L'usine du futur imposera l'enseignement de la cybersécurité des systèmes industriels

Florence LECROQ
Maître de Conférences en Automatismes et en Sécurité des Systèmes Informatiques Industriels
IUT du Havre

L'usine du futur :
des implications dans l'enseignement

Aujourd'hui, nous sommes à l'heure de « l'industrie du futur ». 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). L'approche traditionnelle nous présente l'entreprise industrielle sous la forme d'une pyramide (la pyramide CIM), découpée en couches nommées niveaux, où l'on retrouve les différents éléments constitutifs du système de production. Le niveau 0 est à la base, avec les capteurs, les actionneurs et les pré-actionneurs ; au-dessus, se situe le niveau 1, avec la commande, c'est-à-dire les automates programmables industriels ; vient ensuite le niveau 2, la partie supervision, avec la conduite, l'optimisation et la surveillance du système ; le niveau 3 regroupe la gestion de production, avec l'ordonnancement et le suivi de production, contrôle qualité et le suivi des moyens ; le niveau 4, le dernier, abrite le système d'information de l'entreprise, avec la gestion centralisée de l'entreprise.

Avec l'arrivée de l'industrie du futur, 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 avec l'extérieur et ce à tous les niveaux.

L'utilisation des IIOT (Industrial Internet Of Things), ou encore la télémaintenance, augmente la vulnérabilité des systèmes industriels informatisés. En effet, ces points d'entrée, s'ils ne sont pas convenablement protégés, offrent des opportunités d'intrusion qui peuvent remettre en cause la sécurité des systèmes. Ces faiblesses, aux conséquences parfois catastrophiques et irréversibles, doivent être corrigées. Comme l'a défini l'ANSSI : « *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 urgent de former nos étudiants à cette problématique dans le cadre des cours portant sur les technologies de l'industrie du futur, avec les réseaux industriels et la programmation des automates.

La formation : 1er vecteur de sensibilisation aux risques cybers

Eveil – Veille – Sensibilisation – Formation : ces quatre mots sont une représentation de mon métier. En effet, je travaille sur l'industrie du futur en informatique industrielle pour la formation, ainsi que sur la XR reality pour la recherche avec l'utilisation des mondes virtuels pour la formation. La réalité étendue (XR) regroupe les diverses formes de technologies immersives, comme la réalité augmentée (AR), la réalité mixte (MR) ou la réalité virtuelle (VR). Le métier d'enseignant chercheur est de susciter l'intérêt (l'éveil) de nos étudiants sur différents sujets. Nous nous devons de faire une veille technologique pour eux, pour ensuite les sensibiliser à différents sujets et terminer bien évidemment avec la formation.

Ce principe d'« Eveil-Veille-Sensibilisation-Formation » s'applique parfaitement à la cybersécurité aujourd'hui.

Il n'y a pas une semaine sans qu'on entende parler d'une attaque cyber proche de nous. Comme le rapporte HISCOX [1], assureur spécialiste des cyber-risques, 49% des entreprises françaises ont été la cible d'une cyber attaque en 2020, contre 34% en 2019. 65% ont versées une rançon. Les entreprises françaises sont aussi celles qui ont le moins investi en termes de sécurité des systèmes d'informations. Nos étudiants sont les futurs intervenants dans des entreprises, et notamment celles de la zone industrialo-portuaire du Havre, qui comprend 23 sites Seveso, dont 17 de seuil haut. On peut aisément imaginer les conséquences dramatique d'une attaque cyber d'envergure sur un site de la région. C'est dans ce contexte que nous formons nos étudiants à la cybersécurité des réseaux industriels.

Tout comme lorsque l'on parle de *Safety* dans les métiers de l'automatisme, il s'agit là de protéger l'homme de la machine ; lorsque l'on parle de cybersécurité, il s'agit au contraire de protéger la machine de l'homme. Et les spécialistes s'accordent à dire que 80 % des attaques cybers pourraient être évitées si les personnels étaient formés aux risques cyber.

Cette notion est d'autant plus vraie lorsqu'on connait les conséquences possibles d'une attaque cyber sur un processus industriel.

Il peut bien évidemment y avoir du vol de données, mais surtout le risque d'avoir une destruction de la chaîne de production, avec ses conséquences éventuelles sur l'environnement et la santé humaine. On pourrait énumérer de nombreux exemples d'attaques cyber sur des systèmes industriels, comme BlackEnergy en 2015, qui a privé d'électricité près de 1,5 millions d'Ukrainiens, ou Wannacry en 2017, qui se propage dans 150 pays et touche des sites industriels à travers le monde, ou TRITON en 2017, qui touche le groupe pétrochimique Petro Rabigh en Arabie Saoudite, etc. En 2021, le nombre d'attaques a explosé, ciblant aussi des centres hospitaliers, des laboratoires ou des universités. On peut dire aujourd'hui que personne n'est épargné mais surtout que tout le monde sera touché, ce ne plus qu'une question de temps.

D'où l'importance de la sensibilisation aux risques cyber et surtout de la formation. Car la cybersécurité n'est surtout pas une affaire de spécialistes mais doit être une préoccupation de tous et de tous les jours.

Les outils et les pratiques

Il y a de nombreux outils aujourd'hui pour former les personnels et les étudiants aux risques cyber. Tout d'abord, il existe des aides fournies par l'ANSSI, sur son site [2], avec la SecNumAcadémie, qui donne une formation en ligne avec un MOOC qui rend la cybersécurité accessible à tous. L'ANSSI donne aussi le

label SecNumedu pour les formations spécialisées en cybersécurité et le label CyberEdu pour les formations qui sensibilisent, initient voire forment à la cybersécurité sans faire des experts du domaine.

J'ai récemment travaillé avec les sociétés Stormshield et Schneider sur la mise en place d'une platine d'enseignement sur la cybersécurité des réseaux industriels. De par mon métier, je suis amenée à visiter des entreprises et discuter avec les maîtres de stage de mes étudiants. Et souvent, j'ai été confrontée aux fausses croyances de la cybersécurité industrielle : *« le système industriel n'est pas connecté à Internet, je suis protégé », « la communication est en série, je suis protégé », « tout est redondé, je suis protégé », « avec la cybersécurité, je ne pourrai plus travailler correctement »,* etc. C'est à cause de ces réflexions que j'ai participé à ce projet d'une platine pour l'enseignement qui est à destination de tous les centres de formations (universités, écoles d'ingénieurs, IUT). Cette platine explique qu'une application sur un bus industriel (un variateur associé à un moteur géré par un bus CAN dans cet exemple) peut être impactée par une attaque cyber provenant de l'IT. Dans un des exercices, durant l'attaque lancée, le variateur change la consigne de vitesse du moteur toutes les 3 secondes, et ce, pendant 30 secondes. Cet exemple 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.

Plus récemment, avec mon collègue Jean GRIEU, nous avons monté un *serious escape game* pour une sensibilisation et une formation aux risques cybers. Ce jeu est à destination de nos étudiants mais aussi à destination de tous les personnels, que ce soit de l'université mais aussi des entreprises de la région du Havre qui, je vous le rappelle, comprend 23 site Seveso, et la cybersécurité est l'affaire de tous. Ce jeu, « la règle des 12 », doit se jouer à 12 joueurs, qui doivent trouver 12 entreprises de la région havraise, qui ont été piratées et infestées par un Botnet, parce que 12 règles de cybersécurité n'ont pas été respectées. Les joueurs ont 60 minutes pour sauver la région havraise d'un catastrophe industrielle en découvrant les douze entreprises infestées, l'entreprise qui héberge le maître du botnet, ainsi que l'identité du hacker qui se cache parmi les employés de l'entreprise qui cache le maître des zombies. Ce jeu est basé sur les douze règles de base de la cybersécurité énoncées par l'ANSSI [3]. L'utilisation du jeu comme vecteur d'enseignement permet de mettre en œuvre des pratiques actives, réflexives et sociales, et permettent de développer le sens du partage et l'intelligence collective [4]. Je pourrais terminer en disant que plus les personnes s'amusent en apprenant, et mieux elles retiennent le message de l'enseignant.

Et surtout ne pas oublier que la cybersécurité est l'affaire de tous et surtout pas que des spécialistes.

[1] Hiscox Cyber Readiness report 2021 : Près d'1 entreprise française sur 2 ciblée par une cyberattaque en 2020
https://www.hiscox.fr/sites/france/files/documents/CP%20Hiscox%20Cyber%20Readiness%20report%202021_19042021.pdf
[2] ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information
https://www.ssi.gouv.fr/administration/formations/
[3] ANSSI : Guide des bonnes pratiques de l'informatique, 12 règles essentielles pour sécuriser vos équipements numériques
https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf