

par [Didier Gazagne](#)



La sécurité des systèmes d'information d'EDF : une affaire de stratégie

[Alain Jeandat](#),

Chef du Pôle Sécurité et Conformité Réglementaires des SI, AQSSI d'EDF

1. Pouvez-vous nous dire brièvement en quoi consiste votre activité d'Autorité qualifiée de Sécurité des Systèmes d'Information (AQSSI) d'EDF ?

Comme cela est indiqué dans [l'arrêté ministériel de désignation](#), l'autorité qualifiée est notamment chargée, en liaison avec le HFDS (1) et le FSSI (2) du département ministériel :

- de s'assurer que les dispositions réglementaires sont appliquées
- de gérer les situations d'urgence en conformité avec les plans VIGIPIRATE et PIRANET,
- de s'assurer de la mise en œuvre des procédures réglementaires prescrites pour l'homologation des systèmes
- de vérifier la conformité de la protection des applications, des centres d'hébergement et des moyens de télécommunication
- de s'assurer que des contrôles de sécurité sont effectués et que les actions sont suivies
- de s'assurer de la sensibilisation et de la formation du personnel aux questions de sécurité

Tout ceci est, bien entendu, réalisé et suivi en étroite collaboration avec le Responsable de la Sécurité des SI (RSSI), qui est en charge de piloter l'ensemble de la filière SSI du Groupe.

2. L'accroissement ces derniers mois des cyberattaques mondiales et le déploiement de ransomwares (WannaCry, Petya) modifient-ils vos priorités ?

Comment ne pas réexaminer ses priorités au regard de l'accroissement des cyberattaques, tant en nombre qu'en technicité ? Bien que n'ayant pas eu à déplorer de dégâts au sein d'EDF du fait des ransomwares que vous évoquez, cela a fait l'objet d'un retour d'expérience quant à leur impact et à leur traitement : des actions majeures et immédiates à mettre en œuvre ont été identifiées.

La sensibilisation est bien entendu une priorité pour l'ensemble des acteurs de la SSI ; c'est donc pour moi non seulement une priorité, mais aussi un devoir de par les obligations qui me sont attribuées.

Pour être efficace, celle-ci doit être adaptée aux différentes populations ciblées : utilisateurs, managers, administrateurs, etc. Un utilisateur doit être sensibilisé, alors qu'un manager doit être responsabilisé et qu'un administrateur doit être formé.

3. Quel rôle joue l'ASSSI dans la stratégie de cybersécurité d'une organisation telle qu'EDF ?

Dans notre Groupe, la stratégie en termes de systèmes d'information, d'infrastructures informatiques centralisées et de sécurité SI est élaborée sous la gouvernance de la DSI-Groupe. L'AQSSI est systématiquement consultée afin de recueillir son avis et, pour un certain nombre de cas, son accord.

J'apporte donc un éclairage sur l'ensemble des sujets relatifs à la cybersécurité, avec un prisme articulé autour, d'une part, des obligations réglementaires et, d'autre part, de l'adéquation de la sécurité du SI au besoin de sécurisation des informations traitées.

4. Sur quelle chaîne fonctionnelle de la SSI vous appuyez-vous ?

Au sein d'EDF, deux réseaux irradiant à travers toutes les organisations du groupe : l'un est propre à la sécurité des systèmes d'information et l'autre est centré sur la sécurité du patrimoine d'EDF. Chacun d'eux est un relai, tant pour diffuser les alertes et les directives que pour remonter les incidents, les écarts et les difficultés.

Il m'est donc nécessaire de bien connaître ces réseaux et d'établir des relations de confiance avec leurs acteurs. Bien que de nature très différente, il faut aussi établir des relations de confiance avec les autorités avec lesquelles des échanges doivent être réalisés.

Il faut bien entendu disposer d'un minimum de connaissances et d'expériences dans le domaine de la sécurité des systèmes d'information.

Afin de garantir la complétude et la non-redondance des actions autour de la SSI dans le contexte d'EDF, une collaboration et un partage très importants avec le RSSI sont primordiaux : nous sommes très complémentaires tant par nos missions que par nos expériences.

5. Envisagez-vous de recourir à l'utilisation d'outils de sécurité cognitive à court ou moyen terme ? Dans l'affirmative, quels sont les enjeux ?

Des groupes de réflexion et de travail ont été initiés autour de l'« intelligence artificielle ». Deux axes essentiels sont examinés : celui de l'IA au service de la sécurité et celui de la sécurisation de l'IA. Pour les deux aspects, les outils de sécurité cognitive devront être étudiés, mais nous n'en sommes encore qu'aux débuts de nos travaux.

(1) HFDS : haut fonctionnaire de défense et de sécurité.

(2) FSSI : fonctionnaire de sécurité des systèmes d'information.