Sensibilisation à la cybersécurité des réseaux industriels

Florence LECROQ, Jean GRIEU
Florence.lecroq@univ-lehavre.fr
IUT du Havre – Université Le Havre Normandie

RESUME : Après un rappel des attaques cyber lancées sur des systèmes industriels durant ces dix dernières années, nous présentons un module de sensibilisation et de formation à la cybersécurité des réseaux industriels. Cet enseignement s'adresse à des étudiants non-informaticiens du département GEII. Une platine dédiée à cette formation sera détaillée plus avant avec des exemples d'attaques cyber.

Mots clés : Industrie 4.0, Cybersécurité, automates programmables, réseaux industriels, pare-feu industriel.

1 INTRODUCTION

A la fin du 18ième siècle, la première révolution industrielle prônait l'introduction des machines à vapeur dans l'industrie. La seconde révolution industrielle, au début du 20ième siècle, suivait la production en masse avec l'introduction des usines électrifiées et la division du travail. La troisième révolution industrielle est apparue au début des années 1970, avec l'arrivée de l'informatique industrielle, des automates programmables industriels et des robots. Aujourd'hui, nous sommes à l'heure de « l'industrie du futur ». De nos jours, cette quatrième révolution industrielle est basée sur les systèmes cyber physiques. Ces systèmes, communiquant massivement grâce aux réseaux informatiques, constituent l'un des principaux piliers de « l'industrie 4.0 ». Jusqu'au début des années 2000, les réseaux industriels échappaient aux cybermenaces. En effet, déconnectés de la partie bureautique du système d'information, encore appelée IT (Information Technologies), ils ne présentaient aucune vulnérabilité autre que celles propres aux lignes de production, appelées OT (Operational Technologies). Comme présentée sur la pyramide CIM (Computer Integrated Manufacturing) [1] dans la figure1, la numérisation de l'ensemble des fonctions de l'entreprise engendre une communication verticale entre les différents niveaux de la pyramide, ainsi qu'une communication horizontale et directe entre l'extérieur et ces différents niveaux. L'utilisation des IIOT (Industrial Internet Of Things), ou encore la télémaintenance accroit la vulnérabilité des systèmes industriels informatisés. En effet, ces points d'entrée, s'ils ne sont pas convenablement protégés, offrent des possibilités d'intrusion qui peuvent remettre en cause la sécurité des systèmes. Ces défaillances aux conséquences parfois catastrophiques et irréversibles, doivent être corrigées.

Comme l'a défini l'ANSSI (l'Agence Nationale de la Sécurité des Systèmes d'Informations) [2] : « *La cybersécurité est l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense* ». Constituant un enjeu majeur pour la protection des systèmes industriels, il paraît donc normal de former nos étudiants à cette problématique dans le cadre des cours sur les réseaux industriels et la programmation des automates.

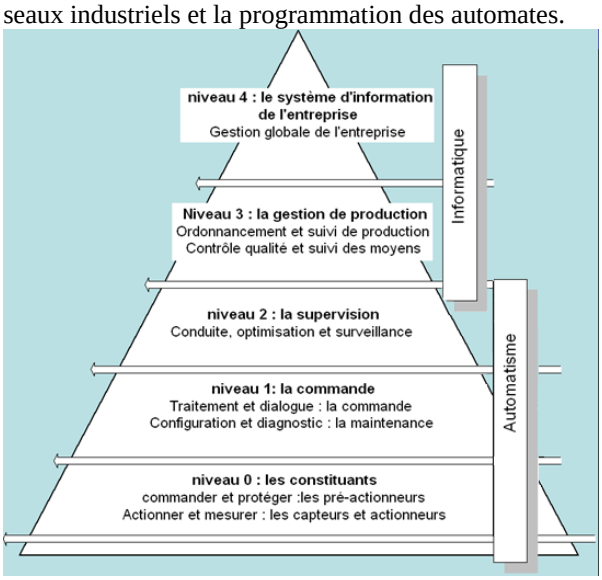

fig 1 : Pyramide CIM

Notre contribution se compose de quatre parties. Après cette introduction, nous présenterons des exemples de cyber-attaques sur des systèmes industriels. Ensuite, nous décrirons un module de cours sur la sensibilisation à la cybersécurité avec une platine pédagogique sur la sécurisation des réseaux industriels développée en partenariat avec les sociétés Stormshield et Schneider pour des étudiants non informaticiens. Enfin, pour conclure, nous présenterons les futurs développements de cette démarche pédagogique.

2 DES EXEMPLES D'ATTAQUES CYBER

2.1 Contexte

Les systèmes de contrôles industriels (ICS, Industrial Control Systems) représentent l'ensemble des systèmes qui traitent une mesure physique issue d'un capteur pour agir sur un procédé de transformation, fabrication, distribution ou pilotage. Aujourd'hui, de plus en plus interconnectés aux systèmes d'information traditionnels

Article publié par EDP Sciences et disponible sur le site https://www.j3ea.org ou https://doi.org/10.1051/j3ea/20222026

(IT), les systèmes de contrôle industriel (OT) constituent des cibles potentielles. Malgré tout, la menace informatique n'est pas toujours ciblée, mais par capillarité et par rebonds, une intrusion dans le système bureautique peut compromettre tout ou partie des équipements de production. Le paragraphe suivant présentera une évolution des attaques cyber qui ont compromis des systèmes industriels.

2.2 Présentation chronologique

La figure 2 présente une chronologie des attaques cyber qui ont compromis des systèmes industriels à travers le monde ces dix dernières années.

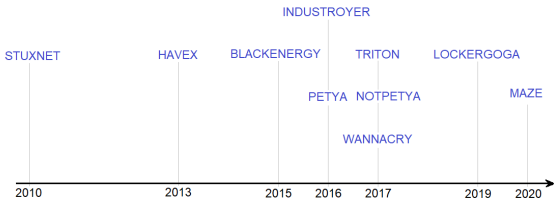

fig 2 : Etude chronologique des attaques cyber

La cybersécurité industrielle commence en 2010 avec Stuxnet [3], qui est la première attaque cyber recensée visant explicitement un site industriel. Au cours de cette attaque, des centaines de centrifugeuses des usines d'enrichissement d'uranium de Natanz en Iran ont été endommagées suite à un changement de programmation des vitesses de rotation des moteurs. Le ver introduit dans le système via une clef USB avait été développé conjointement par les Etats Unis et Israël. Il visait le logiciel de supervision WinnCC développé par Siemens [4]. Le but recherché était le ralentissement du programme d'enrichissement d'uranium de l'Iran.

En 2013, le virus Havex [5] compromet plus de mille entreprises du secteur de l'énergie. Le code malveillant, développé par le groupe « d'hacktivistes » Dragonfly de Russie, était caché dans un fichier PDF. Il visait principalement des entreprises aux Etats Unis et au Canada. Il permettait du vol de données et recherchait des équipements vulnérables pour interagir et contrôler les environnements industriels.

Le 23 décembre 2015, l'attaque BlackEnergy provenant de Russie a privé d'électricité près de 1,5 million d'Ukrainiens. Le code malveillant était inclus dans une macro associée à un fichier EXCEL. Après avoir pris la main à distance sur la supervision du système, les pirates ont envoyés un ordre de coupure aux disjoncteurs. Les employés présents dans l'usine n'ont pas pu se connecter au système car les mots de passe avaient été changés. Parallèlement, une attaque cyber (DDOS : déni de service distribué) du call center empêchait de répondre aux clients car il était saturé par des appels provenant de machines contrôlées par les pirates. Le service sera rétabli manuellement 6 heures après le début de l'attaque par les équipes envoyées sur place. En 2016, le réseau électrique de la capitale Ukrainienne sera de nouveau coupé avec le même mode opératoire durant une heure. C'était le code Industroyer.

En 2016, le rançongiciel (ransomware) Petya fait son apparition. Il remplace la zone d'amorçage du disque dur de la victime par un programme qui réclame de l'argent en échange de la clé de déchiffrement. Cette attaque visait un large public, mais a touché également des industries.

fig 3 : Ecran de compromission de Wannacry

Le vendredi 12 mai 2017, Wannacry est lancé (figure 3). C'est également un rançongiciel, qui va infecter près de 400 000 ordinateurs dans 150 pays. Il a touché également des sites industriels comme Renault, FedEx ou encore Vodafone. Il était présent dans des pièces jointes à des courriels envoyés par des « botnets ». Cette attaque a coûté plus d'un milliard de dollars aux entreprises concernées.

En juin 2017, apparait NotPetya. Il fut d'abord considéré comme une variante de Petya mais fût rapidement démenti par Kaspersky Lab. En effet, il apparait sous la forme d'un ransomware (interface similaire à Petya) mais en fait, il s'agirait d'un « wiper », programme qui détruit les données et ne les crypte pas. Il a touché plus de 100 000 ordinateurs mais également de grosses organisations comme des banques d'Ukraine, des infrastructures de Kiev (métro, aéroport), la SNCF, Auchan et le groupe Saint Gobain. La société Maersk sera touchée par cette attaque, bloquant tous ses terminaux portuaires à travers le monde durant deux semaines et coûtant près de 300 millions à la société.

En août 2017, le « malware » Triton fait son apparition (figure 4) [6].

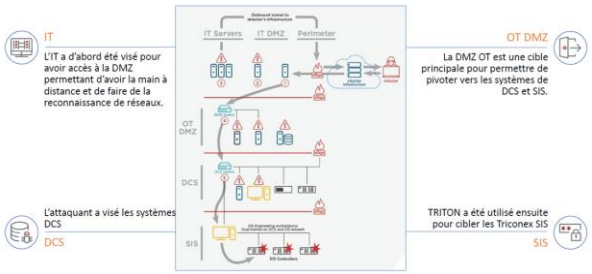

fig 4 : Le schéma d'attaque Triton

C'est le premier malware connu qui cible un automate de sécurité, on peut donc en déduire que cette attaque visait à détruire l'outil de production ou à blesser des personnes. On attribue cette attaque à un groupe en lien avec la Russie contre le complexe pétrochimique Petro Rabigh en Arabie Saoudite. Comme l'attaque n'a pas abouti, il a été possible de retrouver toutes les traces laissées par les pirates dans le système de l'usine. Cette attaque avait été planifiée trois ans auparavant. En 2014, le ver est introduit dans l'usine, par un fichier infecté, joint à un courriel. Il a ouvert une porte dérobée sur le réseau, permettant aux pirates de mettre à jour dans le temps leur virus. Ils ont pu accéder à l'OT de l'usine. Lors de la première attaque, en juin 2017, les automates de sécurité Triconex sont passés en mode sécurité et ont arrêté la production. A la deuxième attaque, en août 2017, les automates sont à nouveau passés en mode sécurité, arrêtant à nouveau la production. Cette nouvelle panne a lancé l'alerte. Après une étude approfondie, l'attaque cyber a été découverte. Ce qui a sauvé le système de production, c'est la méconnaissance par les pirates du principe de redondance contenu dans ces automates. Comme l'attaque n'a pas aboutie, il a été possible de retrouver les traces de l'attaque dans le système de l'usine, car habituellement, les hackers effacent toutes traces de leur passage dans les systèmes. En décembre 2017, les hackers ont lancé une dernière attaque, mais les systèmes étaient alors bien protégés.

En 2019, le malware LockerGoga touche les sociétés Altran en janvier, puis le producteur d'aluminium Norsk Hydro en mars. A la suite d'une campagne de spamming, l'attaquant prend le contrôle d'au moins un compte administrateur pour déposer ses outils de déploiement dans les serveurs des entreprises. Par la suite, il va stopper, désactiver des services, terminer des processus et chiffrer les données. Il s'agit d'un rançongiciel ciblé, qui ne peut pas se diffuser automatiquement, contrairement au rançongiciel Wannacry ou NotPetya qui correspondaient à des campagnes de propagation massive. Cette attaque a obligé l'entreprise à passer en mode manuel pour piloter sa production.

Tout récemment, fin janvier 2020, c'est au tour de l'entreprise Bouygues Construction d'être victime d'une attaque virale par le rançongiciel Maze. C'est la totalité du réseau informatique qui est touché et l'ensemble des serveurs de la société arrêté. Une rançon de 10 millions d'euros aurait été demandée et au moins 200 Go de données volées.

A l'énumération de toutes ces attaques cyber, il nous est apparu primordial de sensibiliser et de former nos étudiants à la sécurisation de leurs futurs outils de travail.

Dans la section suivante, nous présentons notre module de sensibilisation à la cybersécurité.

3 ENSEIGNEMENT DE LA CYBERSECURITE

Tout comme le présentait Stéphane Mocanu aux journées RESSI [8], nos étudiants en formation DUT GEII (Génie Electrique et Informatique Industrielle) ou LP SARII-SII (Systèmes Automatisés Réseaux et Informatique Industrielle, option Supervision des Installations Industrielles) sont des non-informaticiens. Nous avons donc adapté notre module à cette population en trois parties.

3.1 Un cours en présentiel

Ce premier cours est construit à partir des exemples d'attaques cyber présentées plus haut. Il est également basé sur les outils fournis par l'ANSSI dans la maquette CyberEdu [9]. Il permet d'introduire les enjeux de la cybersécurité des systèmes industriels. Il est suivi par une formation à distance.

3.2 La formation à distance

Elle débute par le visionnage de vidéos réalisées par Airbus Group sur Youtube [10]. A la suite de la lecture des six vidéos, ils rédigent un document décrivant la morale de chacune des histoires. Ceci permet une sensibilisation générale à la sécurité sur les outils informatiques. Cette partie est suivie par l'utilisation du MOOC de l'ANSSI [11] SecNum *Académie*. Les étudiants doivent nous remettre leur cetificat de validation de réussite du MOOC. En plus de cette certification qu'ils joignent à leurs CV, nous mettons une note dans le module. Cette partie est obligatoire pour tout étudiant entrant dans le département et nous permet de les sensibiliser à la place de l'homme dans la cybersécurité. Comme le montre l'étude d'OpinionWay sur la cybersécurité dans les entreprises en 2019 [12], le vecteur d'attaque principal est le phishing (79%) avec pour conséquences de ces attaques une usurpation d'identité (35%) et une infection par malware (34%). En lien avec la cybersécurité, la négligence des salariés est relevée dans cette étude par près de la moitié des entreprises (43%).

L'étape suivante de la formation est en présentiel sur du matériel spécifique et traite de la protection des systèmes industriels.

3.3 Utilisation d'une platine dédiée à la cybersécurité

Cette platine a été développée en partenariat avec les entreprises Stormshield [13] et Schneider [14].

3.3.1 Le matériel

fig 5 : Platine cybersécurité des réseaux industriels

La platine présentée figure 5, comprend un automate M580 de la marque Schneider, avec un IHM, un *firewall* (pare-feu) industriel SNi40 de Stormshield, ainsi qu'un variateur associé à un moteur géré par un bus CAN.

3.3.2 L'objectif

L'objectif de cette platine est de présenter la protection d'un système industriel. En effet, il paraissait primordial d'expliquer aux étudiants qu'une application sur un bus industriel peut être touchée par une attaque provenant de l'IT.

3.3.3 La méthode

Le matériel fourni permet de présenter des attaques cyber. Le début des TP consiste à mettre en œuvre un moteur sur le bus CAN par programmation de l'automate M580 et visualisation ou modification de la vitesse de rotation sur l'IHM. On présente également durant cette première phase l'utilisation du serveur web embarqué dans l'automate, avec la possibilité de modifier les variables directement par un accès réseau à la CPU.
Durant le TP suivant, l'étudiant met en œuvre la protection de cette ligne de production, avec le pare-feu industriel Stormshield SNi40. Il peut détailler plus précisément le comportement du pare-feu avec l'analyse du contenu des trames observées sur le réseau. Ensuite, nous étudions la mise en place d'un filtrage par signature personnalisée sur le firewall. Il est alors possible de restreindre la recevabilité d'une demande de modification de la consigne de vitesse à une valeur minimale de x% de sa vitesse maximale.
Sur le TP suivant, un script d'attaque est lancé. Celui-ci fait varier toutes les 5 secondes la consigne de vitesse. Puis, au bout de 30 secondes, il arrête le moteur. On présente alors la protection du réseau industriel avec l'autorisation de connections via le pare-feu sur filtrage par IP spécifique.

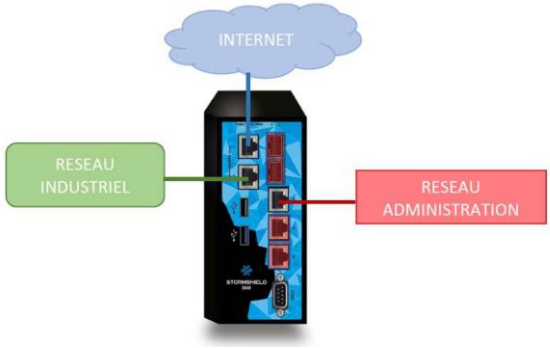

fig 6 : Représentation de la séparation des réseaux

Le TP suivant traite de la séparation des réseaux grâce au pare-feu (figure 6). Cette partie permet d'appliquer les politiques de sécurité réduisant ainsi l'impact de certaines attaques et également d'établir des règles de sécurité spécifiques à chaque sous réseau.
Enfin, le dernier TP a pour objectif d'acquérir les bonnes pratiques concernant la cybersécurité des réseaux industriels. Trois scripts d'attaques sont utilisés. Le premier montre une lecture des informations qui va permettre de récupérer des données sensibles. Cette attaque est dite *passive* car elle se contente de récupérer des données. Le second script présente une attaque par déni de service (DOS : Denied Of Service) qui rend l'automate indisponible, puis en mode erreur, avec un affichage d'attaque réussie sur l'IHM (figure 7).

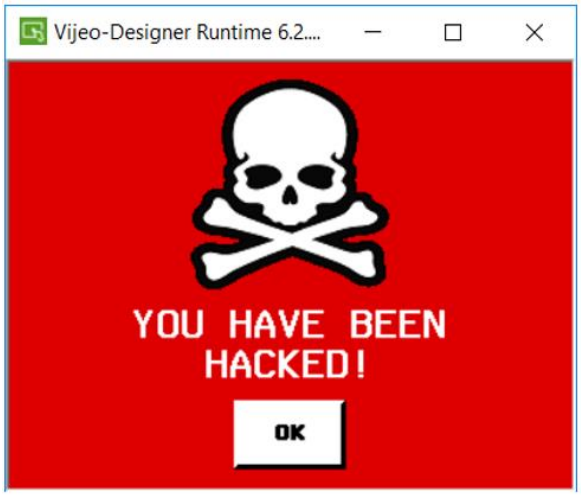

fig 7 : Résultat de l'attaque visible sur l'IHM

Enfin, le dernier script permet une prise de contrôle du système. Durant cette attaque, le variateur change la consigne de vitesse toutes les 3 secondes, et ce, pendant 30 secondes. Ce dernier TP montre qu'avec une mauvaise configuration réseau, ou une mauvaise politique de sécurité mise en place, un attaquant peut prendre le contrôle partiel ou total du réseau industriel. On termine cette séance de TP en appliquant les bonnes règles de sécurité tout en rejouant les trois scripts d'attaques pour s'assurer que l'ensemble du système est protégé et que tout fonctionne normalement.

4 CONCLUSION

Dans cet article, nous sommes revenus sur de nombreux exemples d'attaques cyber à l'encontre d'entreprises industrielles à travers le monde durant ces vingt dernières années. Connaissant ces attaques et étant enseignants sur les réseaux industriels et les automates programmables, il nous est apparu nécessaire de sensibiliser et former nos étudiants aux enjeux de la cybersécurité des réseaux industriels. Ce module de cours de sensibilisation présenté ici permet déjà une première approche du sujet. D'ailleurs, nous observons un changement de comportement des étudiants, notamment avec l'utilisation de supports amovibles en salle de TP. Dans le futur, nous comptons développer plus avant ces enseignements, avec 20 heures de cours en présentiel, en concevant d'autres travaux pratiques, toujours avec du matériel spécifique, comme l'utilisation d'une sonde IDS sur un réseau ou encore la mise en place de cloisonnement et la séparation des réseaux [15] [16].

Remerciements

La platine de travaux pratiques sur la cybersécurité des réseaux industriels a été développée en partenariat avec les sociétés Schneider, Stormshield et F. LECROQ de l'IUT du Havre.

Bibliographie

[1] Bianca SCHOLTEN, " The road to integration, a guide to applying the ISA-95 standard in manufacturing", *JInternational Society of Automation (ISA) (2007), ISBN-13 : 978-0-9792343-8-5.*

[2] Glossaire de l'ANSSI, *https://www.ssi.gouv.fr/entreprise/glossaire/c/*

[3] Symantec, " W32.Stuxnet – Network Information", (2010) *https://www.symantec.com/connect/blogs/w32stuxnet-network-information*

[4] WinnCC Siemens *https://new.siemens.com/global/en/products/automation/simatic-hmi/wincc-unified.html*

[5] Havex, "la roulette russe", (2014) *https://securid.novaclic.com/cyber-securite-industrielle/havex-dragonfly-russe.html*

[6] David GROUT, "Panorama des menaces et retour d'expérience sur le malware Triton", *Société FireEye, Actes de la Journée Technique Exera sur la Cybersécurité des Systèmes Industriels, Paris (France), Septembre 2018.*

[7] ANSSI, "Informations concernant les rançongiciels LockerGoga et Ryuk", (2019) *https://www.cert.ssi.gouv.fr/uploads/CERTFR-2019-CTI-001.pdf*

[8] Stéphane MOCANU, "Formation cybersécurité des systèmes industriels pour les ingénieurs non-informaticiens", *RESSI 2018 : Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information, Nancy (France), mai 2018, sciencesconf.org:ressi2018:187879*

[9] ANSSI, Malette pédagogique CyberEdu, *https://www.ssi.gouv.fr/administration/formations/cyberedu/contenu-pedagogique-cyberedu/*

[10] Videos Airbus Group sur Youtube, *https://youtu.be/kiw4B00iJzs https://youtu.be/yBL4eco0NCs*

[11] MOOC de l'ANSSI SecNum *Académie, https://secnumacademie.gouv.fr*

[12] OpinionWay, "Barromètre de la cybersécurité des entreprises – vague 5 – janvier 2020", *Club des Experts de la Sécurité de l'Information et du Numérique, janvier 2020, https://www.cesin.fr/uploads/files/BJ20433%20-%20Barom%C3%A8tre%20du%20CESIN%20vague%205%20-Vdef.pdf*

[13] Stormshield *https://www.stormshield.com/fr/*

[14] Schneider Electric France *https://www.se.com/fr/*

[15] Jean-Marie FLAUS, "Cybersécurité des systèmes industriels", *ISTE Editions (2019) ISBN : 978-1-78405-534-9*

[16] Romain HENNION, Anissa MAKHLOUF, "Cybersécurité", *Eyrolles Editions (2018) ISBN : 978-2-212-65893-6*