Sécurité des Scada : pourquoi la côte d'alerte est atteinte

A quelques jours de Noël, en décembre dernier, l'Allemagne révélait, dans un rapport gouvernemental, qu'un **haut fourneau d'une aciérie avait été endommagé** suite à une attaque informatique. Si le gouvernement d'outre Rhin n'a pas précisé la nature des dommages subis par cet équipement, l'épisode réveille ce qui demeure la hantise numéro un des services de sécurité des pays occidentaux : la sécurité des systèmes de contrôle industriels (Scada, acronyme de Supervisory control and data acquisition). « *L'Anssi ne va pas s'éparpiller sur des défacements de sites (référence à l'opération OpFrance de ces dernières semaines, NDLR). Notre priorité reste les Scada* », a d'ailleurs expliqué **Guillaume Poupard**, le directeur général de l'Agence nationale de la sécurité des SI lors du Forum International de la Cybersécurité (FIC), qui se tenait en janvier à Lille. Et cet expert d'expliquer s'attendre à une multiplication des événements du type de celui qui a frappé cette usine allemande.

Pourtant, malgré les cris d'orfraie des experts en sécurité, force est constater que les attaques rendues publiques sur les Scada se comptent sur les doigts d'une main. La destruction d'une partie des centrifugeuses iraniennes de Natanz par le **virus Stuxnet** a certes mis en lumière le potentiel destructeur de ce type d'attaques. En 2012, une usine de retraitement d'eau aux Etats-Unis a aussi été victime d'une attaque passant par un système Scada. En juillet dernier encore, un groupe de hackers baptisé Dragonfly avait été mis au jour après avoir infecté un certain nombre de systèmes industriels (mais sans avoir, semble-t-il, utilisé ce potentiel pour affecter des chaînes de fabrication ou des processus industriels). Bref, le haut fourneau d'outre-Rhin, qui ne se serait pas arrêté à temps du fait d'une cyberattaque, ne serait que le quatrième cas avéré de piratage Scada.

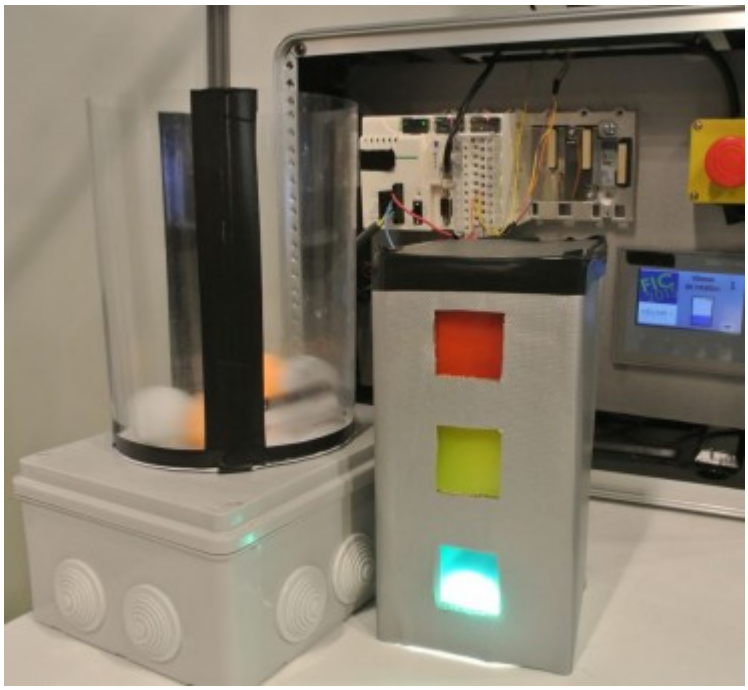
Pas intéressant pour une mafia, sauf…

Dans une interview parue sur Atlantico, **Michel Nesterenko**, directeur de recherche au Centre Français de Recherche sur le Renseignement (CF2R), résume bien la situation actuelle : « *pour les mafias, le coût pour faire une attaque de ce type est démesuré par rapport au son profit potentiel. Quant aux groupes terroristes, ils ne possèdent pas suffisamment de moyens de grande ampleur organisés et coordonnés sauf à enrôler et payer une mafia* ». Toute l'angoisse des services de sécurité et des experts en sécurité réside précisément dans ce 'sauf'.

Car, sur le terrain et malgré les avertissements qui se sont multipliés ces dernières années, le tableau reste inquiétant. D'abord, derrière le terme Scada, se cachent toute une batterie d'équipements industriels mis en service au cours des 20 dernières années. Sans que leur sécurité ait réellement été considérée comme une priorité, voire simplement comme un sujet. « *C'est un héritage du passé qu'il va falloir gérer* », résumait le directeur des activités cybersécurité d'Airbus Defence & Space, **Jean-Michel Orozco**, lors du FIC. « *Il faut donc améliorer le système de patching de ces systèmes, sans provoquer d'arrêt dans les usines ou chaînes de production* », remarque **Arnaud Soullié**, consultant senior chez Solucom.

Récupérer le programme à distance

« *On ne peut pas toucher aux systèmes mis en place il y a 5 ou 10 ans*, complète **Loïc Guézo**, évangéliste sécurité chez l'éditeur Trend Micro. *Or, au cours de cette période, des fabricants de Scada, par exemple dans la santé (machines à IRM), ont introduit des automates basés sur Windows mais vendus comme des boîtes noires. Ces systèmes ne sont donc pas mis à jour. Et des connexions à distance ont souvent été ouvertes sur ces machines, notamment pour assurer des opérations de maintenance.* » En somme, un cocktail détonnant.



Mais résumer la question à un problème de mises à jour de systèmes anciens serait par trop réducteur. « *Même les modèles récents d'automates comportent des vulnérabilités intrinsèques facilement exploitables* », dit Arnaud Soullié. Sur son stand lors du FIC 2015, Solucom mettait en œuvre une démonstration (photo ci-dessus) basée sur **deux automates largement répandus**, de marques reconnues. Et montrait la capacité, via de simples scripts, à **piloter à distance ces appareils**, donc à avoir un réel impact sur le monde réel. Pour les besoins de la démonstration, Solucom prenait la main sur une mini-centrifugeuse (un rappel des effets de Stuxnet) et sur un feu de signalisation. « *Sur un de ces automates, il est possible de récupérer le programme et de le modifier à distance. Cette modification à distance des programmes utiles des automates est présente sur un grand nombre de modèles de toutes marques* », explique le consultant. La détection des systèmes connectés est par ailleurs facilitée par le moteur Shodan.io, moteur de recherche d'adresses IP de terminaux connectés, qui permet en quelques clics de retrouver des automates connectés (voir capture ci-dessous).

Pour faire face à cette situation, l'Anssi pousse à une **classification des sites industriels**, associée à la mise en œuvre de règles strictes de sécurité. Par exemple, au niveau le plus élevé, une interdiction totale de relier les automates à des systèmes connectés à Internet. Mais cette organisation, que décrit l'article 22 de la Loi de programmation militaire (votée en décembre 2013) pour les opérateurs dits d'importance vitale (OIV), tarde à voir le jour. Car le texte de loi doit être adapté, via des arrêtés, aux contraintes spécifiques de 12 secteurs d'activité. Arrêtés qui font nécessairement l'objet de longues discussions avec les organisations concernées. Selon **Franck Gréverie**, le responsable des activités cybersécurité chez Capgemini, la lenteur législative n'a toutefois pas empêché les sociétés concernées de renforcer leurs défenses : « *les grandes entreprises sont aujourd'hui dans l'action, et non plus dans la réflexion* ».

Sécurité versus sûreté

Autre difficulté : l'identification du ou des bons interlocuteurs au sein des organisations. « *Les automaticiens et les DSI ne se comprennent souvent pas trop. Les premiers sont obsédés par la disponibilité et suivent en cela des normes de sûreté, tandis que les informaticiens pensent avant tout en termes de sécurité*, reprend Franck Gréverie. *Notre force, c'est d'arriver avec les compétences des deux mondes*. » A la faveur du rachat d'Euriware (appartenant auparavant à Areva), la SSII s'est en effet doté de compétences spécialisées dans la sûreté de fonctionnement, pour le nucléaire évidemment mais aussi pour d'autres industries comme la chimie ou la production d'énergie. « *Quand la sécurisation des systèmes industriels ne rentre pas dans les attributions du RSSI ou de ses équipes, on a souvent affaire à plusieurs interlocuteurs avec des niveaux de compétence en sécurité très hétérogènes* », note de son côté Arnaud Soullié.

Enfin, les prestataires, rompus à la cybersécurité des SI, sont aussi confrontés à une **offre encore embryonnaire et mal connue**. « *Au sein du partenariat que nous avons noué avec Siemens, nous étudions de futures solutions permettant de sécuriser les environnements du passé. Aujourd'hui, les solutions sur étagère n'existent pas encore »,* explique **Christophe Moret**, vice-président cybersécurité d'Atos, qui s'est également renforcé sur le sujet via le rachat de Bull. Capgemini dit, de son côté, avoir identifié un ensemble de solutions, mais se refuse à en donner les noms pour ne pas orienter ses concurrents ! « *En matière de produits, l'offre est mature sur les firewall réseau et applicatifs, un peu moins sur les sondes* », indique seulement Franck Gréverie, ancien de Bull qui a rejoint tout récemment Capgemini.

La curiosité des Russes, la hardiesse des Chinois

Une bonne partie de cette offre émane de petites sociétés spécialisées aujourd'hui peu connues du monde de la cybersécurité. Même si quelques éditeurs venus de l'IT s'essayent à lancer des produits orientés Scada. Trend Micro a ainsi mis sur le marché deux offres. « *Le fruit d'un effort démarré voici environ deux ans* », indique Loïc Guézo. La société propose notamment une **clef USB embarquant un antivirus**. En cas de détection d'un code infectieux, la diode de cette clef passe de vert à rouge. Un mode de fonctionnement adapté aux processus en usine, selon l'évangéliste. Trend Micro commercialise également une solution **isolant un système industriel**, laissant passer les communications normales mais bloquant tout accès à un nouveau service ou communication inusitée.

Par ailleurs, l'éditeur a mis en place un programme de recherche spécifique, basé sur un réseau de 12 faux sites industriels, simulant le fonctionnement de Scada. Réseau qui a permis d'isoler un grand nombre d'attaques, émanant souvent de Chine ou de Russie. « *Dans ce dernier cas, il s'agit souvent de missions d'observation. Mais les assaillants apparemment issus de Chine sont plus décidés, certains ont été jusqu'à passer des ordres sur nos faux automates* », précise Loïc Guézo. Certaines de ces attaques ont pu être attribuées à APT1 (groupe de hackers chinois identifié par la société américaine Mandiant). Preuve que si les attaques réussies ne barrent pas encore les unes des journaux, les hackers ont déjà beaucoup investi dans la connaissance des Scada.

A lire aussi :

Scada : un virus infecte le nucléaire sud coréen
Thomas Houdy, Lexsi : « Après Dragonfly, réagir sur la sécurité des Scada »
Sécurité des Scada : il est urgent d'agir, selon l'Anssi