Cybersécurité : des Hommes de bonne volonté contre le temps qui passe…

Fabien MIQUET
Product & Solution Security Officer
Siemens Digital Industries France

« Et à chaque fois qu'il y a du temps qui passe, il y a quelque chose qui s'efface » écrivait Jules Romains dans *Les Hommes de bonne volonté* (1932-1946). Alors certes, il visait à travers le récit de destins croisés à dresser un tableau de l'évolution de la société moderne au début du XXème siècle quand il écrivit ces lignes… Néanmoins, transposons cette citation dans notre époque en l'appliquant au monde de la cybersécurité et elle pourrait bien faire du père de l'unanimisme un réel visionnaire !

En effet, le couple Homme-Temps est sans doute celui qui résume le mieux à lui seul la problématique qui me passionne et façonne mon quotidien depuis plus de vingt ans…

L'Homme, d'abord

Bien évidemment. Car malgré l'Intelligence Artificielle, le Big Data et la digitalisation accélérée de notre société, l'Homme restera toujours au cœur de la décision et en particulier acteur de la menace cyber. J'ai souvent utilisé, lors de séances de formations formelles ou même dans le but de sensibiliser mes collaborateurs autour de la machine à café – soit dit en passant le meilleur lieu d'évangélisation qui soit et qui nous manque en ces temps contrariés ! – l'image de la passoire afin d'illustrer le caractère asymétrique de cette menace : un système, quel qu'il soit, peut être symbolisé par une passoire, plus ou moins trouée selon le système considéré, sa maturité, celle de ses « utilisateurs », etc. Le cyber défenseur devra alors s'efforcer de boucher en permanence avec ses dix doigts la totalité des trous, quand un attaquant n'aura qu'à exploiter à un moment donné qu'un seul relâchement de la pression d'un auriculaire sur l'un des orifices pour s'engouffrer dans la brèche… Injuste n'est-ce pas ? Mais le monde est ainsi fait et celui de la cyber n'échappe pas à la règle. On y retrouve d'ailleurs le meilleur, mais aussi le pire de l'être humain et ses *vices* sont une source inépuisable de vecteurs d'attaque et de motivations pour les mal intentionnés : comprendre *Vénalité, Idéologie, Compromission & Contrainte, Ego, Sabotage & Sexe*… Cet acronyme, au passage, n'a rien de nouveau, puisqu'il dérive de son équivalent anglo-saxon, le fameux *MICE* ou « piliers de la manipulation » : *Money, Ideology, Compromise & Coercion, Ego* et résume à l'origine les leviers que les services de renseignements actionnent pour corrompre agents et citoyens d'un pays étranger. Néanmoins, et afin de ne pas noircir davantage le tableau, terminons sur une note positive, car même s'il est souvent cité, et il faut le reconnaître à raison, comme étant parfois le maillon faible de la chaîne,

l'Homme peut (et doit !) aussi devenir le meilleur garant de sa sécurité. Sensibilisations et plus encore formations doivent rester en première ligne de notre arsenal de défense : quels sont les risques cyber ? Pourquoi cela n'arrive pas qu'aux autres ? Pourquoi suis-je aussi une cible potentielle ? Quelles sont les bonnes pratiques et les bonnes réactions au moindre doute ? Il est également bon de rappeler, dans le cadre de certains milieux sensibles, que la négligence dans le monde numérique et virtuel vaut malveillance et qu'elle peut conduire à des sanctions pénales, pour le coup, bien ancrées dans le monde réel…

Ainsi, le facteur humain est, et restera omniprésent, qu'on soit défenseur ou attaquant, victime collatérale ou simple témoin des dérives du cyberespace… Et si l'argent est souvent énoncé comme étant le nerf de la guerre, et ce n'est pas l'expert cyber peinant souvent face à son décideur à remplir la case « Retour sur investissement du budget demandé ? » qui dira le contraire, la maîtrise du temps est une des clés menant à la victoire.

La grandeur Temps, ensuite

Définitivement, l'année 2020 ne ressemblera à aucune autre. Mais n'oublions pas, elle aura également marqué les dix ans de Stuxnet, ce ver s'étant attaqué aux centrifugeuses iraniennes d'enrichissement d'uranium. Définitivement, chez Siemens, il y aura eu un avant et un après Stuxnet en matière de cybersécurité. Certes le groupe en 2010 n'était pas novice en la matière, loin de là et on retrouve trace de la prise en compte de la « Sécurité des Systèmes d'Information » appliquée aux systèmes industriels jusqu'à 25 ans en amont, avec notamment la mise en place des premiers contrôles d'accès par mots de passe sur des switchs du constructeur allemand. Autant dire à une époque où l'on faisait, tel Monsieur Jourdain, de la cybersécurité industrielle sans le savoir !

Mais à partir de 2010, tout s'est accéléré. Une prise de conscience mondiale était née, et avec elle une organisation cyber dédiée (on y revient : « l'Homme, d'abord ! »), forte de 1 500 personnes au niveau mondial visant à maintenir au quotidien la pression sur autant de dizaines de doigts pour reprendre la métaphore précédente. Parmi ces cyber-combattants, une équipe en 365/24/7, le ProductCERT Siemens, qui a pour rôle, entre autres, le traitement des alertes et réaction aux cyber-attaques et la gestion des vulnérabilités. Celles sur les produits du groupe, bien évidemment, mais pas seulement, également sur ceux de ses partenaires et de manière générale sur les logiciels que l'on va pouvoir retrouver dans les usines. Ce ne sont pas moins de 53 000 références qui sont gérées actuellement par les experts au quotidien.

L'après Stuxnet, c'est aussi une volonté de monter drastiquement son niveau de maturité et proposer des équipements sécurisés dignes de ce nom avec une gamme complète d'automates programmables, les S7-1500, qualifiés par l'ANSSI, en 2016 d'abord, puis maintenus en qualification en 2019 ensuite. Une qualification n'est jamais qu'une démonstration de robustesse et de confiance que l'on soumet aux autorités, et la décrocher est déjà en soit une belle prouesse. Rappelons d'ailleurs que, souvent convoitée, aucun autre automate à ce jour n'a réussi à se hisser à la hauteur du S7-1500, même près de cinq ans plus tard. Un maintien en qualification va encore plus loin : par rapport à la qualification initiale, démonstration doit être faite de quelles sont les modifications du firmware effectuées (analyse d'impacts), quelles sont les vulnérabilités potentiellement publiées sur la période écoulée, et surtout ont-elles bien été toutes corrigées… En quelque sorte, un maintien en qualification, c'est faire une démonstration de la confiance dans le temps qui passe.

Mais Stuxnet, dix ans après, c'est aussi le reflet d'une persévérance, celle de conserver son rôle de pionnier, de promoteur, encore et toujours, avec trois nouvelles qualifications ANSSI décrochées et officialisées par Siemens il y a quelques semaines à peine, cette fois pour ses automates redondants, qui illustrent parfaitement l'alliance entre sûreté et cybersécurité. Cette dualité est intéressante tant la frontière entre les deux mondes est perméable et demande souvent aux

experts de jouer les funambules sur celle-ci. Tantôt antagonistes (par exemple, j'ajoute un équipement réalisant une fonction « pure cyber », il peut lui aussi tomber en panne, je défiabilise donc mon système dans sa globalité), tantôt collaboratifs (au service d'un objectif commun : la disponibilité !), « safety » et « security » demandent d'apprivoiser le temps. En effet, vaste problème que celui des mises à jour pour ne citer que lui, quand l'informaticien ne jure que par le « PASAP », comprendre le *Patch As Soon As Possible*, et l'automaticien de lui répondre « PAS TOUCHE » à mon système, il fonctionne, la production avant tout et la sécurité ensuite… un grand écart temporel pour un choc des cultures un brin caricatural, mais pourtant encore bien réel de nos jours !

Une bataille perpétuelle

Ainsi va la vie d'un système industriel aujourd'hui, avec ses hommes et ses cultures qui ont tendance à converger moins rapidement que les technologies de l'IT et de l'OT ! Sans la compétence, j'entends par là si nous n'arrivons pas à mettre autour de la table les gens des métiers, les gens de la sécurité, les gens des process et dans l'idéal aussi des profils hybrides facilitant la discussion entre tous, c'est peine perdue, nous n'avancerons pas. Heureux celui qui arrivera à dompter le temps et la progression de ses niveaux de sécurité au cours de celui-ci : celui de ses produits, de ses process, de ses hommes, pour son simple bénéfice d'abord, mais aussi pour celui de ses clients ensuite. Inspirer la confiance n'est pas quelque chose qui se décrète, mais qui se démontre…avec le temps. Heureux encore celui qui trouvera réponse, au juste besoin, à l'orthogonalité entre sûreté et sécurité, qui passe sans aucun doute par une analyse des risques régulièrement reconsidérée et des objectifs bien ciblés : « ce que tout bien considéré, je décide de protéger et contre quoi ». La cybersécurité est en effet de ces disciplines qui exigent une remise en question permanente et une humilité à toute épreuve : qui se vante d'être invulnérable un jour sera confondu en menteur un autre jour, juste une question…de temps !

C'est donc par cette image d'une bataille perpétuelle, et en hommage à tous nos Hommes de bonne volonté, classe à laquelle vous appartenez sûrement si vous lisez ces quelques lignes, que nous fermons cette parenthèse comme nous l'avons commencé, avec Jules Romains à peine adapté pour l'occasion, et gardons à l'esprit cette sainte maxime : « À chaque fois qu'il y a du temps qui passe, mon niveau de sécurité s'efface »…