Scada : des hackers manipulent le retraitement des eaux

C'est une bien inquiétante histoire que raconte Verizon dans son dernier rapport sur les fuites de données. L'opérateur y explique être intervenu auprès d'une entreprise de traitement des eaux – non identifiée – pour évaluer la sécurité de son réseau. Un audit de sécurité comme il s'en pratique régulièrement dans les entreprises. Ce dernier ciblait tant les systèmes IT traditionnels que les systèmes industriels, supportant la distribution, le contrôle et les mesures sur le réseau régional d'approvisionnement en eau de **2,5 millions d'habitants**.

Verizon met alors en lumière plusieurs vulnérabilités critiques sur le périmètre exposé sur Internet et montre que les systèmes industriels reposent sur des infrastructures dépassées. En particulier, un IBM AS/400 présenté par l'entreprise comme sa plateforme Scada gérant les applications en charge de contrôler les vannes et les flux du réseau de distribution, via des centaines de contrôleurs programmables. Plus baroque, ledit AS/400 héberge aussi les informations de facturation, les données client et les systèmes financiers de l'entreprise. Un mélange des genres des plus détonants. « *Mettre en œuvre des serveurs frontaux Internet, spécialement des serveurs Web, connectés directement à des systèmes de management Scada est tout sauf une bonne pratique* », résume Verizon dans son rapport (lire à partir de la page 39).

Les hackers jouent avec les produits chimiques

Après des entretiens avec les équipes de la DSI, Verizon découvre que celle-ci s'interroge sur des activités suspectes et que l'organisation a enregistré des **actions inexpliquées sur les vannes et conduites d'eau** au cours des 60 derniers jours. Ces opérations consistaient à manipuler les contrôleurs gérant les apports de produits chimiques dans l'eau (afin de la rendre potable) ainsi qu'à modifier les débits, provoquant des interruptions dans la distribution.

L'analyse de Verizon a permis de mettre en évidence des accès à l'application de paiement online émanant d'adresses IP associées à d'autres attaques. « *Il existe une forte probabilité que des accès non autorisés à l'application de paiement exposent aussi des informations sensibles hébergées par le système AS/400* », écrit Verizon. L'enquête du prestataire a montré que **l'exploitation d'une faille connue de l'application de paiement** a abouti à la compromission des données client. Plus grave, avec les mêmes identifiants de connexion que celles employées sur le serveur Web de paiement, les hackers sont parvenus à s'interfacer à quatre reprises avec l'application de contrôle des valves et des flux. « *Au cours de ces connexions, les assaillants ont modifié les paramètres de l'application avec apparemment une faible connaissance de la façon dont ces systèmes de contrôle fonctionnent* », écrit Verizon. Façon de dire que les conséquences auraient pu être plus graves avec des cybercriminels au fait du fonctionnement de ces systèmes.

Scada : le précédent ukrainien

L'attaque, dont les motivations restent obscures selon Verizon, a toutefois été rapidement détectée par les systèmes d'alerte de l'entreprise. Celle-ci a pu corriger les apports de produits chimiques et les débits des valves, limitant l'impact pour le consommateur final.

Même si elle repose largement sur ce qu'on peut qualifier d'erreur d'architecture (un seul système gérant des applications Web et la partie Scada), cette attaque démontre, une fois encore, la réalité du risque sur les systèmes industriels. Les cyberattaques aboutissant à modifier l'environnement ne relèvent plus de la science-fiction, ni même d'une opération savamment orchestrée par des services secrets bien . En décembre dernier, quelque **80 000 foyers ukrainiens ont été privés d'électricité** pendant plusieurs heures, suite à une cyberattaque.

A lire aussi :

Panne de courant via une cyberattaque : les spécialistes ne sont pas surpris

Scada : une cyberattaque peut-elle faire dérailler un train ?

Sécurité des Scada : pourquoi la côte d'alerte est atteinte

Crédit photo : mr.water / Shutterstock