Stations de recharge électrique : la nouvelle cible des cyberattaques

Indispensables à la transition énergétique, les bornes de recharge se sont déployées à grande vitesse, parfois au détriment de leur cybersécurité. Aujourd'hui, la multiplication des attaques révèle un angle mort de la mobilité électrique. Sécuriser ces infrastructures est devenu un enjeu central pour garantir la fiabilité des services et l'adhésion des usagers.

Longtemps perçues comme de simples équipements techniques, les bornes de recharge pour véhicules électriques sont désormais au cœur d'un nouveau front numérique. À mesure que la mobilité électrique s'impose et que les réseaux de recharge se densifient, ces infrastructures essentielles à la transition énergétique attirent de plus en plus l'attention des cybercriminels. Aux États-Unis, le phénomène s'est nettement accentué en 2024, avec une hausse estimée à 39 % des incidents liés à des cyberattaques par rapport à l'année précédente. En Europe, la tendance est similaire, avec des attaques qui se multiplient, gagnant à la fois en fréquence et en sophistication, signe de l'intérêt croissant des hackers.

Ces systèmes interconnectés se situent au croisement entre la mobilité, l'énergie et les services numériques. Et si ces bornes se sont déployées à grande vitesse, leur niveau de sécurité demeure inégal. Véritables objets connectés, elles échangent en permanence avec les véhicules, les applications mobiles des opérateurs et les systèmes de paiement. Cette interconnexion élargit considérablement leur surface d'attaque et expose les utilisateurs comme les exploitants à de multiples risques, allant du vol de données personnelles à l'intrusion de logiciels malveillants susceptibles de

perturber le service.

Parmi les techniques les plus courantes figure le phishing via l’utilisation de faux QR codes apposés directement sur les bornes. Les conducteurs qui les scannent sont redirigés vers des sites frauduleux imitant les interfaces officielles de recharge, facilitant la collecte de données bancaires ou d’identifiants personnels. Des cas de fuites massives de données ont également été observés : noms d’utilisateurs, localisation précise des bornes ou numéros de série de véhicules se sont retrouvés sur le dark web après l’exploitation de vulnérabilités techniques.

Continuer la lecture de Stations de recharge électrique : la nouvelle cible des cyberattaques →

Cet article Stations de recharge électrique : la nouvelle cible des cyberattaques est apparu en premier sur Techniques de l’Ingénieur.