Première édition des **SCADAYS** – 8 février 2018 – LYON

Cybersécurité des systèmes industriels et urbains

avec

David KIMELFELD

Président de la Métropole de Lyon

&

Jean-Christophe MATHIEU

Président du cluster IU Cyber

COMPTE – RENDU

La cybersécurité pour le milieu industriel est un sujet que la Métropole de Lyon et son président David KIMELFELD connaissent bien. Chef-lieu de la première région industrielle de France, Lyon, par la présence de nombreuses industries sur son territoire, se devait de prendre le pas sur un sujet aussi vital que la cybersécurité spécifiquement adressée aux systèmes industriels et urbains. Le territoire dispose de l'ensemble de la chaine de valeur sur la filière cybersécurité : fabricants d'équipements, opérateurs, intégrateurs, éditeurs de logiciels et clients finaux avec notamment la présence de Siemens et Schneider, deux acteurs majeurs en Europe qui représentent 80-85% des systèmes de contrôle-commande en France.

La Métropole de Lyon est fortement engagée dans les domaines liés à la transition numérique : objets connectés, robotique et automatisation, déploiement de la réalité augmentée, utilisation du Big Data, outils de modélisation et de prédiction, sécurité des systèmes d'information. En matière de cybersécurité, cette dernière est tout aussi mobilisée, consciente des nombreux enjeux, tant humains que technologiques, qu'ils représentent pour les industries.

La Métropole de Lyon a une vraie carte à jouer en matière de cybersécurité des systèmes industriels et urbains et se mobilise pour accompagner la transition numérique des entreprises et protéger l'ensemble des citoyens. L'attractivité d'un territoire dépend de deux éléments. D'un côté l'écosystème économique, qui est le moteur du dynamisme local ; et de l'autre la qualité de vie. La vitalité de Lyon puise dans ces deux sources sa force. Capitale des Gaules, capitale de la gastronomie, capitale de la première région industrielle de France, Lyon se lance dans la course pour le titre de capitale de la cybersécurité industrielle.

***« La Métropole de Lyon souhaite faire de la cybersécurité un point fort de l'écosystème local et faire ainsi de la filière cybersécurité un axe d'attractivité de la Métropole. La Métropole fait de la cybersécurité un sujet majeur de sa stratégie économique, source de forte activité pour nos entreprises**. » (**David KIMELFELD**, *Président de la Métropole de Lyon*)

L'ANSSI, à travers son sous-directeur Relations extérieures et coordination, a appelé de ses vœux une évolution de la gouvernance de la cybersécurité au niveau des COMEX (comités de direction) des entreprises. En matière de cybersécurité des systèmes industriels, il y a une forte responsabilité des constructeurs de systèmes industriels : en effet, ces derniers seront présents durant plusieurs décennies pour contrôler des infrastructures critiques. Leur sécurité est ainsi cruciale et vitale. Il est ainsi nécessaire d'effectuer un réel changement de culture en matière de cybersécurité. Le risque cyber se compose de trois éléments : les acteurs, les systèmes et les vulnérabilités. Toute action en matière de cybersécurité doit s'intéresser et s'adresser à ces trois plans. La France est à la pointe de la cybersécurité. L'axe de travail est de l'être au niveau européen et au niveau international.

« L'état de la menace aujourd'hui, la grande préoccupation liée aux cybermenaces, c'est celle de la destruction. Nous sommes passés d'actes d'espionnage à une volonté de destruction avec les années 2010. » (**Yves VERHOEVEN**, *sous-directeur Relations extérieures et coordination de l'ANSSI*)

Nous sommes totalement dépendants des systèmes industriels. La cybersécurité ne peut pas être instaurée sans confiance, et cette confiance doit dépasser les frontières nationales. Dans une dynamique collective européenne pour relever les défis de la cybersécurité des systèmes industriels et urbains, IU Cyber, le cluster Européen dédié à la cyber sécurité des systèmes industriels et urbains, a été créé avec pour vocation de réunir l'ensemble de la chaine de valeur cybersécurité.

« La phase de structuration du cluster touche à sa fin, les adhésions seront bientôt ouvertes pour rejoindre les membres fondateurs » a annoncé **Jean-Christophe MATHIEU**, *Président du cluster IU Cyber*.

PREMIERE TABLE RONDE - PAS DE SMART CITY SANS CYBERSECURITE

Le rôle de l'Etat est très bien construit au niveau national. Mais dans sa décentralisation, la réalité est plus compliquée. Il est nécessaire de travailler sur cet axe. Pour ce faire, les collectivités territoriales doivent adopter un nouveau management, en intégrant la cybersécurité à tous les niveaux de leurs projets. Il faut continuer de sensibiliser : la cybersécurité est l'affaire de tous. Tout projet numérique doit nécessairement intégrer de la cybersécurité.

> ***« Le premier objectif d'une Smart-city c'est le bien-être. Mais son objectif doit aussi être l'équilibre du territoire. La Smart City, ce n'est pas juste pour les grandes collectivités : travailler à l'équilibre territorial, c'est se mettre au rythme du plus faible maillon de la chaîne et l'aider à avancer. Il faut que la plus petite commune française fournisse les mêmes services et les mêmes garanties qu'une grande collectivité. »*** (**Philippe VITEL**, *vice-président du Conseil Régional de la région Provence-Alpes-Côte d'Azur)*

L'Etat a un rôle à jouer pour la cybersécurité auprès de tous les acteurs en matière de cybersécurité, un rôle de conseiller et de guide (notamment pour les startups) pour éviter la fuite des données sur Internet. Il y a une prise de conscience de la part des petits acteurs grâce au RGPD de leur dénuement quant à leur niveau de sécurité numérique.

> ***« Des données non protégées, c'est de l'intelligence qui ne se transforme pas en richesse en France ou en Europe, mais qui se transforme en richesse pour d'autres nations. »*** (**Thierry VINCON**, *Chargé de mission à la Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC) du ministère de l'intérieur)*

La Métropole doit être en mesure de répondre aux besoins et aux attentes des collectivités territoriales et des acteurs privés qui se tournent vers elle en matière de cybersécurité.

> ***« La Smart City, c'est exactement comme le Far West. Les premiers arrivés cherchent le meilleur écosystème où vivre dans les meilleures conditions. Après s'être installés au meilleur endroit, d'autres les rejoignent, puis d'autres, et naissent ainsi des besoins collectifs (routes, magasins, écoles) : le système social prend forme. Comme pour tout système social, arrive aussi le besoin de sécurité : c'est là qu'arrive le Shérif, pour faire respecter un cadre permettant à tous d'évoluer au mieux dans cet écosystème complexe. »*** (**Grégory BITTON**, *Directeur-adjoint Architecture et Gouvernance à la Métropole de Lyon*)

Le cadre réglementaire a évolué, et avec lui la sensibilisation et la prise de conscience des acteurs. La sensibilisation doit être multicanale. Pourquoi passe-t-on des clips de sécurité routière à la télévision et n'y voit-on pas de clips de sensibilisation à la sécurité numérique ? En matière de cybersécurité, il existe trois règles essentielles à respecter : cartographier ses données et ses éléments ayant de la valeur ; savoir où ces éléments de valeur sont stockés ; savoir qui appeler en cas de besoin. Si ces trois règles étaient respectées par tout le monde, il ne s'agirait que d'un petit pas pour chacun, mais il s'agirait d'un pas de géant pour la cybersécurité. Il est nécessaire de sensibiliser tous les acteurs, de tous les secteurs, à tous les niveaux.

DEUXIEME TABLE RONDE - LA CYBERSECURITE, UN DEFI POUR L'INDUSTRIE DU FUTUR

Nous avons certes une sécurité améliorée par rapport à l'état de la sécurité d'il y a 10 ans, mais la sécurité reste encore à améliorer. Il est nécessaire d'impulser une évolution des comportements et des pratiques à tous les niveaux. En ce qui concerne les systèmes industriels et urbains plus spécifiquement, il faut accompagner les concepteurs avec une feuille de route des exigences pour avoir un produit final qui fonctionne et qui respecte les recommandations de sécurité de base. Il faut éduquer et sensibiliser aux règles de sécurité. La cybersécurité n'est pas un coût mais un investissement à moyen et long terme. C'est un surcoût uniquement si elle n'est pas intégrée nativement. Il faut éduquer à la prise de conscience que cet investissement est un investissement qui sera vite rentabilisé. Dans les systèmes industriels, la cybersécurité doit être comme la qualité : intégrée mais invisible.

> ***« L'industrie ne peut plus avancer sans cybersécurité, et sans cybersécurité pas d'industrie du futur. 80% des cyberattaques réussies sont toujours liées à une erreur humaine. »*** (**Stéphane GERVAIS**, *représentant de la Fédération des industries électriques, électroniques et de communication (FIEEC)*)

Le véritable problème de la cybersécurité est le manque à gagner en cas de cyberattaque, non pas le coût de l'investissement : le premier sera toujours plus élevé que le deuxième. La cybersécurité doit être vue comme un avantage compétitif.

> ***« L'objectif est d'avoir de la cybersécurité à la Disneyland : de la cybersécurité présente partout, à tous les niveaux, mais invisible. »*** (**Philippe LOUDENOT**, *FSSI des Ministères sociaux et membre du Club des Experts en Sécurité de l'Information (CESIN)*)

LA question résumant toute l'action à mener en matière de cybersécurité est la suivante : quel risque est-on prêt à prendre ? Le risque 0 n'existe pas, mais il faut accepter et connaître ses vulnérabilités et ses risques propres et prendre les mesures nécessaires en fonction. La deuxième question est : comment protéger ce qui a de la valeur ? Cette question est vraie pour un citoyen, pour une entreprise, mais aussi pour la souveraineté nationale. La cybersécurité se résume à ces deux questions et aux réponses qui y seront apportées.

> ***« Les entreprises doivent véritablement mesurer l'impact d'une cyberattaque sur la continuité de leur activité par une analyse pertinente des risques informatiques qui leur est vitale. »*** (**Chantal CAUDRON DE CAUQUEREAUMONT**, *ICA, Adjoint de pôle SSI à la Direction générale de l'Armement (DGA) du ministère des Armées*)

Doit-on travailler à relancer la filière numérique nationale pour se détacher des sous-traitants étrangers ? Si préférence nationale il doit y avoir en matière de cybersécurité, il faut d'abord travailler à s'assurer que nos industriels et la filière numérique plus largement ne meurent pas ou ne partent pas. Cela nécessite et nécessitera des investissements importants.