Des chercheurs ont testé la sécurité des compteurs communicants : ce qu'ils ont réussi à atteindre à distance dépasse largement votre logement

par **Brice L.** 24 juillet 2026, 15 h 51 min

On imagine souvent que le petit boîtier fixé sur le mur du garage ou dans un placard de l'entrée se contente d'une tâche modeste : compter les kilowattheures et transmettre la facture. Pourtant, une équipe de chercheurs vient de démontrer que cet appareil discret cache une réalité bien plus inquiétante. Ce qu'ils ont réussi à atteindre à distance, en partant d'un simple compteur domestique, dépasse très largement les murs d'un logement.

Le boîtier sur votre mur n'était qu'une porte d'entrée

Le compteur communicant, que beaucoup de foyers français connaissent bien désormais, ressemble à un objet du quotidien totalement anodin. Il enregistre la consommation, dialogue avec le fournisseur et permet des interventions à distance sans qu'un technicien ait besoin de se déplacer. C'est précisément cette connectivité qui fait sa force… et sa fragilité.

Une équipe rassemblant des spécialistes de l'université d'Aalborg, au Danemark, et de l'université du Pendjab, au Pakistan, a conclu que ces compteurs représentent déjà une **vulnérabilité de cybersécurité qualifiée de « massive »**. Le problème ne vient pas de l'électronique visible, mais de ce qui se cache derrière : le firmware, les interfaces réseau et les fameuses API qui font communiquer les appareils entre eux. Autant de composants logiciels dans lesquels une faille peut se glisser. Et une fois cette faille exploitée, le boîtier cesse d'être un simple compteur pour devenir une véritable *porte d'entrée*.

Du salon au poste source : le chemin que personne n'avait cartographié

C'est ici que la démonstration prend une tournure spectaculaire. Les chercheurs n'ont pas seulement montré qu'un compteur pouvait être piraté pour trafiquer des données de consommation ou voler de l'énergie. Ils ont mis en lumière un chemin bien plus profond : partir d'un appareil domestique pour **remonter jusqu'au réseau de distribution électrique lui-même**.

Imaginez une maison dont on aurait toujours cru la porte d'entrée reliée à un simple couloir. On découvre soudain que ce couloir débouche sur les fondations de tout l'immeuble. Le compteur, censé rester cantonné à votre logement, s'avère connecté à ce qu'on appelle l'*infrastructure de comptage avancé*, un ensemble qui relie des millions d'appareils aux fournisseurs. Cette architecture repose sur des mesures en temps réel et sur des commandes de contrôle envoyées à distance. Et ce sont justement ces commandes qui, détournées, pourraient permettre de **déconnecter des millions de compteurs d'un seul coup**.

La téléconduite, ce système invisible qui pilote vos coupures

Au cœur de cette vulnérabilité se trouve un maillon méconnu du grand public : le système de **téléconduite**. C'est lui qui permet aux gestionnaires de réseau de piloter à distance les installations, d'ouvrir ou de fermer des circuits, de rétablir le courant après un incident ou, à l'inverse, de couper une zone. Un chef d'orchestre invisible, en somme, qui dirige la partition électrique sans qu'aucun humain ne soit physiquement présent sur place.

Le scénario redouté est le suivant : une faille exploitée à distance sur un compteur communicant sert de tremplin pour accéder au réseau de distribution via ce système de téléconduite. En clair, l'attaquant n'aurait pas besoin d'un accès physique à un poste électrique. Depuis un ordinateur, il pourrait potentiellement manipuler des commandes destinées à piloter le réseau. Ce sont ces mêmes appareils à bas coût, déployés par centaines de millions, qui peuvent alors être compromis en masse, puis

transformés en armes contre l'infrastructure qu'ils étaient censés servir.

Ce que cette faille révèle sur la fragilité de nos réseaux

Le constat a de quoi donner le vertige quand on prend la mesure du déploiement. À la fin de 2023, l'Europe comptait déjà **plus de 186 millions de compteurs électriques intelligents**. Chacun d'eux constitue, en théorie, un point d'entrée potentiel. Et dans le même temps, les cyberattaques visant les infrastructures critiques ne cessent de progresser à l'échelle mondiale, avec une accélération marquée dans le secteur de l'énergie depuis 2018.

Face à ce danger, les chercheurs ne se contentent pas de tirer la sonnette d'alarme. Ils proposent une piste de défense reposant sur une *méthode de détection d'anomalies*, capable de repérer les comportements suspects grâce à l'estimation d'état et à des seuils statistiques. L'idée : identifier au plus vite quand des données de mesure ou des commandes ont été faussées, avant qu'elles ne perturbent le fonctionnement du réseau. Car une attaque bien menée peut brouiller la vision qu'ont les opérateurs de leur propre infrastructure, un peu comme si l'on trafiquait les instruments de bord d'un pilote en plein vol.

Le message est finalement limpide : le compteur accroché à votre mur n'est plus un objet isolé, mais un fil parmi des millions d'autres tissant la toile de notre réseau électrique. Sa sécurité ne concerne donc pas seulement votre facture, mais la stabilité d'un système dont dépend la vie quotidienne de tout un pays. Reste une question ouverte : nos infrastructures sauront-elles se blinder assez vite pour tenir tête à des attaquants qui, eux, ne cessent d'affûter leurs outils ?