STORMSHIELD

TÉMOIGNAGE CLIENT

Comment rénover les systèmes de pilotage de centrales de production électrique pour plus de cybersécurité

INDUSTRIE

Stormshield et Clemessy, la marque d'Eiffage Énergie Systèmes dédiée à l'industrie, travaillent en partenariat depuis plusieurs années. Dans le domaine de l'énergie, l'éditeur et l'intégrateur ont ainsi accompagné un client commun dans un projet de rénovation du contrôle commande de plusieurs centrales de production électrique.

PLUSIEURS CENTRALES
dans le monde

40
postes par centrale

25
serveurs par centrale

01

Rénover les outils de pilotage sans perturber la production

Ce client souhaitait moderniser ses installations pour faire face à l'obsolescence de son système de contrôle commande, qui permet de piloter la production électrique dans plusieurs centrales, et d'améliorer du même coup sa cybersécurité.

Stormshield et Clemessy ont été sélectionnées pour l'accompagner dans ce projet complexe. En effet, la production d'électricité constitue une activité critique qui ne peut être facilement arrêtée : il fallait donc pouvoir rénover, en perturbant le moins possible les processus opérationnels. Par ailleurs, certaines structures de l'énergie sont classées OIV (Opérateur d'Importance Vitale) selon la Loi de programmation militaire française (LPM) et/ou OSE (Opérateur de Services Essentiels) selon la directive européenne NIS et doivent à ce titre remplir des obligations légales strictes. Par exemple, pour les OIV, les équipements installés doivent être certifiés par l'ANSSI (Agence nationale de la sécurité des systèmes d'information).

« ***Notre mission consiste à trouver le bon équilibre pour offrir un service de contrôle commande sécurisé aux personnels et aux opérateurs de maintenance, sans pour autant bloquer la production*** », précise Emmanuel Lambert Chef de projet chez EES - Clemessy.

Tout commence par l'EBIOS

Ce projet a débuté par la réalisation d'une analyse de risque basée sur la méthode EBIOS Risk Manager publiée par l'ANSSI. Méthode de référence française, elle permet de « déterminer les mesures de sécurité adaptées à la menace et de mettre en place le cadre de suivi et d'amélioration continue à l'issue d'une analyse de risque partagée au plus haut niveau ». Pour en savoir plus, retrouvez ici le guide de la méthode : ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide/



02

Sécuriser l'interconnexion et protéger les postes de travail

Les principaux risques identifiés étaient liés à l'interconnexion du système opérationnel (OT) et du réseau bureautique, qui n'avaient pas le même niveau de sécurité.

Les équipes de Clemessy ont pu y remédier en les interconnectant via un pare-feu Stormshield SN510. Rapidement, plusieurs modules de sécurité ont pu être déployés. Une zone DMZ hébergeant des services Web et de transfert de fichiers a été créée. La solution VPN SSL Client de Stormshield sécurise désormais l'accès de télémaintenance. La protection du système industriel est assurée via un filtrage strict des flux et à l'activation du système de prévention d'intrusion natif aux solutions SNS de Stormshield fonctionnant en mode DPI (Deep Packet Inspection). Les réseaux internes et critiques ont quant à eux été segmentés et une authentification centralisée et sécurisée a été instaurée via deux contrôleurs de domaine (Active Directory) redondants.

Pour compléter ce dispositif de sécurisation de l'infrastructure informatique du contrôle commande, un autre pare-feu Stormshield SN310 a été installé pour sécuriser l'interconnexion avec des sous-systèmes aux niveaux de sécurité différents. Un filtrage avancé, à l'aide de la fonction DPI du pare-feu Stormshield, des commandes de protocoles industriels de type Modbus a été mis en place, permettant de n'autoriser que les commandes de type lecture par exemple.

« Très impliqué dans l'OT, Stormshield est un fournisseur particulièrement intéressant quand nous concevons des systèmes opérationnels pour nos clients. Ses équipements, français, certifiés et qualifiés ANSSI, présentent des fonctionnalités adaptées au monde industriel et ses solutions, faciles à prendre en main, sont très appréciées sur le terrain. »

JEAN SCHNOEBELEN
Responsable d'activité EES - Clemessy

Les équipements informatiques (serveurs, postes de supervision, postes de travail) ont également été dotés de moyens de protection HIPS (host-based intrusion prevention system) à l'aide de la solution Stormshield Endpoint Security. Cette solution présente l'avantage de ne pas nécessiter de mises à jour fréquentes et permet de contrôler l'usage des périphériques et notamment les ports USB.

L'opération de rénovation comprenait également la sécurisation des systèmes d'exploitation Windows, le renouvellement de commutateurs réseaux et de nombreux automates.

LES SOLUTIONS MOBILISÉES

- → DES PARE-FEUX SN710 ET SN310
- → SOLUTION VPN SSL DE STORMSHIELD
- → SOLUTION STORMSHIELD ENDPOINT SECURITY

Formaliser et former pour améliorer la résilience

Clemessy, la marque d'Eiffage Énergie Systèmes a également rédigé la documentation relative aux équipements, matrice de flux, inventaire, plan de sécurité, maintenance et exploitation des solutions mises en oeuvre en vue d'une homologation de l'ANSSI conforme à la Loi de programmation militaire (LPM).
En complément, des formations de sensibilisation aux risques cyber ont été dispensées. Les opérateurs et le personnel de maintenance ont aussi participé à des simulations d'attaque. Leurs réactions ont été étudiées afin de créer des fiches « réflexes » pour améliorer la réponse en cas d'incident.

Cette étape reste indispensable, comme l'explique Théo Gissinger-Schumann, Responsable technique chez EES - Clemessy : « ***la sécurisation n'atteint jamais 100 % : pour des raisons de compatibilité et de fonctionnement, nous pouvons être obligés de dégrader certaines mesures de sécurité. Notre rôle consiste alors à lister ces risques résiduels après sécurisation pour qu'ils soient connus et pris en compte. La sensibilisation et la capacité de réaction du personnel font partie des mesures permettant d'atténuer ces risques résiduels***. »

L'ensemble de ces mesures tend à un seul but : rendre le système OT plus résilient.

Version 1.0 - Copyright Stormshield 2022