La cybersécurité 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 µW x 1 million	10 W
Bande passante	1 kbit/s x 10 000	10 Mbit/s

Tableau 1 : Comparatif technique d'un objet connecté interne à l'entreprise et d'un poste de travail / mobile

Comme l'indique le tableau 1, ci-dessus, les caractéristiques techniques des objets connectés sont jusqu'à 1 million de fois inférieures à celles d'un équipement de bureau, ce qui a plusieurs conséquences en termes de gestion de ces objets :

- un état des lieux difficile à établir et à maintenir à jour ;
- une absence d'information en temps réel ;
- la quasi-impossibilité à mettre en place des agents de surveillance locaux ;
- des coûts de remise en fonctionnement rédhibitoires dus à la dissémination des équipements.

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)	- Impossibilité d'être informé de l'état de l'objet en temps réel - Peu de latitude à intervenir à distance (diagnostic, prise en main)	- Impossibilité d'avoir une vue exhaustive, sûre et en temps réel du parc d'objets - Impossibilité d'être informé rapidement d'attaques en cours, conduisant à une éventuelle réponse inadéquate - Par ailleurs, les objets devenus inaccessibles le resteront (pour des raisons de coût)
Isolement	De peu isolé (automate) à très isolés (capteurs enfouis)	- Pour les plus isolés, une fois l'objet mis en service, il est très onéreux d'intervenir à nouveau - À l'inverse, un retournement, un détournement physique est aisé (mais couteux pour l'attaquant éventuel)	- Si des objets viennent à ne plus être joignables, à moyen terme, le métier est impacté - Conséquences possibles en termes d'image de l'organisation (suite à l'incapacité à assurer le service) - Conséquences financières éventuelles (frais de remise en service)
Connaissances	Rares	Difficultés à adapter les procédures au plus juste	Certains objets ne sont pas pris en compte dans les politiques de sécurité

Tableau 1 : Conséquences et impacts de l'usage des objets connectés

Réviser les outils, les processus et les méthodes

Prévenir les attaques

Face aux enjeux de gestion des objets connectés, un ensemble de bonnes pratiques doivent être adoptées, notamment dans trois disciplines principales de la cybersécurité :

- **La supervision** : il s'agit de surveiller, alerter et remonter les indicateurs générés au plus proche de la source des évènements ce qui permet de prendre des décisions opportunes et justifiables *a posteriori*. La supervision d'un grand nombre d'objets connectés est difficile, car les sources ne communiquent qu'une fois par jour tout au plus et uniquement pour acheminer des données *« métier »,* et non des informations destinées à la sécurité des systèmes d'information. En outre, il est généralement impossible de placer des agents de surveillance sous forme de logiciel sur lesdits objets au vu de leur capacité de mémoire et de calcul ;
- **L'analyse des risques** : il s'agit de mener des audits des systèmes et des configurations, via des tests d'intrusion éventuellement, ainsi que la gestion et la détection des vulnérabilités. Les analyses de risques sur un grand nombre d'objets connectés sont rendues difficiles par le fait que des milliers d'équipements sont disséminés sur un territoire potentiellement très étendu, un pays entier par exemple. De plus, le coût unitaire d'un objet connecté ne peut justifier le déplacement d'un expert pour réaliser une analyse *in situ* ;
- **La conformité** : il s'agit de la conformité aux standards et aux exigences règlementaires, générales ou sectorielles, qui nécessite une révision régulière des équipements. Cette mise en conformité est réalisée via des mises à jour des systèmes rendues difficiles par le grand nombre de dispositifs concernés, dont beaucoup sont difficilement accessibles.

L'approche *« secure by design »*

Un nombre croissant d'acteurs optent aujourd'hui pour une approche dite *« secure by design »*, qui consiste à faire de l'aspect sécurité un élément clé de l'élaboration même du produit. Il s'agit d'une méthode de conception qui prend en compte, dès le début, tous les risques identifiés liés au développement des aspects matériel et logiciel d'un objet connecté.

Afin de faciliter la mise en place de l'approche « *secure by design* » et en complément de celle-ci, il s'agit notamment de :

- Spécifier, en amont, la capacité du micrologiciel (*firmware*) à être « *modulaire* », c'est-à-dire conçu pour que des mises à jour ne concernant qu'une partie de ce micrologiciel puissent être réalisées grâce au réseau (au lieu de mises à jour de l'ensemble du micrologiciel à chaque modification), même si ce dernier dispose de très peu de bande passante. Il s'agira également de spécifier au même moment la capacité à transmettre un « *état de santé* » concentrant en peu de mots, et donc d'octets, un bilan représentant les principales variables d'état de l'objet connecté.
- Mettre au point une méthodologie de mise à jour par d'autres moyens que le réseau principal dans le cas où ce dernier n'est pas en mesure de véhiculer une correction majeure en un temps limité. Les composants radio multi-usages apportant, en plus d'un réseau longue portée, le WiFi et le Bluetooth peuvent alors s'avérer pertinents même si cela implique un déplacement à proximité des objets et impacte la source d'alimentation de ces derniers.
- Établir des spécifications qui garantissent l'innocuité d'une malversation physique, par exemple avec l'utilisation d'un micrologiciel signé, une procédure de démarrage (boot) sécurisée, afin de s'assurer que l'objet ait la capacité à conserver et à prouver l'intégrité de son logiciel et de ses données dans le temps.
- Expliquer, sensibiliser aux concepts de sécurité en amont, avant même l'étape de conception, au niveau des métiers, afin que le cahier des charges exprimé permette d'engager naturellement l'approche « secure by design ».

Conclusion

La dissémination, la quantité des objets connectés et la faible puissance de calcul embarquée, conjuguées à des budgets alloués à la sécurité des systèmes d'information qui augmentent difficilement, rendent caduques les méthodes de déploiement, de supervision et d'analyse actuellement adoptées en la matière. Il est désormais essentiel pour les entreprises et les collectivités d'être en capacité de réagir très rapidement et sur plusieurs fronts à la fois, et pour cela de disposer d'un maximum d'informations remontant du terrain. Ceci implique de revisiter les architectures, de revoir les moyens octroyés et de les répartir différemment, et enfin de former le personnel à ces nouveaux enjeux.

Une piste envisageable pour gérer à la fois la complexité et la sécurité des systèmes, ainsi que la rigueur que cela suppose, consiste à utiliser l'intelligence artificielle dans les métiers de gestion des risques. Cette démarche apparait aujourd'hui comme la plus crédible, notamment dans le domaine des objets communicants mais également dans les domaines plus classiques de la cybersécurité.

Yélé Consulting est un cabinet de conseil spécialisé dans la transformation numérique et la transition énergétique des territoires et des Utilities. Grâce à son expertise *Smart grids* et *Smart cities*, Yélé accompagne ses clients, acteurs du secteur de l'énergie et collectivités territoriales, dans leurs programmes d'expérimentation et d'industrialisation dans le domaine des réseaux intelligents, dans la valorisation des données énergétiques à l'échelle d'un territoire et dans le développement de services urbains innovants et de nouveaux usages intégrés au réseau électrique. Yélé conseille, également, de grands groupes industriels dans leurs orientations stratégiques prises dans le domaine de la cybersécurité et de l'internet des objets.

Créé en 2010, Yélé compte aujourd'hui près de 40 collaborateurs issus de parcours professionnels au croisement des filières énergétique et numérique. Yélé est membre de l'association professionnelle Think Smartgrids et du pôle de compétitivité Systematic Paris-Region dédié au numérique.