Cybersécurité des systèmes automatisés industriels

Culture Sciences de l'Ingénieur

La Revue 3E.I

Édité le 15/02/2024

école normale supérieure paris—saclay

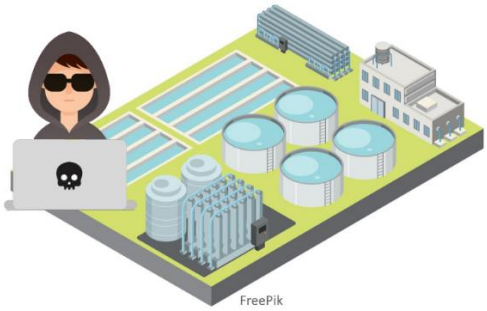
Anthony JUTON[1]

[1] *Professeur agrégé à l'ENS Paris-Saclay – DER Nikola Tesla*

Cette ressource fait partie du N°111 de La Revue 3EI de janvier 2024.

Cet article est une mise à jour l'article publié en juillet 2018 dans la revue 3EI [7]. Il introduit la partie du dossier cybersécurité des systèmes industriels consacrée aux systèmes automatisés. L'automatisme industriel étant essentiellement enseigné en BUT GEII, c'est le public visé par cet article, qui s'efforce de fournir des exemples et des applications pratiques.

Les risques liés à la cybersécurité pour les industries et les services sont réels comme le montre le blocage d'une usine Renault et d'hôpitaux anglais par le ransomware WannaCry en mai 2017 ([3] – Fiche 1). Consciente du risque cyber sur l'industrie et des implications pour le fonctionnement et la sécurité de l'Etat, la loi de programmation militaire de 2013 impose un renforcement de la sécurité informatique à des entreprises privées ou publiques considérées vitales pour la France, regroupées sous le terme Opérateurs d'Importance Vitale (OIV). On trouve notamment parmi les OIV des usines de traitement des eaux, des centrales de production d'énergie, des aéroports, des usines pharmaceutiques.



Ce renforcement concerne l'ensemble des équipements informatiques, ce qui comprend les systèmes gérés habituellement par les services informatiques (IT information technology) normalement sensibilisés à la cybersécurité mais aussi ceux gérés par les services automatisme (OT operational technology), qui doivent se former à ce nouveau risque.

La sécurisation d'une installation industrielle est donc le fruit d'une collaboration entre informaticiens et automaticiens. Cela passe par une implication des informaticiens dans la production et par une formation des automaticiens aux bases de la cybersécurité.

Prenant acte de ce contexte, la licence professionnelle SARII (Systèmes Automatisés Réseaux et Informatique Industrielle) de l'IUT de Cachan (aujourd'hui dissoute dans le BUT3 parcours AII) a créé en 2018 un module de cybersécurité des systèmes industriels pour compléter la formation en automatisme, réseaux et supervision de ses techniciens. Cet article repose essentiellement sur la démarche et les contenus de ce module prévu pour 4h de cours/TD et 12h de TP. L'ensemble s'appuie essentiellement sur les supports proposés par l'Agence Nationale de la Sécurité des

Systèmes d'Information (ANSSI) [1] et par le groupe de travail cybersécurité des systèmes industriels du Club de la Sécurité de l'Information Français (CLUSIF) [2], [3] et [4]. La consultation de ces 4 ressources permettra au lecteur intéressé d'approfondir le sujet.

Dans un premier temps l'article rappelle le risque cyber pour l'industrie, avant d'aborder la démarche proposée par l'ANSSI pour sécuriser un site. L'analyse de quelques incidents récents souligne les bonnes pratiques pour les éviter et l'article termine par une étude de cas d'usine pharmaceutique, support d'une exploitation possible en TD et TP.

1 - L'industrie est soumise à un risque cyber

1.1 - Les types d'attaque

Une attaque peut être ciblée contre l'entreprise (exemple de Stuxnet visant les usines d'enrichissement de l'uranium iraniennes [3] fiche 36 ou de BlackEnergy visant les postes électriques ukrainiens [3] fiche 4) ou non (exemple de WannaCry attaquant tous les systèmes Windows XP ou 7 non mis à jour [3] fiche 1).

L'attaque nécessite une intrusion dans le système (ou dans beaucoup de systèmes extérieurs pour les attaques par déni de service) et un mécanisme de sabotage.

1.1.1 – Solutions pour permettre l'intrusion dans le système

- Un **spyware** ou logiciel espion est un programme qui enregistre les frappes au clavier, webcam, microphone pour récupérer des informations (login et mot de passe notamment). Il peut s'installer lors d'une installation d'un logiciel depuis un site web malveillant, par l'introduction d'un média amovible infecté ou lors de l'ouverture d'un document contenant des macros.
- Le **phishing** ou hameçonnage est un mail utilisant un aspect officiel pour demander la saisie de données personnelles. Plus il est personnalisé (logo de l'entreprise, utilisation de détails concernant la cible), plus il est efficace.
- Un **ver** est un programme qui se reproduit sur plusieurs ordinateurs en utilisant le réseau informatique.

1.1.2 – Mécanisme permettant le sabotage ou la neutralisation du système industriel

- Un **cheval de Troie** est un programme qui permet de prendre à distance le contrôle de l'ordinateur cible. Si un PC de supervision ou de programmation des automates est infecté, le pirate peut modifier dangereusement le comportement du système.
- Un **ransonware** ou cryptovirus est un programme qui chiffre les fichiers et qui demande une rançon pour les déchiffrer. Une fois les fichiers chiffrés, le système est neutralisé.
- Un **virus** est un programme qui s'attache à un autre pour modifier son fonctionnement.
- Le **déni de service** est une attaque qui rend impossible l'utilisation d'un service, notamment via l'utilisation de botnet, réseaux de robots informatiques (souvent installés sur des systèmes informatiques peu protégés) qui vont ensemble saturer un serveur de requêtes.

1.2 - Les opérateurs d'importance vitale

La loi de programmation militaire de 2013 précise les obligations pour 12 secteurs d'opérateurs vitaux pour l'intégrité du territoire de ses habitants ou son économie :

- Activités civiles de l'Etat
- Activités judiciaires
- Activités militaires de l'Etat
- Alimentation
- Communications électroniques, audiovisuel et information
- Energie
- Espace et recherche
- Finances
- Gestion de l'eau
- Industrie
- Santé
- Transports.

Dans ces secteurs, plus de 200 services publics ou entreprises privées dont les activités sont indispensables au bon fonctionnement et à la survie de la Nation sont classés opérateurs d'importance vitale (OIV). La liste est confidentielle, on y trouve des acteurs industriels dans le traitement de l'eau, la production d'électricité, la fabrication de médicaments, la gestion technique des aéroports... La loi impose à ces OIV le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent, nommés « systèmes d'information d'importance vitale » (SIIV).

Les entreprises qui ne sont pas OIV sont également encouragées à prendre des mesures de cybersécurité, ne serait-ce que pour assurer leur survie économique en cas d'attaque.

1.3 - Les spécificités des systèmes industriels

Les systèmes informatiques industriels sont très proches des systèmes informatiques de gestion (utilisation de réseaux Ethernet/TCP/IP, utilisation de PC et serveurs pour la supervision, utilisation de bases de données SQL…) mais ont des spécificités qui les rendent vulnérables et difficiles d'accès aux informaticiens :

- Certains systèmes informatiques industriels (centrales nucléaires, usines en 5x8, aéroports...) doivent être disponibles sans interruptions, rendant difficiles les mises à jour, les tests de vulnérabilité, etc...
- Certains systèmes informatiques industriels mettent en jeu la vie des personnes (centrales nucléaires, machines médicales, usines de production de médicaments…) et pour cela reçoivent des habilitations/qualifications qui ne sont plus valables en cas de mise à jour majeure d'un équipement.
- Les équipements de contrôle-commande ont une durée de vie très longue (on trouve encore en fonctionnement dans les usines de très fiables automates Siemens S5 des années 80) et forment un parc souvent hétérogène (chaque machine peut avoir un modèle d'automate ou pire, une marque d'automate différent). Cela rend le suivi des vulnérabilités et des mises à jour plus fastidieux. Ces automates sont souvent inconnus des informaticiens en charge de la cybersécurité.
- Les productions alimentaires et pharmaceutiques notamment doivent garantir la traçabilité de leur production. Cela rend nécessaire les connexions entre les machines de terrain

(automates, superviseurs, ... regroupés sous le sigle OT Operational Technology) et les machines de l'administration (suivi de la qualité, traçabilité, ... regroupés sous le sigle IT Information Technology).

- Les réseaux de terrain traditionnels (profibus, CANopen, DeviceNet, Modbus RTU...) et certains protocoles TCP/IP largement utilisés en automatisme (Modbus TCP, BACnet/IP, …) ne sont pas sécurisés et pas sécurisables. Ces protocoles sont souvent inconnus des informaticiens en charge de la cybersécurité.
- La maîtrise exigée pour certaines tâches (par exemple la régulation de l'humidité dans des bâtiments d'architecture originale, la mécanique de précision ou l'intégration de robots industriels à des machines automatisées…) demande l'intervention de sous-traitants spécialisés (mécanique, automatisme, robotique, supervision…). A cela s'ajoute la volonté de réduire la masse salariale des entreprises, pratique très présente dans l'automobile. Il est bien sûr plus difficile de maîtriser l'intégrité et la formation en cybersécurité des sous-traitants que celles de ses salariés.

1.4 - Vulnérabilité des systèmes industriels

Pour souligner les vulnérabilités d'un système informatique industriel, voici trois cas représentatifs :

1.4.1 – Système non connecté à Internet

Le système informatique industriel basique comprend typiquement un ou plusieurs automates supervisés par un PC de supervision via un réseau Ethernet, pas forcément connecté à Internet. Un serveur de base de données pour l'archivage peut aussi être présent localement. L'automate contrôle divers équipements via des bus de terrain standard ou basés sur Ethernet.

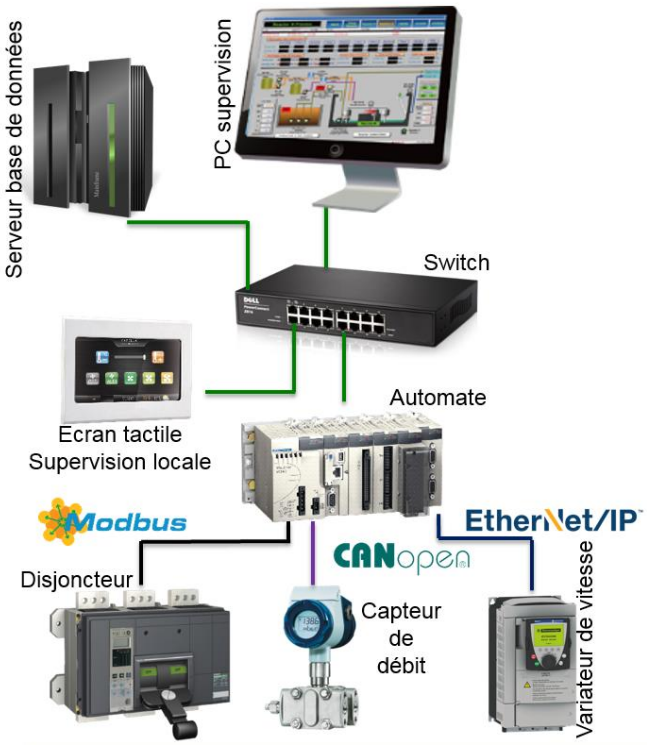


Figure 1 : Architecture type d'un système informatique industriel non connecté à Internet

Les problèmes peuvent survenir de :

- La modification du programme automate via un accès direct à l'automate ou la modification des consignes de supervision par du personnel non autorisé (sous-traitant par exemple),

- L’introduction d’un virus par une clé USB,
- L’introduction d’un virus par un PC maintenance (d’un sous-traitant ou d’un salarié) se connectant au réseau local, pour une mise à jour par exemple.

Le virus peut alors simplement neutraliser le PC de supervision (en chiffrant ses données comme wannacry [3]) ou plus rarement, car beaucoup plus complexe, neutraliser un équipement industriel (automate comme le malware Triton, [3] fiche 7 ou superviseur comme le malware Havex [3] fiche 5) ou plus complexe encore, modifier le programme automate ou les consignes envoyées par le PC de supervision (un seul exemple, Stuxnet [3]).

1.4.2 – Système connecté à Internet

Le réseau de l’atelier est connecté au réseau de l’administration via un routeur. Le réseau de l’administration est lui-même connecté à Internet via un routeur.

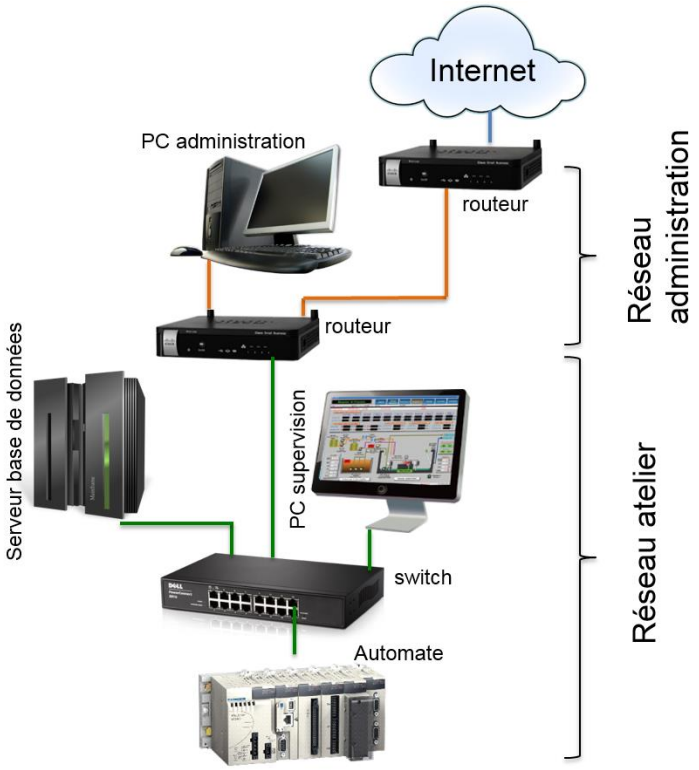


Figure 2 : Architecture type d'un système informatique industriel connecté à Internet

La connexion à Internet, outre une possibilité supplémentaire d’introduction de virus, amène le risque suivant : une personne malveillante peut s’introduire sur le réseau atelier via un accès ouvert (pour la télégestion par exemple) en dérobant des identifiant et mot de passe de connexion ou, plus complexe, via un cheval de Troie installé par un virus sur un PC de bureau par exemple. Cette personne peut alors neutraliser des équipements, les espionner ou en prendre le contrôle à distance.

Tout accès à distance à une installation fait courir le risque d’une prise de contrôle par une personne malveillante. (Exemple de l’attaque d’une station d’épuration, [3] fiche 16, ou [3] fiche 21, parmi beaucoup d’autres)

1.4.3 – Système informatique industriel distribué

Un système distribué désigne un système dont les organes de contrôle-commande (automates, variateurs, modules d’entrées/sorties déportés) ne sont pas localisés dans le même local. Les

grands sites de stockage d'hydrocarbure, les réseaux ferroviaires, les tunnels routiers et les bâtiments en général sont des systèmes distribués.

N'est représentée sur le schéma ci-dessous que la partie contrôle-commande. La supervision et la connexion éventuelle à Internet sont identiques aux architectures présentées ci-dessus.

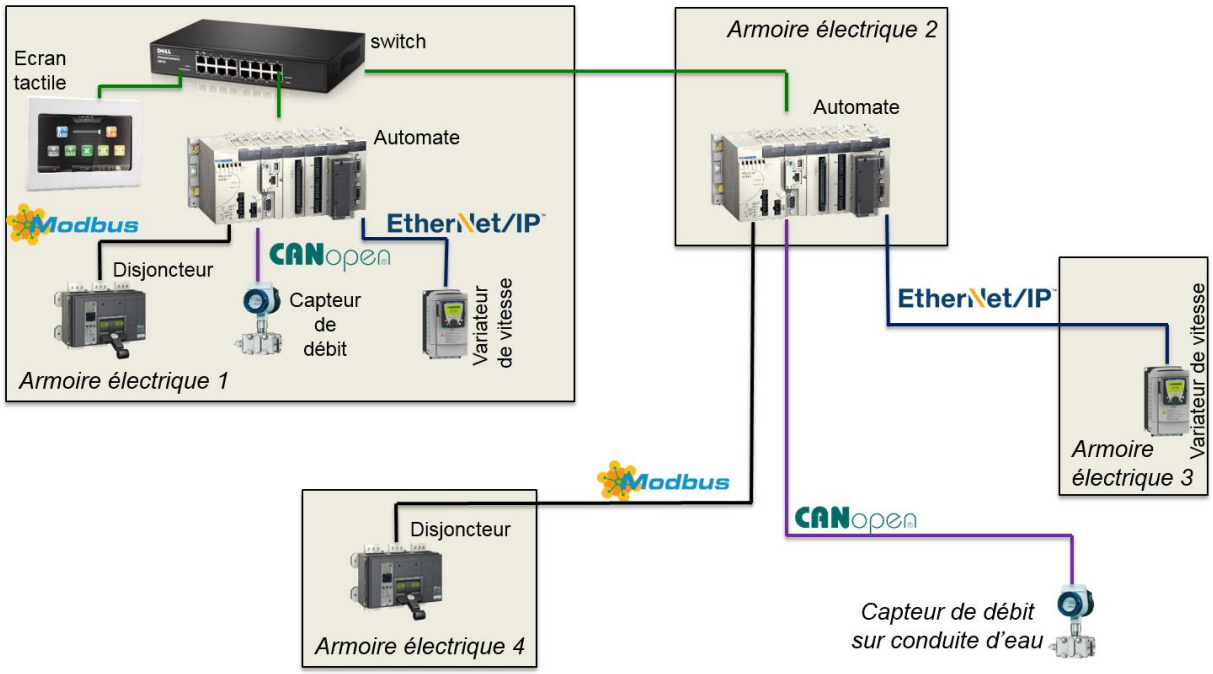


Figure 3 : Architecture type d'un système informatique industriel distribué (partie contrôle/commande uniquement)

Outre les risques précédemment cités, les réseaux de terrain standards, très répandus, très connus dans le monde industriels et très documentés, sur liaison RS485 (Modbus, Profibus, BACnet MSTP), sur bus CAN (CANopen, DeviceNet) ou spécifiques (LON, DALI, KNX…) ne sont pas sécurisés et pas sécurisables simplement (un standard sécurisé de KNX existe mais n'est pas compatible avec les équipements déjà installés). Le passage de ces bus dans des zones publiques ou faciles d'accès fait courir le risque d'une intrusion sur le réseau et de l'envoi sur ce réseau d'informations de capteurs fausses ou de commandes d'actionneurs dangereuses (exemple d'envoi de commande de déversement d'eaux usées en utilisant le réseau industriel local [3] fiche 18 ou exemple de la prise de contrôle d'éoliennes via un accès physique au réseau local [3] fiche 8)

Les réseaux de terrain modernes sur Ethernet (ProfiNet, EtherNet/IP, Ethercat) sont plus récents et leurs standards plus complexes tendent à prendre mieux en compte le risque cyber (authentification de la machine se connectant par exemple). Le protocole OPC-UA, sur Ethernet TCP/IP, utilisé pour la communication entre le superviseur et l'automate, ou entre automates, est même chiffré, ce qui lui donne une popularité certaine actuellement. La ressource [5] traite spécifiquement d'OPC-UA.

2 - Les mesures à appliquer

Une fois les risques présentés, le cours présente alors une version simplifiée de la méthode proposée par l'ANSSI [1] pour la sécurisation des systèmes informatiques industriels et la mise en place d'une politique de sécurité des systèmes d'information (PSSI).

« L'objectif de la Sécurité des Systèmes Informatiques (SSI) est d'étudier les vulnérabilités des systèmes (matériel, logiciel, procédures, aspects humains) afin de déployer des mesures pour les limiter et permettre d'assurer la continuité des fonctions métier à un niveau acceptable. ». Il s'agit

d'assurer la disponibilité, l'intégrité, la confidentialité et la traçabilité du système informatique industriel.

La cybersécurité doit être envisagée par les automaticiens comme la sûreté de fonctionnement des machines :

- On identifie les risques puis la probabilité et les conséquences du risque,
- On met en place des mesures proportionnées au risque (coût et contraintes sur les utilisateurs), sous peine de les voir rejetées.
- On ne peut raisonner en termes de retour sur investissement.

La mise en place de la sécurisation du système informatique industriel doit impliquer les automaticiens, bons connaisseurs de leurs équipements industriels et les responsables cybersécurité de l'informatique générale, formés en cybersécurité mais souvent hermétiques à l'automatisme.

La méthode suit 7 étapes, détaillées ensuite :

1. Sensibilisation des personnels
2. Cartographie des installations et analyse de risque
3. Prévention : concept de la défense en profondeur
4. Surveillance des installations et détection des incidents
5. Traitement des incidents, chaîne d'alerte
6. Veille sur les menaces et les vulnérabilités
7. Plans de reprise et de continuité d'activité

La méthode ne fait appel qu'à des compétences d'automaticien moderne (les compétences en réseaux sont évidemment importantes). Elle montre que la cybersécurité est surtout une question d'organisation et de temps alloué à cette organisation, d'où l'obligation d'un PSSI pour les OIV.

2.1 - Sensibilisation des personnels

La majorité des incidents est liée à l'imprudence des personnels de l'entreprise :

- Utilisation de clé USB,
- Logiciel « cheval de Troie » ou virus installés en ouvrant un fichier ou en installant un logiciel de provenance douteuse,
- Divulgation de ses identifiant/mot de passe en réponse à un mail de phishing,
- Mot de passe écrit sur un post-it ou stocké en clair sur une machine,
- Identifiant/mot de passe identique pour tous les techniciens (y compris ceux qui quittent l'entreprise…),
- Machines non protégées ou avec les identifiant/mot de passe par défaut, avec des mises à jour logicielles non effectuées.

Plus de 10 fiches « incident » du Clusif [3] ont pour origine un vol de mot de passe par une campagne de phishing, plusieurs autres ont un lien aussi avec des manquements à la sécurité des employés (non révocation des accès d'un employé licencié, installation de logiciel infecté...)

La sensibilisation de tous les personnels aux règles d'« hygiène informatique » contribue à réduire fortement les vulnérabilités et les opportunités d'attaques. La sensibilisation doit être régulière car les risques évoluent en permanence et les mauvaises pratiques reviennent.

2.2 - Cartographie des installations et analyse de risque

Comme pour la sécurité des machines, la seconde étape est un audit de l'installation :

- Quels sont les objectifs métier (production, distribution, protection des biens et des personnes…) et les services assurés ?
- Quels sont les impacts en cas d'interruption de service ? En cas de modification du comportement du système ?
- Quelles sont les fonctions indispensables à l'atteinte des objectifs, et en particulier :
  - leurs niveaux d'implication et de criticité dans la réalisation des services,
  - les systèmes qui les portent,
  - si ces systèmes sont centralisés, distribués, accessibles à distance, etc.

Cela amène donc à un inventaire des installations matérielles (référence de l'équipement, version, protections, accès), de l'architecture réseau et des communications entre les équipements internes et externes. Cela amène également à séparer les équipements critiques devant être très protégés des autres. Les plus critiques, systèmes d'information d'importance vitale (SIIV), doivent être déclarés à l'ANSSI.

L'ANSSI propose une méthode d'analyse du risque nommée EBIOS [1].

2.3 - Prévention : concept de la défense en profondeur

On entre ici dans la partie technique de la cybersécurité : la défense en profondeur consiste à protéger les installations en les entourant de plusieurs barrières de protection autonomes et successives, de sorte d'assurer la protection même en cas de compromission d'un équipement. Ces barrières peuvent être technologiques ou liées à des procédures organisationnelles ou humaines.

Première règle : tout est interdit par défaut. On autorise juste les accès nécessaires aux personnes concernées, on n'ouvre que les connexions UDP/TCP utiles, on n'installe que les logiciels indispensables.

Voici les protections à mettre en place :

- **Protection physique** : c'est la protection la plus simple, les équipements de contrôle-commande doivent être dans des armoires fermées à clé, le local de supervision ne doit être accessible qu'aux personnes autorisées. Siemens propose par exemple des verrous bloquant l'accès aux ports Ethernet des équipements (automates, switch...).

Figure 4 : Verrou Siemens pour prise RJ45 : IE RJ 45 Port Lock

- **Pare-feu** : sur les routeurs et sur les Pcs et automates, on bloque les ports UDP et/ou TCP non utilisés pour empêcher les requêtes indésirables d'arriver jusqu'à la machine. Les pare-feux avancés permettent de faire de l'inspection de paquets en profondeur (le pare-feu vérifie que le contenu d'un paquet arrivant sur le port 502, dédié à Modbus, est bien une requête Modbus par exemple).
- **Cloisonnement des réseaux**, notamment pour séparer le réseau industriel (OT) du réseau de l'administration (IT) : Les VLANs et les pare-feux des routeurs permettent de filtrer les échanges entre un sous-réseau et un autre. On veillera notamment à n'autoriser que les requêtes indispensables à entrer dans le sous-réseau atelier. Il est possible d'installer des **diodes réseau** (les informations ne passent physiquement que dans une direction, ce qui interdit les communications TCP) ou passerelles unidirectionnelles (un peu plus avancées, elles acceptent les établissements de connexion TCP et les acquittements, pour permettre un flux d'information TCP dans une seule direction).
  Il est possible également de mettre une **passerelle de rupture protocolaire**. Celle-ci, en passant le message d'un protocole de communication à l'autre, permet d'éviter l'exploitation de failles dans un des protocoles.
- **Protection antivirale**, les PCs (supervision, programmation) doivent avoir un antivirus à jour. Une procédure explicite de mise à jour des antivirus doit exister.
- **Durcissement des configurations** :

  Pour un PC de supervision :

  - Ne garder que les logiciels indispensables à la supervision (pas de logiciel de programmation des automates, pas de navigateur web, pas de logiciels de bureautique…) ;
  - Bloquer les médias amovibles (clés USB) sur les ports usb ;
  - Mettre un mot de passe sur le Bios pour notamment empêcher un démarrage sur un autre support que le disque de la machine ;
  - Supprimer ou désactiver les fonctions non utilisées mais activées par défaut.
  - Mettre à jour le système d'exploitation et le logiciel de supervision. Il peut être nécessaire pour cela d'avoir une installation miroir réduite pour tester les mises à jour avant leur mise en production ;
  - Distinguer clairement les profils (OS et supervision) utilisateur et administrateur. Le PC de supervision est sur un profil utilisateur (pas de droit pour installer des logiciels) et chacun dispose sur la supervision d'un profil adapté à ses besoins. Chaque personne a des identifiant/mot de passe uniques ;
  - Choisir un logiciel de supervision offrant les meilleures caractéristiques pour répondre aux exigences de sécurité et mettre en place ces fonctionnalités : mécanismes d'authentification, ségrégation des droits (la personne chargée de la maintenance peut acquitter les alarmes mais ne peut modifier les consignes du système par exemple) ;
  - Les logiciels de programmation des automates sont sur des PCs éteints et stockés sous clé ;

  Sur les automates :

  - Changer les configurations par défaut (mot de passe par exemple),
  - Mettre à jour régulièrement le firmware de l'automate (disponible sur le site du fabricant),
  - Supprimer ou désactiver les fonctions non utilisées mais activées par défaut (serveur web, utile pour la configuration mais pas pour l'utilisation, serveur FTP...).

Dans ce cadre de défense en profondeur, des procédures accompagnent ces défenses techniques, notamment concernant les interventions des sous-traitants qui doivent être planifiées précisément (mots de passe, accès, utilisation de ses propres outils ou non, échanges de matériels, qualifications…). L'ANSSI publie un guide de l'externalisation pour accompagner les entreprises dans la mise en place des procédures d'intervention des sous-traitants.

2.4 - Surveillance des installations et détection des incidents

Les équipements réseaux proposent des journaux et pour les plus avancés des alarmes permettant d'indiquer un trafic anormal. Surveiller le réseau en lisant ces journaux système et en configurant ces alarmes mais aussi en formant le personnel à détecter et signaler des comportements suspects de leur machine n'empêchera pas un incident mais permettra de le détecter au plus tôt et d'en limiter autant que possible les effets.

Plus un incident sera détecté tôt, plus il sera possible de mettre en place des mesures pour en réduire et confiner les effets comme par exemple :

- Isoler physiquement les installations en cas d'attaque virale pour limiter les risques de propagation (on déconnecte du réseau les machines),
- Arrêter une installation avant sa dégradation si des données de configuration ne sont plus intègres.

2.5 - Traitement des incidents, chaîne d'alerte

Le dispositif de détection des incidents est associé à une organisation et des procédures pour traiter les incidents :

- Que faire lors de la détection d'un incident ?
- Qui alerter ?
- Quelles sont les premières mesures à appliquer ?

La gestion des incidents doit également intégrer une phase d'analyse post incident qui permettra d'améliorer l'efficacité des mesures déployées initialement.

2.6 - Veille sur les menaces et les vulnérabilités

La sécurité informatique est une action continue nécessitant des efforts permanents (on revient à l'importance du PSSI). La ou les personnes en charge de la cybersécurité du système industriel doivent mettre en place une organisation pour :

- Se tenir informés de l'évolution des menaces, des vulnérabilités, sur le site Internet de l'ANSSI ([1] et [6]) et sur celui des équipementiers qui doivent indiquer les vulnérabilités et les mises à jour disponibles de préférence via des envois d'alerte sécurité.
- Mettre à jour régulièrement les micrologiciels (firmwares) des automates et autres équipements (variateurs, écrans tactiles…) et les systèmes d'exploitation et les applications des PCs de supervision et autres serveurs de bases de données. Comme indiqué précédemment, cela peut nécessiter d'avoir une installation miroir réduite pour les tests de ces mises à jour avant leur mise en production.

L'entreprise doit donc accepter un coût et une période de maintenance pour ces mises à jour et les tests associés. La mise à jour doit parfois passer par la migration d'un OS non maintenu à sa version suivante. Précisément, Windows XP n'étant plus maintenu, il ne devrait plus être utilisé sur

des systèmes industriels critiques. Wannacry a mis en évidence la vulnérabilité de Windows XP et le coût potentiel de sa conservation. (Le coût de Wannacry qui exploitait une faille connue de XP a été estimé entre 1 et 4 Milliards de dollars par différentes agences nationales de sécurité informatique).

Pour les systèmes qualifiés avec des versions d'un firmware et d'un système d'exploitation, il est nécessaire lors de la conception du projet, de prendre en compte la mise à jour des firmwares des automates et des logiciels de supervision et systèmes d'exploitation et d'intégrer des mécanismes de requalification des équipements si besoin. Si ce n'est pas possible (système ancien), le système doit être isolé du réseau avec uniquement des communications précises, surveillées et unidirectionnelles vers le réseau.

2.7 - Les plans de reprise et de continuité

L'objectif du plan de reprise est de se préparer à faire face à des événements exceptionnels pour lesquels toutes les mesures précédentes auraient échoué afin de minimiser les impacts et permettre de redémarrer l'activité le plus rapidement possible.

Il est important pour cela de disposer d'une sauvegarde de chaque automate, des équipements réseau et du PC de supervision, des codes sources et des données et de prévoir des modes de fonctionnement dégradé (le système continue la production, mais moins vite ou avec plus d'interventions manuelles). Les sauvegardes doivent être stockées sur des supports amovibles ou sur des machines éteintes ou déconnectées du réseau (sauvegardes froides).

Pour des systèmes critiques, on prévoira un approvisionnement (automates, PC) pour limiter la durée de l'arrêt de la machine.

3 - Analyse d'incidents

La méthode décrite, le cours reprend à partir des fiches du CLUSIF [3] avec 4 incidents de cybersécurité et invite les étudiants à chercher quelle vulnérabilité a été exploitée et quelle étape de la méthode aurait pu empêcher une telle attaque :

- Fiche 16 : Attaque d'une station d'épuration des eaux
- Fiche 19 : Empoisonnement de l'eau potable
- Fiche 32 : Prise de contrôle du système de production d'une aciérie
- Fiche 4 : Coupure générale d'électricité - BlackEnergy

Ces 4 études de cas montrent qu'à chaque fois, ce sont 2 failles successives qui ont permis l'attaque. La mise en place de la méthode de sécurisation des installations, assez accessible, aurait permis de les éviter.

Les fiches étant bien détaillées, le lecteur pourra s'y référer pour organiser une activité similaire, et y puiser d'autres exemples.

4 - Étude de cas pratique

Le cours de cybersécurité termine par une étude de cas fictive de sécurisation d'un site OIV associé à sa mise en œuvre en Travaux Pratiques sur 12h.

Le contexte : on considère une usine pharmaceutique française disposant d'un atelier de fabrication et d'un atelier d'emballage. L'usine produisant de l'insuline (nécessaire aux personnes

diabétiques), elle est classée Opérateur d'Importance Vitale (OIV). De plus, la réglementation pharmaceutique exige une traçabilité importante de la qualité de la production. Le siège de l'entreprise situé au Danemark héberge la base de données comprenant les autorisations d'accès et doit pouvoir récupérer les données de production de l'usine française.

La supervision des deux ateliers a lieu dans un local de supervision situé dans l'atelier. La supervision, outre l'affichage des informations sur le système (mesures, alarmes… utilisées par les services maintenance et qualité), permet au chef d'atelier de passer certaines machines en mode manuel et de modifier les cadences, notamment pour adapter le débit de la production à celui de l'emballage.

Pour travailler en salle de TP, les IP publiques des routeurs site sont remplacées par des IP du sous-réseau 192.168.2.0/24, qui joue le rôle de réseau « public » de la salle de TPs. Une connexion sécurisée VPN relie le site Danois et le site Français.

L'installation est donc la suivante lors de l'arrivée des étudiants « sur site » :

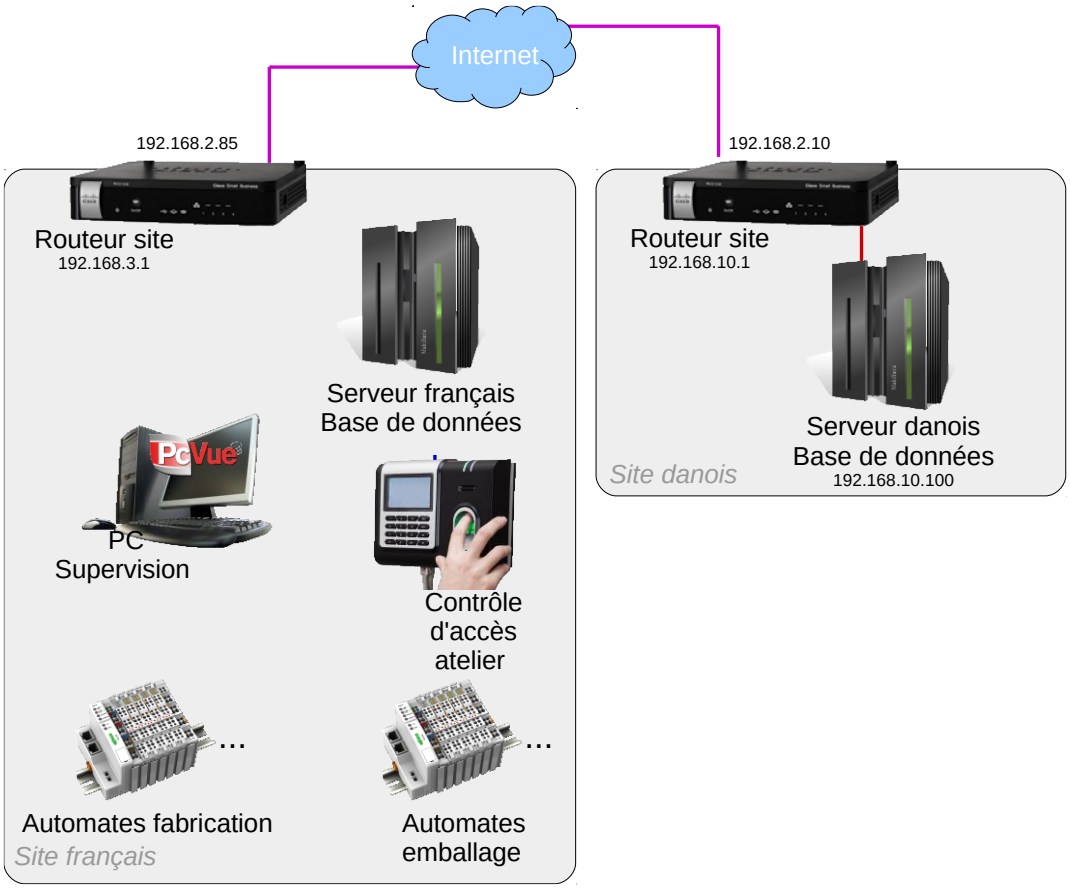


Figure 5 : Equipements de l'entreprise de production avant sécurisation du site

Tout d'abord, les étudiants mettent en place la connexion sécurisée VPN site-à-site entre les 2 routeurs (Cisco RV215W).

Ensuite, les étudiants mettent en place une supervision simplifiée : une entrée Tout ou Rien de l'automate de fabrication remonte à la supervision en modbus TCP. Celle-ci contrôle également une sortie Tout ou Rien de ce même automate.

Les étudiants demandent ensuite au superviseur PCVue le stockage des valeurs de l'entrée et de la sortie de l'automate dans le serveur de base de données SQLServer (requête SQL passant sur TCP/IP).

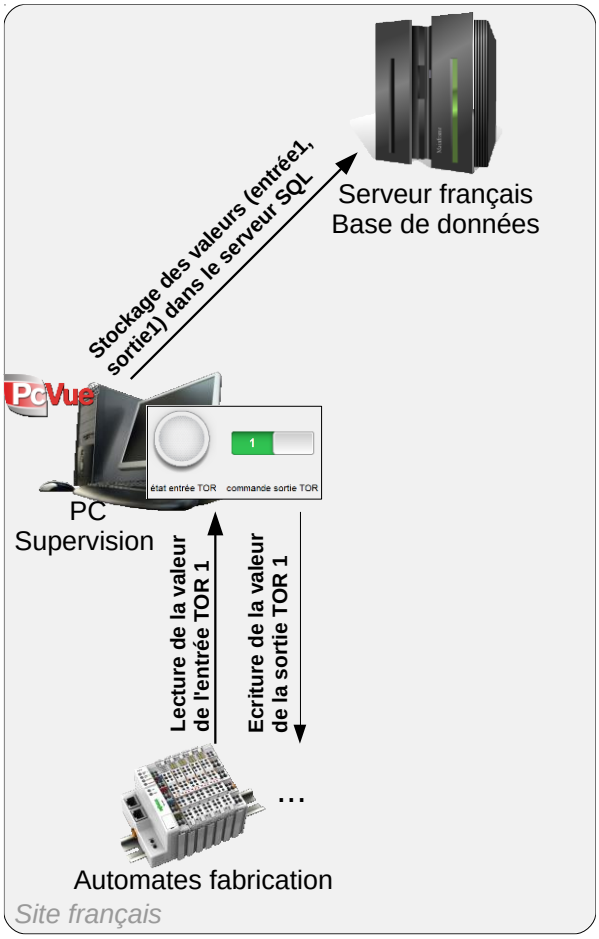


Figure 6 : Echanges entre les équipements du site français

On reprend alors à travers ce TP les différentes étapes de la méthode pour sécuriser un site :

4.1 - Sensibilisation des personnels

Les étudiants doivent expliquer rapidement la mise en place d'une politique de sensibilisation des personnels à la sécurité du site et à la cybersécurité, en insistant notamment sur le phishing, les clés USB, les fichiers douteux, le choix et le non stockage des mots de passe et l'alerte à donner en cas de détection d'un comportement suspect de machine.

4.2 - Cartographie des installations et analyse du risque

Le site étant d'importance vitale et un contrôle à distance non nécessaire (un chef de production est toujours présent sur le site), l'analyse du risque amène à choisir de bloquer tous les accès entrants dans l'atelier.

Les données de traçabilité doivent tout de même être disponibles pour les Danois. Elles seront partagées via un serveur SQL situé à l'extérieur de l'atelier, dans une DMZ. Une DMZ (zone démilitarisée, en référence à la zone « neutre » servant notamment pour l'échange de prisonniers entre les 2 Corées) est un sous-réseau du site accessible depuis l'extérieur et depuis les sous-réseaux sensibles du site (ici, l'atelier). Il n'est pas possible d'accéder au réseau atelier depuis la DMZ. Les équipements des sous-réseaux sensibles y déposent les données que les équipements extérieurs viendront y chercher, sans avoir besoin d'entrer dans le sous-réseau sensible.

Les données pourraient aussi, en plus, être stockées localement sur le PC de supervision (ou sur un serveur SQL dans l'atelier) si l'on voulait être sûr de les conserver en cas d'attaque. Pour tenir en 12h, ce dernier point n'est pas retenu.

Dans les ateliers, l'isolation des réseaux amène à un VLAN et sous-réseau par atelier (192.168.4.0/24 pour la fabrication et 192.168.5.0/24 pour l'emballage) et un VLAN et sous-réseau (192.168.6.0/24) pour le contrôle d'accès du bâtiment. Ainsi, l'infection d'une machine aura plus de mal à se propager d'un atelier à un autre, les zones de diffusion étant segmentées. Le PC de supervision doit communiquer avec les deux VLANs des ateliers. Pour cela, soit sa carte de réseau accepte les VLANs tagués et est rattachée aux 2 VLANs ateliers, avec 2 IP, soit on met 2 cartes réseaux dans le PC de supervision chacune attachée à un VLAN avec une IP dans le sous-réseau associé.

La cartographie des installations et l'analyse du risque amènent les étudiants à proposer l'architecture réseau suivante :

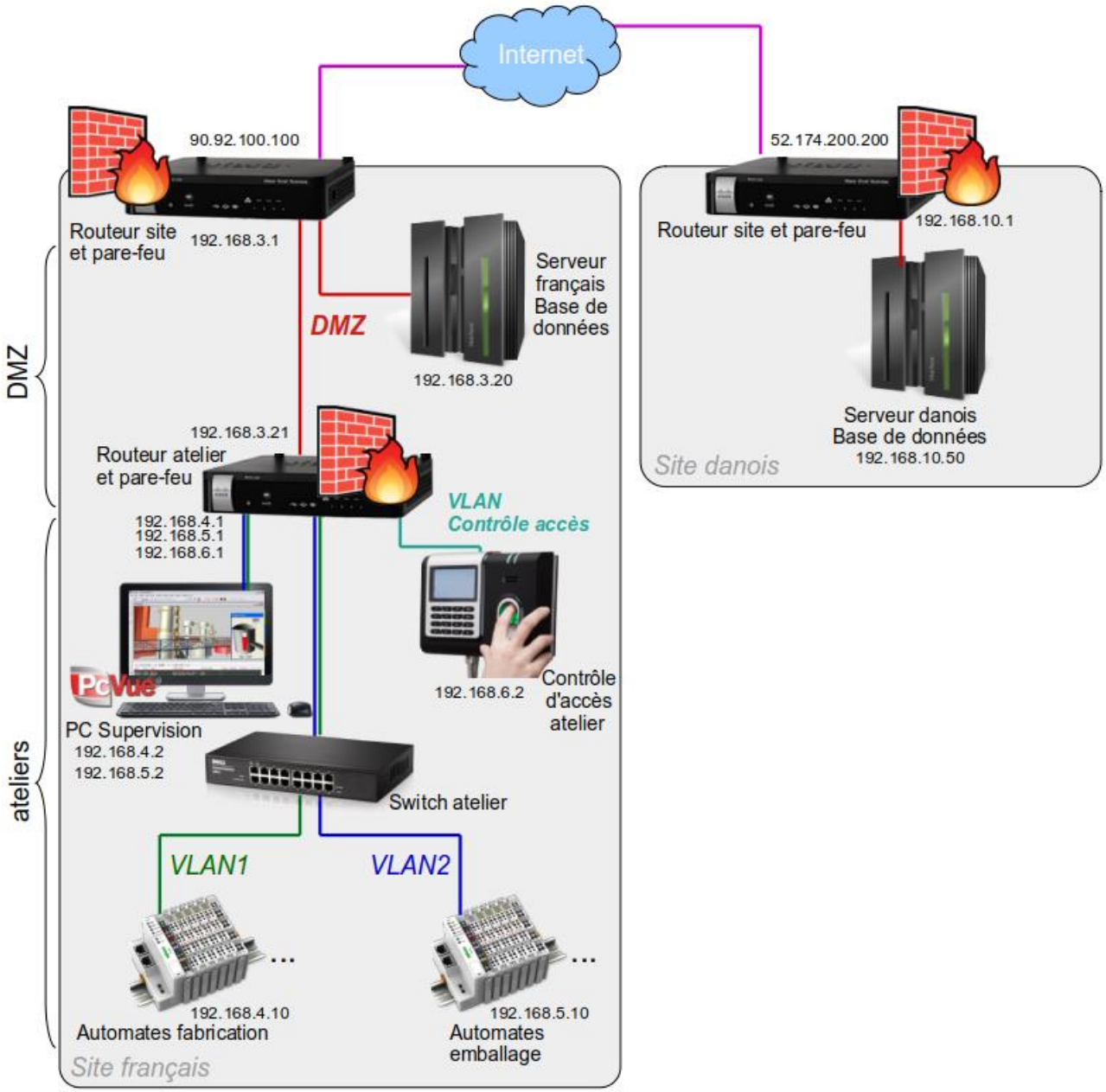


Figure 7 : Architecture réseau de l'entreprise de production de médicaments

4.3 - Prévention : défense en profondeur

Les étudiants câblent leur réseau et abordent alors les différents aspects de la défense en profondeur de l'installation.

4.3.1 – protection physique des équipements

Les étudiants doivent indiquer les mesures de protection physique minimales : armoires électriques et réseaux sous clés, accès à l'atelier et au local de supervision soumis à un contrôle d'accès strict, suppression des accès des employés ayant quitté l'entreprise.

4.3.2 – Cloisonnement des réseaux et durcissement de leur configuration

Les étudiants configurent les pare-feux :

- Le routeur atelier refuse toutes les requêtes entrantes (fonctionnement en passerelle unidirectionnelle) et n'accepte que les requêtes sortantes du PC de supervision vers le port 1433 du serveur SQL.
- Le routeur site français refuse également les requêtes entrantes. Il est configuré en VPN site-à-site avec le routeur site danois, ce qui permet un accès au serveur de base de données français par le serveur danois.

Sur les serveurs de base de données (des PCs équipées de SQL Server Express), SQL Management Studio Express sert de client SQL permettant de lire dans une base de données locale ou distante.

4.3.3 – Durcissement du PC de supervision

Sur le PC de supervision, sur lequel les étudiants sont administrateurs :

- Vérification de l'activation du firewall du PC,
- Établissement d'un identifiant/mot de passe pour chaque utilisateur (le chef d'atelier et le technicien de maintenance) avec des droits limités (pas de possibilité d'installation de logiciels et pas de possibilité de modifier la configuration réseau),
- Établissement également d'une ségrégation des droits sous PCVue. Le chef d'atelier a les droits pour modifier la variable de sortie de l'automate. Le technicien de maintenance peut juste observer les variables,
- Blocage des médias amovibles usb : blocage de la détection des périphériques de stockage USB, désactivation du pilote de gestion des périphériques de stockage USB, désactivation de l'exécution automatique, en suivant la procédure proposée sur le site de l'ANSSI.
- Indication du fait qu'il faudrait supprimer les logiciels autres que le superviseur PCVue du PC, en particulier les logiciels de programmation des automates, très dangereux (ils permettraient à une personne prenant le contrôle du PC de supervision de modifier les programmes de production des médicaments), et les logiciels de bureautique, très attaqués.
- Le PC de supervision étant client des automates serveurs et client SQL, son pare-feu doit être configuré pour ne pas accepter les requêtes entrantes. C'est la configuration par défaut du pare-feu windows. On peut vérifier qu'elle est correcte et que le pare-feu est bien activé au lancement du PC (Menu Sécurité Windows des paramètres de la machine)

4.3.4 – Durcissement des automates

Les étudiants récupèrent le firmware à jour chez le fabricant et le chargent dans les automates.

Ils désactivent le serveur web embarqué de l'automate. Les serveurs web embarqués sont très utilisés pour la configuration des équipements industriels mais sont vulnérables car utilisant des technologies web standard (parfois anciennes, les automates ayant une longue durée de vie).

4.4 - Surveillance des installations et détection des

- Les étudiants utilisent le port mirroring du routeur site et Wireshark (avec des filtres bien choisis) pour surveiller les échanges réseaux. Ils peuvent vérifier que les trames extérieures au site sont bien chiffrées (protocole ESP) et détecter les incidents ;

	Time	Source	Destination	Protocol	Length	Info
379	17.166214	192.168.2.10	192.168.2.85	ESP	310	ESP (SPI=0x51d0f1a7)
380	17.173467	192.168.10.100	192.168.3.102	TDS	246	SQL batch
381	17.174008	192.168.3.102	192.168.10.100	TDS	142	Response
382	17.175583	192.168.2.85	192.168.2.10	ESP	214	ESP (SPI=0x11bfd739)

```
Frame 379: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface 0
Ethernet II, Src: Cisco_aa:c7:24 (10:bd:18:aa:c7:24), Dst: Cisco_ab:c6:99 (10:bd:18:ab:c6:99)
Internet Protocol Version 4, Src: 192.168.2.10, Dst: 192.168.2.85
Encapsulating Security Payload
```

```
Frame 380: 246 bytes on wire (1968 bits), 246 bytes captured (1968 bits) on interface 0
Ethernet II, Src: Cisco_ab:c6:98 (10:bd:18:ab:c6:98), Dst: Dell_04:14:53 (d8:9e:f3:04:14:53)
Internet Protocol Version 4, Src: 192.168.10.100, Dst: 192.168.3.102
Transmission Control Protocol, Src Port: 4854, Dst Port: 1433, Seq: 20248, Ack: 7069, Len: 192
Tabular Data Stream
```

Figure 8 : Surveillance des échanges au niveau du routeur site

- Les étudiants ouvrent les journaux du routeur pour connaître l'historique des connexions VPN ;
- Les étudiants ouvrent les journaux du serveur SQL (accessibles par SQL Management Studio) pour connaître l'historique des connexions au serveur SQL.

4.5 - Traitement des incidents, chaîne d'alerte

Les étudiants proposent une procédure en cas de virus sur le serveur SQL : mise en place d'un archivage (archivage obligatoire pour la traçabilité de la fabrication de médicaments) local par exemple en attendant la remise en état du serveur SQL.

4.6 - Veille sur les menaces et les vulnérabilités

Les étudiants proposent un plan de veille sur les mises à jour de sécurité du fabricant des automates, de Windows et de PCVue.

4.7 - Les plans de reprise et de continuité d'activité

Les étudiants sauvegardent les programmes automates, l'application de supervision et les configurations des 2 routeurs sur un dossier qu'ils expliquent devoir garder sous clé sur une machine ou un support non connecté au réseau.

5 - Étude de cas simulée

Période propice aux discussions sur l'importance vitale de l'industrie pharmaceutique, mai 2020 a amené à faire le TP cybersécurité à distance. Cisco Packet Tracer permet de travailler sur la configuration des équipements réseaux (VPN, pare-feu, VLAN, DMZ), sans toutefois apporter l'ensemble des savoir-faire d'un véritable TP : programmation du superviseur, ségrégation des droits, configuration des restrictions sur les PCs, mise à jour des automates, mise en place des requêtes SQL…

Le fichier pkt « professeur » est donné à titre indicatif en pièce jointe à cette ressource. Toutes les fonctionnalités n'ont pas été testées.

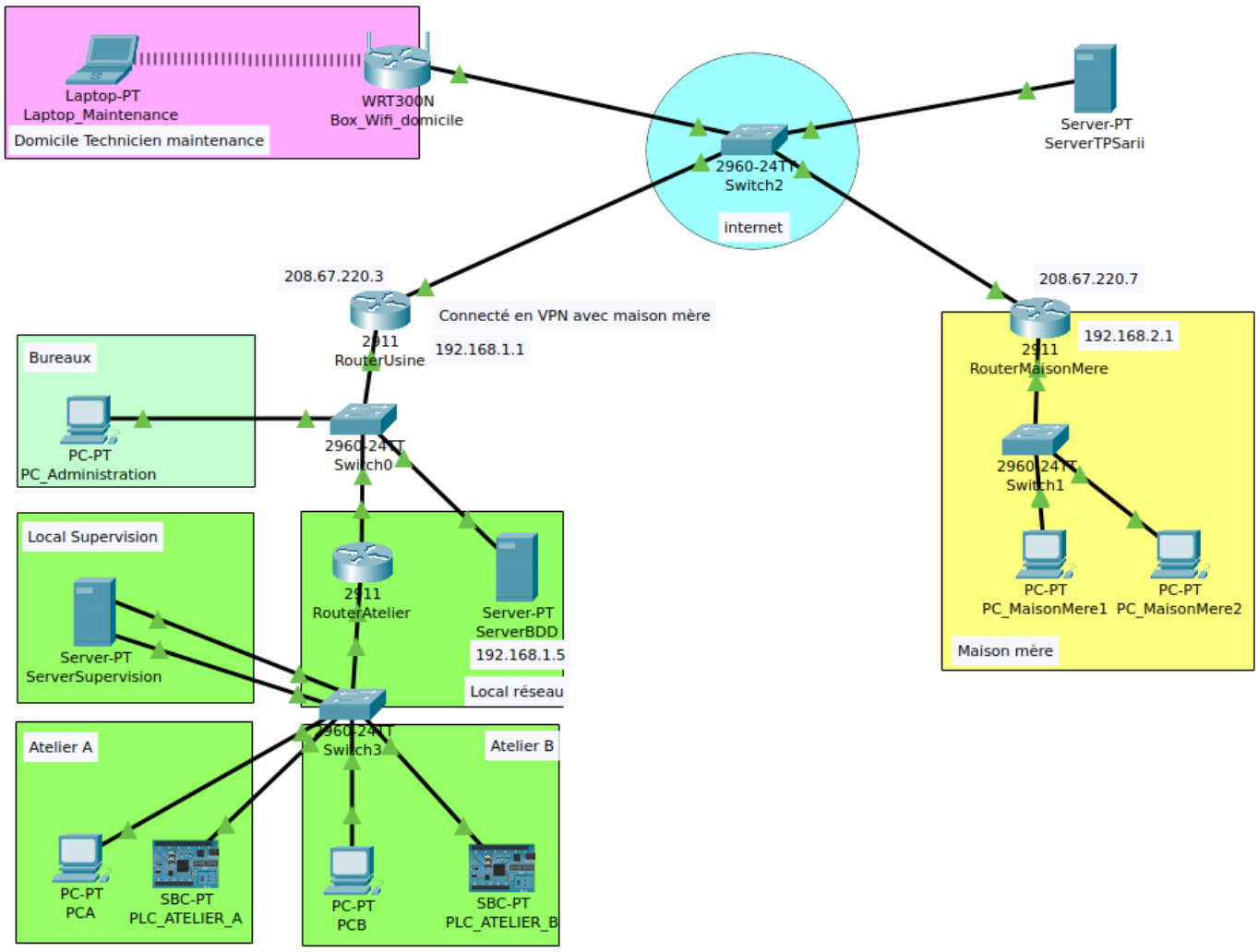


Figure 9 : copie d'écran de l'installation pharmaceutique sous cisco packet tracer

6 - Conclusion

Le cours et le TP cybersécurité des systèmes automatisés industriels permettent aux étudiants d'être sensibilisés au risque cyber, de connaître les principales mesures à mettre en place pour sécuriser un site. Cette séquence pédagogique leur fait prendre conscience que ces mesures, à leur portée, permettent de contrer la plupart des attaques ciblées ou non contre un réseau informatique industriel.

Ce cours/TP est à compléter par la présentation et l'exploitation du protocole sécurisé OPC-UA, pris en compte par les automates industriels modernes (Siemens S7-1500, Schneider M251 par exemple) et objet d'une seconde ressource de ce dossier [5].

Références :

[1]: ANSSI : Publications sur la cybersécurité des systèmes industriels
https://cyber.gouv.fr/publications/la-cybersecurite-des-systemes-industriels

[2]: Guide Cybersécurité des systèmes industriels, Clusif, 2021
https://clusif.fr/publications/guide-cybersecurite-des-systemes-industriels-2021/

[3]: Fiches incidents cyber si industriels, Clusif, 2022
https://clusif.fr/publications/fiches-incidents-cyber-si-industriels/

[4]: Panorama des référentiels - Cybersécurité des systèmes industriels https://clusif.fr/publications/panorama-des-referentiels-2eme-edition-2/

[5]: OPC UA, un protocole sécurisé pour l'automatisme industriel (à paraître)

[6]: ANSSI – CERT-FR : Centre Gouvernemental de veille, d'alerte et de réponse aux attaques informatiques. https://www.cert.ssi.gouv.fr/

[7]: La Revue 3EI – N°93 - juillet 2018 : Cyber-sécurité et réseau électrique, https://eduscol.education.fr/sti/si-ens-paris-saclay/ressources_pedagogiques/3ei-n93-juillet2018-cybersecurite-et-reseau-electrique