Cybersécurité : les choses avancent

Plus de doute, la défense face aux pirates de tous crins est devenue une priorité pour tous, industriels comme pouvoirs publics. Un an après l'édition du guide de l'Anssi les initiatives se multiplient encore pour protéger les industriels et leurs données.

En 2014 comme en 2013, il ne se passe pas une semaine sans que l'on nous parle de sécurité informatique ! De fait, la cybersécurité est devenue une priorité pour les industriels et l'Etat. « *On observe une véritable prise de conscience et des changements notables sont opérés. Les équipementiers renforcent la sécurité de leurs équipements, les utilisateurs comprennent la nécessité de sécuriser leurs installations, on voit l'introduction de la cybersécurité dans certaines offres et l'Etat engage des actions importantes* », note Stéphane Meynet, chef de projet sécurité des systèmes industriels à l'Agence nationale de la sécurité des systèmes d'information (Anssi). La dernière en date ? Selon la dernière mouture de la Loi de Programmation Militaire, les entreprises au caractère critique pour le bon fonctionnement de la Nation (on parle d'OIV, pour organismes d'importance vitale) devront bientôt faire preuve de leur capacité à résister à de potentielles cyber-attaques. Cette LPM renforcera la sécurité des systèmes critiques autour de quatre grands thèmes : obligation de déclarer les incidents, obligation de mettre en place des moyens de détection, contrôle par les services de l'Etat de l'installation et possibilité d'agir en cas de besoin. Ça bouge, donc…

Tout évolue

L'univers de la cybersécurité est encore très flou. « *Quelle est la menace ? Je n'en sais rien* », lançait ainsi Stéphane Meynet à la dernière réunion du Club Automation, consacrée à ce sujet. Mais une chose est sûre, « *toute entreprise fera l'objet d'une attaque ciblée à un moment ou à un autre, explique-t-il. Si vous n'êtes pas attaqué, c'est que votre boîte ne vaut pas un clou !* » Et les techniques des pirates évoluent aussi. On parle ainsi désormais de pillage de données de façon totalement invisible, de demandes de rançons logicielles, qui consistent à vous infecter

Stéphane Meynet, de l'Anssi.

Un forum dédié à la cybersécurité

La cybersécurité est décidemment un sujet chaud. Au point qu'il existe désormais un événement dédié à ce sujet : le FIC, pour Forum International de la Cybersécurtié, dont la sixième édition se tenait à Lille les 21 et 22 janvier dernier. L'événement, ouvert cette année par Manuel Valls, Ministre de l'intérieur, réunit chaque année les experts de la sécurité (RSSI, DSI…) et des décideurs « non spécialistes » (chefs d'entreprises, DRH, directeurs juridiques…) de tous secteurs. Au programme du « salon européen de référence en matière de confiance numérique » cette année, 40 ateliers et conférences sur deux jours, sur des sujets brûlants tels que « Cloud et sécurité : comment sécuriser la donnée de bout en bout ? », « Cyber menaces : des modes opératoires de plus en plus sophistiqués », « Logiciel libre et cybersécurité » ou encore « La sécurité des systèmes industriels ».

« Mettre la cybersécurité au même niveau que la sûreté de fonctionnement »

Anthony Di Prima, consultant senior en risk management et sécurité de l'information chez Solucom

« Les motivations des pirates sont variées. Elles peuvent être idéologiques, financières, montrer un besoin de suprématie, viser le vol d'informations aux industriels et d'espionnage… Début 2013, L'ANSSI a édité ses 40 réponses minimales de protection contre des attaques diffuses ponctuelles et a récemment publié un ensemble de mesures avancées de cybersécurité pour les SI industriels critiques. Face aux menaces ciblées, il faut aller plus loin et adopter une posture de détection et de réaction. Des solutions techniques et organisationnelles existent. En premier lieu, il est important de mener des audits de sécurité pour mesurer son exposition, mener des analyses de risque cyber, faire des bilans de conformité à des standards. Il faut aussi mobiliser la direction pour réunir le budget nécessaire et réfléchir à la gouvernance à mettre en place. Par exemple, dans l'industrie, les entreprises n'ont pas toujours un Responsable de la sécurité des systèmes industriels. Il faut en nommer un !

Tout est potentiellement important, il faut regarder ce qui est le plus critique et apporter la sécurité au bon endroit. Dans ce domaine, les fournisseurs de matériel ont un rôle à jouer. Les industriels doivent essayer de les influencer pour qu'ils intègrent des fonctions de sécurité, notamment dans les Scada et els automates. La cybersécurtié représente généralement un surcoût de 15 à 20 % sur un produit, mais on obtiendra des gains significatifs si cela est pensé dès la conception.

Certains points sont essentiels. Par exemple, parmi les utilisateurs, les administrateurs doivent être particulièrement surveillés car ils peuvent être davantage ciblés par des attaques. De même, on ne peut pas toujours ne pas autoriser d'interconnexions entre SI de gestion et SI industriels. Il faut donc disposer des barrières successives et mettre en place des systèmes de supervision de passage illégitime d'un système à un autre. Enfin, il est utile de garder une traces des entrées et sorties du personnel et d'utiliser des outils de maintenance sécurisés.

Il reste encore beaucoup de cas où l'on pose des rustines. La crise fait que le marché se tend mais les demandes sont toujours là. Pour avancer, la cybersécurité doit rentrer dans les meurs or, les automaticiens n'ont pas souvent cette culture. Il faut mettre la cybersécurité au même niveau que la sûreté de fonctionnement. C'est comme ça que l'on pourra atteindre la cible. »

avec un virus et à vous faire payer pour obtenir l'antidote, évidemment sans garantie de résultat… Certains pirates emploient également des techniques dites du « point d'eau ». Comme dans la savane, les cybercriminels, patients, empoisonnent un site que vous fréquentez souvent (votre point d'eau) plutôt que de s'attaquer directement à votre structure informatique.

Fort heureusement, « *depuis 2010, les choses changent et le niveau de sécurité augmente dans les équipements* », note Stéphane Meynet. Et au-delà de la LPM, l'Etat s'engage. Il a notamment récemment lancé un programme d'investissements d'avenir sur les moyens de sécurité et un plan de relance industrielle, le plan 33, dédié à la cybersécurité et dirigé par l'Anssi. Et un an après la sortie d'un premier « guide sur la cybersécurité des systèmes industriels », les travaux se poursuivent au sein de l'Agence. Le groupe de travail créé en février 2013 bûche désormais sur une classification des systèmes industriels et la création d'un label pour les produits et les prestations. Objectif : « *labelliser, d'ici à deux ans, tous les nouveaux systèmes industriels critiques* », annonce le chef de projet. L'Anssi se dirige ainsi vers une classification à trois niveaux et proposera des mesures adaptées à chacune des classes. Deux documents devraient donc bientôt être édités : l'un décrivant la méthode de classification et les mesures principales correspondantes, l'autre indiquant les mesures détaillées pour protéger les systèmes. Ensuite, « *nous allons décliner le référentiel par secteur, labéliser des produits et des prestations. Nous sommes en début de réflexion* », déclare Stéphane Meynet. Affaire à suivre…