Entreprises et spectre électromagnétique

Aujourd'hui, de plus en plus d'applications utilisent les ondes électromagnétiques, que ce soit pour l'échange d'informations (ex : GSM, WIFI, BLUETOOTH, RFID…), les télécommandes (ex : domotique, contrôles d'accès), la détection (ex : détecteurs de mouvement) ou la géolocalisation (GPS). Ces systèmes sont souvent installés clés en main et le client ignore la plupart du temps le procédé ou les gammes de fréquences utilisés. Tant que le matériel remplit la fonction qu'on attend de lui, peu de personnes se posent des questions. Cependant, la sensibilisation aux vulnérabilités cyber amène petit à petit les clients, principalement des entreprises, à auditer l'ensemble de leurs systèmes informatiques et réseaux afin de se prémunir contre des attaques ou des fuites d'informations. Mais l'approche cyber n'est qu'une partie de la menace ; la multiplication des applications sans fil et l'arrivée massive de l'Internet des objets doivent conduire à une réflexion quant à leur vulnérabilité si une attaque venait à être commise via ce moyen. Il est vrai qu'aujourd'hui, il est difficile pour les citoyens de percevoir cette menace – à la différence de la menace cyber – car les médias communiquent peu à ce sujet, par simple ignorance.

Connaître ce que l'on utilise :

Dans leur grande majorité, les entreprises (et les particuliers) ignorent totalement le niveau de leur dépendance aux ondes électromagnétiques ainsi que les gammes de fréquences qui sont utilisées par leurs différents équipements. En conséquence elles ignorent aussi totalement quelles seraient les conséquences d'un brouillage, d'une perturbation (interférences), d'un déni de services ou d'une attaque de type guerre électronique sur leurs systèmes. Elles sont donc dans l'incapacité d'évaluer l'impact que ces évènements pourraient avoir sur le fonctionnement de l'entreprise ou sur sa sécurité.
A l'image de ce qui est fait pour le cyber, il faut aussi être maître de l'utilisation des ondes électromagnétiques afin d'en mesurer les vulnérabilités potentielles (fuites d'informations ou importance sur le processus de fonctionnement) et de mettre en place des mesures de contournements. Sans le savoir, beaucoup d'activités économiques sont très vulnérables à des attaques de type guerre électronique (https://www.cf2r.org/rta/guerre-electronique-une-menace-qui-concerne-aussi-le-secteur-civil/).
Il est aujourd'hui nécessaire pour chaque entreprise de connaître exactement l'usage qu'elle a des ondes électromagnétiques. Il lui faut donc répertorier l'ensemble des services qu'elle utilise reposant sur les ondes ainsi que l'ensemble des équipements émettant des ondes électromagnétiques, même sans le savoir. Qui sait que bon nombre de systèmes électroniques (systèmes de vidéo conférence par exemple) disposent en interne de puces GSM qui renvoient périodiquement au constructeur un diagnostic du système ? Il faut bien connaître l'existence de ces systèmes si on veut faire une analyse de risque. Ce type de diagnostic est même nécessaire avant tout audit de cyber sécurité car il permet de révéler l'existence de moyens dont la sécurité demande à être vérifiée.
A partir de cette liste exhaustive, il faut une analyse du niveau de criticité que représente chaque usage. Il est évident que le risque engendré par l'utilisation d'une cartouche d'encre reposant sur une puce RFID aura peu d'importance comparé à celui encouru par un entrepôt utilisant des puces RFID pour assurer la traçabilité de son stock ; de même la télécommande des climatisations aura peu d'importance par rapport aux détecteurs de mouvement reliés à l'alarme du site.

Responsabilités des employeurs :

A côté de la notion de risques et de vulnérabilités pour l'entreprise, il existe aussi, depuis le 1er janvier 2017, une obligation pour les employeurs de relever et de surveiller le niveau d'exposition de leur personnel aux rayonnements électromagnétiques, en application de l'article R4453-1 du Code

du travail. Si aujourd'hui tout particulier, ou toute entreprise, peut demander à l'ANFR (Agence Nationale des Fréquences) de faire faire, gratuitement, des mesures de niveau d'exposition aux champs électromagnétiques, ces mesures sont faites de manière globale (https://www.anfr.fr/fr/controle-des-frequences/exposition-du-public-aux-ondes/la-mesure-de-champ/faire-realiser-une-mesure/). C'est-à-dire que la mesure prend en compte l'ensemble du rayonnement électromagnétique sur une zone donnée sans que l'on connaisse les sources d'émissions et même sans savoir si elles viennent de l'entreprise ou si elles sont extérieures. Les mesures doivent être plus précises afin de définir les éventuelles responsabilités en cas de problème de santé déclaré chez un salarié. Ce type de problème risque fort de se poser rapidement alors que, d'une part les sources d'émission des ondes électromagnétiques sont de plus en plus nombreuses et que d'autre part, de plus en plus de cas d'électrosensibilité apparaissent (https://www.cf2r.org/rta/renseignement-dorigine-electromagnetique-pour-tous/).
Il devient alors important pour l'employeur de connaître toutes les sources d'émissions dans les locaux de son entreprise ainsi que le niveau de rayonnement que chacun de ses équipements génère. Ce sera la seule façon de pouvoir prouver que l'on respecte les normes en interne, même si l'environnement peut être soumis à des rayonnements extérieurs à l'entreprise beaucoup plus forts.

*

Que ce soit pour des raisons de sûreté, de sécurité ou de santé publique, il devient indispensable d'avoir une vue précise de l'ensemble des équipements émettant des ondes mais aussi de connaître leur niveau de rayonnement. Cette démarche est complémentaire des différents audits de sécurité, de cyber vulnérabilité ou de respect des normes HSCT (hygiène, Sécurité, Condition de Travail) mais devient indispensable dans le cadre de la protection des entreprises.

Olivier Dujardin a 20 ans d'expérience dans la guerre électronique et le traitement des signaux radar. Il a successivement assuré des fonctions opérationnelles dans la guerre électronique radar, dans l'étude des systèmes radar et de guerre électronique, dans l'analyse/recueil des signaux et dans la surveillance spectrale (TSCM). Il est chercheur associé au CF2R et consultant indépendant.