Veille Technologique : Cybersécurité – Menaces internes et secteur du transport

Menaces internes boostées par l'IA et cybersécurité dans le transport

Les menaces internes, amplifiées par l'intelligence artificielle, deviennent une préoccupation majeure pour les entreprises à travers le monde. Le phishing personnalisé généré par l'IA et l'usage non autorisé d'outils d'IA générative représentent des risques importants pour les données sensibles et la continuité des activités. Ces nouvelles méthodes permettent aux cybercriminels de créer des attaques plus ciblées et plus difficiles à détecter par les employés.

Parallèlement, le secteur du transport routier de marchandises est particulièrement exposé aux cyberattaques, telles que les rançongiciels, l'usurpation de RIB ou les attaques par déni de service. Les systèmes vulnérables incluent les serveurs, messageries, outils de traçabilité et capteurs connectés. Des incidents récents, comme l'attaque subie par le groupe Sinari en mars 2025, ont montré que l'absence de mises à jour régulières et de mesures de sécurité adaptées peut entraîner des pertes financières et opérationnelles importantes.

Cette double problématique met en évidence la nécessité pour les organisations de renforcer la cybersécurité interne, de contrôler l'usage des outils d'IA et de mettre en place des pratiques robustes de protection des systèmes, adaptées aux spécificités de chaque secteur. La formation des employés, la supervision humaine et la vigilance face aux nouvelles techniques d'attaque sont des éléments clés pour limiter les risques.

Sources :

- ITRnews – Cybersécurité : les menaces internes boostées à l'IA deviennent la première préoccupation mondiale
- Journal du Poids Lourd – Cybersécurité : les transporteurs passent en mode sécurisé