INDUSTRIE

RÉGIE D'EAU D'UNE MÉTROPOLE

OPTIMISER LA CYBERSÉCURITÉ EN TENANT COMPTE DES CONTRAINTES OPÉRATIONNELLES

1,3 million
D'HABITANTS

60
COMMUNES

100
CHÂTEAUX D'EAU

Des réseaux de plus en plus interconnectés

La sécurisation des installations d'eau est un enjeu majeur pour les agglomérations. Les échanges d'information deviennent permanents entre les réseaux informatiques et opérationnels. Mais cette optimisation de la gestion des infrastructures augmente la surface d'attaque. Pour exemple, en mars 2016, un piratage a visé une usine d'eau potable américaine. Des personnes malveillantes avaient modifié la quantité de composants chimiques présents dans l'eau. Plus récemment, en avril 2020, le gouvernement israélien a rendu publique une série d'attaques informatiques sur ses installations d'approvisionnement et de traitement de l'eau. L'agence de cybersécurité israélienne a demandé à tout le personnel des entreprises actives dans les secteurs de l'énergie et de l'eau de changer les mots de passe de tous les systèmes connectés à Internet.

Le contexte

La métropole d'une grande région française, comptant une soixantaine de communes et plus d'un million d'habitants, a lancé un appel d'offre pour rationaliser la gestion de son réseau d'eau potable. Depuis plusieurs années, cette distribution de l'eau était gérée par trois opérateurs de distribution privés. L'objectif étant à présent de n'avoir plus qu'un seul opérateur unique. Au-delà de cette rationalisation du service, la métropole souhaitait également moderniser son architecture informatique en élevant le niveau de sécurité.

Les trois opérateurs existants se sont alors retrouvées en concurrence pour gérer le service public de production, de transport, de stockage et de distribution d'eau potable sur la majeure partie du territoire.

Et pour renforcer la sécurisation de ses réseaux opérationnels, la métropole souhaitait une architecture permettant de protéger de manière indépendante, via la mise en place de pare-feux :

- le réseau bureautique IT,
- les concentrateurs VPN centraux,
- l'informatique industrielle et de sûreté,
- les sites distants.

La solution retenue

Cet appel d'offre a été remporté par l'opérateur de référence sur le marché français, qui a fait appel à Stormshield pour l'accompagner dans la sécurisation de cet environnement industriel.

Les principales fonctionnalités attendues et activées sur cette architecture globale étant le contrôle et le filtrage de chaque communication avec DPI (principalement le protocole Modbus) ainsi que la mise en place d'une solution de VPN Ipsec pour protéger les communications.

Des contraintes industrielles fortes, gérées via une solution unique

La sécurité du site central a ainsi été renforcée par la mise en place de pare-feux entre le réseau bureautique et les installations métiers. Ces installations sont dispatchées sur deux réseaux distincts (sûreté et industriel), chacun protégés par un cluster de pare-feux destinés à assurer les fonctionnalités de concentrateur VPN. Cette architecture permet ainsi d'interconnecter ces mêmes applications aux différents châteaux d'eau.

Dans le détail, un cluster de pare-feux SN3100 a été retenu par l'opérateur pour sécuriser le réseau opérationnel et la sûreté et garantir un fonctionnement sans interruption, du fait de la double alimentation et des disques RAID intégrés à ces équipements.

Trois clusters de pare-feux SN710 ont également été déployés pour la zone VPN concentrateur (communication IT/OT). Grâce à des rapports interactifs personnalisables, le client dispose instantanément des informations essentielles sur l'activité de son réseau et les évènements liés à sa sécurité. Basé sur plusieurs méthodes de détection comportementales et directement intégré au cœur des produits, le moteur de prévention d'intrusion (IPS) assure une protection efficace contre les menaces « Zero-day », tout en maintenant des performances haut débit.

Enfin, 100 châteaux d'eau ont été équipés individuellement de deux clusters (l'un pour la partie sûreté et le second pour la partie industrielle) de pare-feux durcis SNi40 pour sécuriser les flux entre les différents sites et les applications. Ces derniers sont spécifiquement conçus pour protéger les API (Automates Programmables Industriels) et permettent également de monter les tunnels VPN IPSec vers les sites centraux.

L'offre industrielle proposée par Stormshield répondait parfaitement aux différents besoins exprimés par l'opérateur. Par ailleurs, l'adaptabilité de la solution proposée permettait à la fois de gérer des sites de type standard jusqu'à des environnements avec fortes contraintes industrielles (température, humidité, Rail DIN, alimentation industrielle). Ceci, avec un seul et même firmware déployé sur l'ensemble de la gamme Stormshield Network Security et une console d'administration unique, Stormshield Management Center, pour gérer l'ensemble du parc de pare-feux.

Par ailleurs, au-delà du rapport fonctionnalités/prix et indépendamment des fonctions standard (VPN, segmentation…), le client a été fortement séduit par la fonctionnalité IPS des protocoles industriels, dont la granularité est la plus aboutie sur le marché, et qui permet une évolution de la sécurité de ces systèmes sensibles en parallèle de la modernisation des infrastructures.

Une offre de services adaptée aux environnements industriels complexes

En matière de maintenance et d'exploitation, pour garantir la disponibilité du service aux usagers, le client était confronté à des problématiques d'accessibilité et de sensibilité de certains sites. Pour pallier à ces contraintes, Stormshield et l'opérateur retenu ont mis en œuvre un accompagnement adapté, avec :

- La mise en œuvre d'une procédure permettant à un agent technique n'ayant pas de compétences réseau/sécurité de remplacer un pare-feu défaillant et de remettre le site en mode opération avec le bon niveau de sécurité;
- Une activation du mode sécurité (bypass) pour 5% des sites qui ne sont équipés non pas d'un cluster, mais d'un seul pare-feu unique. Ceci, afin de privilégier la disponibilité des systèmes industriels ainsi que la sûreté, en lieu et place de la sécurité;
- Une offre de services professionnels pour accompagner la métropole dans son process d'industrialisation de la configuration sur les premiers sites pilotes.

L'ensemble du projet et son déploiement a été mené de bout en bout avec succès et dans les meilleurs délais, grâce à une implication et une cohésion forte du binôme opérateur/éditeur. La mise en œuvre de procédures dédiées pour répondre aux exigences métiers de ce contexte industriel a également été très apprécié par le client final.

Et la relation continue, puisque Stormshield a réalisé d'autres projets et répondu à d'autres appels d'offres au côté de cet opérateur, qui l'interroge également en interne dans le cadre de la modernisation de son activité et l'adaptation de ses offres à ce contexte de sécurité IT/OT. Ce sujet devenant de plus en plus primordial lorsque l'on parle d'infrastructures critiques et sensibles, dont les risques cyber peuvent avoir de lourdes conséquences économiques, écologiques et humaines.

STORMSHIELD

Partout dans le monde, les entreprises, les institutions gouvernementales et les organismes de défense ont besoin d'assurer la cybersécurité de leurs infrastructures critiques, de leurs données sensibles et de leurs environnements opérationnels. Les technologies Stormshield, certifiées et qualifiées au plus haut niveau européen, répondent aux enjeux de l'IT et de l'OT afin de protéger leurs activités. Notre mission : cyber-sérénier nos clients pour qu'ils puissent se concentrer sur leur cœur de métier, si cruciale pour la bonne marche de nos institutions, de notre économie et des services rendus aux populations. Choisir Stormshield, c'est privilégier une cybersécurité européenne de confiance. Pour en savoir plus : www.stormshield.com