L’eau d’une station d’épuration manipulée par des hackers – Sciencesetavenir.fr

	L’eau d’une station d’épuration manipulée par des hackers

L'opérateur de télécommunications américain Verizon révèle dans un rapport une cyberattaque ayant touché à la composition et à la distribution d'eau potable d'une station. Le système informatique était perclus de failles.

Le bilan dressé par l'opérateur américain Verizon publié en mars 2016 et consacré aux fuites de données a de quoi faire frémir. Il recense pas moins de cinq cents incidents de cybersécurité dans quarante pays en 2015 (le rapport en anglais ici**).** Parmi eux, l'un attire tout particulièrement l'attention : il concerne la Kemuri Water Company (KWC), une station d'épuration bien réelle mais dont le nom a été changé et le pays d'implantation non divulgué pour éviter de la compromettre. Et pour cause ! Verizon relate la façon dont des hackers ont réussi, très facilement, à manipuler la composition chimique de l'eau qui est redistribuée aux habitants après traitement ! Le tout, sans même en avoir eu l'intention au départ…
L'affaire a été révélée lorsque la société a décidé de faire appel aux équipes chargées du cyber-risque de Verizon pour renforcer son système d'information afin d'anticiper tout problème éventuel. Or, une fois sur place, les experts ont constaté avec stupeur que la station d'épuration était déjà la proie de pirates informatique depuis deux mois ! Et que ses responsables s'en doutaient… Des mouvements suspects de valves et de tuyauteries avaient été remarqués. Beaucoup plus grave ! Les gestionnaires avaient constaté des modifications inexpliquées de dosage dans les produits injectés dans l'eau pour la rendre portable. Sans conséquence désastreuse heureusement…

« Pour tout dire, KWC était un candidat tout trouvé pour une fuite de données. Son interface Internet présentait plusieurs failles à haut risque dont on sait qu'elles sont souvent exploitées» mentionne le rapport de Verizon. Et son système opérationnel, qui commande les applications industrielles (traitement des eaux, gestion du débit), reposait quant à lui sur une infrastructure informatique vieille de plusieurs dizaines d'années.
En outre, de nombreuses fonctions de ce système cohabitaient avec des applications « business » de l'entreprise sur un même et unique serveur, un AS/400 d'IBM, ordinateur commercialisé en… juin 1988. En clair, si des hackers pénétraient le système, ils pouvaient sans peine passer du contrôle du traitement des eaux aux informations financières et aux données de facturation de la compagnie. Et c'est exactement ce qui s'est passé.

L'opérateur liste une série de failles assez confondantes

Au cours de son enquête, Verizon s'est rendu compte que des adresses IP de hackers déjà rencontrées dans trois autres affaires s'étaient connectées au système de paiement en ligne de la KWC, cette interface permettant aux clients d'accéder à leur compte à distance (depuis un ordinateur, un mobile) ; c'est a priori par cette voie que les hackers sont passés, comme d'autres l'ont fait lors du piratage en octobre 2015 de l'hydrolienne Sabella.

2,5 MILLIONS. L'opérateur liste ensuite une série de failles confondantes : l'accès aux données clients n'était protégé que par un login/mot de passe, sans double authentification ; une « *connexion directe par câble* » existait entre l'application de paiement en ligne et l'AS/400, ce dernier ayant un accès ouvert à Internet, avec une adresse IP et des données d'identification administrative disponibles sur le serveur web de paiement, écrites en clair dans un fichier ! Au final, les pirates ont pu sortir du système 2,5 millions de dossiers clients avec leurs données de paiement. Pour l'heure, il semble qu'ils n'en aient pas fait usage.

ALERTE. Mais le plus grave restait à venir. Une fois à l'intérieur du réseau, les pirates se sont en effet rendus compte qu'ils pouvaient accéder aux fonctions opérationnelles.
En se servant des données d'identification administrative, ils ont ainsi pu intervenir sur des fonctions clés : le débit de l'eau potable, son traitement chimique et le temps de remplissage des réserves. A priori – et c'est une chance – les hackers ne semblent pas avoir eu l'intention de nuire et ne poursuivaient pas un but précis, mais les autorités frémissent à l'idée des conséquences dramatiques qu'une telle ingérence aurait pu occasionner. « *Si les attaquants avaient eu un peu plus de temps et avaient été un peu plus familiers du système de contrôle industriel, la KWC et les populations locales auraient pu subir de sérieux dommages* » conclut le rapport… [Lire la suite]

Réagissez à cet article

Source : *L'eau d'une station d'épuration manipulée par des hackers – Sciencesetavenir.fr*