système multimédia lorsqu'il dispose d'une connectivité Wifi (le mot de passe était dérivé de la date de première mise en circulation)
- En cas de non connectivité Wifi, le système multimédia communique sur le réseau mobile de l'opérateur Sprint.
- Une fois dans le système multimédia, celui-ci est relié à un contrôleur (V850) qui est relié au bus CAN. Le contrôleur ne peut pas écrire sur le bus, mais il peut être modifié pour pouvoir écrire sur le bus
- Le bus CAN pilote le moteur, la transmission, les freins…

- Source[3]

4.1.3 IOT Drone Hack

En 2016, une drône prend le contrôle d'un éclairage piloté en Zigbee :

- Video[4]
- Source[5]

4.1.4 Prise de contrôle d'un Pacemaker

Les pacemakers sont maintenant reprogrammables sans nécessiter d'opération chirurgicale, ce qui est plutôt bien. Toutefois, le firmware des pacemakers est mis à jour depuis un logiciel qui récupère lui-même ses mises à jour sur un site contrôlé par le fabricant. Les mises à jour n'étant pas signées (au sens des signatures cryptographiques), des firmware malveillants intégrés à la plate-forme peuvent être utilisés par les médecins lors des mises à jour, sans qu'ils puissent s'en rendre compte (2018).

- Source 1[6]
- Source 2[7]

4.1.5 Domotique dans le cloud…

En mars 2019, le cloud Google a connu quelques problèmes de performance, ralentissant ou bloquant les services qui l'utilisent… y compris le matériel domotique *Nest* qui utilise le cloud Google :

> But an especially annoying side effect of Google Cloud's downtime was that Nest-branded smart home products for some users just failed to work. According to reports from Twitter, many people were unable to use their Nest thermostats, Nest smart locks, and Nest cameras during the downtime. This essentially meant that because of a cloud storage outage, people were prevented from getting inside their homes, using their AC, and monitoring their babies.

[3] https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/
[4] https://www.youtube.com/watch?time_continue=2&v=Ed1OjAuRARU&feature=emb_logo
[5] https://www.theverge.com/2016/11/3/13507126/iot-drone-hack
[6] https://www.cnbc.com/2018/08/17/security-researchers-say-they-can-hack-medtronic-pacemakers.html
[7] https://www.wired.com/story/pacemaker-hack-malware-black-hat/

- Source[8]

4.2 Impacts sur la collectivité

4.2.1 Sirènes de Dallas

La nuit du 7 ou 8 avril 2017, les sirènes d'alerte de la vile de Dallas retentissent pendant 1h30.

La municipalité est finalement obligée de désactiver le système complet (utilisé pour prévenir en cas de danger météorologique)

- Source[9]
- Vidéo[10]

4.2.2 Transports Suisses

En juillet 2019, les transports en commun à Fribourg sont perturbés par un ransomware.

Le système a pu repartir au bout de 2h environ, grâce à des sauvegardes, et les systèmes de signalisation n'ont pas été impactés, car **ils ne sont pas reliés aux autres systèmes** (ce qui n'est malheureusement pas si courant que ça).

- Source[11]

4.2.3 Mirai

Fin 2016, le ver Mirai (codé en C et Go, et affectant Linux, répandu sur les caméras IP IoT) se répand chez les particuliers. Il se propage en testant simplement les identifiants par défauts des objets connectés.

Le botnet, composé d'environ 150 000 objets provoque un déni de service distribué chez différents acteurs (OVH en France, Dyn, lui même utilisé par Paypal, Twitter…).

OVH reçoit des débits allant jusqu'à 1Tb/s.

- Article Wikipédia[12]
- Source 1[13]
- Source 2[14]

[8] https://www.fastcompany.com/90358396/that-major-google-outage-meant-some-nest-users-couldnt-unlock-doors-or-use-the-ac

[9] https://www.numerama.com/tech/247844-un-hacker-declenche-toutes-les-sirenes-durgence-de-dallas-les-habitants-paniquent.html

[10] https://www.youtube.com/watch?v=4zkTaLUVvJI

[11] https://www.zataz.com/transports-publics-suisses-impactes-par-une-attaque-informatique/

[12] https://fr.wikipedia.org/wiki/Mirai_(logiciel_malveillant)

[13] https://www.zdnet.fr/actualites/ovh-noye-par-une-attaque-ddos-sans-precedent-39842490.htm

[14] https://www.silicon.fr/a-louer-botnet-mirai-400-000-objets-ddos-163618.html