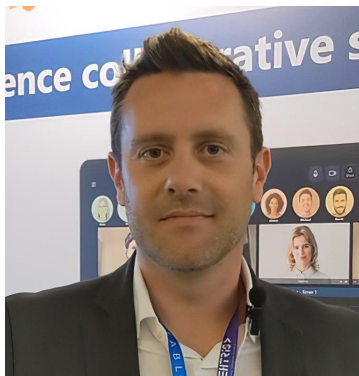


**Espionnage voiture électrique.**  
**Volkswagen soupçonne des hackers chinois d'avoir volé  
des documents confidentiels**

Le [20 avril 2024](#), le magazine d'investigation *Der Spiegel* et la chaîne de télévision allemande ZDF ont révélé conjointement que Volkswagen a été victime d'une campagne d'espionnage et de cyberpiratage par des hackers chinois. Les révélations, qui précèdent la visite du chancelier Olaf Scholz en Chine du 15 au 16 avril, soulignent sans accuser directement la Chine que le constructeur automobile allemand s'est fait voler plus de 19 000 documents sensibles sur la mobilité électrique en 5 ans.

Cette campagne d'espionnage s'insère dans un contexte plus global dans le secteur de la mobilité électrique où la Chine tente d'inonder le marché européen avec ses véhicules électriques.

**Jean-Philippe Commeignes - Directeur chez Tixeo, formé à l'IRIS**



« La Chine a démarré ces efforts significatifs sur l'électrification (hors batterie) en 2009, en étant le premier marché des allemands. Cet espionnage de 2010 à 2015 s'inscrit dans sa stratégie pour combler ses lacunes industrielles alors même qu'on nous informe maintenant que [la Chine inonde le marché européen](#). Le fait que cette nouvelle revienne maintenant n'est pas anodin vu ce contexte de perte de vitesse d'un des piliers de l'économie allemande (l'export de voitures) et la visite de Scholz en Chine pour le défendre.

Sur le plan organisationnel, les entreprises doivent adopter une approche proactive en matière de cybersécurité. Cela implique la mise en place de politiques de sécurité robustes, incluant la sensibilisation des employés aux risques de sécurité, la formation régulière sur les bonnes pratiques en matière de sécurité informatique et la création d'une culture d'entreprise axée sur la sécurité. Les équipes de sécurité doivent être habilitées à identifier et à contrer les menaces potentielles dès leur apparition, en mettant en œuvre des protocoles de surveillance et de réponse efficaces.

D'autre part, sur le plan technique, les organisations n'ont d'autres choix que d'investir dans des solutions de sécurité avancées, telles que la surveillance continue du réseau, la détection des intrusions et la protection avancée des terminaux. Par ailleurs, l'adoption de technologies de sécurisation des communications, comme un véritable chiffrement de bout en bout, est indispensable pour garantir la confidentialité des échanges.

Enfin, dans ce contexte de concurrence internationale exacerbée, la directive NIS2 prend tout son sens : elle impose des obligations aux entreprises en matière de protection des infrastructures numériques.

*En se conformant à NIS2, les organisations peuvent renforcer leur résilience face aux cybermenaces, ce qui est particulièrement crucial dans des industries aussi stratégiques que l'automobile. En soutenant et en appliquant pleinement NIS2, l'Union européenne garantit la sécurité de ses entreprises face aux menaces croissantes d'espionnage industriel et de cyberpiratage, tout en renforçant la souveraineté numérique de l'Europe. »*

### **A propos de Jean-Philippe Commeignes**

Jean-Philippe Commeignes est Directeur Commercial chez Tixeo, éditeur français de visioconférence sécurisée. Avec une expérience de 20 ans dans la tech, incluant les télécoms et la cybersécurité dans les secteurs critiques, il possède une double expertise technique et commerciale lui permettant d'appréhender l'industrie sous plusieurs angles. Passionné par la cybersécurité et la géopolitique, il a suivi une formation à l'IRIS en défense, sécurité et gestion de crise pour structurer et approfondir ses connaissances. Il partage la vision d'une Europe plus active dans l'articulation entre ses dépendances et ses intérêts.

### **A propos de Tixeo :**

Créée à Montpellier en 2004, Tixeo est leader européen de la vidéo-collaboration sécurisée. Unique acteur français proposant une technologie de visioconférence certifiée (CSPN)/qualifiée par l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et reconnue par la CNIL, Tixeo a conçu ses solutions sur un ensemble de mécanismes innovants permettant d'assurer un niveau de sécurité encore jamais atteint pour des réunions en ligne. La conception et le développement de ses logiciels sont exclusivement réalisés en France (100% Made in France) et la technologie n'est pas soumise aux législations étrangères. La technologie française Tixeo est labellisée « France Cybersecurity » et « Cybersecurity Made in Europe ». Tixeo est membre de l'Alliance pour la Confiance Numérique (ACN), du CLUSIF, d'HEXATRUST et de la European Champions Alliance

En savoir plus : [www.tixeo.com](http://www.tixeo.com)