Association Nationale des Dirigeants en Sciences de l'Information
www.andsi.fr

Informatiques « industrielles » et « de gestion » : quelle convergence ?

Compte rendu rédigé par ANDSI

En bref…

François GUYOT et Benjamin MENESTRET proposent une réflexion sur les possibilités de convergence de 2 « informatiques traditionnellement séparées, les informatiques « industrielles » et « de gestion ».
Cette thématique conduira sera illustrée au travers du prisme de la cybersécurité et de l'arrivée massive des IoT dans les entreprises.

L'Association Nationale des Directeurs des Systèmes d'Information organise des débats et en diffuse des comptes-rendus, les idées restant de la seule responsabilité de leurs auteurs. Elle peut également diffuser les commentaires que suscitent ces documents.

François GUYOT, ex DSI Corporate de Plastic Omnium, a connu une carrière dans les industries automobile (Plastic Omnium), pharmaceutique (Laboratoires Fournier) et de défense (GIAT Industries), au cours de laquelle il a observé/géré les relations entre ces deux « mondes ».
Benjamin MENESTRET indique qu'il dispose d'une expérience de quinze ans dans le domaine de la cybersécurité, dont six ans au sein de Palo Alto où il s'occupe des comptes globaux dans les secteurs de l'énergie et de l'industrie. Palo Alto Networks est un des acteurs leaders en matière de cybersécurité avec :

- 75 000 clients sur 150 pays ;
- 3 milliards d'euros de chiffre d'affaires ;
- 20 % de croissance annuelle.

Cette croissance illustre que la réponse technologique aux enjeux cyber que propose Palo Alto Networks est adaptée aux attentes des clients sur la sécurité des infrastructures réseau, du cloud et l'efficience des opérations de sécurité.

L'organisation de la DSI

François GUYOT présente un organigramme classique d'une DSI (Etudes, Infrastructures, Support, ..), et souligne que l'organisation classique de la DSI dans l'industrie renvoie à la nécessité de gérer un mix de ressources homogènes (par technologie ou métier) au profit d'actions et de projets hétérogènes (projets). Cette organisation pour fonctionner suppose que la communication entre ces composantes soit réelle .. du fait de l'animation apportée par le DSI.

Par ailleurs, sur les thèmes touchant à la R&D, l'industriel, il importe de relever une dépendance très forte vers le métier. La communication s'avère délicate. Il convient de conserver à l'esprit que dans le passé, les fonctions informatiques dans l'industrie étaient marginales.

S'agissant de la réalité des deux périmètres :

1. « informatique classique » qui a une logique d'infrastructure,
   - infrastructures internes (applications, réseaux, systèmes de communication),

- infrastructures externes (services *cloud*)
- équipements de l'utilisateur (stations de travail, équipements mobiles, usages autorisés).

2. périmètre « métier industriel ».
   - les fonctions (automatismes industriels, applications, etc.),
   - les données accumulées (données de process, de contrôle, etc.)
   - des infrastructures dispersées (juxtaposition de serveurs, standards imposés par le fournisseur industriel, etc.).

Concernant les évolutions constatées dans l'industrie, il convient d'abord de mentionner une montée des convergences de facto sur les thèmes de la gestion et du pilotage des SI utilisés dans le monde industriel :

- du signal vers la donnée ;
- de la transmission *machine to machine* vers le traitement algorithmique/applicatif ;
- des plateformes spécifiques vers les standards technologiques du marché (OS, moteurs de bases de données, réseau LAN, parc IoT (Internet of Things) en croissance exponentielle).

Pour illustrer ces analogies, le prisme de la mise en place des IoT dans le périmètre industriel et ses problématiques de Cybersécurité va être présenté et rapproché des problématiques Cybersécurité pratiquées par les DSI classiques.
De ce cas une généralisation de l'analogie est mise en perspective.

La convergence IT/OT

Benjamin MENESTRET souligne que les différentes menaces informatiques peuvent être traitées de manière uniforme sur l'ensemble des périmètres, d'où un besoin de convergence.

A ce jour, l'industrie est « 4.0 » ou « hyper connectée ». Les automates sont de plus en plus connectés. Des mécaniques propres au monde IT (Information Technologies – SI d'entreprise ou informatique de gestion) à l'instar du *big data* sont désormais transférées dans les usines. Par ailleurs, les objets OT (Operation Technologies - Systèmes Industriels) se transforment en IoT et viennent modifier le fonctionnement OT traditionnel. Le nombre de *devices* devient de plus en plus important, avec des croissances exponentielles. Une adoption massive des objets IoT et leur intégration dans l'environnement IT, et donc traditionnellement moins protégé que les environnement OT, augmente la surface de risques. Il a été montré à travers des études que le niveau d'exposition des objets connectés aux menaces est important, d'où l'augmentation de la surface de risque. Faire converger la cybersécurité IT et OT permettrait de mettre en place un framework global pour répondre aux besoins de protections des métiers.

François GUYOT rappelle le modèle de sécurité type dans un environnement de sécurité industriel:

- zone verte : contrôle effectué en interne ;
- zone orange : zone de semi-contrôle (collaborateurs à l'extérieur, les partenaires, etc.) ;
- zone rouge : absence de visibilité et de contrôle.

Dans ce cadre, les systèmes de gestion sont localisés dans les usines.

Benjamin MENESTRET fait état d'une évolution vers des modèles plus connectés, avec l'installation de *sensors*, à savoir des *smart sensors*, des *sensors* qui collectent de l'information, des *sensors* qui génèrent un grand nombre de données.

Au-delà de la couche outils, il convient de mentionner création d'une couche d'interconnexions qui seront connectées au reste du réseau. L'IoT renvoie à des équipements capables de se connecter en Bluetooth ou en 4G vers d'autres outils.

L'industrie 4.0 conduit à l'établissement d'une couche de services (gestion, sécurité, stockage, etc.). Le principe dans le cadre de cette industrie consiste à collecter un maximum d'informations pour comprendre ce qui se passe sur l'usine. Les priorités du *cloud* permettent de mettre à l'échelle l'infrastructure pour stocker un nombre toujours plus important de données et de mieux les analyser afin de disposer une capacité de calcul pour effectuer de la *maintenance prédictive et optimiser les lignes de productions* par exemple.

François GUYOT ajoute que l'univers des services applicatifs est relativement nouveau dans le monde industriel et ancien dans le monde de la gestion.

Des sources de risques identifiées

Benjamin MENESTRET évoque les principales sources de risques relatives aux objets hyper connectés. Tout d'abord, 98 % du trafic lié à l'IoT n'est pas chiffré, ce qui induit un risque d'intégrité sur la donnée et de confidentialité par rapport aux données métier. Ensuite, 57 % des *devices* sont vulnérables à des attaques. Enfin, 83 % des systèmes d'imagerie médicale fonctionnent sur des OS qui ne sont pas supportées.

Ces vulnérabilités sont déjà exploitées et on l'illustre à travers deux exemples de cyberattaques
Une première attaque intéressante se rapporte à GreyEnergy dont l'objectif consistait à extraire le maximum d'information sur la cible. Il relève ensuite deux principaux scénarios d'attaque. Le premier renvoie à l'utilisation de *phishing* ciblé pour forcer l'utilisateur à cliquer. L'autre scénario correspond à la compromission du web serveur à distance, ce qui permet ensuite d'accéder sur l'infrastructure et de s'installer sur les postes de travails ou serveurs qui sont les plus disponible : serveurs applicatifs et poste de contrôle des lignes de production. Cet exemple montre que la convergence constitue une obligation. La menace doit être traitée de bout en bout.

Un second exemple d'attaque se rapporte à l'IoT en tant que vecteur de menace. L'exemple de « Miraï » est significatif. Dans ce cadre, des caméras de surveillance ont été utilisées pour lancer des attaques massives sur les infrastructures. Cet exemple montre que l'IoT peut constituer un vecteur d'attaque.

Trois menaces majeures concernent les environnements IT/IoT :

- exploitation de la vulnérabilité des *devices* ;
- faiblesse des *passwords* ;
- *ransomware*.

Concernant ce dernier point, il convient de mentionner Silexbot dont l'objectif était de mettre hors service des *devices* IoT. Ce type de menace s'observe aussi bien dans l'IT que dans l'IoT. Les surfaces de risque renvoient notamment aux *browsers* ou aux *operating systems* qui ne sont pas à jour.

Vers une réduction du risque

Deux approches sont envisagées pour réduire le risque. La première qui correspond à l'approche tactique implique les éléments suivants :

- disposer d'une visibilité sur l'ensemble des *objets* sur le parc pour prendre les bonnes décisions ;
- patcher autant que possible les équipements ;
- segmenter les réseaux ;
- être capable de monitorer en temps réel le comportement des objets pour vérifier qu'il est conforme à ce qui est attendu.

La seconde est l'approche stratégique (*zero trust security strategy*). Elle renvoie aux éléments suivants :

- définition du métier et compréhension des besoins relatifs à l'objet ;
- question des accès de l'objet et mise en place d'une segmentation adatpée
- inspection du trafic pour vérifier le comportement de l'objet/

Par ailleurs, le cycle de vie d'un objet IoT peut être comparé à celui d'une application :

- identifier quand un nouvel objet est détecter sur le réseau, quelles données il va utiliser et comprendre son niveau d'exposition aux risques
- intégrer cet objet dans le réseau existant
- déployer le niveau de sécurité adapté.
- superviser l'utilisation de cet objet, les données réseau, les menaces pour adapter
- déterminer la fin de vie de cet objet quand il ne peut plus être maintenu et que son niveau de risque est trop élevé.

François GUYOT relève un réflexe différent dans le monde industriel : en effet, un objet qui fonctionne est conservé « en l'état », tout changement étant un risque d'interruption de fonctionnement.

Benjamin MENESTRET explique que les bases permettant de sécuriser l'industrie 4.0 et les objets IoT existent déjà.

Une réponse du marché (parmi d'autres) : l'approche Palo Alto sur la sécurité

L'approche portfolio Palo Alto Networks consiste à donner un maximum de visibilité sur l'ensemble des infrastructures du périmètre du SI : Sites distants, datacenter, Cloud pour appliquer les contrôles de sécurité adaptés. Un firewall Palo Alto peut répertorier l'ensemble des applications qui passent sur le réseau ainsi que les users, les *devices et les menaces*. Un autre point clé se rapporte à la consolidation des services de sécurité sur un *firewall* unique afin d'améliorer l'administrabilité et la mise à l'échelle de l'infrastructure cyber. De surcroît, une offre de services dédiée à la sécurité des environnements *cloud* est proposée pour répondre spécifiquement aux besoins des applications « cloud natives », s'intégrant dans les processus DevOps.

Enfin, dans une approche de plateforme de cybersécurité globale, un travail est conduit afin d'automatiser et d'intégrer les différentes composant. A ce jour, 55 % des entreprises interrogées possèdent plus de 25 équipements de sécurité différents. Il apparaît donc délicat de manager 25 équipements, tant d'un point de vu complexité d'infrastructure que de posture de sécurité. C'est la raison pour laquelle un travail d'intégration est mené entre les services et solutions Palo Alto Networks.

Le service de sécurité OT/IOT proposé par Palo Alto Networks, s'appuie sur ces principes d'intégration et de consolidation : sur chaque firewall déployé, le service va pouvoir être activé et permettre de donner une visibilité sur les actifs, vulnérabilités et menaces associées, puis d'appliquer des contrôles de sécurité adaptés.

Conclusion

En synthèse, François GUYOT constate que « *le cyber de l'un est le cyber de l'autre* ». Une convergence de fait se met en place sur le marché en ce qui concerne les besoins en *know how* des savoirs faire « informatique » maintenant nécessaires au périmètre « industriel ».
En bref, la DSI « historique » **sait faire** : qu'elle se positionne pour occuper ce terrain et permettre une accélération de la transformation.

A titre d'illustration, Dassault Aviation déploie une organisation triptyque avec des représentants des sites, la Direction Générale des opérations industrielles et la Direction Générale des systèmes d'information. L'objectif est d'aboutir à une équipe conjointe afin d'analyser des besoins et définir les priorités pour instaurer un dialogue. L'OT est en mesure de définir ses besoins. Néanmoins, l'IT peut l'aider à propos de la gestion des serveurs et des applications.

Débat

Int : Les industriels ont réalisé le bénéfice qu'ils avaient à tendre vers l'interconnecté. Dans ce cadre, il est intéressant de conduire une approche par la sécurité. En outre, les informaticiens rencontrent souvent des difficultés à convaincre le métier. Sur les aspects afférents à la sécurité, les acteurs de l'industrie font souvent preuve d'une crainte exagérée.

FG : Chez Plastic Omnium nous faisons du Palo Alto depuis 2010 car la DSI a su convaincre. Notre travail de DSI consiste à convaincre des actions à réaliser tout en restant raisonnable. C'est notre capacité d'influence en direction des métiers.

BM : La notion de gestion du cycle de vie d'objet constitue un point important.

Int : Dans le monde de l'automobile, le défi au-delà de l'obsolescence, se rapporte à l'arrivée d'objets différents des PC et qui se connectent au wifi à l'instar des tablettes. Nous ne disposons d'aucune idée à propos de la manière d'appréhender la sécurité. Nous avons travaillé sur des certificats et nous essayons d'y intégrer ces objets wifi.

FG : Nous devons anticiper le risque que les matériels subissent un piratage.

BM : Il apparaît nécessaire de déployer une solution de sécurité pouvant être facilement adoptée et offrant un niveau de défense attendu.

FG : Dans le nouveau monde, un risque significatif se rapporte à l'absence de norme, ce qui soulève une réelle problématique de sécurité. Il importe d'anticiper et de poser des garde-fous.

Présentation des orateurs
François GUYOT ex Corporate CIO de PLASTIC OMNIUM, est diplômé de l'ISG et ENSIMAG. Il a commencé sa carrière en 1979 comme développeur (GAN...) puis en tant qu'IT Manager chez GIAT Industries où il est resté 10 ans puis en 1996 chez FOURNIER Pharma pour occuper le poste de CIO jusqu'en 2007. A Partir de 2007 il rejoint PLASTIC OMNIUM pour occuper le poste de CIO au sein de la division AUTO EXTERIOR puis devient en 2010 CTO Groupe, en 2012 CIO Corporate, et en 2017 Directeur Cyberdéfense.

Benjamin MENESTRET, de formation ingénieur Télécom, a commencé sa carrière chez Apixit comme Ingénieur Système & Sécurité, puis chez Accenture en 2010 comme Security Consultant, puis chez Rhode & Schwartz en 2013 comme Technical Account Manager et depuis 2015 chez Palo Alto Networks en tant que Pre-Sales Systems Engineer.