La Cybersécurité chez Eiffage Energie Systèmes

La Revue 3E.I
Culture Sciences de l'Ingénieur

Édité le 01/02/2024

école normale supérieure paris—saclay

Jocelyn ZINDY[1] – Franck LE GALL[2]

[1] *Eiffage Energie Systèmes,* [2] *ISEN Brest*

Cette ressource fait partie du N°111 de La Revue 3EI de janvier 2024.

Cet article est issu d'un entretien avec M. Zindy, directeur du développement commercial Cybersécurité - Industries du Futur de Eiffage Energie Systèmes. Il présente d'une part le cadre général de la Cybersécurité dans le domaine de l'OT (Operational Technology) en précisant les spécificités de l'OT vis-à-vis de l'IT et d'autre part comment un grand groupe comme Eiffage intègre celle-ci dans ses offres.

1 - Introduction

Les cyberattaques sont devenues monnaie courante dans nos sociétés modernes. Elles touchent les réseaux internet, mobiles, Wifi et les systèmes qui leurs sont connectés. On pense en premier lieu aux ordinateurs et à tout l'univers de l'IT (Information Technology) mais cette menace est aussi bien réelle pour le monde industriel. Les grandes entreprises du domaine sont particulièrement attentives à ces évolutions et proposent des solutions pour y remédier.

Le groupe Eiffage exerce dans de nombreux domaines : construction, infrastructures, concessions et énergie. Il s'agit du troisième groupe de constructions et de concessions français, derrière Vinci et Bouygues, et du quatrième groupe européen. En 2023, il comprend plus de 70 000 collaborateurs. C'est dans la branche « Energie systèmes » qui compte environ 29 000 personnes que travaillent une trentaine d'experts en cybersécurité.

Dans le monde de la cybersécurité, Eiffage Energie Systèmes n'est ni un « pure player », ni spécialisé dans la cybersécurité IT, il reste proche de son cœur de métier en offrant un volet cybersécurité dans le domaine de l'OT (Operational Technology). En tant qu'intégrateur multi technologies, il propose à ses clients de répondre aux clauses de cybersécurité qui sont maintenant présentes dans les appels d'offre.

Il existe de nombreuses entreprises qui proposent des solutions de cybersécurité. On peut citer Atos ou Sopra Steria qui bien que très majoritairement orientées vers l'IT (environ 95%) réalisent aussi des prestations orientées OT (environ 5%). D'autres acteurs de plus petite taille (quelques dizaines de personnes), sont des « pure players » c'est-à-dire des petites entreprises spécialisées dans la cybersécurité OT.

Figure 1 : La cybersécurité dans l'Operational Technology

2 - OT versus IT

Qu'est que l'OT ? Nous sommes habitués à entendre parler de l'IT qui est exploité au sein des systèmes d'information d'entreprise alors que l'OT est mise en œuvre pour la gestion et la prise en charge des systèmes d'Information Industriels ou techniques. Alors que l'IT concerne principalement les réseaux, les logiciels, la téléphonie, c'est à dire la gestion de l'entreprise, l'OT est plus proche des process et prend en compte les automates, les capteurs …. Le marché de la cybersécurité se réparti actuellement à hauteur d'environ 80 % d'IT et 20 % d'OT.

La frontière n'est pas étanche entre ces deux domaines d'autant plus que l'évolution des usages fait que la demande de remontée d'informations, de mesures est croissante. La nécessité de connecter des outils industriels qui étaient souvent déconnectés du réseau (filaire ou Wifi) se fait de plus en plus présente ouvrant ainsi mécaniquement une porte d'accès pour des malveillants.

Le besoin de continuité numérique et d'analyse de données a, par exemple, amené les hôpitaux à développer leurs réseaux en connectant de plus en plus de systèmes sur internet et en offrant des accès Wifi. Ces réseaux mal sécurisés ont fait l'objet de nombreuses attaques ces dernières années avec des demandes de rançons sous la menace de divulgation de dossiers confidentiels ou une paralysie des services et des soins critiques comme, par exemple les salles d'opération. Dans cet exemple, le vol de dossiers confidentiels peut être rangé dans le domaine de l'IT alors que la prise de contrôle d'une salle d'opération le sera dans celui de l'OT.

Autre exemple moins médiatisé mais tout aussi problématique. Celui d'une station traitement des eaux dont les opérateurs ont perdu le contrôle de vanne sous l'effet d'une cyberattaque, menaçant ainsi de contaminer des circuits d'eaux potables. On comprend bien que de telles actions, sans être nécessairement d'une grande complexité, peuvent entraîner des conséquences délétères sur la santé des personnes et l'intégrité des matériels.

Alors, comment distinguer l'IT de l'OT ? Comme nous l'avons écrit, la frontière est poreuse mais l'OT comporte tout de même deux contraintes spécifiques :

- Les contraintes liées aux process. Nombreux process industriels nécessitent un fonctionnement en continu avec des exigences élevés en temps de réponse. Il est alors plus difficile d'intervenir et d'implémenter une solution cyber, et de la maintenir à jour …
- L'hétérogénéité des équipements : les systèmes industriels comportent de nombreux systèmes, capteurs, ordinateurs, automates … dont les caractéristiques sont très

hétérogènes. Les intervenants doivent posséder une solide culture industrielle pour y implémenter des solutions cyber.

Eiffage Energie Systèmes propose ses services de cybersécurité (majoritairement OT) dans l'industrie, les infrastructures et réseaux, le tertiaire et les villes et collectivités. Ils proposent de sécuriser les composantes de systèmes complexes (Serveur, postes utilisateurs, réseaux, automates, logiciels …) (figure 2).

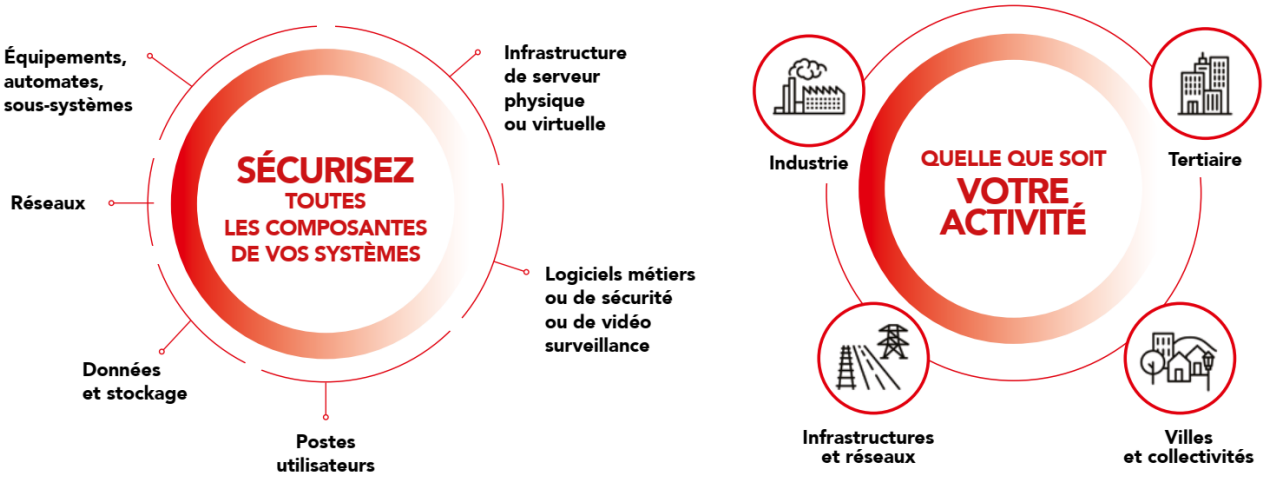

Figure 2 : Les domaines de la cybersécurité OT chez Eiffage

3 - Une prise de conscience d'un besoin à grande échelle

Ces menaces sont largement prises au sérieux par les autorités qui ont chargé l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) d'un rôle de communication et de préconisation auprès des opérateurs et des industriels.

On peut lire sur son site que « L'ANSSI, autorité nationale de cybersécurité, propose au premier ministre les mesures destinées à répondre aux crises affectant la sécurité des systèmes d'information des autorités publiques et des opérateurs régulés. Elle coordonne l'action gouvernementale et anime l'écosystème national. »

L'ANSSI a donc pour interlocuteurs des entreprises qui sont classées en fonction de leur importance lors de crises de cybersécurité. Ce sont des :

- Opérateurs d'Importance Vitale (OIV) : environ 200 organisations ayant des activités indispensables à la survie de la nation ou dangereuses pour la population [Wikipédia]. C'est le cas, par exemple, des gestionnaires d'installations nucléaires ou d'alimentation en eau, des acteurs du secteur militaire, ou des organismes opérant dans le domaine de la santé. Ces OIV sont tenus de développer des stratégies de cybersécurité pour protéger leurs activités.
- Opérateurs de Services Essentiels (OSE) : environ 1000 « opérateurs, publics ou privés, offrant des services essentiels au fonctionnement de la société ou de l'économie et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture desdits services » (Article 5 de la loi du 26 février 2018.) Pour être considéré comme un OSE, l'entreprise doit répondre à trois critères :
    - Fournir au moins un service essentiel à la continuité d'activités économiques ou sociétales critiques ;

- Être tributaire des réseaux et des systèmes d'information pour la fourniture de ce service ;
- Être confronté à un risque de suspension de ce service en cas de cyber-incident.

Afin que ces OIV et OSE atteignent leurs objectifs l'ANSI édite en particulier :

- Des recommandations ;
- Un référentiel PIMSEC pour l'intégrateur (PAX pour le Neuf, PAMS pour la maintenance) ;
- Une méthode de gestion des risques EBIOS.

Les entreprises comme Eiffage Energie Systèmes qui proposent leurs services peuvent obtenir des qualifications pour les audits, la détection d'incident ou encore l'intervention après incident.

En complément des actions de l'ANSSI on peut noter que certaines collectivités territoriales sont pro actives dans ce domaine. Ainsi, la région Grand-Est propose une aide aux entreprises en prenant en charge 50% du coût d'un diagnostic de cybersécurité.

4 - Quelques « Success Stories »

Les projets réalisés par Eiffage Energie Systèmes sont très variés et basés sur trois types de prestations :

- **Audit, diagnostic et conseils :** il s'agit d'inventorier, d'évaluer les risques, de proposer un plan d'action pour atteindre un niveau de sécurité homologué.
- **Maintien en conditions de sécurité :** la veille de vulnérabilité et détection/qualification de nouvelles menaces, la formation de sensibilisation, l'amélioration continue, la simulation d'attaques et la réponse sur incident permettent de maintenir le niveau de sécurité à un niveau acceptable.
- **Sécurisation des systèmes :** l'intégration de solutions matérielles et logicielles (détection et protection), la remédiation et l'évaluation des risques résiduels permet de protéger les systèmes des risques de cyberattaque.

Á titre d'exemple de sécurisation, on peut citer :

- La sécurisation du contrôle-commande d'une ventilation nucléaire qui a nécessité la prise en compte de 3 000 entrées sorties physiques, 400 synoptiques.
- La sécurisation du contrôle-commande d'unité de contrôle des opérations sur le banc d'essai des accélérateurs à poudre situé à Kourou en Guyane française.
- La rénovation du système de vidéo-surveillance d'un site militaire par l'étude des risques de sécurité (cyberattaques, intrusions, piratages…) à l'aide de la méthode EBIOS.
- La rénovation du système de contrôle-commande d'une centrale électrique munie de groupes thermiques Diesel.
- La sécurisation de l'application TETRA de communication opérationnelle interne aux agents de la RATP.

Figure 3 : Visuel cybersécurité de Eiffage Energie Systèmes

La méthode suivie lors de ces projets commence par du « bon sens » : par exemple pour la sécurisation d'un automate, il faut renforcer les mots de passe, fermer les ports inutilisés, utiliser un VPN, segmenter l'architecture, ajouter des sondes …. Au-delà de ces premières mesures, il s'agit principalement d'un travail d'intégration basé sur la Norme de sécurisation de l'OT (ISO 62443).

Pour certains projets, il est nécessaire de réaliser des développements sur mesure. Ainsi dans le cas d'un système de supervision de contrôle commande avec des contraintes temps réel trop élevées, il a été nécessaire de développer un logiciel ad hoc.

5 - Et demain …

Chez Eiffage Energie Systèmes, on estime que le secteur de la cybersécurité OT est en pleine croissance et qu'il va falloir de nombreuses années pour mettre au niveau les systèmes industriels.

En effet, les menaces cyber ne font que croitre et les autorités souhaitent rehausser les niveaux de protection. Dans ce cadre, la directive NIS-2 (Directive Network and Information System Security 2) prévue pour le mois octobre 2024, aura pour conséquence de multiplier par 30 à 40 le nombre d'entreprises qui seront obligées de se cyber-sécuriser.

Ainsi, alors qu'aujourd'hui, Eiffage Energie Systèmes dispose de compétences Cyber dans quelques entités opérationnelles, il paraît fort probable qu'il faudra à terme des équipes cyber réparties sur tout le territoire au plus près des utilisateurs. Le potentiel d'emploi dans ce domaine est donc prometteur.

Ressource publiée sur Culture Sciences de l'Ingénieur : https://eduscol.education.fr/sti/si-ens-paris-saclay