Un enjeu crucial pour le réseau électrique et les Smart Grids

Depuis plusieurs années, l'actualité nous fournit des exemples de cyberattaques qui touchent les infrastructures énergétiques, souvent dans les zones de conflit (Ukraine), mais pas uniquement (États-Unis par exemple).
Les systèmes énergétiques sont en effet des actifs stratégiques majeurs, et le nombre d'actions cybernétiques malveillantes va croissant : une vingtaine de cyberattaques de grande ampleur ont concerné des systèmes énergétiques dans le monde depuis 1982, avec une accélération du rythme depuis 2010.
Dans le cadre du déploiement des Smart Grids, le développement des applications numériques et des objets connectés génère de nouveaux flux d'informations. Cette instrumentation et ces flux de communication représentent des enjeux supplémentaires en termes de sécurisation et de résilience des systèmes électriques.

Les cibles

L'événement le plus redouté est l'écroulement du réseau, qui peut être atteint par l'attaque massive de moyens de production ou d'éléments réseaux pilotés à distance (tels que des disjoncteurs aux postes de transformation ou interrupteurs divers en réseau, compteurs électriques notamment).
Mais bien d'autres menaces existent, par exemple sur la confidentialité des données individuelles, ou encore sur la sécurité des biens et des personnes.

Le cadre réglementaire

La cybersécurité des infrastructures énergétiques relève désormais de la compétence militaire dans plusieurs pays. Ainsi, aux États-Unis, la cyber résilience de l'industrie électrique relève de la compétence du Secretary of Defense (et non de l'Énergie), tandis qu'en France la protection des installations électriques est régie par la Loi de Programmation Militaire de 2013.

En France, L'ANSSI, l'Agence nationale de la sécurité systèmes remplace depuis 2009 la Direction centrale de la sécurité des systèmes d'information. Elle assure la mission d'autorité nationale en matière de sécurité des systèmes d'information. À ce titre, elle est chargée de proposer les règles à appliquer pour la protection des systèmes d'information de l'État et de vérifier l'application des mesures adoptées.
L'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (OIV). Le domaine de l'énergie, notamment électrique, est considéré comme l'un des 12 secteurs d'activités d'importance vitale (SAIV).
«Maîtrise du risque numérique L'atout confiance»
L'ANSSI et l'AMRAE 2 ont publié ce document 3 le 18 novembre 2019, un guide en 15 étapes pour accompagner les dirigeants des organisations publiques et privées de toutes tailles dans la construction d’une politique de gestion du risque numérique.

L'analyse de risques

Il faut savoir qu'aucun système n'est infaillible, tout dépend des moyens de l'attaquant. Afin de sécuriser un système il s'agit d'identifier ses failles, pour mieux les sécuriser. Pour ce faire, il faut mener une analyse de risques, afin de classer ceux-ci en matière de gravité et de probabilité pour déterminer les actions à mener.
C'est la première étape à réaliser impérativement pour la sécurisation d'un système.

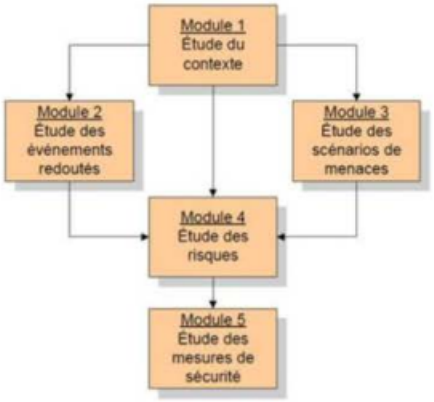
Critères de sécurité

On dénombre 4 critères de sécurité, pour s'assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu :
• La confidentialité : les données ne doivent être accessibles qu'à ceux qui sont autorisés ;

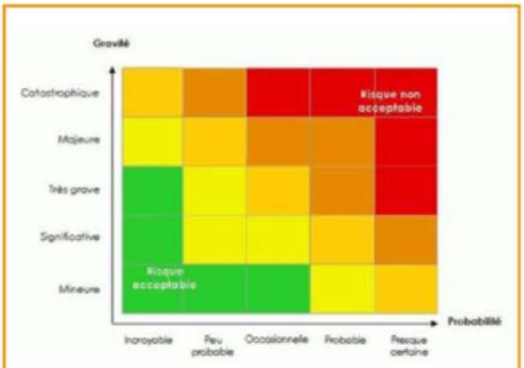
• L'intégrité : les données ne doivent pas être altérées de façon fortuite, illicite ou malveillante : les éléments considérés doivent être exacts et complets;
• La disponibilité : les données doivent être accessibles et utilisables par leur destinataire autorisé à l'endroit et à l'heure prévue ;
• La traçabilité : les traces de l'état et des mouvements de l'information doivent être conservées.

Méthodologies
Diverses méthodologies d'analyses de risques existent. La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), créée en 1995 par l'ANSSI et régulièrement mise à jour par celle-ci, permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information (SSI). Elle permet aussi de communiquer à leur sujet au sein de l'organisme et vis-à-vis de ses partenaires, constituant ainsi un outil complet de gestion des risques SSI.

La méthode EBIOS se déroule en 5 étapes. Elle commence par une étude du contexte : identification des éléments à protéger et des éléments d'infrastructure sur lesquels ils reposent.
On détermine alors les événements redoutés, à savoir la compromission des éléments à protéger, auxquels on attribue une gravité ; puis les scénarios de menaces, c'est-à-dire les biais d'attaque de l'infrastructure, et leur probabilité en fonction des caractéristiques de l'infrastructure et des attaquants potentiels. Ces aspects sont évalués selon les 4 critères de sécurité énoncés plus haut.
Finalement, en recroisant les éléments à protéger avec les infrastructures sur lesquels ils transitent, on peut ainsi déterminer des risques, auxquels sont associés une gravité et une probabilité.



Etapes de l'analyse de risques EBIOS



Exemple de tableau de classement des risques identifiés, auxquels sont associées une gravité et une probabilité

Il s'agit ensuite de traiter ces risques. On peut tout d'abord les accepter, si leur gravité et/ou leur probabilité sont suffisamment faibles, ou suffisamment faibles par rapport aux coûts des mesures suivantes pour les traiter. Pour réduire la probabilité eUou la gravité d'un risque jusqu'à ce qu'il devienne acceptable, on peut choisir de le transférer (à une assurance, par exemple), le réduire (en mettant en place des mesures techniques, organisationnelles, etc.), voire l'éviter (en modifiant ou arrêtant l'activité concernée).
L'analyse de risques doit être tenue à jour périodiquement, ou lors d'évolutions du système ou des mesures de sécurité.

La sécurisation des systèmes

Lorsque l'on entend cybersécurité, il est commun de penser en premier lieu au chiffrement des données. Or l'ensemble des mesures à mettre en œuvre est bien plus vaste.

Sécurité humaine/organisationnelle

La menace peut provenir d'un espion au sein de l'organisation ou d'anciens collaborateurs. Mais la probabilité la plus élevée repose sur des erreurs d'inattention ou de non-respect des consignes organisationnelles de sécurité de la part des employés : mots de passe faibles ou notés sur des post-it, clés USB externes ou utilisées en dehors de l'entreprise, autorisations d'accès données avec trop de largesse, etc.

Authentification

L'authentification permet de gérer les droits d'accès aux ressources concernées et maintenir la confiance dans les relations d'échange. Ce sujet est à la croisée des mesures organisationnelles, telles que le renouvellement régulier des mots de passe, leur non-divulgation, et de mesures techniques qui peuvent être mises en place, telles que la double authentification (2FA).

Sécurité des communications

La sécurisation des communications peut concerner un ou plusieurs des critères de sécurité (confidentialité, intégrité, disponibilité, traçabilité), en fonction de leur criticité selon ceux-ci. On retrouve ici par exemple la mise en place de chiffrement (confidentialité), signature (intégrité), ou encore de pare-feux pour surveiller les flux de données voire créer des « zones démilitarisées » (DMZ).
La cryptographie « par l'obscurité », qui repose sur l'espoir que les attaquants n'arrivent pas à percer une solution propriétaire, a été complètement désavouée. La mise en place de cybersécurité fiable repose sur des systèmes de chiffrement connus : lorsque ceux-ci sont largement étudiés et qu’aucune attaque significative n'est connue, ils sont considérés d'autant plus sûrs.

Sécurité physique

La sécurité des communications ne serait rien sans la sécurisation physique des équipements eux-mêmes, permettant d'assurer la sécurisation du système de bout en bout. L'accès aux équipements doit être protégé, que ce soit l'accès aux salles serveurs ou aux équipements dans des locaux et la connexion locale à ceux-ci, ou le durcissement physique des équipements déployés sur le terrain. Cette sécurité physique peut aller jusqu'à l'utilisation d'un « secure element » (comme les cartes bancaires), qui permet de stocker physiquement les clés et certificats et sert de boîte à outil pour réaliser les opérations cryptographiques, le tout de manière très sécurisée.

Sécurité des logiciels

La sécurisation concerne aussi les logiciels utilisés, que ce soit les systèmes d'exploitation ou encore les applicatifs. Les premiers doivent pouvoir être mis à jour pour suivre la découverte inéluctable de failles. Le développement des seconds et de leurs mises à jour doit s'inspirer des bonnes pratiques en la matière, et leur traçabilité doit être assurée.

Détection d'intrusions
Aucun système n'étant infaillible, et certaines mesures de sécurité potentiellement trop coûteuses, il est recommandé de mettre en place des systèmes de supervision qui permettent de détecter et réagir à des attaques.

Sécurisation des SI
Les SI métiers utilisés pour les opérations doivent également être sécurisés. Cela passe notamment par une bonne gestion de l'authentification, la sécurité physique des serveurs, la mise en place de DMZ, etc.

SI sécurité
Toutes ces mesures nécessitent la mise en place de systèmes d'information capables de gérer les ressources dont elles ont besoin : génération et distribution des clés et des certificats, suivi de versions et déploiement de mises à jour, supervision des installations, etc.

La cybersécurité dans les projets de recherche accompagnés par l'ADEME

Plusieurs projets accompagnés par l'ADEME dans le domaine des Systèmes Électriques Intelligents ont permis d'appliquer ou de développer des solutions pour sécuriser la communication et les données, par exemple:

Le projet VAF-IA
Le porteur de projet a développé une solution spécifique et unique, l'API METRON-DR permettant de communiquer avec les agrégateurs. L'API est hébergée derrière un pare-feu avec un accès strictement contrôlé. Chaque demande de communication est doublement sécurisée, d'une part via une API à clé chiffrée et d'autre part via une authentification de l'utilisateur à l'aide d'un nom et d'un mot de passe. La communication entre l'API METRON-DR et la METRONLab (collecteur de données placé sur le site industriel) est gouvernée par un serveur OPC dont la connexion se fait à l'aide d'un réseau VPN SSL privé et l'accès via une authentification à l'aide d'un nom et d'un mot de passe.

Le projet BienVenu
Au sein du projet, un lien de communication a été mis en place entre un équipement du gestionnaire de réseau de distribution, placé dans un poste HTA/BT, et le superviseur de grappe de recharge d'un immeuble accueillant la solution BienVEnu et raccordé à ce poste HTA/BT. Cette expérimentation a permis de valider la faisabilité technique de faire communiquer ces équipements en CPL G3 FCC avec une qualité de service suffisante pour transmettre les consignes de puissance entre le gestionnaire de réseau de distribution et le superviseur de l'infrastructure. La sécurisation de ce lien est faite par l'isolation du sous-réseau et le chiffrement des communications au niveau de la couche 2 (en référence au modèle OSI). Des études ultérieures sont à prévoir sur les aspects de cybersécurité si ce lien vient à être exploité de manière industrielle.

Le projet SOGRID
Le système développé dans le projet s'intègre dans un outil industriel existant qui possède déjà ses propres processus et mécanismes de sécurité. Dans le cadre de SOGRID, l'enjeu était de proposer un système efficace et pratique s'intégrant dans l'écosystème existant. Ainsi, les mesures de cybersécurité proposées par Trialog et Enedis, et mises en œuvre dans le cadre du démonstrateur SOGRID, visent à protéger l'accès au médium de communication, et à sécuriser les flux. L'accès aux médiums de communication est protégé par la sécurisation physique (l'environnement où le lien est présent est à accès restreint, par exemple un poste source ou un poste HT A/BT), et par une sécurisation protocolaire : le CPL G3 offre un mécanisme d'authentification des participants du réseau et de protection des communications par chiffrement. Les flux sont quant à eux sécurisés en

point-à-point soit au niveau applicatif, par exemple via l'utilisation des mécanismes de sécurité offerts par DLMS/COSEM, soit au niveau réseau, par l'utilisation de tunnels IPSec.

Le projet Postes Intelligents
Concernant les aspects cybersécurité du projet, l'ensemble des moyens de communication et l'ensemble des signaux transmis (hors réseaux LORA) ont fait l'objet d'une analyse de risque et de propositions techniques selon la méthodologie EBIOS version 2010 préconisée par l'ANSSI. Ces documents ont été présentés à titre informatif à l'ANSSI et les solutions techniques proposées ont été déployées dans le cadre du démonstrateur. Les travaux concernent l'ensemble des réseaux et technologies de communication du poste : réseau fibre optique du poste, passerelle de télécommunication entre le gestionnaire de réseau de transport et le gestionnaire de réseau de distribution, échanges inter-postes ...
Un des axes de travail fort du projet a porté sur la redondance des équipements.

Le projet SMART SUN
La passerelle WebdynSUN PM est interfacée en continu avec un système d'information distant à travers un lien Ethernet ou 4G. Le concentrateur WebdynSUN PM accepte jusqu'à 2 serveurs, chaque serveur pouvant avoir son propre protocole de communication. Les protocoles supportés pour établir un lien avec le SI sont : ftp, ftps, http, https, mqtt, mqtts. Toutes les données échangées sont sécurisées (chiffrement). La passerelle WebdynSUN PM dispose, si nécessaire, d'un « secure element » (« coffre-fort ») pour conserver les clés de chiffrement.

Le projet ABIILE
Les flux de données sont sécurisés (https) et les accès à la plateforme contrôlés (login/mdp et détection d'intrusion). Enfin, les indicateurs et livrables produits sont mis à disposition des clients (des fournisseurs) via API sécurisés, sans information nominative, et via des accès contrôlés (liste blanche IP, chiffrement).

Le projet SEE PROJECT
L'utilisation d'une base de données Big Data conçue pour fonctionner de manière répartie sur plusieurs serveurs, permet d'opérer un service sécurisé (données redondées sur plusieurs serveurs et plusieurs centres d'hébergement), hautement disponibles et aptes à gérer de gros volumes d'informations (plusieurs dizaines de milliards de points de mesure soit plusieurs Teraoctets).

Le projet SOLENN
Dans le cadre du projet SOLENN, les données de consommation individuelles ont été transmises via un canal SI dédié entre Enedis et Niji, au travers de flux webservices REST sécurisés par un mécanisme SSL two-way. La sécurité lors du transit des données était également assurée par une authentification (0Auth2). Les jetons d'accès utilisés ont une durée de vie très limitée, ce qui participe à la bonne sécurité des données. Côté publication des données aux partenaires du consortium, les échanges se font via des flux spécifiques dédiés et sécurisés (tunnel VPN).
Le consentement d'un expérimentateur auprès d'Enedis, acquis lors d'un parcours de consentement sécurisé tentant de rester le plus simple possible pour le particulier, donnait lieu au partage d'un « Access Token » unique pour qu'il accède à ses données.