Pour la plupart des entreprises interrogées, la cybersécurité OT/ICS est une priorité majeure

Munich, Paris, Londres, 25 juin 2018 – Une nouvelle étude réalisée par PAC, une société du groupe CXP, pour le compte de Kaspersky Lab, révèle que 77% des entreprises mondiales des secteurs de la fabrication, du transport, des services publics et de l'énergie accordent une priorité majeure à la cybersécurité OT/ICS. Sans surprise, 77% des entreprises estiment une attaque de cybersécurité dans le domaine du ICS comme probable ou très probable. Les entreprises déclarent qu'elles s'attendent à des risques supplémentaires liés au déploiement de l'Internet Industriel des Objets (IIoT) ; néanmoins la grande majorité d'entre elles utilisent encore cette technologie. Cela se traduit également dans les priorités d'investissement : 91% des entreprises estiment que les dépenses pour les logiciels de cybersécurité OT/ICS seront identiques ou en augmentation à l'avenir.

La cybersécurité du ICS est une priorité pour la quasi-totalité des entreprises interrogées à travers le monde, même s'il existe des différences entre les géographies.

Les entreprises interrogées indiquent une probabilité croissante d'être la cible de cyberattaques dans le domaine de l'OT/ICS : 32% des entreprises interrogées supposent qu'elles sont très susceptibles de devenir une cible, soit 7% de plus que selon les résultats du sondage de l'année dernière.

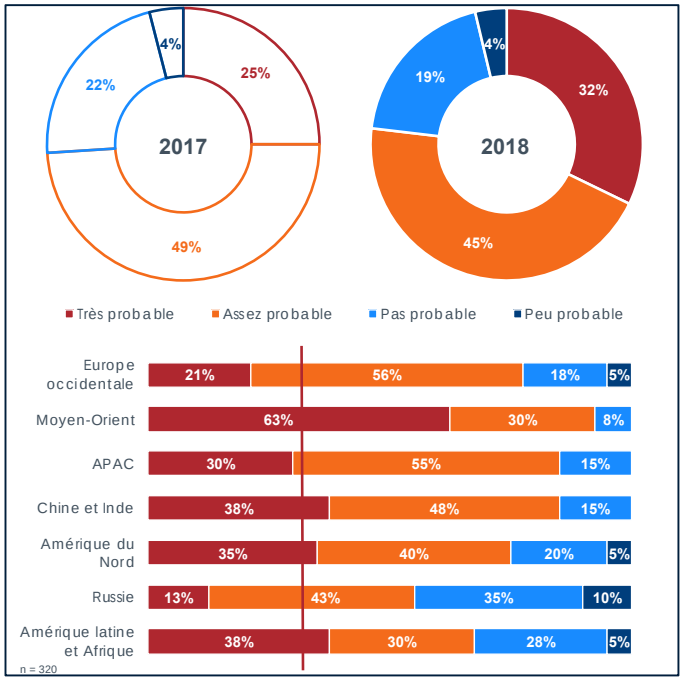

Fig. 1 : Auto-évaluation des risques en matière de sécurité OT/ICS

Difficiles à mesurer, les préjudices financiers restent un sujet délicat. Au total, 20 % des entreprises interrogées ont connu une augmentation des coûts financiers et des autres préjudices liés aux incidents. Par rapport aux années précédentes, 48 % ont constaté les mêmes coûts financiers et autres préjudices, tandis que 27 % ont noté une diminution des coûts. Compte tenu de la croissance constante des cyber-attaques, même dans le domaine OT/ICS, au moins dans certaines entreprises, les projets en matière de cybersécurité donnent des résultats positifs.

Un examen par région permet de constater que la répartition des entreprises déclarant une augmentation des coûts financiers et des autres préjudices est assez diversifiée. Alors qu'en Chine et en Inde, 31 % des entreprises interrogées font état de coûts et de préjudices plus élevés, cette proportion n'est que de 13 % en Amérique latine. Il en ressort que le fait d'accorder une priorité majeure à la cybersécurité dans l'espace OT/ICS permet de prévenir les incidents et de limiter les coûts et les préjudices associés.

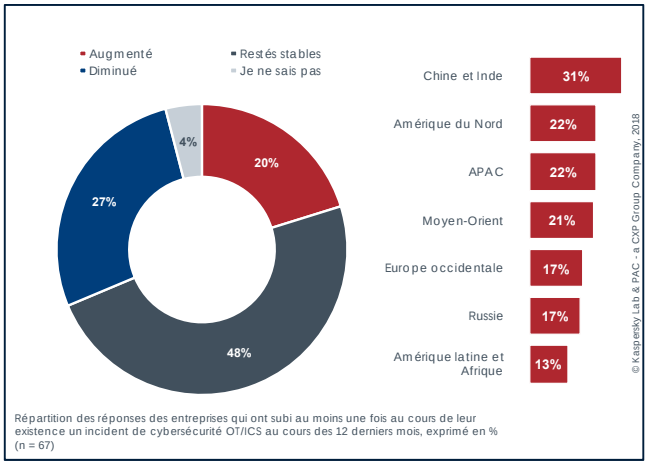

Fig. 2 : Est-ce que les coûts financiers globaux/les préjudices des incidents que vous avez subis ont augmenté, sont restés les mêmes ou ont diminué par rapport aux années précédentes ?

Les entreprises gérant des infrastructures critiques et plusieurs entreprises de fabrication ont déjà pris conscience de l'importance de la cybersécurité pour l'IIoT. Elles sont en première ligne, et même si la maturité de la cybersécurité OT/ICS reste faible, de nombreuses entreprises ont compris les risques et sont en train de réaliser des investissements. C'est d'autant plus vrai que la majorité des entreprises interrogées s'attendent à une probabilité croissante de risques de cybersécurité du fait de leur transformation numérique. Les principaux enjeux des organisations interrogées comprennent les difficultés à faire face à un facteur de sécurité clé dans le ICS/OT, et/ou la collaboration entre le personnel des IT et des OT.

Wolfgang Schwab, consultant principal à PAC et auteur de l'étude, a déclaré : "Les avantages de l'Internet Industriel des Objets l'emportent sur les risques potentiels. Par conséquent, les entreprises investissent dans cet espace et feront de la cybersécurité OT/ICS leur priorité du moment."

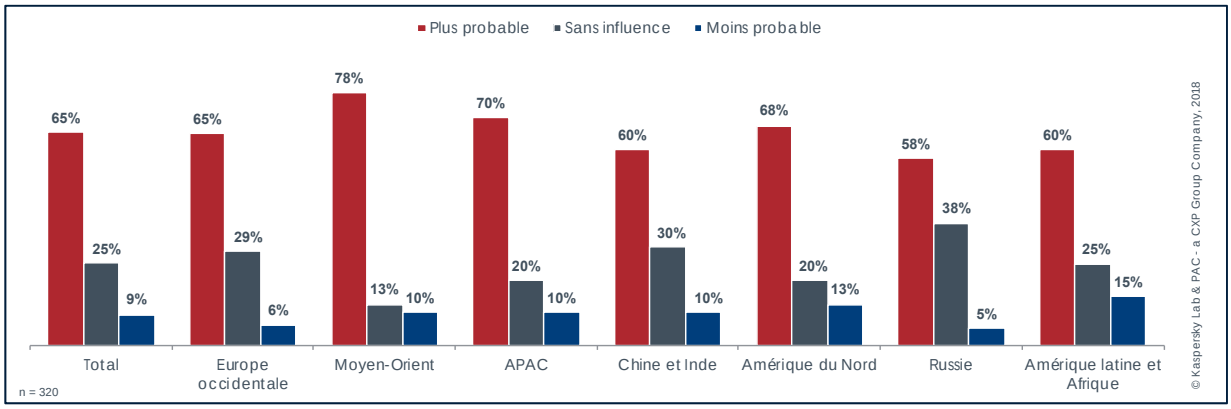

Fig. 3 : Influence de IoT sur les risques de cybersécurité en OT/ICS

Selon Mathieu Poujol, chef de la cybersécurité à PAC et coauteur de l'étude : « Quand on compare la sécurité informatique avec la cybersécurité OT/ICS, il est important de noter que dans le premier cas, les dommages sont principalement limités à l'espace informatique, donc plutôt virtuels, alors que dans le second cas, les dégâts peuvent aussi être physiques. Cela a un impact totalement différent sur la réduction des risques et sur les responsabilités auxquelles ces entreprises pourraient être confrontées »

À propos de l'étude

L'étude PAC, " L'état de la cybersécurité industrielle 2018 ", réalisée par PAC pour le compte de Kaspersky Lab, analyse le statu quo et les évolutions futures à l'échelle mondiale en matière de cybersécurité industrielle. Elle est le résultat d'une enquête CATI auprès de 320 décideurs ayant une influence sur la sécurité de l'OT/ICS ainsi que de 12 autres interviews d'experts.

L'étude peut maintenant être téléchargée à l'adresse suivante :

https://ics.kaspersky.com/the-state-of-industrial-cybersecurity-2018/

À propos de PAC

Fondé en 1976, Pierre Audoin Consultants (PAC) fait partie du CXP Group, le premier cabinet européen indépendant d'analyse et de conseil dans le domaine des logiciels, des services informatiques et de la transformation numérique.

Il offre à ses clients un service complet d'assistance pour l'évaluation, la sélection et l'optimisation de solutions logicielles, l'évaluation et la sélection des prestataires de services informatiques et les accompagne dans l'optimisation de leur stratégie de sourcing et dans leurs projets d'investissements. Ainsi, le CXP Group accompagne DSI et directions fonctionnelles dans leur transformation numérique.

Enfin, le CXP Group aide les éditeurs et les prestataires de services informatiques à optimiser leurs stratégies et leurs approches de commercialisation à travers des analyses quantitatives et qualitatives ainsi que des prestations de conseil opérationnel et stratégique. Les organisations et les institutions publiques se réfèrent également à nos études pour développer leurs politiques informatiques.

Capitalisant sur 40 ans d'expérience, implanté dans 8 pays (avec 17 bureaux dans le monde) et fort de 155 collaborateurs, le CXP Group apporte chaque année son expertise à plus de 1 500 DSI et directions fonctionnelles de grands comptes et entreprises du mid-market et à leurs fournisseurs. Le CXP Group est composé de 3 filiales : Le CXP, BARC (Business Application Research Center) et Pierre Audoin Consultants (PAC).

Pour en savoir plus, visitez le site www.pac-online.com ou suivez-nous sur Twitter, sur LinkedIn ou sur notre blog

Contact

Mathieu Poujol
Consultant principal
Tél : +49 171 222 3772
E-mail : m.poujol@pac-online.com