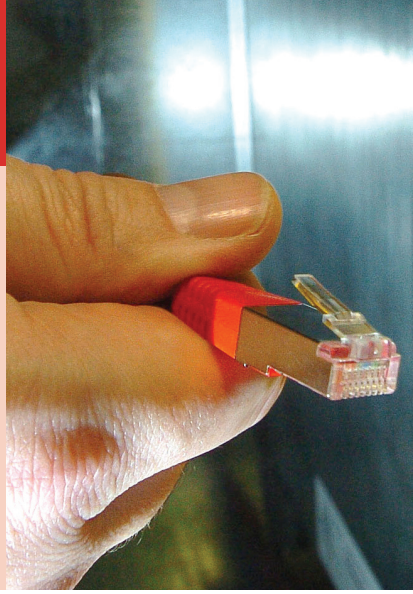


Cybercriminalité, une réalité dans le contrôle/commande

Un grand dossier qui tombe à point nommé. Nous le préparions de longue date, et Stuxnet est venu nous donner le coup de pouce nécessaire. Des parades face à la cybercriminalité existent, mais souvent le bon sens prime.

S'il est un sujet à la mode depuis cette rentrée, c'est bien celui de la cybercriminalité. Même s'il est déjà abordé dans la presse technique, il restait le plus souvent cantonné aux systèmes informatiques dédiés à la bureautique. Le monde industriel étant toujours persuadé qu'il était isolé et puis, coup sur coup, les mauvaises nouvelles sont tombées. L'Iran voyait ses usines d'enrichissement nucléaire tomber en carafe, tout au moins incapable de réaliser certaines actions. Bref, de virtuel, la cybercriminalité rentrait dans le monde du réel industriel.

A priori, rien de plus normal, à partir du moment où les offreurs et les fournisseurs ont décidé, de concert, d'acheter moins cher pour les uns et de rentabiliser leur production pour les autres, tout allait dans le même sens, c'est-à-dire l'utilisation de matériel, aussi bien hard que soft, « grand public ».

Du fil Ethernet standard qui aura été durci au passage, aux clés USB devenues les grands pourvoyeurs de virus, en passant par les outils nomades Iphone et autres tablettes, les industriels se sont, en quelque sorte, tiré une balle dans le pied.

Mais il est trop tard pour faire machine arrière. Qui est prêt à redévelopper des connections différentes entre le monde de la production et celui de la bureautique ? A implanter ses logiciels de supervision sur des OS non Windows, ou Linux ? A proposer des connexions vers l'extérieur via Minitel ?

PAR OÙ COMMENCER ? COMMENT FAIRE ?

Donc, il faut faire avec. Seulement comment faire ? Par où commencer ? Au secours ! crient certaines entreprises, d'autant que dans le même temps la DCRI (Direction Centrale de Renseignement Intérieur), ex-DST, multiplie les conférences de présentations au sein même des entreprises. Ce qui leur permet de voir parfois le regard serein de certains responsables informatiques se transformer au fil des explications, pour devenir trouble en fin de journée.

Lors d'une journée d'information, l'Exera en a remis une couche, mais a également apporté quelques solutions. Vous trouverez, dans ce dossier, des extraits du Guide sur ce thème que l'association vient de publier et qui est un outil indispensable et, à notre connaissance, le seul qui fasse pour l'instant référence dans le monde industriel, la littérature bureautique, l'inverse, ne manquant pas.

Autre élément de ce dossier, le fameux StuxNet, le virus de l'été. Nous vous proposons un décryptage exclusif. Une enquête au cours de laquelle nous n'avons pas tenté de savoir qui étaient les commanditaires : Américains, Russes ou ... car personne ne saura jamais. A l'inverse, il semblerait (tout étant au conditionnel, la démocratie iranienne n'ayant pas fourni d'informations précises et n'ayant pas répondu à nos demandes) que le cheminement du virus ait bien commencé par une clé USB introduite dans un PC hébergeant un superviseur WinCC de Siemens, et qui profitant de quatre vulnérabilités 0-day de Windows, et faisant état de codes de sécurité de chez Realtek semiconductor et de Jmicron Technology, aurait donné des ordres aux automates programmables. Rapidement, un patch a été proposé par Siemens, mais ce n'est visiblement qu'un début. Tout logiciel fonctionnant sur un OS standard pourrait bien faire les frais de virus type Stuxnet.

Lors de la journée de l'Exera, il était intéressant de noter que Frédéric Lenoir, d'EDF RTE, qui, originairement, vient du monde du contrôle/commande, expliquait que ce virus était connu des responsables informatiques en charge de la bureautique, mais totalement inconnu dans l'atelier. Justement, il prône un regroupement de tous les services informatiques au sein de l'entreprise, « *l'époque d'une direction informatique pour la bureautique et d'une direction informatique pour le contrôle/commande doit prendre fin. Nous avons plus de 600 Firewall qu'il faut administrer sans qu'ils deviennent des points bloquants pour*

le réseau. La séparation entre la production et la bureautique était devenue aberrante et contre-productive ».

Une solution appliquée chez RTE depuis deux ans et qui porte ses fruits depuis quelques années. *« Le virus StuxNet, nous le connaissions bien avant qu'il ne pénètre dans le monde du contrôle/commande »*, détaille-t-il.

Il est vrai que les problèmes deviennent redondants, que se passe-t-il lorsque l'IP est en panne ? Plus personne ne peut téléphoner si le téléphone est sur IP, et pour la télémaintenance ? Même résultat. *« Attention que votre télémaintenance ne devienne pas une télécommande »*, prédit Frédéric Lenoir.

COMMENT LE FBI EST ARRIVÉ À CLERMONT-FERRAND

Vous avez sûrement entendu parler de cette descente des Américains dans la ville auvergnate. Tout commencé par un particulier au chômage qui passait son temps à se promener sur Internet. Il est, un jour, tombé sur le nom d'un des patrons de Twitter, puis, de fil en aiguille, a découvert que cet individu avait un site personnel.

Sur ce dernier il a appris plein de détails, jusqu'à trouver qu'il avait un compte Yahoo pour son travail. Trouvant comme excuse la perte de son mot de passe, il a récupéré la classique question *« Quelle est votre lieu de naissance ? »*, en allant sur le site de la personne, il ne fut pas très difficile de répondre.

Prenant la main sur les mails Yahoo, il a déniché certains mots de passe confidentiels de ce patron et a pu rentrer sur le site de Twitter et parvenir à se faire une renommée, en récupérant toutes les informations concernant Barack Obama. Au lieu de fermer son PC et d'en rester là, il a décidé de faire partager sa découverte, le monde des Hackers étant friand de reconnaissance.

Seulement, le FBI s'est penché sur les découvertes de notre Auvergnat, ce qui lui a valu une arrestation et une condamnation. Visiblement, il aurait prouvé ensuite que, certes, il savait naviguer sur le Web, mais n'avait pas de connaissance informatique particulière. Le jeu était, presque, à la portée de tout désœuvré.

UNE ÉVOLUTION RAPIDE VERS L'ÉCONOMIE

Cette cybercriminalité a changé depuis quelques années, elle est devenue véritablement économique avec la volonté de nuire en bloquant les entreprises. A l'origine, on retrouve dans certains pays, comme les pays de l'Est, des centaines de personnes formées dans le domaine informatique avec un travail pour seulement 10 % d'entre eux, le solde s'occupant comme il le peut.

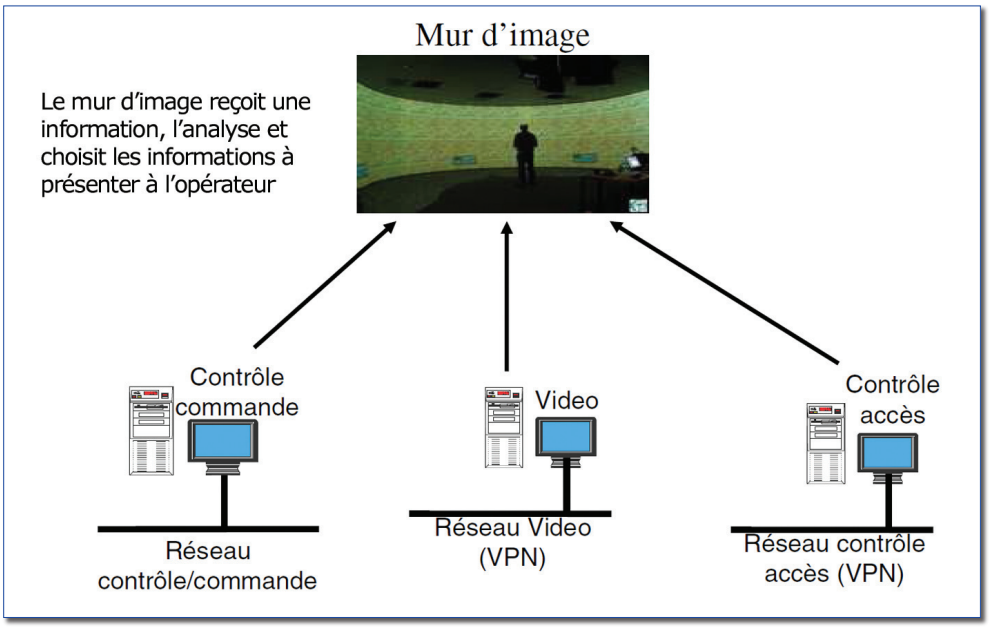
Pour arrêter cette délinquance, c'est pratiquement mission impossible. Il suffit de passer par les mules (ces PC de particulier infectés dans le monde) pour traverser des pays non contrôlables, et le tour est joué.

Et attention à votre smartphone, il n'a pas forcément été prévu pour le monde industriel. Surtout s'il s'agit d'un outil de type Iphone avec des milliers d'applications gratuites dont personne ne sait ce qu'elles contiennent en réalité. La DCRI annonce un tiers d'applications douteuses. Alors pour éviter de vous demander ce qui se passe entre votre PC relié à internet et votre Iphone, lorsque vous les synchronisez, ne mettez en place que des applications dont vous connaissez l'origine. L'application de la RATP devant, a priori, ne pas poser de difficulté, à l'inverse de certains jeux reliés au GPS.

Autre élément à éviter, la clé USB. Certes plus facile à dire qu'à faire. Mais il existe des outils permettant de n'utiliser que des clés codées spécifiques. Le PC rejetant toutes autres clés introduites par erreur.

QUELQUES RECETTES

Lors de cette journée de sensibilisation de l'Exera, chacun y est allé de sa recette. C'est le cas de Jean-Noël Massot, d'Aéroport



de Paris (ADP), pour qui il est difficile de tirer des câbles pour relier deux systèmes distants. *« Les distances d'ADP sont telles que nous n'avons parfois que la solution du Sans-fil »*. Vaste débat, si le code est en tant que tel difficilement cassable, il reste possible de prendre la main sur les équipements en attaquant les couches basses.

Pour Jacques Coutelan, des Eaux de Paris, qui alimente plus de deux millions d'habitants franciliens en eau au travers de 1.800 kilomètres de conduite, il faut *« fermer l'usine Scada. Lorsque nous avons un problème, le Scada envoit automatiquement un SMS, mais il est impossible de lui renvoyer un accusé de réception ou de prendre la main à distance. L'opérateur se déplace »*. Il faut dire qu'en matière d'eau, tout le monde se rappelle un cas de hacking en 2000, en Australie, où un ancien consultant, mécontent, avait à distance ouvert les vannes, déversant des eaux usées dans la rivière. Il avait tout simplement gardé ses codes d'accès à l'usine de traitement. Il serait passé 46 fois, en voiture, devant l'installation, déclenchant l'ouverture des soupapes de décharge.

« Aux Eaux de Paris, nous avons créé un mur d'images qui reprend le signal du système de contrôle/commande, les informations vidéo, les contrôles d'accès... Chaque système décide de lui-même quels types d'images il envoie au mur, ce n'est pas l'opérateur qui les sélectionne à distance. C'est de l'hypervision qui nous permet d'avoir accès en même temps à des informations qui ne communiquent pas entre elles ».

A l'inverse des Eaux de Paris, la firme Total se trouve à la tête d'usines dispersées à travers le monde, le plus souvent en partenariat sur le terrain avec des entreprises d'origines diverses. Pourtant il faut bien que le tout communique, c'est ainsi que Fabien Brière, Group Cybersecurity Manager chez Total, détaille la mise en place d'un réseau dédié. *« Nous avons un responsable sécurité dans chaque site, sur chaque projet, dans chaque branche. Au total ce sont 200 personnes dans le monde qui sont en charge de la sécurité sur le terrain »*. Ce fut le seul moyen de faire appliquer un référentiel commun au groupe. Mais au-delà des bonnes pratiques écrites, restent des soucis qui *« proviennent en majorité de clés USB non-autorisées certes, mais également de virus gravés dans les CD officiels de certains fournisseurs »*. Et pour la télémaintenance, *« dans certains pays, c'est parfois le seul moyen qu'il nous reste pour que le fournisseur sache ce qui se passe »*. Mais à manier avec extrême précaution.

LES FAUSSES BONNES IDÉES

Reste que beaucoup d'informations restent fausses, ou tout au moins erronées. Pascal Sitbon, d'EDF, en cite à la pelle.

Les Firewall ? *« Ils ne protègent en rien des éléments qui passent par lui. Un Pdf traverse le Firewall sans difficulté mais qu'y a-t-il dans le Pdf ? »*. Le seul Firewall qui pourrait avoir grace à ses yeux serait un Firewall unidirectionnel strict, c'est-à-dire sans retour d'un accusé de réception indiquant que le message est bien arrivé car le fait de laisser passer une validation, en retour, laisse une porte ouverte.

Les logiciels sont propriétaires ? N'importe quoi. *« Surtout pour les logiciels dit « propriétaires » qui fonctionnent sur Windows. StuxNet en est l'exemple parfait »*.

Les systèmes sont isolés ? Faux. *« Sur le papier, il est interdit de connecter un portable, une clé USB mais dans la réalité, cela ne marche jamais »*.

La réponse est donc technique ? « Surtout pas ». Le facteur humain reste le plus souvent la clé d'une bonne défense. *« Et ne croyez pas qu'il existe une grille de correspondance entre les problèmes et les solutions »*. Fermez le banc, et n'en jetez plus. ■

APRÈS LES SIL, LES SAL

Vous connaissez les SIL, ce moyen de valider la sûreté d'une installation automatisée, voici qu'apparaissent leur pendant pour la sécurité : les SAL, pour Security Assurance Levels. Ils sont basés sur un principe similaire d'attribution d'une note de 1 à 4, et découpé en 7 tranches, qui va permettre de déterminer le niveau de sécurité d'une installation.

Pour les SIL, le niveau SIL d'un équipement n'a pas intrinsèquement grand intérêt s'il est implanté dans une architecture de SIL inférieur. Pour les SAL, c'est pareil, si vous avez une zone en SAL 1, il faudra la faire évoluer pour avoir un ensemble homogène en SAL 3.