La cybersecurité des objets connectés

Le développement des objets communicants soulève de nombreuses questions liées à la protection des systèmes d'information et de communication, notamment pour les entreprises et les collectivités qui doivent se prémunir contre les attaques et le détournement de leurs systèmes.

Une nouvelle donne : la volumétrie croissante des objets connectés

La volumétrie croissante, au sein des organisations, des objets connectés, vont contraindre ces dernières à repenser et adapter leurs outils, processus et méthodes dans le domaine de la cybersécurité des objets et des systèmes.

L'actualité l'a douloureusement rappelé : le moindre objet connecté disposant d'un accès IP peut être utilisé de manière à menacer les plus gros fournisseurs d'infrastructures au monde, comme en ont par exemple fait l'expérience le blog de Brian Krebs hébergé par Akamai, la société Dyn ou encore l'hébergeur français OVH. L'attaque qu'a subie ce dernier a cumulé un débit proche de 1 Tbit/s et a impliqué environ 200 000 objets. Ces objets étaient de plusieurs types : routeurs Wifi, « *boxes* », lecteurs multimédia, systèmes Hi-Fi, caméras, thermostats, détecteurs de présence, voire des réfrigérateurs ou encore des téléviseurs connectés. Des « *maliciels* » (logiciels malveillants) tels que Mirai, Rakos, LizardStresser ou Leet, peuvent infecter ces objets connectés en exploitant des failles connues et/ou en bénéficiant de leurs configurations par défaut. Ils les organisent ensuite en « *botnets* » (réseau d'automates informatiques souvent destinés à des usages malveillants) prompts à déferler sur une cible.

Avec plus de 20 milliards d'objets connectés à l'horizon 2020, la sécurisation de ces objets s'avèrera difficile. Il y a en effet fort à parier qu'une partie non négligeable de ces objets comportera des failles d'origine que leur détenteur ne s'efforcera pas de corriger soit par négligence, soit par méconnaissance ou par incompétence. Ils conserveront vraisemblablement également une configuration par défaut relative, notamment, au mot de passe administrateur. Or, à ce jour, aucune règlementation n'impose un minimum de bonnes pratiques aux constructeurs.

Cette problématique des objets connectés dits « *grand public* », externes aux organisations, est largement relayée par la presse. Elle est par conséquent bien identifiée et en voie de traitement dans le cadre des mesures de protection mises en place. Mais dans les prochaines années, les entreprises et les collectivités seront confrontées à une autre problématique, moins connue et moins immédiatement perceptible, celle des objets connectés internes à ces organisations.

Les objets connectés internes aux entreprises et collectivités

Une partie non négligeable des milliards d'objets envisagés dans le futur sera constituée

d’instruments de mesure, notamment le compteur évolué Linky, - qui doit être déployé dans 35 millions de foyers et entraînera l’installation parallèle de 700 000 concentrateurs installés dans les postes de distribution publics à l’horizon 2021 -, de capteurs, d’actionneurs déportés ou encore de détecteurs de présence communicants. Tous ces objets seront placés sous la gouvernance d’entreprises privées, de services publics et de collectivités.

Le tableau ci-dessous compare les principales caractéristiques techniques d’un objet connecté avec celles d’un équipement de bureau (poste de travail et mobile, désormais bien gérés par la sécurité des systèmes d’information).

Objet connecté d’entreprise		**Poste de travail / mobile**
Mémoire vive	100 ko **x 20 000**	2 Go
Stockage	256 ko **x 1million**	256 Go
Fréquence	32 MHz **x 100**	3 GHz
Consommation	10 ?W **x 1 million**	10 W
Bande passante	1 kbit/s **x 10 000**	10 Mbit/s

Ces différentes conséquences rendent la gestion des risques associée à ces objets complexe et incertaine.

De plus en plus de systèmes critiques sont appelés à être pilotés, informés et guidés par des systèmes complexes et autonomes constitués en partie d’objets connectés, et ce dans de nombreux domaines tels que les transports (véhicules autonomes), la météo ou la gestion des flux au sein d’une collectivité (fluides, trafic). Cette automatisation vise à accroître la sécurité et la fiabilité des systèmes et promet des gains d’efficacité à court terme. Outre les difficultés intrinsèques que comportent de telles infrastructures, celles-ci attireront certains « *agresseurs* » déterminés à prendre en otage leur propriétaire par différents moyens, comme l’usurpation, le détournement des informations ou le sabotage. Il s’agit donc, pour les gestionnaires de risques au sein des organisations concernées, de faire évoluer leur politique de sécurité des systèmes d’information afin d’assurer efficacement la gestion, la supervision et le respect de la conformité de ce type de parc d’objets connectés.

Les impacts de l’utilisation des objets connectés sur les organisations

Les objets connectés au sein des entreprises et des collectivités peuvent être caractérisés par plusieurs dimensions qui influencent leur fonctionnement ainsi que les politiques à mener en matière de sécurité des systèmes d'information :

- leur nombre, ou leur volumétrie ;

- leurs capacités (puissance de traitement, quantité de mémoire) ;

- la fragmentation des environnements qu'ils utilisent ;

- les capacités de communication (débits disponibles et régularité) ;

- leur isolement (possibilité d'agir sur eux physiquement) ;

- la diffusion des connaissances concernant ces configurations (plus un environnement est connu, plus le risque de manipulation est élevé).

Le tableau 2, ci-dessous, présente les effets de l'utilisation d'un parc d'objets connectés sur le fonctionnement d'une organisation, ainsi que sur la gestion de la sécurité des systèmes d'information, en fonction de ces différentes dimensions.

Dimension d'étude	Caractéristiques	Impact sur le fonctionnement de l'organisation	Impact sur la gestion de la sécurité des systèmes d'information
Nombre	Des dizaines de milliers	Difficultés à être à jour dans la prise en compte de tous les objets	Nécessite des ressources en personnel ou une automatisation poussée des procédures
Capacités	Un microcontrôleur et quelques dizaines de kilo-octets	Incapacité à accueillir des outils locaux de supervision et de contrôle	Difficulté de supervision
Fragmentation	Très fragmenté (nombreux écosystèmes)	Peu de factorisation possible dans les méthodes et les procédures	Nécessite des ressources en personnel ou une automatisation poussée des procédures
Communication	Rarement connecté et très peu de débit (par exemple, technologies radio à longue portée)		