Sécurité IoT : les 5 recommandations du rapport Deloitte

La multiplication des dispositifs connectés et des flux de données massives étend la surface d'attaque. Sans attendre la diffusion de l'informatique quantique, les organisations ont tout intérêt à placer la sécurité de leurs dispostifs et réseaux IoT au premier plan.

C'est le point de vue défendu par le cabinet Deloitte, rapport* à l'appui. Voici 5 des recommandations délivrées par la firme d'audit et de conseil :

Endpoints, AIOps, logistique, partenaires, SOC

1. **Identifier tous les enpoints** >

Avoir une vue d'ensemble et à jour des points de terminaison (endpoints) est essentiel, selon Sean Peasley, associé chez Deloitte & Touche LLP. « L'IoT couvre autant les environnements opérationnels que les vêtements, les voitures et les produits connectés. Les entreprises devraient planifier proactivement la manière d'identifier, suivre, corriger et répondre aux impacts éventuels sur leurs écosystèmes. »

L'objectif est de renforcer la cybersécurité.

2. **Aligner solutions, opérations et sécurité IT** >

Ne pas se noyer dans l'informatique héritée (Legacy IT) tout en adopant des technologies de pointe. « Les organisations devraient adopter une approche proactive, sécurisée dès la conception, tout en travaillant à la surveillance et à la correction des équipements, logiciels et infrastructures hérités », a ajouté le consultant.

3. **Connaître les acteurs de l'écosystème** >

Les matériels, les logiciels et les services tiers interconnectés peuvent être à l'origine d'une atteinte à la sécurité. « Idéalement, les contrats avec les tierces parties devraient tous adresser les enjeux et les mises à jour de sécurité. »

La chaîne logistique dans son ensemble est concernée.

4. **Intégrer IA et Machine Learning** >

« L'intelligence artificielle dédiée aux opérations informatiques (AIOps) est passée d'une catégorie émergente à une nécessité », a souligné Sean Peasley. Les organisations devraient l'associer à « une approche de la sécurité dès la conception de projets (DevSecOps). »

Selon un autre cabinet d'analystes (Capgemini Research Institute), près de 7 responsables informatiques sur 10 pensent que, sans IA, leur organisation ne sera pas en mesure de répondre aux cyberattaques à venir.

5. **Evaluer les vulnérabilité des appareils** >

Des tests de base à la surveillance fournie par des centres d'opérations de sécurité (SOC), Deloitte, qui prêche pour son Cyber IoT Studio, préconise une sécurité 24/7.

**(Deloitte – The future of cyber survey 2019)*

(photo : Green Energy Futures via Visualhunt / CC BY-NC-SA)