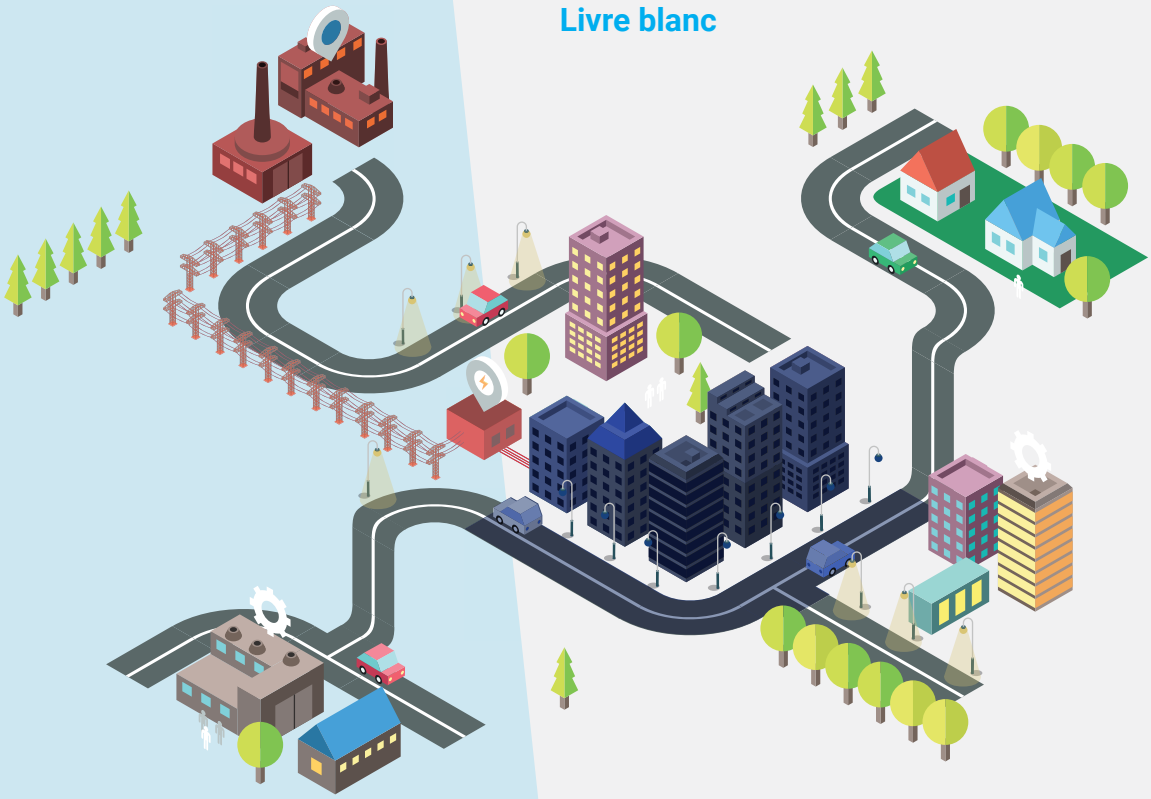
STORMSHIELD

De 2015 à demain : les cyber-intrusions dans les réseaux électriques

Livre blanc



Executive summary

Si vous vouliez nuire à un pays, quelles cibles attaqueriez-vous en priorité ? Une réponse vient immédiatement à l'esprit : ses réseaux de production d'énergie.

Et pour cause : aujourd'hui, rien ne fonctionne sans électricité. De nos industries aux sociétés du tertiaire, en passant par les villes (qu'elles soient déjà *smart* ou pas) pour aller jusqu'aux foyers. Des cyberattaques bien menées, au point de paralyser une centrale électrique voire de causer un *black-out*, peuvent ainsi avoir des impacts majeurs sur les populations et les États. Pouvoir porter atteinte aux réseaux électriques, c'est détenir un moyen de déstabilisation fort, politique et financier.

Les cyber-criminels l'ont bien compris et n'ont pas manqué, ces dernières décennies, de se concentrer sur les systèmes énergétiques. L'Observatoire de l'Industrie Électrique a ainsi relevé plus de vingt cyberattaques majeures concentrées sur ce secteur dans différents pays depuis 1982, avec une forte accélération depuis 2010. Et cette tendance se confirme depuis cinq ans – que ce soit au niveau des réseaux informatiques (IT) ou opérationnels (OT).

La numérisation et la connexion à Internet dont ont bénéficié les réseaux électriques ces dernières années ont largement contribué à leur exposition aux menaces cyber. Ces systèmes opérationnels, élaborés avec le souci constant d'assurer la sûreté de leur fonctionnement, n'ont cependant pas été conçus pour intégrer les risques en matière de cybersécurité – malgré des avancées réglementaires en ce sens avec le standard NERC-CIP et la directive européenne NIS. Avec le déploiement exceptionnel des technologies de l'information et de la communication (TIC), les réseaux électriques sont aujourd'hui intelligents. Capables de traiter un volume considérable de données, ils s'appuient également sur des outils de prévision et de modélisation, ainsi que sur des technologies de stockage. Résultat : ils affinent désormais leur gestion du flux d'électricité en temps réel, en fonction des informations transmises entre fournisseurs et consommateurs. Mais cette optimisation de la distribution d'énergie porte en elle une faiblesse : celle d'ouvrir involontairement aux cyber-criminels de nouvelles portes d'entrée au sein du système de gestion de l'énergie électrique.

Face à cette menace évolutive et contagieuse, de nombreux États se mobilisent à tous niveaux (nationaux comme internationaux). Certains pays n'hésitent pas à ériger la sécurité informatique au rang de priorité nationale, souvent en réaction directe à des attaques subies, ou suite à une prise de conscience des risques.

Parallèlement, les acteurs économiques privés se sont aussi organisés afin de se protéger efficacement contre la cyber-criminalité. Pour les aider, des sociétés comme Stormshield se sont spécialisées dans la sécurité des infrastructures critiques, des données sensibles et des environnements opérationnels en concevant des solutions de sécurité complètes.

Aussi, élaborer cet opus, consacré à l'évolution des cyberattaques des réseaux électriques depuis 2015, s'inscrit-il, pour Stormshield, dans le prolongement naturel de ce qui constitue son cœur de métier : analyser les actes de cybermalveillance, anticiper les risques à venir et proposer des solutions.

I.
2015-2020 : rétrospective des principales cyberattaques du monde électrique

1. Analyse rétrospective
2. De nouvelles pratiques dans les menaces

II.
Les réseaux électriques : une cible de choix

1. Des raisons sectorielles
2. Des raisons techniques

III.
La nature de la menace

1. Les acteurs du cyberespace
2. Les principaux objectifs visés par les cyber-menaces
3. Les modes opératoires
4. Les failles humaines

IV.
Les stratégies de protection

1. Le volet réglementaire
    - En France
    - En Europe
    - Aux USA
2. Les normes
3. La protection des infrastructures électriques en pratique

V.
Et demain ?

1. Vers des tensions géopolitiques qui s'accélèrent
2. L'Europe est-elle prête à faire face ?
3. Les entreprises sont-elles en ordre de marche ?

I. 2015-2020 : rétrospective des principales cyberattaques du monde électrique

Ces cinq dernières années, un certain nombre de cyberattaques ont marqué le monde de l'énergie électrique et ont, pour certaines, insufflé des prises de conscience et des changements en matière de cybersécurité. Focus sur leurs modes opératoires et impacts.





Cible : une partie du réseau électrique ukrainien (Ivano-Frankivsk, dans l'ouest du pays)

Date des faits : 23 décembre 2015.

Dégâts causés : mise hors service, pendant plusieurs heures, d'une centrale électrique, plongeant 80 000 personnes dans le noir; suivie de plusieurs semaines perturbées avant un retour à la normale.

Mode opératoire : les attaquants ont appâté leurs premières cibles avec une campagne de spearphishing. Celle-ci a permis d'introduire dans les réseaux de la centrale ukrainienne un cheval de Troie, nommé BlackEnergy, combiné à un module « KillDisk », capable d'effacer des données et de détruire des disques durs. Une fois les ordinateurs infectés et maîtrisés, l'attaque s'est étendue au système de contrôle et d'acquisition de données. En parallèle, les cyber-criminels ont lancé une attaque DDoS sur les centres d'appel d'urgence, rendus ainsi inaccessibles aux personnes touchées par le black-out.

Particularité de cette cyberattaque : il s'agit de la première cyberattaque à provoquer une panne électrique intégrale et de longue durée. D'après Tarik Zeroual, Global Account Manager au sein de Stormshield, « *d'autres attaques avaient auparavant ciblé des infrastructures du secteur de l'énergie, notamment des industries pétrolières, mais aucune n'a eu cet impact sur la population. Certains analystes la considèrent comme un cas d'école en matière de sabotage industriel* ».







Cible : le réseau électrique desservant la capitale de l'Ukraine (Kiev)

Date des faits : décembre 2016.

Dégâts causés : coupure partielle de courant dans Kiev pendant une heure.

Mode opératoire : pour obtenir ce résultat, les cyber-attaquants ont eu recours à un malware nommé Industroyer ou CrashOverride. En pratique, ils ont utilisé des backdoors pour accéder aux PC des administrateurs du réseau électrique. Ils ont ensuite installé des modules de prise de contrôle à distance et de scan du réseau, tout en effaçant les fichiers système des PC infectés. Objectif : supprimer les éventuelles traces de leur intrusion (data wiper).

Particularité de cette cyberattaque : Industroyer a été spécialement conçu pour s'attaquer aux réseaux électriques, notamment ukrainiens. Mais il a ensuite été constaté que le malware s'adaptait aux sites européens, asiatiques ou du Moyen-Orient. Plus inquiétant, des chercheurs en cybersécurité ont précisé qu'il était en mesure d'infecter d'autres cibles majeures. En effet, pour atteindre les différentes installations du réseau électrique, il a employé leurs protocoles de communication, vulnérables, et qui servaient également dans diverses infrastructures de réseaux hydrauliques ou du trafic routier. Par ailleurs, selon certains experts, le malware n'aurait pas été utilisé au maximum de ses capacités. Leur hypothèse ? Puisqu'avec Industroyer, les cyber-attaquants peuvent se déplacer via des protocoles de communications sans les connaître, ils étaient en mesure d'atteindre les disjoncteurs d'un ou plusieurs transformateurs et de provoquer ainsi un black-out. Mais ils ne l'ont pas fait. Cette opération peut-elle se réduire à une simple démonstration de force ? Dans tous les cas, elle n'a pas manqué d'être comparée à Stuxnet et représenterait la menace la plus puissante pour les systèmes de contrôle industriels depuis la fameuse cyberattaque de la centrale iranienne de Natanz.





Cible : Burlington Electric Department, un fournisseur d'électricité du Vermont (USA)

Date des faits : décembre 2016.

Dégâts causés : aucun. Malgré l'introduction d'un malware dans l'un des ordinateurs portables de la compagnie d'électricité de l'état du Vermont, non connecté au réseau opérationnel, l'attaque a été sans conséquence. Mais son objectif était probablement de servir de test de vulnérabilité pour une opération ultérieure.

Mode opératoire : les cyber-attaquants auraient opéré par phishing pour obtenir les mots de passe des employés du fournisseur du réseau électrique américain afin de pénétrer celui-ci.

Particularité de cette cyberattaque : les Américains n'ont pas pris cette menace à la légère, considérant que des cyber-criminels avaient tenté d'avoir accès à des fournisseurs pour pouvoir potentiellement manipuler le réseau électrique et le couper au beau milieu de l'hiver. Suite à cette attaque, le Department of Energy a renforcé la protection des réseaux électriques et gaziers. Ce qui a été suivi, le 11 mai 2017, par l'adoption d'un Executive order par le Président Trump afin de préserver les infrastructures vitales américaines contre les cyberattaques.

PASSWORD

Cible : le réseau électrique américain (ainsi que des compagnies pétrolières et gazières)

Date des faits : de 2019 à 2020.

Dégâts causés : vaste opération d'espionnage industriel.

Mode opératoire : en novembre 2019, Microsoft décèle des activités suspectes de ratissage de mots de passe, à grande échelle (password-spraying) à l'encontre de compagnies américaines d'électricité. Plus discrète qu'une tentative par force brute, cette technique consiste à deviner des mots de passe de faible niveau de sécurité, communs à un maximum de comptes.

Particularité de cette cyberattaque : elle s'inscrit, fin 2019 et début 2020, dans un contexte de tensions exacerbées entre les États-Unis et l'Iran. Même si, selon les experts, les techniques employées n'étaient pas suffisamment sophistiquées pour accéder aux infrastructures OT des réseaux électriques, elles l'étaient assez pour affecter leurs systèmes IT, tenter de trouver des failles, les paralyser ou ouvrir le champ à des attaques ultérieures destructrices.

MALWARE

Cible : une ferme éolienne française liée au réseau de distribution électrique géré par Enedis

Date des faits : janvier 2018.

Dégâts causés : tentative d'intrusion déjouée avant d'avoir causé des dommages.

Mode opératoire : sans plus de précision sur son introduction, un malware sophistiqué (une variante de BlackEnergy) a été découvert dans une ferme éolienne française.

Particularité de cette cyberattaque : les autorités françaises ont pleinement pris la mesure de cette opération qui s'est apparentée à un acte d'espionnage, voire de sabotage. L'hypothèse : les cyber-criminels avaient pour objectif de s'enfoncer plus profondément au sein du réseau de distribution électrique géré par Enedis afin d'y installer des implants dormants. Ces derniers auraient permis d'affecter de manière importante le fonctionnement du réseau électrique.

PHISHING RANSOM-WARE

Cible : le réseau interne d'Elexon, une société anglaise cruciale dans la chaîne d'approvisionnement en électricité britannique

Date des faits : mai 2020.

Dégâts causés : infection du réseau interne, blocage des boîtes mail professionnelles et des ordinateurs portables de l'entreprise.

Mode opératoire : Suite à une opération de phishing sur un employé en télétravail, les cyber-criminels ont eu recours à un logiciel pour chiffrer les données de l'entreprise. Il s'agirait d'un rançongiciel (connu sous le nom de Sodinokibi et REvil). En attendant de restaurer ses sauvegardes et de finir d'analyser son système, Elexon s'est trouvée paralysée. Des experts estiment que la cyberattaque a été favorisée par le VPN utilisé par l'entreprise, qui n'était plus à jour depuis plusieurs mois.

Particularité de cette cyberattaque : les cyber-criminels ont ciblé un acteur important de la chaîne d'approvisionnement en électricité, mais moins surveillé que la National Grid Agency.

De nouvelles pratiques dans les menaces

Au fur et à mesure des années, les cyber-menaces pesant sur les réseaux électriques se sont perfectionnés. Si le monde de l'énergie électrique peut parfois être la cible de pirates indépendants, il est le plus souvent exposé à des menaces précises et minutieusement préparées par des groupes de cyber-attaquants organisés. Ceux-ci montrent de plus en plus de patience et de sophistication dans le déploiement de leurs attaques et l'analyse de toutes les opportunités, mêmes indirectes. Et certaines opérations n'auraient sans doute pas vu le jour sans le soutien d'États, dont nous étudierons les motivations plus loin (cf. *II les réseaux électriques : une cible de choix*).

Les cyber-criminels ont conscience qu'en ciblant « simplement » les réseaux IT d'une compagnie d'électricité, ils peuvent occasionner des dommages importants : aux réseaux de distribution, bien sûr, mais également aux « outils business » d'une entreprise (comme dans le cas d'Elexon), afin de bloquer ses interfaces commerciales et paralyser ainsi son activité. Souvent moins bien protégés, les fournisseurs et prestataires de la cible réelle des cyber-criminels peuvent aussi servir involontairement de points d'entrée à une cyberattaque (à l'image de l'attaque sur Elexon, c'est notamment ainsi que les cyber-criminels du groupe Dragonfly seraient parvenus à pénétrer régulièrement le réseau d'énergie des États-Unis entre 2015 et 2018, voire avant).

Plus rarement, des attaques très ciblées parviennent à atteindre les systèmes de surveillance (SCADA) et de contrôle (ICS) des cibles. Dans le cas du malware Industroyer employé en Ukraine en 2016, les cyber-criminels l'ont pourvu de modules de communication capables de se connecter aux stations de pilotage du réseau électrique relevant des réseaux informatiques des opérateurs nationaux et régionaux. Une fois infiltré, le malware a pu directement communiquer avec les automates programmables (API) des réseaux électriques, lui permettant de s'emparer de données et de mener des actions de sabotage, comme couper la communication entre la station de pilotage et les sous-stations électriques et priver ainsi les opérateurs d'informations sur l'état du réseau.

II. Les réseaux électriques : une cible de choix

Les installations nucléaires et les réseaux de distribution d'électricité figurent au premier rang des infrastructures critiques et des environnements opérationnels sensibles d'un pays. Porter atteinte à leur intégrité, c'est affecter considérablement la sécurité économique et l'ordre public. Ce qui explique pourquoi les cyber-criminels redoublent d'activité afin d'exploiter les failles des réseaux électriques, davantage à leur portée qu'auparavant.

1. Des raisons sectorielles

Indispensable depuis la moitié du XXe siècle, l'électricité occupe un rôle central dans le fonctionnement de l'économie de nos pays. Dans un monde où la quasi-totalité des moyens de production et d'échanges reposent entièrement sur elle, les cyber-criminels ont bien compris qu'ils étaient en mesure de causer des dommages considérables s'ils parvenaient à entraver sa génération et sa distribution. Les réseaux électriques sont donc particulièrement à risque car ils constituent des leviers d'action très forts, exploitables à distance.

Selon l'Observatoire de l'Industrie Électrique, c'est en 2017 qu'un véritable changement s'opère. Les systèmes industriels, énergétiques, d'importance vitale et de transport deviennent la cible de cyberattaques initiées par des États ou des groupes terroristes. « *La cyberdéfense et la cyberattaque s'imposent progressivement comme de nouvelles armes stratégiques visant tout particulièrement le fonctionnement des États* », souligne l'Observatoire. Car cibler une infrastructure électrique peut causer des impacts économiques plus importants que de viser directement un État, mais c'est aussi un objectif plus facile à atteindre que des sites gouvernementaux majeurs mieux protégés. Les réseaux électriques présentent en effet des failles spécifiques que les cyber-criminels ne manquent pas d'exploiter (cf. *partie 2 Des raisons techniques*).

De plus, recourir à une cyberattaque permet de déstabiliser un pays en restant à couvert, avec un risque de conflit moins important qu'en optant pour la force armée, tant il est en difficile d'en déterminer l'auteur – et encore plus le commanditaire réel. Imputer officiellement une opération de cyberattaque à un autre état relève d'ailleurs de considérations diplomatiques sensibles, loin d'être anodines. En mars 2019, le président vénézuélien, Nicolás Maduro, accusait ainsi les États-Unis d'être responsables des coupures d'électricité et de communications du pays.

Mais tous les États ne se sont pas dotés de l'arsenal pour répliquer, ne disposant pas forcément des moyens techniques pour peser dans le cyberespace, désormais zone de conflits géopolitiques larvés. Comme souvent en cybersécurité, ce seront bien souvent les mêmes noms qui reviendront dans les hypothèses avancées.

Les conséquences d'une cyberattaque en pratique

S'attaquer aux réseaux des centrales électriques peut générer des dommages matériels majeurs (comme le dérèglement de centrifugeuses conduisant à leur destruction physique), entraver l'économie d'une région et perturber considérablement le quotidien des citoyens.

Dans un rapport de 2011, l'*Office of Technology Assessment* allemand a envisagé quelles seraient les conséquences d'une panne de courant de longue durée. Une fois les groupes électrogènes hors de fonction (suite à la pénurie de diesel) et les télécommunications réduites à l'essentiel (information des citoyens et fonctionnement de l'armée, des hôpitaux, de la police, et de l'administration), les services publics et les entreprises seraient paralysés. L'approvisionnement en eau et en nourriture (rupture de la chaîne du froid) deviendrait rapidement problématique ; les transports ne fonctionneraient plus, ainsi que les hôpitaux, occasionnant un chaos généralisé. Il faudrait plusieurs mois pour revenir à une situation normale.

1 000

Milliards de dollars

Le coût d'une panne électrique aux États-Unis

En 2015, l'assureur anglais Lloyd's a imaginé, avec le *Center for Risk Studies* de l'Université de Cambridge, les implications financières d'une cyberattaque majeure en utilisant le réseau électrique américain comme exemple. Ainsi, le coût d'une panne électrique plongeant 15 États américains (soit 93 millions de personnes) dans le noir s'élèverait à 243 milliards de dollars, voire 1 000 milliards dans la version extrême du scénario. Selon Tom Bolt, directeur de la gestion des performances chez Lloyd's, cette hypothèse « *montre l'énorme impact et les ravages qui pourraient résulter d'une cyberattaque majeure contre les États-Unis. La réalité est que le monde moderne, numérique et interconnecté crée les conditions de dommages importants, et nous savons que des acteurs hostiles ont les compétences et le désir de causer du tort* ».

2. Des raisons techniques

En parallèle de leur rôle vital dans le fonctionnement d'un pays, les infrastructures électriques sont également choisies par les cyber-criminels en raison de leurs vulnérabilités techniques. Et humaines.

L'interconnexion des réseaux : une porte d'entrée au réseau électrique

Les installations nucléaires précisément – et les réseaux OT de l'industrie énergétique en général – ont le plus souvent été conçus pour fonctionner sans connexion directe à Internet (parce qu'ils sont pour beaucoup antérieurs à son utilisation ou parce qu'ils n'en avaient tout simplement pas besoin alors). Toutefois, nous avons vu que les cyber-attaquants visent les systèmes d'information classiques dits « IT » des réseaux électriques, lesquels sont connectés et ouvrent donc la voie aux actes de cybermalveillance. D'une part, ils peuvent chercher à paralyser l'approvisionnement en électricité en infectant, par exemple, le système de gestion ou les commandes logistiques qui sont gérés via les systèmes IT.

D'autre part, les cyber-criminels peuvent, par le biais de ces mêmes systèmes IT, chercher à affecter les réseaux OT. « *Même si initialement les réseaux opérationnels n'étaient pas connectés avec les systèmes IT*, précise Tarik Zeroual, Global Account Manager chez Stormshield, *les deux types de systèmes sont devenus avec le temps de moins en moins cloisonnés* ». Notamment du fait de la numérisation de l'ensemble des processus et du traitement des flux de données. C'est le revers de l'efficacité et de l'immédiateté assurées par l'interconnexion des réseaux opérationnels électriques via les réseaux informatiques. La mutualisation des systèmes constitue d'importants points de vulnérabilité car, une fois introduit dans une partie d'un réseau, un virus peut se propager de manière redoutable dans le cas d'une segmentation défaillante.

On constate que les équipes métiers sont peu sensibilisées aux règles de cybersécurité de base.

Ainsi, l'une des grandes vulnérabilités des systèmes énergétiques réside dans le fait qu'ils ont été conçus à une époque où le risque cyber n'existait pas. De réseaux industriels cloisonnés et difficiles d'accès, ils sont passés en quelques décennies à des systèmes ouverts, pilotés par des technologies interconnectées.

L'Internet des objets : une augmentation des cyber-risques

Le déploiement assez révolutionnaire de l'Internet des objets (*Internet of Things* ou IoT), notamment dans l'environnement industriel (IIoT, *Industrial Internet of Things*) a élargi la surface d'attaque des cyber-criminels en augmentant le nombre de points d'entrée d'exploitation des vulnérabilités au sein des réseaux et en leur donnant accès à des cibles jusqu'alors hors d'atteinte.

En 2014, à l'occasion de la conférence *Black Hat Europe*, deux chercheurs espagnols ont ainsi démontré qu'ils pouvaient prendre le contrôle à distance de compteurs intelligents déployés en Espagne et en détourner les fonctionnalités ; par exemple, pour couper l'électricité chez un voisin ou récupérer les données des autres compteurs. Mais, le principal danger résulte selon l'Observatoire de l'Industrie Électrique de l'invalidation des sources « *qui rend les objets connectés inopérants ou coupe les accès du gestionnaire au pilotage des systèmes* ».

Les équipements anciens : une vulnérabilité dure à corriger

Les réseaux OT ont une durée de vie très longue, généralement plus de 25 ans. C'est le cas des infrastructures électriques, pensées pour fonctionner pendant plus de 50 ans. La plupart d'entre elles sont basées sur des technologies obsolètes et donc hautement vulnérables en matière de sécurité.

Pour ajouter encore à leur fragilité, les systèmes électriques ont souvent recours à des systèmes clés en main, qui n'ont pas été conçu pour recevoir des correctifs. Toute modification apportée à ce type de système nécessiterait du temps (et notamment l'arrêt de certains équipements, donc éventuellement de la production d'énergie) ainsi qu'un lourd investissement financier. Et

puisque les systèmes utilisés sont disponibles sur le marché depuis un certain temps, ils sont potentiellement étudiés par des cyber-criminels.

L'humain : un maillon dans un système faillible

La plus grande brèche dans les dispositifs de cyberdéfense des systèmes OT et IT se situe « *entre l'écran et le siège* » : elle est le fait de l'utilisateur. D'autant que, comme le précise Vincent Nicaise, Industrial Partnership and Ecosystem Manager au sein de Stormshield, « *globalement dans les société industrielles, on constate que les équipes métiers sont peu sensibilisées aux règles de cybersécurité de base, contrairement au personnel de l'IT qui, au fil des années, s'est formé et s'est vu imposer un certain nombre de règles de sécurité (recours à des mots de passe complexes à changer régulièrement, prudence dans l'ouverture des emails…). Dans l'OT, des opérateurs peuvent parfois utiliser les mêmes mots de passe ou utiliser des clés USB personnelles à des fins professionnelles* ».

Énergies renouvelables : plus exposées ?

Plus récents que les réseaux dédiés à l'exploitation des énergies fossiles, les équipements de production des énergies renouvelables pourraient sembler moins vulnérables car conçus avec la connectivité en tête. En effet, pour gérer le rendement intermittent de l'éolien et du solaire, ils ont été dotés de technologies numériques spécifiques afin de les piloter à distance et de réguler ainsi la production d'électricité à intégrer au réseau et à stocker.

Mais force est de constater que de nombreux constructeurs n'ont pas été sensibilisés aux risques de cyberattaque contre leurs équipements. Ce qui n'a pas échappé aux cyber-criminels du groupe Dragonfly, qui auraient réussi à introduire des malwares au sein de plusieurs entreprises d'énergies renouvelables aux États-Unis et en Europe en 2013. Parvenant à en exploiter les failles, ils ont pu atteindre les systèmes de contrôle industriels proprement dits. Si leur objectif était d'espionner leurs cibles, il a été prouvé qu'ils étaient en mesure de prendre le contrôle physique des infrastructures. En 2017, un chercheur en cybersécurité a démontré que les onduleurs fabriqués par la société allemande SMA, connectés à Internet et permettant de transformer le courant continu des panneaux photovoltaïques en courant alternatif, présentaient une vingtaine de vulnérabilités. Parmi ses hypothèses, il évoquait la possibilité de prendre le contrôle à distance de ces équipements et de stopper le flux d'électricité. Heureusement, les politiques de transition énergétique européennes intègrent de plus en plus les problématiques de cybersécurité. En 2016 par exemple, la Commission européenne a préconisé, dans ses « *Propositions législatives en vue d'une énergie propre pour tous les Européens* », d'identifier les cyber-risques potentiels pour chaque nouvelle technologie verte. Certains experts attirent l'attention sur l'importance de renforcer les impératifs de sécurité cyber à tous les niveaux des systèmes de production d'énergie, y compris domestiques.

III. Nature de la menace

Ces dernières décennies, les attaques subies par des installations énergétiques sont vraisemblablement toutes intervenues par voie externe et numérique. Les trois derniers sabotages réalisés en interne (par des employés le plus souvent) dateraient, en effet, de 1992 (centrale nucléaire d'Ignalina en Lituanie ; raffinerie dans le Richmond aux États-Unis) et 1999 (gazoducs appartenant à la compagnie Gazprom en Russie). Depuis, les actes malveillants sont initiés via des virus ou des vers électroniques introduits depuis l'extérieur.

1. Les acteurs du cyberespace

Au travers de notre rétrospective, nous avons vu se dessiner les traits et procédés d'individus qui agissent à couvert pour lancer des cyberattaques contre les infrastructures électriques. Le plus souvent, ces opérations (comme celles menées avec les malwares Stuxnet ou BlackEnergy) sont officieusement commanditées par des acteurs étatiques et bénéficient d'importantes ressources humaines et financières, étant donné les enjeux politiques que ces cibles énergétiques représentent. Plus rarement, ces cyberattaques peuvent être le fait de cyber-criminels isolés, aux moyens modestes.

Selon une analyse de l'univers cyber dans sa globalité par les analystes de Thales et Verint, quatre grandes catégories d'attaquants sévissent sur Internet et se distinguent selon leurs motivations et leurs objectifs. Ainsi, la soixantaine de grands groupes d'attaquants analysés se répartit de la manière suivante :

- **49 % des cyber-criminels seraient des groupes parrainés par des États** afin, le plus souvent, de voler des données sensibles à des cibles d'intérêt géopolitique et/ou des fournisseurs d'infrastructures essentielles. Ils sont à l'origine de la plupart des opérations qualifiées de « menaces persistantes avancées » (ou APT de l'anglais *Advanced Persistent Threat*). Ces cyberattaques minutieusement préparées et ciblées leur permettent d'infiltrer un réseau et de rester inaperçus pendant une longue période afin d'en surveiller l'activité.

- **26 % des cyber-criminels seraient des « hacktivistes »**, animés par des motivations idéologiques (communautaires, religieuses, politiques, etc.). Pour arriver à leurs fins, ils emploient majoritairement des attaques DDoS ou la défiguration de sites Internet (en dégradant ou en effaçant les informations et en les remplaçant par des contenus servant leur objectif de prosélytisme ou de désinformation).

- **20 % des cyber-attaquants seraient uniquement motivés par le gain financier.** Sans réel lien direct avec le secteur de l'énergie, ils aiment recourir aux ransomwares ou attaquer des places d'échange de cryptomonnaies ainsi que de monnaies virtuelles de jeux vidéo.

- **5 % des groupes analysés seraient des cyber-terroristes.** Ils cherchent à recruter de nouveaux membres ou à détruire des données (en utilisant des wipers par exemple), ou des

infrastructures (en effaçant des données ou en utilisant des outils d'intrusion souvent accessibles au public sur Internet).

Si les pourcentages sont amenés à changer légèrement s'ils étaient appliqués au seul secteur électrique, celui-ci est tout de même exposé à ces différents acteurs et ces différentes menaces – qu'elles soient étatiques, hacktivistes, terroristes voir même financières avec les attaques par ransomwares. La connaissance d'un tel panorama permet ainsi aux acteurs du secteur électrique d'être conscient des risques et ainsi de se préparer face à ces potentielles cyberattaques.

Un point sur le marché des malwares : du sur-mesure à la version modifiable

Les premières cyberattaques sophistiquées étaient conçues sur la base de programmes malveillants élaborés sur mesure. Le ver Stuxnet, découvert en 2010, a été spécialement créé pour dérégler le convertisseur de fréquence contrôlant la vitesse des moteurs des centrifugeuses de la centrale de Natanz : il a ainsi pu les ralentir et les accélérer de façon répétée afin de les détruire.

Mais l'analyse des attaques les plus récentes montre que la tendance actuelle ne serait plus d'élaborer leurs propres « *outils* », mais d'acheter des logiciels malveillants sur le Dark Web, réutilisés tels quels ou modifiés selon les besoins (Industroyer en est un bon exemple puisqu'il intègre une boîte à outil qui ne nécessite aucune connaissance des protocoles industriels utilisés dans l'infrastructure).

Ainsi, même les cyber-criminels de haute volée, soutenus par des États, ne créent pas forcément leurs propres malwares. Beaucoup d'entre eux recourent à des virus développés par d'autres cyber-criminels spécialisés et les intègrent dans leur stratégie de cyberattaque.

2. Les principaux objectifs visés par les cyber-menaces

Les cyber-criminels louent leurs services pour toutes sortes de cause, quand ils n'agissent pas pour leurs propres intérêts. Il existe ainsi trois types d'objectifs qui peuvent motiver une cyberattaque :

- **Le sabotage militaire ou terroriste fondé sur des raisons politiques** voire géopolitiques et qui va chercher à interrompre la disponibilité d'un service ou d'un système.
- **L'espionnage, le vol de données ou le chantage** basé sur des motivations financières ou économiques, avec pour but d'exfiltrer des informations ou de surveiller une activité.
- **Le test de méthodes ou l'action de notoriété** qui visent à altérer des informations ou des processus.

3. Les modes opératoires

Comme cela transparaît au travers des principales cyberattaques que nous avons présentées, les infrastructures électriques peuvent être mises en danger par des attaques ciblées (comme celle qui a sévi en Ukraine avec le malware Industroyer). Celles-ci sont conçues pour infiltrer un type spécifique d'équipement et ont donc recours à des

méthodes d'attaque adaptées, parfois inédites (révélant une vulnérabilité *Zero-day* c'est-à-dire une faille informatique sans correctif connu). Souvent planifiées en détail, ces cyber-opérations nécessitent des ressources supérieures à la moyenne et des compétences techniques élevées. Les groupes de cyber-criminels liés aux menaces persistantes avancées (APT) fonctionnent le plus souvent de cette manière.

Pour autant, les installations électriques font aussi l'objet d'attaques qui n'ont pas été spécialement « calibrées » pour le secteur énergétique, mais pour affecter les systèmes IT des organismes publics ou privés, par Internet ou par courriel. Elles peuvent ainsi toucher de manière indirecte des éléments des réseaux OT tels que les systèmes de contrôle industriel (*Industrial Control Systems* – ICS). C'est le cas de la cyberattaque mondiale lancée avec le malware NotPetya en juin 2017 : quand les cyber-criminels du groupe Lazarus sont parvenus à infecter des milliers d'ordinateurs dans le monde, dont des équipements de sociétés ukrainiennes, russes, américaines et françaises (notamment la SNCF, Auchan et Saint-Gobain). De manière collatérale, cette attaque a mis hors service les outils de mesure de la radioactivité d'une centrale nucléaire ukrainienne.

4. Les failles humaines

Cibler les employés d'une structure reste la porte d'entrée la plus facile à franchir. Les cyber-criminels comptent ainsi sur l'erreur, l'inattention ou l'intervention humaine pour injecter leurs malwares dans les réseaux, pourtant protégés par des mécanismes de défense qu'ils ne parviendraient souvent pas à déjouer sans cela. Certaines techniques employées ont d'ailleurs des appellations très imagées : hameçonnage (*phishing*) ou attaque par point d'eau (*water holing*) que nous détaillerons plus loin. L'objectif est de piéger un employé de la cible et de l'amener, à son insu, à commettre l'action qui ouvrira l'accès au réseau.

Support amovible vérolé (comme une clé USB), partage d'identifiants par e-mail, connexion au réseau de l'entreprise via un Wifi public : certains biais pour accéder au réseau ciblé ne sont pas particulièrement élaborés mais restent très efficaces. Selon les propos d'un employé travaillant dans une installation industrielle, la manière la plus simple pour y introduire un malware serait « *de disperser des clés USB infectées sur le parking de l'entreprise. Il suffirait ensuite d'attendre qu'un employé s'en serve sur le site* ». Dans d'autres cas, les cyber-criminels font preuve de beaucoup d'imagination. En 2015, un groupe de cyber-criminels a ainsi réussi à susciter l'intérêt de certains employés d'une centrale électrique grâce à un e-mail semblant provenir du parlement ukrainien, les invitant à ouvrir un document Microsoft Office infecté (avec leur malware BlackEnergy ; cf. la première cyberattaque de notre rétrospective). Quant au groupe Dragonfly, il est parvenu en 2017 à s'introduire dans les réseaux énergétiques anglais en imitant une plateforme web utilisée par les employés de la cible pour récupérer des codes d'accès.

Comme n'importe quelle entreprise qui possède un réseau OT, les entreprises du monde de l'énergie électrique sont sensibles à une série de techniques d'attaque cyber. Revue rapide.



PHISHING

Pourtant bien connues du public, les **campagnes d'hameçonnage (*phishing*)** restent assez employées par les cyber-criminels. Elles consistent à envoyer de manière massive des mails, généralement non personnalisés, afin d'obtenir une réponse du destinataire. Et lui soutirer des informations le concernant ou sur son entreprise, ou le faire cliquer sur les pièces jointes qu'ils comportent.



WATERING HOLE

Le site Web falsifié constitue lui-même un autre type de piège : **l'attaque par point d'eau (*watering hole*).** Comme le font les fauves, placés en embuscade à un point d'eau qu'ils savent fréquenté par leurs proies, les cyber-criminels orientent et/ou attendent leurs cibles sur un site Web qu'ils ont compromis. Par ce biais, ils obtiennent des informations essentielles (comme des identifiants et mots de passe) pour ensuite poursuivre leur cyberattaque sur l'entreprise ciblée, ou procèdent à un téléchargement sur l'ordinateur de l'utilisateur du site à son insu.



SPEAR PHISHING

L'harponnage (*spearphishing*), davantage sophistiqué, est beaucoup plus difficile à détecter car il contient des informations sur son destinataire (coordonnées, fonction, centres d'intérêt...). L'expéditeur peut se faire passer pour une personne de sa connaissance et presse souvent à agir dans l'urgence pour éviter une situation irrémédiable (fermeture d'un compte, pertes importantes...), laissant peu de temps pour réfléchir. Comme le phishing, le spearphishing peut contenir des pièces vérolées ou un lien vers un site Web falsifié.



DRIVE BY DOWNLOAD

Les **attaques par téléchargement furtif (*Drive by Download*)** sont, quant à elles, très utilisées pour propager des logiciels malveillants. En pratique, les cyber-criminels visent un site Web mal sécurisé et insèrent un script malveillant dans le code HTTP ou PHP de l'une de ses pages, pour installer un malware directement sur l'ordinateur du visiteur qui s'y rend. Celui-ci n'a pas besoin de cliquer sur un lien de téléchargement ou d'ouvrir une pièce jointe pour être infecté. C'est ainsi que l'attaque par le virus NotPetya a été lancée en 2017, via la mise à jour d'un logiciel de comptabilité.

IV. Stratégies de protection

Les enjeux liés aux infrastructures énergétiques sensibles ont fait prendre conscience aux pouvoirs publics qu'il était nécessaire d'organiser des cadres réglementant leur cybersécurité. Différentes normes ont également été élaborées afin de donner des lignes directrices en la matière. Tour d'horizon.

1. Le volet réglementaire

En France

C'est avec la **loi de programmation militaire (LPM) adoptée en 2013** que la France a posé les bases de sa politique en matière de cybersécurité. Cette loi a notamment imposé des mesures de protection et des obligations strictes aux opérateurs d'importance vitale (OIV), dont des infrastructures électriques. Elle les a incités ainsi à renforcer la sécurité des systèmes d'information critiques qu'ils exploitaient : les systèmes d'information d'importance vitale (SIIV). En août 2016, la France a pris des **arrêtés sectoriels pour ses OIV**, dont l'un porte sur les activités d'approvisionnement en énergie électrique. Elle fixe pour les OIV de ce secteur des règles de sécurité, à la fois organisationnelles et techniques, s'appliquant aux SIIV ainsi que des modalités d'identification de ces derniers et de notification des incidents de sécurité les affectant.

En Europe

C'est également en 2016 que la directive portant sur la sécurité des réseaux et des systèmes d'information, dite NIS (*Network and Information Security*) a été adoptée. Transposé en France en 2018, ce premier texte législatif européen sur la cybersécurité a posé un cadre pour le développement de normes européennes fondées sur des critères communs aux opérateurs de services essentiels (OSE).

Franchissant une nouvelle étape dans la politique de coopération européenne en matière de cybersécurité, le Parlement européen et le Conseil de l'Union européenne (UE) ont adopté en 2019 (respectivement en mars et en juin) le **règlement européen *Cybersecurity Act***, qui prévoit la création d'un ensemble de s**ystèmes de certification à l'échelle de l'UE** et d'une **agence de l'UE pour la cybersécurité**. Ce règlement a établi un cadre de certification de cybersécurité pour harmoniser à l'échelle européenne les méthodes d'évaluation et les différents niveaux d'assurance de la certification. Toujours en 2019, le Conseil a instauré un cadre permettant à l'UE d'imposer des **mesures restrictives ciblées visant à décourager et contrer** les cyberattaques qui menacent l'Union ou ses États membres « *y compris les cyberattaques dirigées contre des pays tiers ou des organisations internationales, lorsque des mesures restrictives sont jugées nécessaires pour réaliser les objectifs de la politique étrangère et de sécurité commune* ».

Aux USA

Dès 2005, les autorités américaines ont intégré dans leur *Energy Policy Act* des grands axes de développement en matière de cybersécurité s'appliquant au secteur de l'énergie, et particulièrement de l'électricité. C'est dans ce cadre qu'une organisation privée, la *North American Electric Reliability Corporation* (NERC), a été désignée en tant que *Electric Reliability*

Organization (ERO) afin d'établir les standards de sécurité pour le réseau électrique à l'échelle fédérale, placée sous la supervision de la *Federal Energy Regulatory Commision* (FERC).

Une série de normes ciblant les infrastructures de production et de transport de l'électricité ont ainsi vu le jour en 2008 : les NERC-CIPS (*Critical Infrastructure Protection Standards*). Parmi les plus détaillés au monde, ces standards sont obligatoires pour les 3 000 fournisseurs d'électricité (*utilities*) aux États-Unis.

2. Les normes

En parallèle des réglementations nationales et internationales, un certain nombre de normes régissent le secteur de l'électricité. Tour d'horizon des principales normes :

- **IEC 62443 :** norme internationale proposant un cadre de cyberdéfense des systèmes industriels. Auparavant, la sécurité des systèmes d'information était régie par la norme ISO 27000 et, parallèlement, la sécurité industrielle relevait de l'IEC 61508 et de normes sectorielles. La norme IEC 62443 sert désormais de liant à ces deux environnements.

- **IEC 62645 :** ensemble de mesures pour prévenir, détecter et réagir aux actes de malveillance commis par les cyberattaques sur les systèmes informatiques des centrales nucléaires. Elle s'aligne sur les changements d'ISO/IEC 27001 et tient compte des évolutions techniques et des différentes pratiques nationales en matière de cyber-protection.

- **IEC 62859 :** cadre pour gérer les interactions entre la sécurité et la cybersécurité pour les systèmes de centrales nucléaires. Elle adapte et complète les normes ISO/IEC 27001 et ISO/IEC 27002 au contexte nucléaire et est coordonnée avec la série de normes IEC 62443 sur la cybersécurité dans les processus d'automatisation et de contrôle industriels.

- **NERC-CIP :** normes nord-américaines s'appliquant à toutes les installations des USA et du Canada, produisant ou transportant de l'électricité à partir d'un seuil fixé à 1 500 MW. Elles couvrent l'ensemble des aspects de la sécurité, y compris le processus de déclaration d'un incident, et celui de continuité d'activité (PCA).

- **IEC 61850 :** norme de communication utilisée par les systèmes de protection des sous-stations dans le secteur de l'énergie électrique. Ce standard est spécifiquement employé dans les échanges entre les dispositifs électroniques intelligents (même provenant de différents fabricants) localisés au niveau des postes de distribution d'un réseau électrique.

3. La protection des infrastructures électriques en pratique

Diverses solutions peuvent être employées pour assurer la sécurité des équipements sensibles d'une infrastructure énergétique. Plusieurs d'entre elles gagnent à être intégrées au sein d'une stratégie de défense en profondeur, opposant aux cyber-attaquants des strates de protection indépendantes et de différentes

natures, qui prennent le relais en cas de défaillance de l'une d'elles.

Ainsi, un bon niveau de sécurité peut être atteint en respectant des principes de sécurité de base comme séparer les réseaux IT et OT, segmenter le réseau OT, recourir à des pare-feux, changer les éléments d'authentification par défaut des équipements des systèmes et imposer des mesures d'hygiène numérique aux collaborateurs (comme l'autorisation de connexion des seuls terminaux maîtrisés, ou l'interdiction de stocker physiquement ou numériquement les mots de passe en clair).

Les solutions Stormshield

Mais pour mettre en place ces systèmes de sécurité, les infrastructures électriques requièrent, du fait de leurs spécificités, des moyens de protection adaptés. Depuis des années maintenant, Stormshield développe, en ce sens, des solutions innovantes en co-production avec de grands noms du secteur tels que Schneider Electric et Siemens, mais aussi avec des pépites françaises comme Seclab.

Parmi l'éventail de ses produits, Stormshield a mis au point des solutions afin de sécuriser les messages opérationnels, avec notamment le contrôle des protocoles définis par le standard IEC 61850 pour les réseaux de distribution d'énergie. « *En analysant et en filtrant les données qui passent dans les instructions et les protocoles échangés au sein des systèmes, nos solutions permettent de réduire les risques de commandes illégitimes* », précise Tarik Zeroual, Global Account Manager chez Stormshield. De plus, le pare-feu industriel SNi20 répond aux contraintes environnementales électriques avec une certification IEC 61850.



SNi40

SNi20

Stormshield
Industrial Security

V. Et demain ?

Le monde de l'énergie électrique n'a pas fini d'être le terrain de jeu favori des cyber-criminels… Notamment parce qu'il sert aussi de territoire virtuel sur lequel certains états se livrent des luttes de pouvoir souvent ignorées du grand public.

1. Vers des tensions géopolitiques qui s'accélèrent

Dès qu'une cyberattaque est décelée contre une infrastructure électrique, qu'elle ait généré d'importants dommages ou pas, la question de l'attribution se pose immédiatement. Quel pays en est à l'origine ? Quelles étaient ses véritables intentions ? Comment rassurer les administrés, le cas échéant ? Quelle suite donner si l'attaque s'inscrit réellement dans un conflit préexistant avec une autre nation ?

Le cyberespace est devenu depuis plusieurs années une zone de tests et de démonstrations de force, avant d'être celui de conflits ouverts. Les exemples présentés dans ce livre blanc ne manquent pas entre la Russie qui ne serait ainsi pas étrangère aux deux black-out dont a souffert l'Ukraine en 2015 et 2016 et les réseaux d'énergie américains qui auraient régulièrement été infiltrés en 2017, également par les Russes, et qui seraient convoités par les cyber-criminels iraniens depuis 2019. Sans compter le fourmillement d'activités auxquelles se livrent les cyber-espions coréens et chinois et les puissances occidentales qui ne sont pas en reste non plus.

Face à cet environnement numérique mouvant et délétère, que d'aucuns qualifient de cyberguerre, comment les états doivent-ils réagir ? Selon Julien Nocetti, chercheur à l'Institut français des relations internationales, « *la tendance actuelle est au renforcement des capacités cyberdéfensives des États. Toutes les doctrines cyber élaborées par les Occidentaux ces dernières années insistent sur le renforcement capacitaire, humain et financier de la lutte informatique défensive et offensive* ».

2. L'Europe est-elle prête à faire face ?

Il y a quelques années, le constat n'était pas rassurant. Les réseaux électriques européens étaient déjà fortement connectés les uns aux autres mais, parallèlement, l'Europe souffrait d'un manque d'harmonisation des stratégies de cybersécurité de ses états membres. Certains pays (Grèce, Danemark, Suède…) n'avaient toujours pas élaboré de politique nationale de cyberdéfense ou de plan de protection de leurs infrastructures critiques (Portugal, Luxembourg…). Autant de brèches dans les réseaux électriques européens qui s'avéraient préoccupantes. Il était en effet imaginable qu'une attaque bien ciblée contre un système moins bien protégé puisse se propager au-delà des frontières du pays concerné, à l'image de l'incident (non cyber) entre l'Italie et la Suisse en 2003 qui s'était propagé jusqu'en Slovénie.

Les instances européennes ont toutefois pleinement saisi l'importance d'inciter les états membres à se mettre à niveau et l'année 2018, notamment, a été marquée par les transpositions

nationales de deux directives : NIS et SRI. Là où la directive NIS imposait l'identification des OSE, la directive SRI imposait quant à elle la mise en place d'une stratégie nationale de cybersécurité. Cette dernière a également astreint chacun d'eux à créer un centre d'appel national (CERT) et à organiser des procédures de notification, en cas d'incident, aux autorités nationales par les opérateurs critiques. En parallèle, la Commission européenne avait mis en œuvre, dès 2014, un programme de financement (*Connecting Europe Facility*) de 60 millions d'euros sur sept ans (2014-2020) pour aider les états les moins avancés à s'équiper et à se former. Un partenariat avec l'association de cybersécurité européenne (*European Cyber Security Organization*) a également vu le jour en 2016 afin de stimuler la recherche en cyberdéfense.

Tous ces efforts ont abouti à un résultat plutôt rassurant : en 2020, l'ensemble des pays de l'Union européenne dispose au minimum d'une politique nationale de cybersécurité, et la majorité a instauré un plan de protection des infrastructures critiques, si l'on en croit la *National Cyber Security Strategies - Interactive Map*, consultable sur le site de l'ENISA. Même si le risque zéro n'existe pas, cette harmonisation des réponses européennes aux cyber-menaces permet de réduire fortement l'exposition des systèmes électriques aux risques et d'améliorer leur résilience en cas d'incident.

Près de

80 %

des entreprises françaises ont reconnu avoir des difficultés à recruter des cyberspécialistes

3. Les entreprises sont-elles en ordre de marche ?

Faire face à la rapidité et à la complexité technique des cyberattaques demande de la réactivité. Les entreprises doivent donc pouvoir compter sur des effectifs formés et entraînés. C'est l'un des principaux enjeux de demain. Près de 80 % des entreprises françaises ont reconnu avoir des difficultés à recruter des cyberspécialistes, selon une étude réalisée par le cabinet Vanson Bourne. La formation des équipes et la détection des talents doivent donc dès à présent faire partie de leurs priorités.

La prise de conscience de l'existence des cyber-risques par l'ensemble des acteurs du monde électrique constitue également un enjeu de taille, qui peut paraître paradoxal. En effet, comment concevoir que des spécialistes du secteur électrique ne soient pas sensibilisés à ces questions et organisés en conséquence ? Pourtant, nous trouvons encore, par exemple, des équipements connectés vendus sans aucun niveau de sécurité. Les prestataires, et de manière plus large toute la chaîne d'approvisionnement des compagnies électriques, représentent eux aussi des vecteurs potentiels de risques. Et d'une manière plus indirecte, tout autre acteur économique également, participant à son niveau à l'ultra-connexion des systèmes IT. Pour répondre au mieux à cette menace, les entreprises du secteur semblent opérer un renforcement du management de la cybersécurité à travers des

budgets consacrés, des travaux sur les dispositifs de crise ou encore sur la sensibilisation et formation des équipes.

Enfin, et heureusement, si les cyber-criminels n'hésitent pas à communiquer entre eux, voire à échanger des procédés, les sociétés du privé ne restent pas inactives et isolées. Beaucoup ont compris qu'il est important de savoir quelles menaces pèsent sur elles et comment celles-ci surviennent. Les entreprises osent d'ailleurs de plus en plus communiquer sur les attaques qu'elles ont subies afin d'aider les organisations des secteurs privé et public à mieux détecter et anticiper les risques à venir. C'est grâce à cette démarche de coopération et de partage de connaissances sur les cyber-menaces, à mener sans relâche, que les futures attaques pourront être plus facilement absorbées.



Références bibliographiques

Observatoire de l'Industrie Électrique, *La cyber résilience des système électriques*, novembre 2017, https://observatoire-electricite.fr/IMG/pdf/oie_-_note_conjoncture_-_cyber_resilience_des_systemes_electriques_-_novembre_2017.pdf

Long form de Numerama, *Ukraine, anatomie d'une cyberguerre — épisode 1 : la menace au quotidien*, 5 septembre 2017, https://www.numerama.com/politique/283573-en-ukraine-la-cyberguerre-au-quotidien-episode-1-la-menace-permanente.html

Article de Futura Sciences, *Le malware Crash Override-Industroyer est-il plus redoutable que Stuxnet ?*, 13 mai 2017, https://www.futura-sciences.com/tech/actualites/informatique-malware-crash-override-industroyer-il-plus-redoutable-stuxnet-25307

Retombée presse du Point international, *États-Unis : un fournisseur d'électricité piraté par des Russes, 31 décembre 2016*, https://www.lepoint.fr/monde/etats-unis-un-fournisseur-d-electricite-pirate-par-des-russes-31-12-2016-2093899_24.php

Article de L'Usine Digitale, *Elexon, maillon crucial du réseau électrique au Royaume-Uni, victime d'une cyberattaque*, 15 mai 2020, https://www.usine-digitale.fr/article/elexon-maillon-crucial-du-reseau-electrique-au-royaume-uni-victime-d-une-cyberattaque.N964926

Article de L'energeek, *Le coordinateur européen des transporteurs d'électricité victime d'une cyber-attaque*, 11 mars 2020, https://lenergeek.com/2020/03/11/coordinateur-europeen-transport-electricite-cyber-attaque/rique-au-royaume-uni-victime-d-une-cyberattaque.N964926

Chronique de Libération, *L'attribution des cyberattaques, un bras de fer diplomatique*, 5 octobre 2018, https://www.liberation.fr/planete/2018/10/05/l-attribution-des-cyberattaques-un-bras-de-fer-diplomatique_1683201

Chronique de Libération, *Les cyberattaques sont des fantômes*, 17 mars 2019, https://www.liberation.fr/planete/2019/03/17/les-cyberattaques-sont-des-fantomes_1715230

Rapport de l'*Office of Technology Assessment, What happens during a blackout: Consequences of a prolonged and wide-ranging power outage*, 2011, https://www.tab-beim-bundestag.de/en/pdf/publications/books/petermann-etal-2011-141.pdf

Rapport de Lloyd's et du *Center for Risk Studies de l'Université de Cambridge, Business Blackout*, 6 juillet 2015, https://www.lloyds.com/news-and-risk-insight/risk-reports/library/society-and-security/business-blackout

Article de 01.net, *Compteur électrique intelligent : quand le hacking mène au black-out général*, 17 octobre 2014, https://www.01net.com/actualites/compteur-electrique-intelligent-quand-le-hacking-mene-au-black-out-general-628914.html

Publication de l'Institut français des relations internationales, *Cyberattaques et systèmes énergétiques : faire face aux risques*, 2017, https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cybersecurite_2017_2.pdf

Publication de l'Institut français des relations internationales, *Cybersécurité des infrastructures énergétiques : regards croisés Europe/États-Unis*, 2018, https://www.ifri.org/fr/publications/etudes-de-lifri/cybersecurite-infrastructures-energetiques-regards-croises-europeetats

Tribune de Nicolas Mazzuchi sur L'energeek, *Cybersécurité et énergie : une complémentarité fondamentale*, 21 octobre 2019, https://lenergeek.com/2019/10/21/cybersecurite-energie-renouvelables-attaques-nicolas-mazzuchi/

Rapport de Thales & Verint, *Cyber Threat Handbook Thales – Verint*, 10 juillet 2019, https://www.thalesgroup.com/en/group/journalist/press-release/cyberthreat-handbook-thales-and-verint-release-their-whos-who

Rapport de Thales - General Electric, *Report on Cyber Threats to Operational Technologies in the Energy Sector*, 2020

Décret n° 2006-212 du 23 février 2006, et loi française n° 2013-1168 du 18 décembre 2013, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028338825/2020-0928/

Communiqué de presse du Conseil de l'UE, *Cyberattaques : le Conseil est désormais en mesure d'imposer des sanctions, 17 mai 2019*, https://www.consilium.europa.eu/fr/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

Article d'Usbek & Rica, *Nous sommes dans une situation de cyberguerre froide*, 30 avril 2019, https://usbeketrica.com/fr/article/nous-sommes-dans-une-situation-de-cyberguerre-froide

Page web de la Commission de régulation de l'énergie, *Électricité : Interconnexions*, 17 décembre 2019, https://www.cre.fr/Electricite/Reseaux-d-electricite/interconnexions

Carte interactive de l'ENISA, *National Cyber Security Strategies - Interactive Map*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

STORMSHIELD

Le choix européen de la cybersécurité



Partout dans le monde, les entreprises, les institutions gouvernementales et les organismes de défense ont besoin de s'appuyer sur des partenaires de confiance pour accompagner leur transformation numérique et assurer la cybersécurité de leurs infrastructures, de leurs utilisateurs et de leurs données. Les technologies Stormshield, certifiées au plus haut niveau européen (EU Restreint, OTAN Restreint, Critères Communs EAL3+/EAL4+, qualifications et visas ANSSI), répondent aux enjeux de l'IT et de l'OT afin de protéger vos activités. **Nos solutions de sécurité vous redonnent la liberté d'entreprendre en toute sérénité.**

www.stormshield.com

Toute diffusion, reproduction ou représentation, même partielle de ce livre blanc, à d'autres fins qu'une utilisation privée sur un quelconque support, est interdite et pourrait engager la responsabilité civile et pénale de la personne qui ne respecterait pas cette interdiction.