En route vers l'Internet of Everything

Le pionnier anglais de la technologie Kevin Ashton, cofondateur du Massachusetts Institute of Technology (MIT) est connu pour être l'inventeur de la notion d'Internet of Things (Internet des objets). Le concept d'«Internet des objets» est une vision du futur dans laquelle les systèmes sont en mesure d'établir, via Internet, des liaisons entre eux ainsi qu'avec le monde physique.

Au cours de la conférence Cisco Live 2013 à Orlando, à laquelle assistaient quelque 20.000 décideurs en informatique, John Chambers, PDG de Cisco, annonçait la prochaine étape de la vie d'Internet of Things, dans laquelle les choses (Things) seraient remplacées par Tout (Everything) soit en abrégé IoE. Dans ce «Tout» seront connectés, via Internet, selon John Chambers, les gens, les données et les choses. Internet of Everything concerne non seulement la communication de machine à machine, mais aussi entre machines et personnes, et même, dans la vision de Cisco, de personne à personne. Bref, un mélange total de communications entre humains, humains et machines, et entre machines. Tout ceci devant conduire à plus de connaissances et plus de productivité. L'un des fondements d'Internet of Everything est la convergence toujours plus forte entre la bureautique (Information Technologies ou IT), l'automatisation de la production (Operational Technologies ou OT) et la sécurisation physique. Cisco joue ici un rôle moteur.

La bataille de l'Internet of Everything est en cours et évolue rapidement. Ce dernier est hétérogène et englobe tant les produits et services horizontaux que verticaux. Il peut être appliqué à des infrastructures câblées ou sans fil. Ces infrastructures peuvent être situées à l'intérieur comme à l'extérieur. L'infrastructure Internet of Everything est peuplée d'appareils allant des ordinateurs aux dispositifs intelligents ou «smart devices», lesquels possèdent des fonctionnalités «intelligentes» en raison des infrastructures et services auxquels ils sont raccordés. Un dispositif intelligent ou «smart device» est un appareil électronique connecté à d'autres appareils ou réseaux tels qu'Internet, Bluetooth, Zigbee, Near Field Communication (NFC), WiFi, 3G et 4G. En première approche, ce sont des appareils basés sur la technologie IP (Internet Protocol). L'IoE facilite la vie des consommateurs et des entreprises et influence tous les aspects quotidiens de la vie moderne en communauté.

Les infrastructures basées sur la technologie IP jouent ici un rôle crucial. L'Internet of Everything a pour objectif d'offrir une infrastructure intelligente, maîtrisable et sûre pouvant être étendue à des milliards d'appareils conscients de leur environnement. Le réseau intelligent écoute, apprend et réagit avec des interfaces ouvertes, pour une meilleure protection, une simplicité, une fiabilité, une continuité, une innovation plus grandes, et peut-être plus de confort que jamais auparavant.

Exigences concernant les appareils IoE

Il est clair qu'Internet of Everything pose des exigences aux appareils utilisés. Grosso modo, on distingue cinq caractéristiques importantes auxquelles devront répondre les appareils:

- Chaque appareil connecté devra disposer d'une adresse IP unique, qui sera utilisée pour l'identification et la communication.
- Chaque appareil connecté, mobile ou fixe, devra posséder une localisation unique (parfois virtuelle). Ceci est indispensable pour que les infrastructures de communication sous-jacentes puissent fonctionner efficacement.
- Il s'agit d'une situation dans laquelle un appareil doit traiter ou générer des informations. La quantité d'informations dont nous parlons ici dépassera assez rapidement les informations transmises par les gens.
- Il faudra des dispositifs complexes assurant la sécurité, l'analyse et la gestion, afin de permettre de former des groupes d'appareils reliés entre eux via des réseaux IP.
- Pour le traitement ou la génération d'énormes quantités de données, le temps et la place seront d'une importance cruciale.

Rôle important de la sécurité

L'IoE comporte également des risques, plus élevés encore; ce sera pour les hackers un objectif d'attaque très intéressant. Avec la croissance de l'IoE, les risques d'attaque ne feront que croître. Il est donc d'importance capitale que la sécurité reçoive beaucoup d'attention.

La protection d'IoE peut être en grande partie facilitée grâce à l'architecture du réseau. En réalisant cette architecture par couches, il est également possible de paramétrer la sécurisation par couche. Dans la couche la plus profonde se trouvent les points terminaux (ou «end points»). Ce sont les systèmes intégrés, les capteurs, les actionneurs, les caméras et autres. Bref, un éventail très large d'appareils qui sont souvent très bon marché et destinés à ne remplir qu'une seule fonction. De nombreux points terminaux peuvent être raccordés sur un réseau IP. Malgré cette possibilité, le nombre »

» de points terminaux effectivement raccordés est encore très bas. C'est parfois dû au fait que l'infrastructure nécessaire n'existe pas. Dans un certain nombre d'autres cas, les systèmes d'assurance qualité et la réglementation n'autorisent pas ce type d'appareils. Il existe ainsi sur le marché des détecteurs à infrarouge pouvant être raccordés sur un réseau IP, mais le système d'assurance qualité relatif aux installations anti-intrusion, la réglementation dite BORG aux Pays-Bas, ne permet pas d'utiliser de tels détecteurs à infrarouge IP. Heureusement, de nombreux points terminaux fonctionnent de manière autonome.

Au-dessus de la couche inférieure comportant les points terminaux, on trouve la couche multiservice. Cette dernière comporte l'appareillage de réseau en liaison avec les points terminaux. La couche multiservice facilite une série de protocoles et de techniques. Il faut éviter que des points terminaux ne soient pas protégés. Les services de sécurité au sein de la couche multiservice jouent ici un rôle important. Comme indiqué ci-dessus, le trafic point à point (peer to peer) entre les divers points terminaux constitue une donnée importante sur le plan de l'efficacité du réseau. Au-dessus de la couche multiservice se trouve le cœur de réseau IP/MPLS et les centres de données, avec tous leurs mécanismes de protection informatique.

Sécurisation physique

Dans le cadre de la sécurisation physique, la transition vers la technologie IP a lieu depuis des années déjà, si l'on en croit les acteurs de la branche. En pratique, nous voyons encore souvent dans un bâtiment une séparation physique entre les différents réseaux IP. Souvent, le réseau IP de bureautique est séparé physiquement du réseau de sécurisation, également à technologie IP. Les réseaux d'automatisation de processus (PCS, SCADA) sont très souvent séparés des autres réseaux IP. De ce fait, les fondements du concept Internet of Everything sont altérés. Bien que Cisco s'investisse dans Internet of Everything et veuille y associer la sécurisation physique, elle se limite au contrôle d'accès et à la vidéosurveillance. Les autres types de sécurisation physique tels que la détection intrusion n'entrent pas encore dans la vision «Internet of Everything» de Cisco. Il devrait être toutefois possible de faciliter le fonctionnement de la détection intrusion grâce à «Internet of Everything». Comme dit précédemment, il existe sur le marché, par exemple, des détecteurs à infrarouge pouvant être raccordés à un réseau IP. On pourrait aussi, à la place de détecteurs à infrarouge, utiliser des caméras à détection de mouvement. Il devrait être possible de créer cette fonction à partir des données issues de ces points terminaux (à savoir les détecteurs infrarouge et les caméras).

Tendance du marché

La tendance vers une convergence entre la bureautique, l'automatisation de processus et la sécurisation physique est nettement perceptible au niveau du marché. Les premières adjudications pour lesquelles il est demandé une telle convergence sont déjà sorties. On peut y ressentir une tension naturelle entre la pensée traditionnelle et la vision «Internet of Everything». Kristian Steenstrup, Vice-président Recherche auprès de l'analyste de marché indépendant Gartner signale également que la nature de l'automatisation de processus est en train de changer. Ces systèmes et les technologies sous-jacentes ont de plus en plus les caractéristiques de l'informatique grand public. Il le voit également se produire au niveau des plates-formes, des logiciels, de la sécurisation et de la communication. Selon Kristian Steenstrup, les responsables informatiques sont influencés par la convergence entre informatique grand public et automatisation de processus. Dans le bureau de direction aussi perce à présent l'idée que cette convergence peut être rentable et donc permettre une gestion plus efficace. Bien que les défis posés par l'intégration convergente de la bureautique (IT), de l'automatisation de processus (OT) et de la sécurisation physique soient grands, elle présente suffisamment d'avantages, tels que: budgets simplifiés, planning coordonné, décisions technologiques cohérentes, et pouvoir d'achat maximisé.

Par Ronald Eygendaal (Principal security consultant chez Eygendaals Services, membre du bureau de l'Association néerlandaise des Professionnels de la Sécurisation (Vereniging Beveiligingsprofessionals Nederland (VBN))