CYBER ET DOMOTIQUE

MICKAEL KARATEKIN
consultant - formateur
en sécurité informatique
chez Sysdream

Avec la domotique, la cyber se convoque dans le quotidien des particuliers (et ce n'est pas de la science-fiction).

Un brief simple et digne d'un scénario de film d'action : « Vous êtes devant une maison fermée. Dans le garage, une voiture flambant neuve de la marque Tesla, dont la clef est dans un coffre-fort à l'étage. La clef du coffre ? enregistrée dans un ordinateur portable à l'intérieur de la maison. La maison est sous alarme, bien sûr, avec capteurs d'ouverture de porte, caméra wifi, etc. » Ce brief est donné, en ce 19 juin 2019, à la Maison de la Chimie, à l'occasion du Hack in Paris, événement international annuel de cybersécurité, devant une maison de poupée qui représente la maison en question : et les participants à cet atelier « maison de poupée connectée » ont pour objectif d'être les premiers à sortir la Tesla sans déclencher l'alarme.

Si tout l'environnement a été miniaturisé pour l'exercice du 19 juin 2019, les équipements sont bien réels et les technologies exactement celles qu'on retrouve dans une maison sous alarme. Bien sûr l'imaginaire de la Tesla projette les participants dans un autre monde, mais tous les éléments sont d'une banalité technologique à la portée du grand public ou des PME : une porte de garage avec une commande d'ouverture UHF (433 MHz), des contrôles d'accès NFC, des ordinateurs et iPhone sous wifi, des caméras wifi et des capteurs d'intrusion communiquant avec la centrale de l'alarme. Rien qui ne puisse s'acheter chez Darty ou être installé par des professionnels de systèmes d'alarme. D'ailleurs l'idée de la configuration du garage nous est venue à partir d'une alarme réelle d'une moto personnelle.

Hacker une maison connectée pour voler une voiture : un simple challenge pour ingénieur

Le challenge ne repose d'ailleurs pas tant sur la mise en œuvre de prouesses techniques, que sur la mise en œuvre d'une stratégie d'attaque suivant un cheminement logique : vous êtes devant une maison affichant un sticker wifi « maison connectée » et vous réfléchissez par quel biais l'attaquer pour arriver à vos fins. Sachant que les faiblesses technologiques auxquelles vous allez vous confronter n'ont rien de très différent de ce que l'on trouve dans la vraie vie : des clefs wifi aux protocoles insuffisamment sécurisés, des iPhones qui sont très « bavards » quand ils se reconnectent régulièrement au wifi et des protocoles NFC insuffisamment chiffrés qui peuvent être recopiés, de telle sorte qu'avec un simple smartphone grand public sous Android vous pourrez ensuite leurrer le contrôle d'accès et ouvrir votre porte de garage. Et les défis à relever (cloner un badge de porte, pirater un wifi et désactiver le système d'alarme, accéder à des données sur un ordinateur, désactiver une caméra et intercepter le système radio) peuvent tous être faits à l'aide d'un simple ordinateur portable, d'un smartphone grand public (sous Android) et d'un peu de logique. Faut-il

↖ À un atelier du *Hack in Paris*, munis d'un simple ordinateur portable et d'un smartphone, des participants essaient de hacker un système complet d'alarme de maison, challenge à la portée d'ingénieurs un peu geeks.

↓ Si tout est miniaturisé dans une maison de poupée, pour l'occasion de l'atelier du *Hack in Paris*, les équipements sont bien réels et les technologies celles qu'on retrouve dans une maison sous alarme : commandes de porte en UHF, contrôle d'accès NFC, alarmes et capteurs d'intrusion connectés, caméra wifi, etc.

être hacker professionnel pour ce faire ? C'est vrai que l'équipe gagnante qui a réussi à voler la Tesla en 45 mn était composée de hackers éthiques professionnels d'une grande entreprise. Mais d'autres équipes qui ont réussi le challenge en une heure étaient simplement composées d'ingénieurs réseaux juste un peu « geeks ».

La faible maturité de la domotique en termes de protection cyber est problématique

Sans entrer dans des scénarios de science-fiction, la domotique couvre déjà des champs très larges de notre quotidien : contrôle d'accès (badges sans contact), ouverture de portes (garage, voiture, etc.) et interphones, alarmes sans fil, capteurs domotiques, drones, abonnements urbains (cartes Vélib', Autolib', Navigo, etc.), réseaux cellulaires (FSM, DECT), bureautique sans fil (souris, claviers, casques), etc. Or cette innovation du quotidien ne s'est pas toujours accompagnée d'une forte sécurisation, alors même que les équipements présentent des vulnérabilités directement matérielles (capacité à lire des infos ou hacker directement les puces électroniques), logicielles (pas de protection contre des attaques DDoS, mots de passe par défaut jamais changés à l'installation) ou liées aux communications avec l'extérieur (protocoles radio utilisés trop peu sécurisés ou mal utilisés). Et s'attaquer à ces vulnérabilités n'est pas réservé aux agences de renseignement, mais peut se faire *via* des matériels grand public. Sans compter que certains matériels connectés installés ne font l'objet d'aucun suivi dans le temps. Une simple visite sur le moteur de recherche Shodan permet de visualiser l'étendu du parc d'objets de votre domicile, connectés et accessibles *via* Internet simplement. De la même façon que pour des systèmes d'information classiques, les objets connectés du quotidien devraient pourtant être l'objet de cybersécurité renforcée : sécurité *by design* de la part des constructeurs, installations s'assurant de la mise en œuvre de bonnes pratiques (ne pas laisser des *login* / mots de passe « admin » configurés par défaut), prise en compte au fil de l'eau par les constructeurs des publications de failles de vulnérabilité faites par les chercheurs et hackers, et application des correctifs ; et enfin, pour les entreprises, le réflexe de tester systématiquement les systèmes installés (à l'aide notamment d'audits visant à contrôler le code source, le système, la configuration, accompagnés de tests d'intrusion) pour vérifier notamment la sécurité de l'installation des équipements.