Vingt ans de cyberattaques contre le monde de l'eau

Secteur critique autant qu'essentiel, le monde de l'eau doit, depuis une vingtaine d'années, jongler avec les menaces cyber. Arme de déstabilisation entre pays, santé publique… Les cyber-criminels ont mille raisons de vouloir s'attaquer à l'eau. Et tous les pays ne semblent d'ailleurs pas égaux face à la montée de cette tendance criminelle, sur fond de vengeances d'anciens collaborateurs ou de questions d'ordre géopolitique.

2000
AUSTRALIE

— Au cours des mois de mars et d'avril 2000, un ancien prestataire technique de la station d'épuration de Maroochy en Australie a pris le contrôle des systèmes de l'usine à des fins malveillantes. Après que sa demande d'emploi ait été refusée, il aurait ainsi détourné l'activité de plusieurs pompes en envoyant de fausses commandes. L'une des pompes aurait alors cessé de fonctionner, provoquant le déversement d'eaux usées dans les fonds marins, l'empoisonnement de la faune et de la flore locales, et la propagation d'odeurs nauséabondes aux alentours… Avant de réussir, l'individu aurait réalisé pas moins de… 46 essais pour pénétrer les systèmes d'information de l'usine, sans jamais être détecté. Une attaque qui mettra en exergue la fragilité du monde de l'eau face aux menaces cyber.



STORMSHIELD

2007
ÉTATS-UNIS

— À l'été 2007, un ancien employé d'un petit réseau de canaux californiens (Tehama Colusa Canal Authority, à Willows) a été accusé d'avoir installé un logiciel non-autorisé sur un ordinateur utilisé pour dériver l'eau de la rivière Sacramento à des fins d'irrigation. Une installation qui a endommagé l'ordinateur, faisant partie du SCADA. Cet ancien superviseur, responsable des systèmes informatiques de l'entreprise, bénéficiait encore de ses droits d'accès sur site.

2013
ÉTATS-UNIS

— En avril 2013, c'est une attaque physique qu'a subi l'installation d'eau potable d'une petite ville de Géorgie du Nord. Aucune effraction aux portes ou fenêtres, les attaquants se seraient introduits dans la station en passant par-dessus les barbelés avant d'accéder au système de supervision. Ils ont ensuite modifié les réglages des taux de fluor et de chlore — conduisant la société gestionnaire à déconseiller aux 400 habitants d'utiliser l'eau du robinet pendant quelques jours.

Interrogé sur les potentiels auteurs, le Directeur général de la station déclarait que les véhicules des employés étaient trackés et qu'aucun n'était présent à côté de la station au moment de l'attaque. Avant d'ajouter que les anciens employés pouvaient encore avoir des clés ou des accès qu'il ne connaissait pas...

2016
ÉTATS-UNIS

— Dans l'État du Michigan, le fournisseur public d'eau et d'électricité The Lansing Board of Water & Light (BWL) est victime d'un ransomware. Un employé aurait malencontreusement cliqué sur une pièce-jointe malveillante contenue dans un email. L'attaque n'a a priori pas eu de conséquences sur les systèmes de distribution d'eau et d'électricité mais le ransomware a rendu indisponible une partie des activités de BWL, dont les lignes téléphoniques et le service client.

Les dirigeants auraient alors choisi de payer les 25 000 dollars de rançon exigée par les cyber-criminels pour reprendre le cours normal de leur activité. À ne pas reproduire chez vous.



STORMSHIELD

2018
ÉTATS-UNIS

— Début octobre 2018, la Onslow Water and Sewer Authority (ONWASA), située à Jacksonville en Caroline du Nord, a subi une double intrusion informatique. Le 3 octobre, le ransomware Emotet se serait propagé dans les systèmes d'information de la société, suivi par le ransomware Ryuk une dizaine de jours plus tard. La société qui approvisionne pas moins de 150 000 foyers en eau s'est vue dans l'obligation de stopper l'activité d'une partie de son parc informatique pour limiter la propagation des malwares. La double attaque n'aurait pas perturbé le fonctionnement des systèmes de distribution d'eau et de traitement des eaux usées, mais de nombreuses bases de données et des éléments clés d'ONWASA auraient été cryptées.

L'entreprise a donc été contrainte de ralentir son activité durant plusieurs semaines et de reconstruire une partie de ses systèmes d'information.

2019
ÉTATS-UNIS

— En mars 2019, la compagnie publique de distribution d'eau du comté d'Ellsworth au Kansas, a été à son tour la cible d'une action malveillante de la part d'un ancien collaborateur. Celui-ci aurait pris le contrôle à distance des systèmes d'information de l'entreprise pour altérer le traitement de l'eau potable, destinée à la population.

L'ancien employé travaillait justement sur les systèmes de monitoring de l'usine, et ses accès n'avaient pas été révoqués lors de son départ de l'entreprise.

2019
ISRAËL

— Étape au Moyen-Orient dans cette liste, et plus précisément en Israël. En avril 2020, des cyber-criminels suspectés d'être affiliés au régime iranien auraient attaqué plusieurs stations de pompage et de traitement des eaux usées, et tenté d'augmenter le niveau de chlore dans certains systèmes d'approvisionnement d'eau qui alimentent une partie de la population israélienne.
Le gouvernement aurait rapidement contre-attaqué, notamment en incitant toutes les infrastructures d'eau et d'énergie du pays à modifier les mots de passe de l'ensemble de leurs systèmes SCADA, pour parer à toute autre éventuelle intrusion.

2020
ISRAËL

— En juin de la même année, les autorités israéliennes indiquaient que des pompes à eau dédiées à l'agriculture dans la région de Galilée auraient également été attaquées, ainsi qu'un système d'approvisionnement d'eau de la province de Mateh Yehuda. Les détails de l'attaque n'ont pas été publiés, mais il semblerait que, là encore, les cyber-criminels aient tenté d'altérer la qualité de l'eau en modifiant le niveau de chlore.



STORMSHIELD

2020
ISRAËL

— Annus horribilis en Israël, puisque début décembre 2020, une faille dans le système de contrôle d'un réservoir d'eaux recyclées aurait été révélée par un groupe d'attaquants iraniens. Selon les cyber-criminels, le système IHM (Interface Homme Machine, HMI en anglais) aurait été accessible depuis Internet sans aucune authentification requise, permettant ainsi à n'importe quel individu mal intentionné d'atteindre et de prendre le contrôle de certains paramètres comme la température ou la pression de l'eau.

2021
ÉTATS-UNIS

— Retour aux États-Unis, du côté de la baie de San Francisco, en Californie. Un attaquant aurait pris, en janvier 2021, le contrôle d'une station d'épuration de la région et aurait supprimé les programmes informatiques impliqués dans le traitement de l'eau potable. L'attaque est toujours en cours d'analyse par les autorités américaines et selon les premiers éléments de l'enquête, le cyber-criminel aurait pénétré les systèmes de l'usine à l'aide d'identifiants d'anciens employés, utilisés pour se connecter au logiciel de prise de contrôle à distance TeamViewer.

Le mois suivant, en février 2021, la ville d'Oldsmar, en Floride, a frôlé de peu une catastrophe sanitaire. Des cyber-criminels auraient pris le contrôle de la station d'épuration de la ville, dont les systèmes informatiques étaient mal protégés. En effet, d'après les premiers éléments de l'enquête, deux points d'entrée auraient permis l'attaque : d'une part, les attaquants auraient collecté des identifiants de connexion TeamViewer partagés par plusieurs employés, et d'autre part, ils auraient exploité des failles présentes au sein d'un système d'exploitation Windows 7. Cette intrusion aurait permis aux cyber-criminels d'augmenter nettement le niveau d'hydroxyde de sodium, rendant l'eau potable extrêmement toxique. Par chance, les équipes de la station ont pu rapidement reprendre le contrôle de la situation et ainsi éviter à quelques 15 000 habitants de la ville d'Oldsman d'être intoxiqués.

2021
NORVÈGE

— Volue, une société norvégienne qui équipe plusieurs infrastructures de traitement des eaux en applications et logiciels, aurait été victime du ransomware Ryuk. Les faits se seraient produits début mai 2021 et le ransomware se serait propagé aux systèmes d'information de 200 fournisseurs publics d'eau du pays, clients de Volue. Plusieurs plateformes front-end clients auraient été impactées et l'entreprise aurait rapidement mis en place des moyens pour isoler puis restaurer les systèmes infectés, et ainsi limiter l'impact auprès de ses clients. Volue indique qu'en l'état actuel des choses, 70% de ses clients n'auraient pas été impactés par l'attaque ou seraient désormais hors d'attente. Cependant, tous les tenants et aboutissants de cette cyberattaque ne sont pas encore connus et l'enquête suit son cours.



STORMSHIELD