STORMSHIELD

TÉMOIGNAGE CLIENT

Renforcer la sécurité du réseau interne : une priorité pour les collectivités

INFRASTRUCTURE PUBLIQUE

Dans un monde de plus en plus numérique, les communautés de communes et collectivités se sont modernisées pour proposer de nouveaux services connectés. Mais cette connexion entraîne deux risques : celui d'exposer encore plus des informations confidentielles que les collectivités sont amenées à traiter et de voir ces services compromis ou interrompus par des personnes malveillantes.

D'où la question du renforcement du niveau de sécurité de leurs réseaux informatiques, afin d'assurer une continuité de service et de protéger les administrés face aux cyberattaques. C'est la décision prise par une communauté de communes en Allemagne de 200 000 habitants.

Des infrastructures critiques et informations sensibles à protéger

Pour gérer et administrer tous les services réseaux de la communauté de communes (électricité, gaz, eau potable, chauffage urbain…) et ses infrastructures publiques (éclairage public, parkings, piscines municipales, transports…), la communauté des communes a créé une société dédiée, qu'elle détient à 100%.

En complément des tâches de mise en œuvre et d'exploitation courante des infrastructures et services proposés, un portail web est mis à disposition des administrés pour retrouver l'ensemble des informations utiles et réaliser certaines demandes via des formulaires web.

Aux vues de la criticité de ses activités et des données qui transitent et sont stockées dans son Système d'Information, il devenait impératif pour cette société de renforcer son niveau de sécurité.

Un niveau de sécurité renforcé

Le client a donc pris la décision d'ajouter un second pare-feu, en complément de son équipement actuel, afin d'assurer une double protection de son réseau informatique interne.

En effet, étant considéré comme « critique » selon l'ordonnance KRITIS de l'Office fédéral allemand pour la sécurité de l'information (BSI), ce client ce doit légalement de sécuriser de manière adéquate son Système d'Information, essentiel au bon fonctionnement des services publics. Cette double protection étant l'une des briques de sécurité renforcée mise en place pour assurer la continuité de ses activités.

Pour ce nouveau matériel, le client ne souhaitait pas retenir le même constructeur afin de complexifier la tâche en cas de tentative d'intrusion, le contournement de deux technologies différentes étant de facto plus difficile à réaliser.

Conseillé par son intégrateur Phalanx IT, le choix s'est porté sur la solution Stormshield Network Security, plus particulièrement un cluster de pare-feux SN6100, et la console de gestion centralisée Stormshield Management Center.

Au-delà de la qualité et des performances de ces deux solutions, faire appel à un acteur européen, dont les solutions sont reconnues et certifiées au plus haut niveau, a également pesé dans la balance.

LES SOLUTIONS MOBILISÉES

→ SN6100
→ Stormshield Management Center

Des performances et fonctionnalités en adéquation avec les besoins client

Après un déploiement réalisé par les équipes certifiées de Phalanx IT en toute satisfaction pour le client, ce dernier dispose à présent d'un cluster de pare-feux Next Generation qui répond à toutes ses exigences en matière de performance et de fonctionnalités.

Conçu pour les infrastructures critiques de grande taille, le SN6100 offre en effet un débit de 170 Gbps et la plus haute densité de ports du marché, indispensable pour anticiper les futures évolutions des besoins de sécurité de l'infrastructure réseau.

Le client bénéficie également d'une haute disponibilité et d'une sécurité renforcée grâce à une segmentation du réseau et la mise en place de règles strictes, qui lui permettent de mieux contrôler le flux de trafic vers les zones les plus critiques. Le SN6100 dispose également de composants (alimentation et ventilation) redondés afin d'éviter tout risque de pannes.

En complément, le client a déployé la solution de gestion centralisée Stormshield Management Center. Cet outil lui permet ainsi d'optimiser ses tâches de supervision, de configuration et de maintenance de ces pare-feux.

Au-delà du gain de temps pour les administrateurs et de la minimisation des risques d'erreur, cet outil, spécialement conçu pour répondre aux besoins des réseaux multisites, s'inscrit dans la même logique d'anticipation d'un futur besoin d'évolutivité du réseau.

STORMSHIELD

Version 1.1 - Copyright Stormshield 2023