Hexatrust planche sur la cybersécurité et l'industrie du futur

Comment «cybersécuriser» l'Industrie du futur (comme on la nomme en France) ou 4.0 (en Allemagne)? Cette question, schématique, s'inscrivait dans les débats de l'Université d'été de Hexatrust, jeudi 1er septembre à Paris. Pour **Jean-Pierre Tual**, directeur des relations industrielles chez Gemalto et président du groupe Confiance Numérique et Sécurité de Systematic, *« l'Industrie du futur repose sur trois principes: connecter, sécuriser et monétiser »*. La connectivité *« est une façon de repenser l'interaction entre des objets et des humains en intégrant le fait que chacun d'entre eux dispose des capacités d'apprentissage et d'intervention »*.

Sécuriser ces interactions impose le principe de la sécurité de bout-en-bout avec toute la problématique de gestion de cycle de vie des droits que cela entraine ainsi que la façon de repenser la protection des données avec la «cloudification» des applications. *« Il faudra avoir des outils capables de décrire l'ensemble des traitements, des analyses d'impact sur les traitements sensibles, et d'appliquer des mécanismes fondamentaux technologiques qui vont garantir cette confidentialité*, avance-t-il. *Ça pose des problèmes très compliqués. »* Par exemple, *« comment empêcher la réplication d'un prototype fabriqué à partir d'une imprimante 3D? »* s'interroge Jean-Pierre Tual. Enfin, la monétisation *« restructure les relations de l'ensemble de la chaine de paiement d'une entreprise entre ses fournisseurs et ses sous-traitants »*. Si aux yeux du responsable on est, en France, assez bon sur la connectivité et la sécurisation, des progrès restent à faire sur la monétisation et *« le codesign de l'ensemble »* afin de *« créer le backbone du manufacturing 4.0 »*.

L'intégrité des informations, un enjeu majeur

Une vision que partage **Eric Payan**, responsable des systèmes d'information de Bosch Rexroth et du projet Industrie 4.0 de l'industriel en France. Pour lui, *« l'Industrie du futur ne touche pas l'industrie mais l'entreprise »* pour laquelle *« l'intégrité de l'information est un enjeu majeur »*. Une mauvaise information, dans des ordres de production par exemple, peut engendrer *« des pertes considérables »*. Une problématique qui dépasse les seules questions de production pour déborder sur les usages grand public.

« Demain, en 2018, du lave-linge à la cafetière en passant par le réfrigérateur, tout les objets de la maison seront connectés, et si en tant que consommateur je ne peux pas avoir confiance dans la protection de ma maison par les outils électroniques, ça ne marchera pas. » Autrement dit, l'adoption ne prendra pas. La voiture autonome et ses nombreuses expérimentations grandeur réelles qui fleurissent un peu partout dans le monde actuellement en est un bon exemple. *« Je veux être sûr que le véhicule autonome m'emmène où je veux et pas dans un platane*, insiste Eric Payan. *Elle ne sera adoptée que si le grand public a une confiance absolue dans le système. »*

Mais comment apporter cette confiance (au-delà des opérations de communication à caractère publicitaire)? Peut-être en remplaçant les prototypes physiques par des prototypes virtuels. *« Valider virtuellement un produit vise à évaluer sa sécurité »*, propose **Dominique Lefebvre**, Product

Management Director chez ESI Group. Qui ajoute que *« la quantité de données générée dans une simulation est loin d'être pleinement exploitée. »* Et, de cette *« énorme quantité de données générée »*, qui dépasse celles produites par les expérimentations physiques, *« on va s'intéresser aux signaux faibles, ceux qui donnent éventuellement un effet catastrophique au niveau du système »*. L'utilisation des technologies et algorithmes de simulation permet ainsi de *« simuler de bout en bout la conception des produits futurs qui seront connectés »*.

Le Cloud acteur de la cybersécurité

Ce n'est pas **Jean-Christophe Mathieu** chez Siemens France qui le contredira alors que l'industriel investit massivement dans le logiciel. *« L'industrie 4.0 se caractérise par l'arrivée du logiciel dans la chaîne de production »*, souligne le responsable sécurité produit et solution. A condition de *« faire travailler les gens ensemble »*. Autrement dit les équipes IT, sécurité et process doivent collaborer *« afin de garantir que les données entrées dans le logiciel ne vont pas fuiter »*. Le responsable en profite pour remercier l'Anssi (Agence nationale de la sécurité des systèmes d'information) *« qui a fait bouger les choses »* en mettant en œuvre l'attribution de la certification d'Etat aux équipements de production pour les amener à des niveaux de sécurité *« fort raisonnables »*. *« On est le premier équipementier mondial à prouver que l'on prend en compte la cybersécurité dans nos processus et particulièrement dans le développement et la production »*, se félicite-t-il.

Chez Schneider Electric, également en cours de certification Anssi, **Jean-Michel Brun**, expert Group Senior, confirme la palette de mesures précédemment évoquées à suivre pour garantir la sécurité. Un processus de *security development life cycle* qui passe par du test de pénétration, de l'analyse de risque, du *secure coding*, etc., mais aussi fournir des architectures de référence, apporter du service et avoir des équipes de CERT. Quant à l'aspect Cloud, si *« la connectivité en tant que telle est ambivalente car elle amène potentiellement une faille, elle apporte aussi un aspect de sécurité puisqu'on pourra surveiller à distance les équipements »*. Ce qui l'amène à conclure que *« le Cloud va contribuer à renforcer la cybersécurité »*.

Lire également
50 milliards d'euros pour l'industrie 4.0 européenne
La transformation digitale jugée secondaire pour les chefs d'entreprise
Une alliance pour l'industrie du futur avec l'Afdel et Syntec Numérique