Centrale-Énergies

Flash 65

Juin 2019

SOMMAIRE

NOS PROCHAINES CONFERENCES

Octobre
Autoconsommation : où en est-on, où va-t-on ?

Novembre
Cybersécurité des réseaux électriques

Décembre
Comment parler énergie et climat avec un économiste ?

Inscriptions sur notre site internet
http://www.centrale-energie.fr/spip/

DE L'EXPOSITION DES RESEAUX ELECTRIQUES SUR INTERNET

Maxime Alay-Eddine

Maxime Alay-Eddine a fait ses premiers pas dans la sécurité informatique en 2002.
Diplômé de l'Ecole Centrale de Nantes en 2013, il a co-créé Cyberwatch en 2015, logiciel spécialisée dans la gestion des vulnérabilités et conformités utilisé par de nombreuses administrations et grandes entreprises françaises.
Pour le contacter : maxime@cyberwatch.fr / https://www.cyberwatch.fr

La modernisation des réseaux électriques passe par l'intégration de ces derniers dans des systèmes de plus en plus connectés. Ces connexions servent notamment à faciliter l'administration et la maintenance des différents composants, tels que les automates industriels, et passent par l'exposition de services sur des réseaux comme Internet.

Cette exposition n'est pas sans danger : en cas d'erreur de configuration ou de procédure, ces services particulièrement sensibles deviennent accessibles pour tout internaute.

Pire encore : il est possible de parcourir l'ensemble des machines connectées à Internet dans un pays ciblé, afin d'identifier des systèmes industriels potentiellement intéressants à attaquer.

Cet article présente deux approches (une outillée, et une à l'aide d'un moteur de recherche) permettant d'effectuer de telles recherches, ainsi que des cas concrets d'attaques informatiques menées sur des systèmes industriels énergétiques.

2018 était une année majeure pour la sécurité des systèmes d'information : outre Atlantique, un nouveau record a été atteint grâce à la publication de 16 516 vulnérabilités dans la National Vulnerability Database (NVD) (1), sorte d'encyclopédie des failles affectant les principaux logiciels du marché. En France, l'année a été marquée par l'entrée en vigueur du Règlement général sur la protection des données (2) (RGPD) le 25 mai dernier, et la transposition de la directive Network and Information Security (3) (NIS).
Cette directive, bien que moins connue du grand public, vient compléter une vision française de la cybersécurité, où les actions de protection découlent essentiellement de dispositions réglementaires.
Aujourd'hui, la législation définit deux types d'entités particulièrement importants : les Opérateurs d'importance vitale (OIV) et les Opérateurs de service essentiel (OSE), qui exercent des activités dont le dommage, l'indisponibilité, ou la destruction limiterait gravement le fonctionnement de l'économie ou de la société.
Parmi ces opérateurs figurent évidemment les fournisseurs d'énergie. Mais pourquoi un équipement producteur d'énergie serait-il connecté à Internet ? Est-il facile d'identifier de tels dispositifs en France ? Quel est le risque de l'exposition d'un tel système à Internet ? Et quelle serait la conséquence d'une attaque informatique réussie sur un réseau électrique ? C'est à ces questions que nous nous proposons de répondre.

Dans son guide « Maîtriser la Sécurité des Systèmes d'Information (SSI) pour les systèmes industriels », l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) distingue deux familles de systèmes d'information : les systèmes dits « de gestion », dont l'objectif est de traiter des données dans un environnement essentiellement dématérialisé, et les systèmes « industriels », dont l'objectif est de piloter des installations, de réguler des procéder, d'acquérir et de traiter des données dans le monde physique.
Ces familles de systèmes d'information sont manipulées par des opérateurs aux cultures très différentes. D'un côté, nous avons des informaticiens qui déploient des systèmes dans des environnements contrôlés (salle serveur, fournisseur de Cloud Computing…), et qui peuvent régulièrement mettre à jour les différents composants (la durée de vie moyenne d'un système « de gestion » est de 5 ans). De l'autre, nous avons des automaticiens, des électrotechniciens, dont les systèmes sont soumis à des contraintes physiques fortes (vibrations, averses, température…), et dont chaque brique déployée est faite pour durer (la durée de vie d'un système « industriel » dépasse souvent 10 ans, voire 30 à 40 ans).
Or, à des fins d'optimisation et de rationalisation (récupération de données, mutualisation d'infrastructure réseau, télémaintenance), les systèmes « de gestion » et les systèmes « industriels » ont besoin de communiquer. Ces écosystèmes très différents se retrouvent ainsi mis en réseau, grâce à des protocoles comme Supervisory Control And Data Acquisition (SCADA), Programmable Logic Controller (PLC), ou Safety Instrumented System (SIS). Et parfois, ces interconnexions entraînent une exposition sur Internet.

Dès lors, toute personne disposant d'un ordinateur et d'une connexion Internet peut partir à la recherche de systèmes « industriels » potentiellement accessibles. En effet, toute machine destinée à fournir un service via Internet expose un ou plusieurs « ports ». Ces ports, qui reposent sur les protocoles Transmission Control Protocol (TCP) ou User Datagram Protocol (UDP), agissent comme des points d'entrée permettant d'atteindre un service bien spécifique sur une machine donnée. Pour illustrer cela, on peut représenter un ordinateur comme un immeuble dans lequel il y aurait 65 536 appartements (un appartement = un port). Une requête réseau devient alors une lettre envoyée par La Poste, où le facteur remet la lettre au destinataire approprié en frappant tout simplement à la porte de l'appartement ciblé.
Or, beaucoup de ports sont associés à des technologies précises : par exemple, le port 80 en TCP est généralement associé à une requête HTTP (web sans chiffrement), tandis que le port 443 en TCP est quant à lui associé à une requête HTTPS (web chiffré). Ces associations entre ports et technologies sont réalisées par l'Internet Assigned Numbers Authority (IANA), et disponibles publiquement (4). On y découvre par exemple que le port 502 en TCP est destiné au protocole « Modbus over TCP », utilisé pour piloter de nombreux systèmes « industriels » et déployé par des constructeurs spécialistes de l'énergie comme Engie (5). Pour reprendre

l'exemple de l'immeuble aux 65 536 appartements, cela signifie qu'une personne peut dans ces conditions parcourir tous les immeubles de France, en frappant chaque fois aux portes des appartements n°502. Si une telle porte s'ouvre, il est fort probable que l'appartement visité héberge un système « industriel » piloté avec du « Modbus over TCP ».

A des fins de recherche, les membres de la communauté de la sécurité informatique ont même publié une liste des principaux ports utilisés par des systèmes « industriels » (6). Avec cette liste, et à l'aide de logiciels libres comme Masscan (7), il est possible de scanner toute machine exposée sur Internet à la recherche de ports caractéristiques d'un ordinateur destiné à contrôler des systèmes « industriels ». On parle alors d'Industrial Control System (ICS).

Une telle opération est « rapide » : un scan Masscan lancé sur le port TCP 502 sur toutes les adresses IP françaises prend 30 minutes, et identifie plus de 21 000 machines.

Mieux encore, le chercheur en sécurité informatique John Matherly a créé un moteur de recherche spécialisé dans les scans massifs sur Internet : Shodan (8). Depuis quelques années, ce moteur de recherche dispose d'une page dédiée aux ICS (9).

Ce site met à disposition des fichiers recensant toutes les machines qui constituent a priori des ICS, en détectant les protocoles les plus classiques des systèmes « industriels » tels que Bacnet (port 47808), DNP3 (port 20000), Ethernet/IP (port 44818), Niagara Fox (ports 1911 et 4911), IEC-104 (port 2404), Red Lion (port 789), Modbus (port 502), et Siemens S7 (port 102) …

Les fichiers fournis par Shodan, dont figure un exemple ci-dessous, contiennent alors des données détaillées au format JavaScript Object Notation (JSON) et indiquent par exemple le fournisseur de connexion internet (ISP), les éléments d'identification du système industriel (data), le port exposé, les noms de domaine identifiés (hostnames), mais aussi des informations géographiques (location).


{"timestamp": "2014-02-06T11:02:25.594942", "isp": "Orange", "data": "Unit ID: 0\n-- Slave ID Data: ILLEGAL FUNCTION\n-- D
evice Identification: Schneider Electric BMX NOE 0100 V2.30 \n\nUnit ID: 255\n-- Slave ID Data: ILLEGAL FUNCTION\n-- Devic
e Identification: Schneider Electric BMX NOE 0100 V2.30 \n\n", "port": 502, "hostnames": [], "location": {"city": "Paris",
 "region_name": null, "area_code": null, "longitude": 2.3333000000000084, "country_code3": "FRA", "latitude": 48.866700000
00001, "postal_code": null, "dma_code": null, "country_code": "FR", "country_name": "France"}, "ip": 1515473503, "domains"
: [], "org": "Orange France Wireless", "os": null, "asn": "AS28708", "ip_str": "90.84.74.95"}
{"timestamp": "2014-02-06T10:26:45.041753", "isp": "Orange", "data": "Unit ID: 0\n-- Slave ID Data: ILLEGAL FUNCTION\n-- D
evice Identification: Schneider Electric SAS TSX P57 5634M V2.9 \n\nUnit ID: 255\n-- Slave ID Data: ILLEGAL FUNCTION\n-- D
evice Identification: Schneider Electric SAS TSX P57 5634M V2.9 \n\n", "port": 502, "hostnames": [], "location": {"city":
"Paris", "region_name": null, "area_code": null, "longitude": 2.3333000000000084, "country_code3": "FRA", "latitude": 48.8
667000000000001, "postal_code": null, "dma_code": null, "country_code": "FR", "country_name": "France"}, "ip": 1515507513, "
domains": [], "org": "Orange France Wireless", "os": null, "asn": "AS28708", "ip_str": "90.84.207.57"}
{"timestamp": "2014-02-06T09:48:37.523584", "isp": "Orange", "data": "Unit ID: 0\n-- Slave ID Data: ILLEGAL FUNCTION\n-- D
evice Identification: Schneider Electric BMX P34 2020 v2.5 \n\nUnit ID: 255\n-- Slave ID Data: ILLEGAL FUNCTION\n-- Devi
ce Identification: Schneider Electric BMX P34 2020 v2.5 \n\n", "port": 502, "hostnames": ["MMarseille-651-1-233-206.w86-
210.abo.wanadoo.fr"], "location": {"city": "Gap", "region_name": null, "area_code": null, "longitude": 6.08189999999992,
"country_code3": "FRA", "latitude": 44.561499999999995, "postal_code": null, "dma_code": null, "country_code": "FR", "coun
try_name": "France"}, "ip": 1456662734, "domains": ["wanadoo.fr"], "org": "Orange", "os": null, "asn": "AS3215", "ip_str":
 "86.210.232.206"}
{"timestamp": "2014-02-06T08:43:15.211792", "isp": "Orange", "data": "Unit ID: 0\n-- Slave ID Data: ILLEGAL FUNCTION\n-- D
evice Identification: Schneider Electric BMX NOE 0100 V2.60 \n\nUnit ID: 255\n-- Slave ID Data: ILLEGAL FUNCTION\n-- Devic
e Identification: Schneider Electric BMX NOE 0100 V2.60 \n\n", "port": 502, "hostnames": ["LMontsouris-656-01-95-203.w193-
251.abo.wanadoo.fr"], "location": {"city": "Paris", "region_name": null, "area_code": null, "longitude": 2.333300000000008
4, "country_code3": "FRA", "latitude": 48.866700000000001, "postal_code": null, "dma_code": null, "country_code": "FR", "co
untry_name": "France"}, "ip": 3254468043, "domains": ["wanadoo.fr"], "org": "Orange", "os": null, "asn": "AS3215", "ip_str
": "193.251.61.203"}

Figure 1 Récupération des services ModBus liés à des machines Schneider Electric BMX via Shodan

A partir des résultats obtenus, il est donc même possible de construire une carte des systèmes « industriels » identifiés dans le monde, comme ci-dessous :

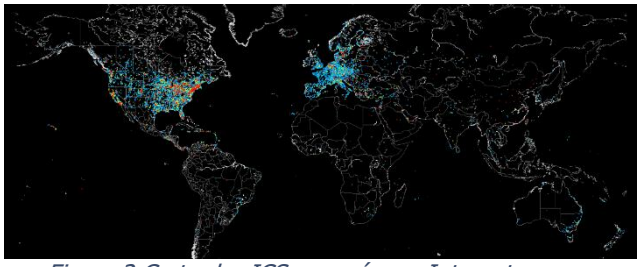

Figure 2 Carte des ICS exposés sur Internet, source https://icsmap.shodan.io/

Un internaute intéressé par la sécurité des ICS peut donc soit faire un scan par ses propres moyens avec Masscan, ou ré-exploiter le travail de la communauté avec Shodan, le tout à un coût extrêmement faible.

Mais un système « industriel » qui expose son interface de contrôle sur Internet est-il nécessairement vulnérable ? Fort heureusement non, car les protocoles exposés sont complexes et encore trop peu maîtrisés par les attaquants les plus fréquents, à savoir les « script-kiddies », qui se contentent d'utiliser des scripts disponibles sur Internet pour lancer une offensive sur une grande quantité de systèmes. Cependant, comme nous l'avons vu précédemment, l'interconnexion des systèmes « de gestion » avec les systèmes « industriels » entraîne un mélange des cultures entre informaticiens et automaticiens. Ce mélange génère des risques potentiels bien plus simples à attaquer.

En effet, les attaques les plus simples et fréquentes sur un système d'information portent sur l'utilisation de failles publiques appelées vulnérabilités « connues » (10). Ces vulnérabilités, référencées dans la National Vulnerability Database, disposent bien souvent

d'exploits (11), c'est-à-dire de kits d'attaque qu'il suffit de télécharger et d'exécuter pour porter atteinte au système ciblé. Pour parer à ces vulnérabilités, il faut simplement installer les mises à jour de sécurité fournies par les éditeurs comme Microsoft, Adobe, Oracle…

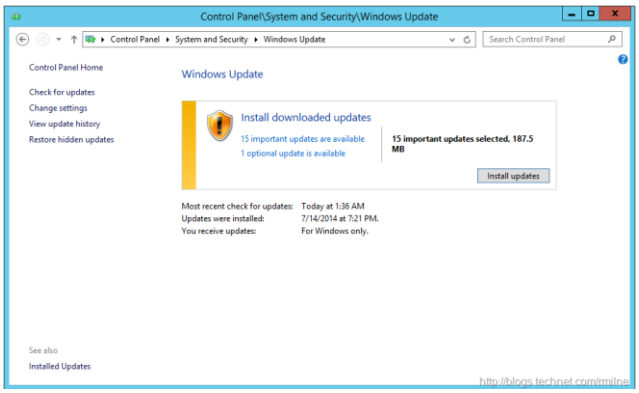

Figure 3 Ecran de Windows Update, qui permet de mettre à jour Microsoft Windows, et qui résout bien des problèmes…

Pourtant, ces mises à jour de sécurité sont rarement installées dans des délais raisonnables sur des systèmes « de gestion ». Si l'on prend le cas de la vulnérabilité CVE-2017-0143 (WannaCry), les correctifs étaient disponibles depuis Mars 2017, et pourtant le monde entier a été attaqué avec succès deux mois plus tard en Mai 2017. Pire encore, en avril 2019, il est fréquent de trouver cette vulnérabilité au cours d'un test d'intrusion, sorte de simulation d'attaque informatique menée à des fins préventives. Les systèmes « de gestion » sont donc fortement concernés par ces fameuses « vulnérabilités connues », avec pour cause la difficulté pour le management à établir un process de gestion des vulnérabilités.
Côté systèmes « industriels », deux problèmes s'ajoutent aux difficultés de management : une contrainte de disponibilité 24h/24 et 7j/7, et un besoin de qualification de chaque modification d'un composant logiciel avant mise en production. Ainsi, toute mise à jour de sécurité doit d'abord être testée sur un environnement dédié, et toute opération nécessitant le redémarrage d'un système doit être planifiée plusieurs mois à l'avance. Ces contraintes sont suffisamment fortes pour que l'on continue, en 2019, à trouver des systèmes totalement obsolètes comme Microsoft Windows Server 2003, qui ne reçoit plus aucune mise à jour de sécurité depuis 2015.
Face à ces difficultés pour mettre à jour un système « industriel » et neutraliser les vulnérabilités connues, la sécurité d'un système d'information de ce type dépend avant tout de la capacité à en empêcher l'accès réseau, et repose donc sur la capacité à protéger les ICS des systèmes « de gestion » qui les entourent. L'approche la plus pragmatique consiste donc à déployer une défense en profondeur, de sorte à transformer le système d'information en forteresse de Vauban.

Si cette stratégie de défense en profondeur limite le risque d'une attaque automatique causée par un « script-kiddie », qui représente le sinistre de fréquence classique dans la sécurité informatique, les Responsables de la Sécurité des Systèmes d'Information (RSSI) en charge d'un système « industriel » ne doivent pas pour autant écarter les sinistres d'intensité, représentés par des attaques ciblées et longuement préparées par des groupes activistes, terroristes ou des institutions. Mais quelles seraient les conséquences d'une telle attaque ?

En 2007, le Laboratoire National de l'Idaho et le Département de la Sécurité intérieure des Etats-Unis ont réalisé une simulation d'attaque informatique sur les composants d'un réseau électrique. Cette opération, nommée « Aurora generator test », consistait à ouvrir et fermer les disjoncteurs d'un générateur diesel de sorte à créer un déphasage entre le générateur et le réseau électrique alimenté. A chaque fermeture des disjoncteurs, le couple généré par le déphasage entraînait une secousse assez puissante pour détruire des éléments du générateur, pour finir par déclencher son explosion en moins de 3 minutes.

3 années après ce test, les médias dévoilaient Stuxnet, ver informatique destiné à détruire un système « industriel » Siemens utilisé dans le programme nucléaire iranien (12), et ce sans même que celui-ci ne soit exposé à Internet. En l'absence d'une connexion directe au réseau ciblé, l'attaque fut lancée via des clés USB piégées, malencontreusement branchées par des employés peu méfiants sur des ordinateurs reliés aux ICS. Les mesures de protection informatique restent ainsi extrêmement sensibles aux défaillances humaines.

De la même manière, en décembre 2015, plus de 200 000 personnes se sont retrouvées sans électricité à cause d'une cyber-attaque ciblant

l'Ukraine. Les pirates ont réussi à pénétrer dans le réseau des systèmes « industriels » responsables de l'approvisionnement électrique de plusieurs régions via une campagne ciblée d'hameçonnage (spear-phishing), afin de piéger le personnel de l'équipe informatique et d'en dérober les identifiants VPN (13) (14).
Ces éléments démontrent la réalité du risque « cyber » portant sur les réseaux « industriels » et notamment les fournisseurs d'énergie.

Figure 4 Aurora Generator Test, vidéo disponible sur https://www.youtube.com/watch?v=LM8kLaJ2NDU

En conclusion, si le risque d'attaque « cyber » portant sur une infrastructure énergétique est bien crédible, nous devons aussi prendre en compte que ce type de menace risque statistiquement surtout de nuire aux systèmes d'information « de gestion » : autrement dit, un système « industriel » affecté par une cyberattaque peut ainsi simplement constituer le dommage collatéral d'une attaque automatisée balayant tout l'Internet à la recherche de systèmes « de gestion » mal entretenus…
Pour autant, le risque d'attaque ciblée existe aussi, mais dans ce cas, l'Histoire montre que quel que soit le niveau de protection technique déployé, la faille la plus simple à exploiter est toujours la même : l'Humain.

BIBLIOGRAPHIE

1. **National Institute of Standards and Technology.** NVD - Statistics. *National Vulnerability Database.* [Online] Avril 2019. https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=last3years.
2. **Commission nationale de l'informatique et des libertés.** Comprendre le RGPD. *CNIL.fr.* [Online] https://www.cnil.fr/fr/comprendre-le-rgpd.
3. **Agence Nationale de la Sécurité des Systèmes d'Information.** Directive Network and Information Security. *ANSSI.* [Online] https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/.
4. **Internet Assigned Numbers Authority.** Service Name and Transport Protocol Port Number Registry. *Internet Assigned Numbers Authority.* [Online] https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.
5. **Engie Axima.** Projets & Réalisations. *GTC Automatisme.* [Online] https://engie-axima.fr/nos-metiers/genie-climatique-installation/gtc-automatisme/.
6. **DC423.** Control-Systems-Ports. *GitHub.* [Online] Août 23, 2016. https://github.com/DC423/Control-Systems-Ports/blob/master/README.md.
7. **Graham, Robert David.** Masscan. *GitHub.* [Online] Juin 23, 2018. https://github.com/robertdavidgraham/masscan.
8. **Shodan.** Shodan. *Shodan.* [Online] https://www.shodan.io.
9. **Industrial Control Systèmes on the Internet. *Shodan.io.* [Online] https://icsmap.shodan.io/.**
10. **Gartner. Gartner's Top 10 Security Predictions 2016. *Gartner.* [Online] https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/.**
11. **Exploit-DB. The Exploit-Database. *The Exploit-Database.* [Online] https://www.exploit-db.com/.**
12. **McMillan, Robert. Iran was prime target of SCADA worm. *ComputerWorld.* [Online] Juillet 23, 2010.**

https://www.computerworld.com/article/2519584/iran-was-prime-target-of-scada-worm.html.

13. Sentryo. *Threat Intelligence Report - Cyberattacks against Ukranian ICS.* s.l. : Sentryo, 2017.

14. *How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid.* Julia E. Sullivan, Dmitriy Kamensky. 3, s.l. : Elsevier, 2017, Vol. 30.