Club de la sécurité de l'information français

Conférence CLUSIF

SI Industriels en 2017 :
Incidents, enjeux et… parades

Club de la sécurité de l'information français

CLUSIF

Fiches Incidents Cyber SI Industriels

CLUSIF – Groupe de Travail SCADA

Avril 2017

Présentation du Groupe de Travail "Sécurité SCADA"

GT SCADA

- Le Groupe de Travail SCADA est un groupe d'échange et de partage entre les acteurs de la sécurité informatique du monde industriel. Il regroupe notamment des RSSI, des architectes, des éditeurs et des consultants.
- Les objectifs du groupe sont d'échanger sur les pratiques en matière de cybersécurité des systèmes industriels, d'analyser les tendances actuelles et les évolutions réglementaires.
- Le groupe, créé en 2013, a mené plusieurs travaux qui ont abouti entre autres à la publication d'un panorama des référentiels de sécurité[1].
- En 2016, le GT s'est penché sur les enseignements à tirer des cas d'incidents et d'attaques survenus sur des systèmes industriels avec des conséquences plus ou moins graves selon les cas.

[1] https://clusif.fr/publications/cybersecurite-des-systemes-industriels-par-ou-commencer-synthese-des-bonnes-pratiques-et-panorama-des-referentiels/

Fiches Incidents Cyber SI Industriels

Objectifs

- Les fiches présentées dans ce document ont pour objectif de sensibiliser à la cybersécurité en environnement industriel à partir de cas réels d'attaques, d'incidents ou de preuves de concept pour leur dimension didactique.

- Outre les responsables sécurité des systèmes d'information, le document s'adresse à une population plus large, telle que des techniciens, mainteneurs, intégrateurs, éditeurs, responsables informatiques, responsables d'exploitation et industriels voire des directions générales, amenés à traiter cette problématique.

Démarche adoptée

1 Identification

Dans un premier temps il a été décidé d'**énumérer** l'ensemble des incidents connus des membres du GT.

L'ensemble de recherche était ouvert à **tous les secteurs d'activité**, **tous les pays**. Aucune restriction temporelle n'a d'ailleurs été fixée.

Les contributeurs ont identifié une multitude d'attaques et incidents cyber.

L'apport a été réalisé à partir de **sources ouvertes, publiques**.

2 Sélection

Les incidents selectionnés ayant fait l'objet d'une fiche devaient répondre aux critères suivants:

- **Suffisamment d'éléments** disponibles pour décrire les incidents, le déroulé de l'attaque et les impacts;
- **Sources multiples, concordantes et vérifiables** (magazines, sites web d'information, rapports émanant d'organismes);
- **Atteinte du SI industriel** ou **de son environnement proche**, **ou impact sur la production ou l'exploitation industrielle**.

3 Restitution

Les membres du GT se sont répartis la rédaction des fiches incidents.

Chaque fiche est constituée de 2 pages:

- **Un visuel** et une **description synthétique de l'attaque**;
- Le **déroulé et les impacts** basés sur les sources préalablement identifiées ainsi que les **recommandations du Clusif**.

Comment lire les fiches? 1/2

Présentation du contexte de l'attaque:
- Année(s) au cours de laquelle s'est déroulée l'attaque;
- Secteur d'activité de l'entité touchée;
- Lieu où se trouve l'entité touchée par l'attaque.

Titre de la fiche

Description succincte du scénario d'attaque ou de l'incident et son impact

Visuel illustratif de l'incident

Vulnérabilité exploitée pour mener l'attaque

Club de la sécurité de l'information français

Comment lire les fiches? 2/2

La gravité de l'attaque dépend des impacts constatés. 4 niveaux de gravité ont été identifiés:

- Faible: pas ou peu d'impact
- Moyenne : perte de production ponctuelle, pas d'impact humains, pas d'impacts écologique
- Élevée : perte de production lourde, blessés mais pas de décès, impact écologique
- Majeure : impacts financiers et/ou humains très lourds

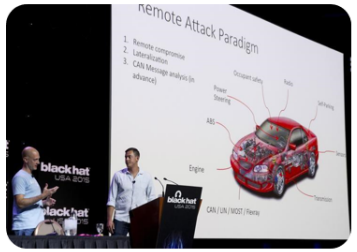
Une description du déroulé de l'attaque basée sur les informations recueillies et consolidées par les contributeurs du GT.

Prise de contrôle d'un véhicule automobile

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Élevée	Sensibilisation	Élevée

Déroulement de l'attaque

- Certaines voitures sont équipées d'une option permettant au conducteur de **contrôler la console de bord par WiFi**. Les chercheurs ont réussi, en découvrant la clé Wifi, à s'introduire dans le réseau sans fil. Ils ont pris le contrôle de la console de bord en **exploitant ses vulnérabilités**.
- Les véhicules du même modèle sont connectés au réseau GSM. En utilisant une antenne GSM, les chercheurs ont réussi à **accéder à distance à la console de bord**.
- Cette console est connectée au CAN bus (réseau interne interconnectant les fonctions du véhicule), à travers un autre composant, le V850.
- En **modifiant le firmware** du V850, les chercheurs ont envoyé des commandes au véhicule.



Moyens mis en

- Deux personnes a… bonnes connaissan…
- Une antenne GSM … ebay
- Un nouveau firmware … reverse engineering

Enseignement à tirer, préconisation et contre-mesures

- Comme pour les SI industriels, les véhicules doivent **cloisonner les fonctions vitales / importantes de transport des fonctions de divertissement**. Les accès au… informatique du véhicule doivent être protégés :
  - La clé Wifi ne doit pouvoir être prédictible (date de sortie de l'usine)
  - Des mécanismes de contrôle d'accès doivent permettre de protéger les véhicules contre des actions non autorisées
- Les mesures suivantes auraient permis de s'en prémunir:
  - **Utiliser un algorithme assurant une génération de clé non prédictible**
  - Mettre en place un **mécanisme empêchant la mise à jour du Firmware** du contrôleur V850 par un code non signé
  - Assurer un **filtrage des communications** entre le contrôleur V850 et le CAN bus (ACL, pare-feu…)

Fiche 13

2015	Transport	Saint Louis, USA	Wired

Les conclusions à tirer de cette attaque ainsi que les messages à transmettre sont présents dans cet encadré.

Rappel du contexte

Quelque(s) source(s) utilisée(s) pour l'élaboration de la fiche

La complexité de l'attaque dépend des moyens mis en œuvre. 4 niveaux de complexité ont été identifiés:

- Faible : pas d'outil nécessaire
- Moyenne : outillage nécessaire, compétence technique simple à acquérir par l'attaquant
- Élevée : outillage nécessaire, compétence technique forte et spécifique
- Très Elevée: développement spécialisé pour l'attaque avec des moyens financiers et humains très importants

Incidents analysés

Énergie

Fiche 1	Interruption de production d'électricité	France	2015
Fiche 2	Coupure générale d'électricité - BlackEnergy	Ukraine	2015
Fiche 3	Exfiltration de données de compagnies d'énergie - Havex	Europe/USA	2013-2014
Fiche 4	Compromission du réseau informatique	Canada	2012

Pétrole & Gaz

Fiche 5	Explosion d'un pipeline	Turquie	2008
Fiche 6	Destruction d'un système d'information - Shamoon	Arabie saoudite	2012
Fiche 7	Explosion d'un gazoduc	URSS	1982

Incidents analysés

Eau/assainissement

Fiche 8	Attaque d'une station d'épuration des eaux	N/C	2015
Fiche 9	Mise hors service d'un superviseur de dérivation d'eau	USA	2007
Fiche 10	Déversement d'eaux usées	Australie	2000
Fiche 11	Empoisonnement de l'eau potable	USA	2013

Transport

Fiche 12	Prise de contrôle de l'aiguillage d'un tramway	Pologne	2008
Fiche 13	Prise de contrôle d'un véhicule automobile	USA	2015
Fiche 14	Perturbation des systèmes de signalisation ferroviaire – Sobig/Blaster	USA	2003

Incidents analysés

Industrie

Fiche 15	Déni de service sur usines automobiles - Zotob	USA	2005
Fiche 16	Prise de contrôle du système de production d'une aciérie	Allemagne	2014

Nucléaire

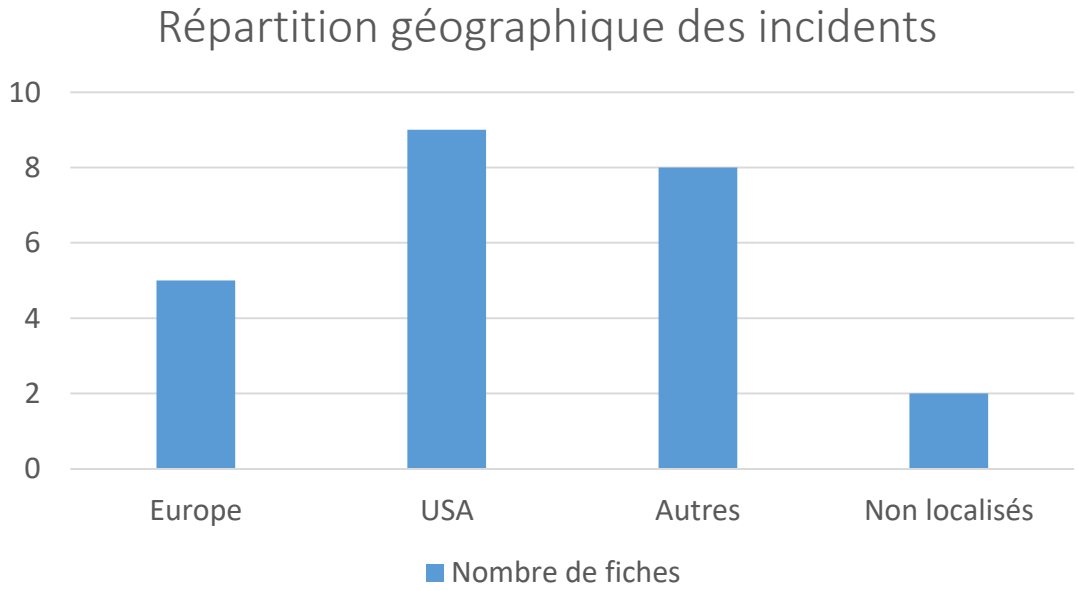
Fiche 17	Divulgation de documents d'une centrale nucléaire	Corée du Sud	2014
Fiche 18	Sabotage d'un processus industriel - Stuxnet	Iran	2009-2010
Fiche 19	Infection par ver dans une centrale nucléaire - Slammer	USA	2003
Fiche 20	Arrêt d'urgence d'un réacteur nucléaire	USA	2008

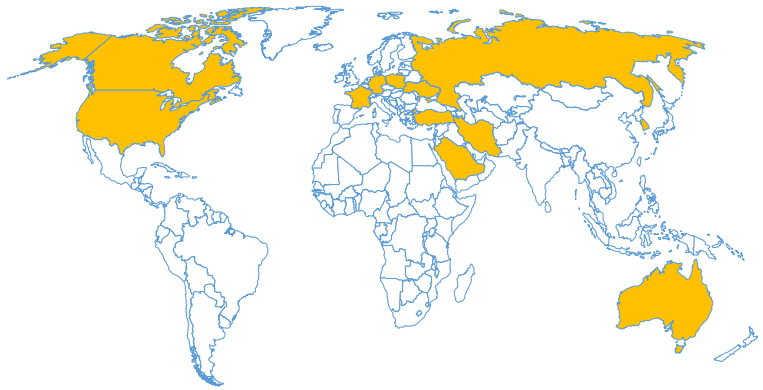
Autre

Fiche 21	Détournement d'un drone de reconnaissance	Iran	2011
Fiche 22	Attaque de terminaux de points de vente - BlackPOS	USA	2013
Fiche 23	Attaque sur une pompe à insuline	Monde	2011

Analyse des incidents

- L'analyse de la répartition géographique des incidents dévoile plusieurs éléments sur la situation économique et réglementaire des pays. En effet on remarque que :
  - Les pays les plus touchés sont les pays industrialisés disposant d'une industrie automatisée.
  - Le pays le plus représenté par ces fiches est les USA. Ceci pourrait s'expliquer par la culture de transparence sur ces sujets, avec de plus une réglementation obligeant les entreprises à signaler certains incidents.

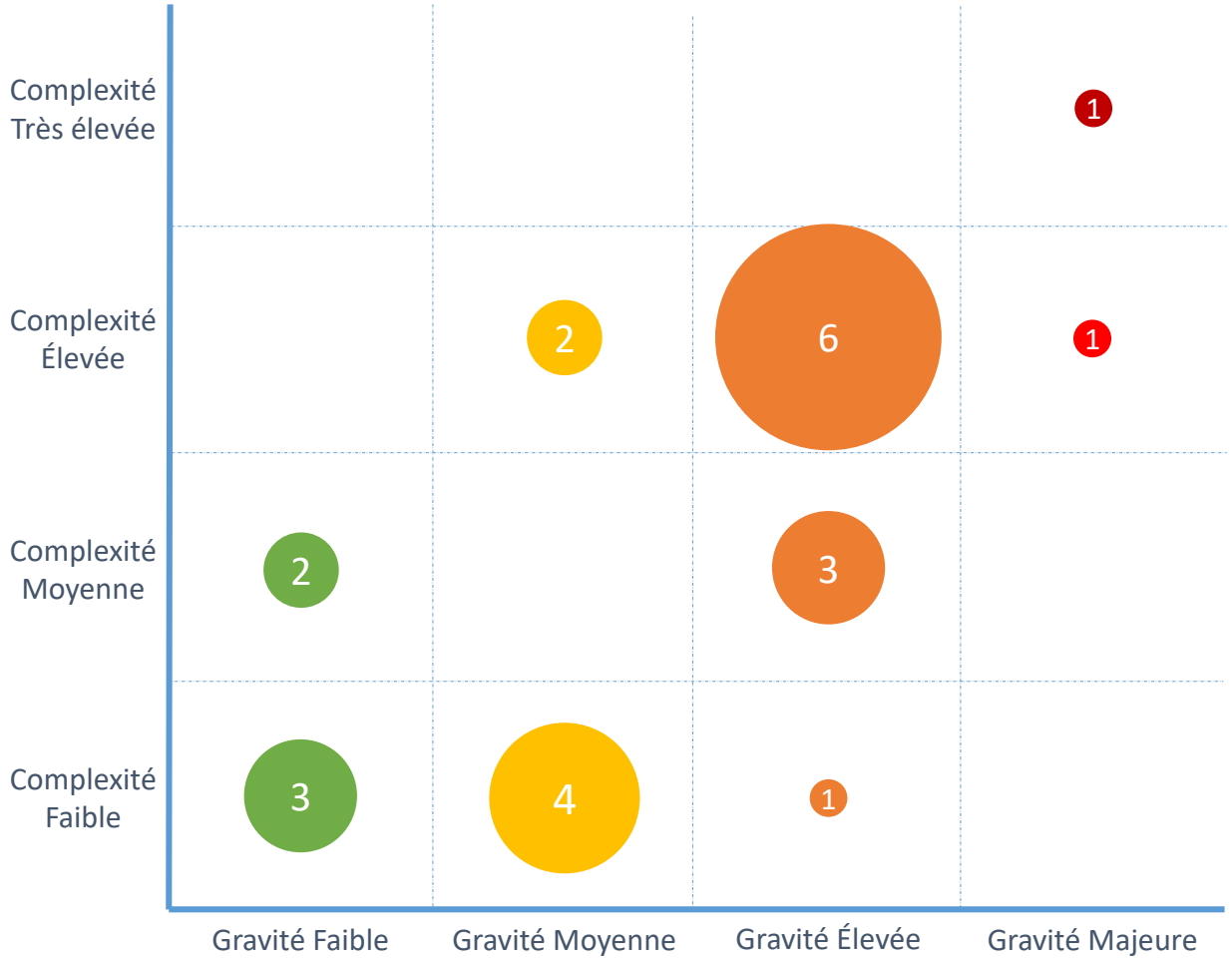




Analyse des incidents

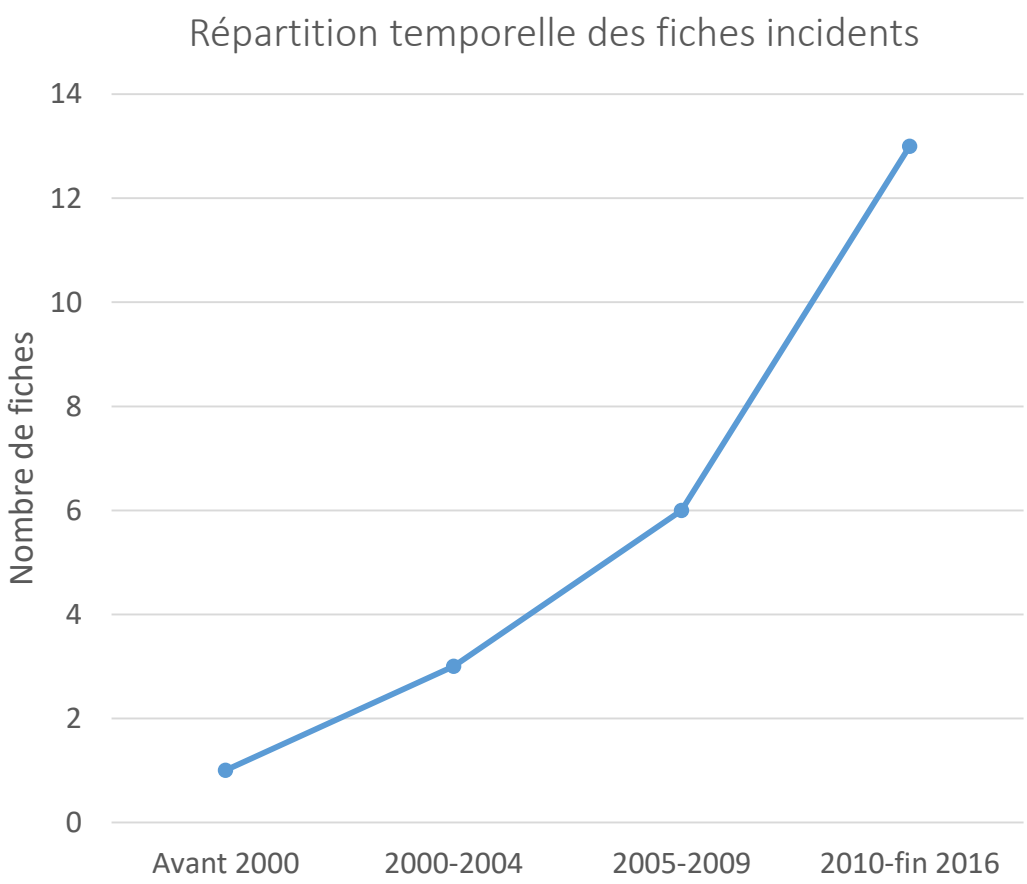
- Le GT SCADA a référencé des attaques sur systèmes industriels dont se sont fait écho la presse et les organismes de sécurité, et cela **quelle que soit leur gravité**.
- Les fiches ont été réparties selon **4 degrés de gravité** (faible, moyenne, élevée et majeure). Pour chaque incident, la complexité de l'attaque a été évaluée selon **les informations disponibles et publiques**. L'évaluation de la complexité s'est faite sur **4 niveaux** (faible, moyenne, élevée et très élevée).
- L'étude croisée de la gravité et complexité des attaques ou incidents permet d'en tirer quelques enseignements :
  - Les attaques de gravité majeure ont un niveau de complexité élevé voire très élevé: elles sont rendues possibles si l'attaquant dispose de **moyens financiers et matériels conséquents** et un **haut niveau d'expertise**. En effet, une attaque sur un système industriel nécessite une connaissance pointue du métier et des processus associés.
  - Cette connaissance ne peut être atteinte que lorsque d'importants moyens ont été mis en place pour la conception de l'attaque, par exemple dans le cas de l'attaque sur le système de distribution d'électricité en Ukraine. Ceci peut expliquer en partie pourquoi **de telles attaques sont encore peu nombreuses**.
  - Le graphique montre que **plusieurs attaques de faible complexité** ont pu avoir des **impacts de gravité moyenne voire élevée**. Ceci illustre bien que **les bonnes pratiques en matière de sécurité ne sont pas toujours appliquées sur les systèmes**.

Nombre de fiches par gravité/incidents



Analyse des incidents

- Les incidents présentés dans ce document représentent une partie des attaques sur les systèmes industriels relayées par la presse ou par les organismes de sécurité.
- Il est à noter que dans le périmètre de ce travail, les attaques ayant eu un impact sur les systèmes de production ou les systèmes d'information industriels (ou réseau proche) sont en **constante augmentation**. Plusieurs facteurs peuvent expliquer cette tendance qui se confirme d'année en année, mais la plus importante est **la connectivité numérique accrue des systèmes industriels**.
- En effet, l'**ouverture** des systèmes industriels aux technologies qui étaient propres au domaine de la bureautique a rendu ces systèmes **vulnérables aux attaques informatiques**.
- De plus, il transparaît au travers de l'analyse de ces différentes attaques que cette transformation des systèmes industriels n'a pas été accompagnée par des **mesures de sécurité adéquates**. **Toutes les mesures possibles sont détaillées par des référentiels de sécurité dont le CLUSIF a dressé un panorama en 2014**. Ce panorama fait actuellement l'objet d'une mise à jour par les membres du GT SCADA, dont la publication est prévue en 2017.



Synthèse

Les incidents sont en nombre croissant, avec plusieurs causes :

- La généralisation des standards des technologies de l'information (IT) : la plupart des protocoles industriels sont à présent déclinés sur TCP/IP, et de plus en plus de logiciels de niveau 2 (supervision, historisation…) voire des composants de niveau 1 (PLC, RTU…) fonctionnent sur des systèmes d'exploitation issus du monde IT.
- L'interconnexion des réseaux industriels avec les réseaux de bureautique, dans des objectifs de performance, de reporting et d'économie.
- Plus généralement, l'ouverture à des systèmes tiers : la sous-traitance des projets, les astreintes distantes et l'externalisation de la maintenance multiplient les accès aux réseaux industriels.

Les principales mesures qui auraient été efficaces au vu de cette liste d'incidents sont :

- Le contrôle des flux logiques (réseaux) et physiques (circulation des personnes, clés USB, PC portables…) aux interconnexions entre le SI de gestion et le SI industriel, et au sein du SI industriel.
- La maîtrise des accès externes aux systèmes industriels avec authentification forte, validation locale, procédure d'isolement en cas d'alerte.
- La surveillance des flux afin de détecter des attaques: les intrusions les plus complexes étant précédées de phases de reconnaissance, la maitrise par l'exploitant des flux légitimes sur son réseau industriel doit permettre de repérer les activités anormales.

Quelles tendances pour les années à venir?

- L'évolution croissante, mais modérée, des incidents reflète en partie **l'augmentation du niveau de menace et de la vulnérabilité** des SI industriels
- La « **démocratisation** » des logiciels d'attaque, comme par exemple la publication du code source Mirai[1], permet à des acteurs avec des moyens limités de réutiliser ces outils à moindre frais : à chaque attaque étatique (Stuxnet, Shamoon, Ukraine) il y a transfert d'idées voire d'outils. Avec **l'émergence de l'industrie 4.0**, l'introduction massive des objets connectés au niveau terrain risque **d'étendre considérablement le niveau d'exposition des SI industriels.** Leur utilisation en contexte urbain introduit aussi des problématiques liées à **la protection des données à caractère personnel** (jusqu'à présent restreintes aux SI de gestion).
- Les **réglementations** se renforcent et exigent dorénavant un niveau minimum de cybersécurité pour les infrastructures critiques qui pour la plupart d'entre elles sont constituées de systèmes industriels.
- Les états se dotent d'un **arsenal cyber** afin d'être en mesure de mener des opérations sur le théâtre cyber : **les systèmes industriels étant des cibles de premier choix** pour la déstabilisation d'un état au regard des impacts que peuvent engendrer les attaques.

Dans ce contexte l'enjeu est de savoir si la prise de conscience du niveau de risque et les plans de sécurisation vont se faire assez rapidement et être suffisamment ambitieux avant que des incidents graves ne surviennent.
Le CLUSIF espère y contribuer via ce jeu de « fiches incidents ».

[1] https://fr.wikipedia.org/wiki/Mirai_(logiciel_malveillant)

Fiches incidents

Interruption de production d'électricité

Impact

Arrêt de production d'électricité pendant **15 jours**

Scénario d'incident

Impossibilité d'accéder au système de communication avec l'hydrolienne à cause d'un **rançongiciel**

Vulnérabilité

Connectivité directe à Internet du système sans protection (absence de pare-feu)

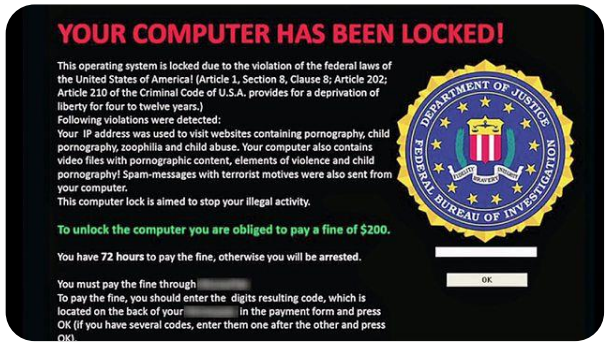
Interruption de production d'électricité

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Faible	Financière	Faible

Déroulement de l'attaque

- Les attaquants ont **chiffré le serveur** permettant la connexion satellitaire avec l'unité de pilotage de l'hydrolienne.
- Ils ont demandé **une rançon de 4000$** à payer par PayPal ou par bitcoin afin de rétablir la connexion.
- Sabella a refusé de payer ce qui a conduit à **une interruption du système** en phase de test pendant 15 jours.



Moyens mis en œuvre

- Un rançongiciel
- Connexion internet

Enseignement à tirer, préconisation et contre-mesures

- **Améliorer le contrôle** et la protection des **systèmes d'accès à distance** (authentification forte).
- Les mesures suivantes auraient permis de s'en prémunir:
  - **Sécurité périmétrique** : Installation d'un pare-feu, passerelle de rebond
  - Mise en place d'un **système redondant** afin d'assurer la continuité de la production
- **Maîtriser la communication de crise** :
  - Éviter de commenter les investigations en cours au risque de donner des informations erronées (attribution de l'attaque à des hackers russo-cubains) risquant d'impacter l'image de l'entreprise (Sabella était en cours de négociation pour développer de nouveaux marchés internationaux)
  - Ne pas dévoiler les nouveaux moyens de protection mis en œuvre

2015 | Énergie | Ouessant, France | Ouest France, Usine Nouvelle

Empoisonnement de l'eau potable

Impact

400 résidents privés d'eau

Scénario d'incident

Modification réglages des taux de fluor et de chlore

Vulnérabilité

Manque de surveillance de l'installation. Accès physique possible sans levée d'alerte

Empoisonnement de l'eau potable

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Moyenne	Vengeance?	Faible

Déroulement de l'attaque

- Les attaquants se sont introduits dans la station **en passant au-dessus des barbelés**.
- Aucune effraction aux portes et aux fenêtres.
- Les attaquants ont eu accès au **système de supervision** et ont **modifié les réglages** des taux de fluor et de chlore.
- Les véhicules des employés possèdent des GPS et attestent qu'aucun d'entre eux n'était près de la station durant l'incident.
- La société gestionnaire de la station a informé la population de l'attaque.

Moyens mis en œuvre

- Une ou plusieurs personnes avec une connaissance de la station
- Pas d'investissement financier

Enseignement à tirer, préconisation et contre-mesures

- La **sécurité des accès physiques** est un paramètre à prendre en compte lors de la sécurisation des SI industriels.
- Les mesures suivantes auraient permis de s'en prémunir:
  - **Contrôle d'accès physique** renforcé
  - **Surveillance des zones à risques**
  - **Révocation des accès au départ d'un employé**
  - **Supervision de la sécurité**

Attaque sur une pompe à insuline

Impact

Modification potentielle des doses d'insuline

Scénario d'incident

Altération et envoi de commandes radio

Vulnérabilité

Données non chiffrées et manque d'authentification des sondes

Attaque sur une pompe à insuline

Club de la sécurité de l'information français

Gravité de l'attaque	Motivation de l'attaquant	Complexité de l'attaque
Faible	Sensibilisation	Moyenne

Déroulement de l'attaque

- Après l'analyse de la documentation constructeur (manuel d'utilisation, analyse des brevets, numéro de série de l'appareil…) un chercheur est parvenu à **intercepter les communications** échangées entre les capteurs et sa pompe à insuline.
- L'analyse des logs a montré que la pompe utilisait entre autre une application JAVA **non obfusquée** qui pilote l'équipement. Le chercheur a alors pu établir la liste des **codes de commande utiles de l'équipement**.
- Le chercheur a imaginé plusieurs scénarios d'attaques : **rejeu** de valeurs transmises à la pompe par les sondes, **envoi de commandes forgées** directement à la pompe (accès physique requis pour connaître le numéro de série nécessaire à l'envoi).

Moyens mis en œuvre

- Antenne radio (pour moins de 100€ sur ebay).
- Connaissances des outils et technologies « radio »

Enseignement à tirer, préconisation et contre-mesures

- Les objets connectés présentent plusieurs vulnérabilités liées au **manque d'intégration de la sécurité lors de leur conception**. De plus, les équipements autonomes **ne présentent pas de système de sécurité (safety)** comme dans les systèmes industriels classiques rendant une attaque potentiellement plus dangereuse.
- Les mesures suivantes permettent de sécuriser ce types d'équipements de santé :
  - Forcer **l'authentification mutuelle** des sondes et pompes à insuline ;
  - **Chiffrer** les signaux échangés ;
  - En conclusion: intégrer la **sécurité dans la phase de conception** de ces objets.