SystÃ¨mes Industriels : des menaces mal comprises

SÃ©curitÃ©

PostÃ© par : JulieM
PubliÃ©e le : 12/5/2015 14:00:00

DerriÃ¨re le terme gÃ©nÃ©rique de â□□systÃ¨mes industrielsâ□□ se cache une multitude d'environnements, parfois mÃ©connus. Tous prÃ©sentent une caractÃ©ristique commune : ils sont dÃ©sormais vulnÃ©rables aux cyberattaques.
Ces menaces sont-elles aussi importantes que les films de cinÃ©ma - Hacker - ou les jeux vidÃ©os - WatchDogs - voudraient nous le faire croire ? Tour dâ□□horizon de lâ□□Ã©tat des menaces qui pÃ¨sent sur le monde rÃ©el.

â□□SystÃ¨me Industrielâ□□ Ã©veille dans notre inconscient collectif les images du film de Chaplin, les Temps Modernes : des ouvriers Ã la chaÃ®ne, exÃ©cutant des tÃ¢ches rÃ©pÃ©titives et produisant des piÃ¨ces mÃ©caniques. En rÃ©alitÃ©, cette image surannÃ©e est totalement fausse. Dâ□□abord, parce que les usines modernes sont largement automatisÃ©es ; elles Ã©voluent vers un usage massif du numÃ©rique. Ensuite, parce que la majoritÃ© des services dont nous bÃ©nÃ©ficions en tant que citoyens sont des systÃ¨mes industriels.

La production et la distribution dâ□□Ã©nergie, quâ□□elle soit nuclÃ©aire, Ã©olienne ou hydroÃ©lectrique, ou le raffinage et la distribution dâ□□hydrocarbure, sont des systÃ¨mes industriels. Mais nos transports publics, les bÃ¢timents intelligents Ã Ã©nergie positive ou encore les datacenters et leurs climatisations essentielles, et donc toujours disponibles, sont aussi des systÃ¨mes industriels. Cette expression doit Ãªtre comprise avec un spectre large: â□□tout ce qui interagit avec le monde rÃ©elâ□□. Câ□□est pourquoi, dans la littÃ©rature, lâ□□expression Cyber Physical System est souvent employÃ©e.

Le bon fonctionnement de ces systÃ¨mes industriels est assurÃ© par des rÃ©seaux sur lesquels on trouve une multitude de composants. Ces automates, instruments, calculateurs ou encore stations de supervision sont de plus en plus intelligents. A titre d'exemple, les derniers dÃ©bit-mÃ¨tre -- Ã©quipements permettant de contrÃ´ler le dÃ©bit d'un fluide dans un process -- sont Ã©quipÃ©s d'une carte Ã©lectronique faisant tourner Linux et possÃ©dant mÃªme un serveur web oÃ¹ lâ□□on peut configurer et superviser le composant.

Quand on sait qu'il existe des centaines, voire des milliers, de ces Ã©quipements, on touche du doigt lâ□□idÃ©e de l'Internet Industriel : un ensemble de rÃ©seaux interconnectÃ©s, composÃ©s d'objets intelligents, de Cyber Physical Systems. Lâ□□objectif de ces rÃ©seaux, Ã la diffÃ©rence des rÃ©seaux â□□informatiquesâ□□ dont lâ□□objet est de traiter de lâ□□information, est de piloter et contrÃ´ler un processus physique (contrÃ´le / commande).

Câ□□est pourquoi, mÃªme sâ□□ils emploient pour partie des technologies identiques, les prioritÃ©s en terme de protection sont elles trÃ¨s diffÃ©rentes. Chaque partie est animÃ©e par un logiciel. Ainsi, l'ensemble de ces objets comportent-ils des failles, des vulnÃ©rabilitÃ©s apportÃ©es par ces logiciels.

Ces menaces sont-elles illusoires ? RelÃ¨vent-elles uniquement des films hollywoodien Ã succÃ¨s ? Dans Hacker, le dernier film de Micheal Mann, la centrale nuclÃ©aire de Chai Wan, Ã Hong Kong, a Ã©tÃ© piratÃ©e et l'insÃ©curitÃ© informatique mondiale conduit Ã lâ□□Ã©croulement des marchÃ©s.

Malheureusement, si le piratage totale dâ□□une centrale nuclÃ©aire relÃ¨ve encore de la fiction, de nombreux exemples rÃ©els et concrets nous montrent la rÃ©alitÃ© de ces menaces.

Le 2Ã¨me port europÃ©en victime dâ□□une cyber attaque

En 2011, le port dâ□□Anvers a Ã©tÃ© la cible cyber-attaque d'envergure par une organisation mafieuse de trafic de drogue. Les trafiquants ont recrutÃ© des pirates afin de pÃ©nÃ©trer les systÃ¨mes informatiques qui contrÃ´lent le mouvement et l'emplacement des conteneurs maritimes. Ils cachaient leur butin au dÃ©part et, grÃ¢ce aux pirates, envoyaient des chauffeurs, armÃ©s de mitrailleuses, rÃ©cupÃ©rer leur chargement avant que les dockers du port ne les aient dÃ©barquÃ©s et ouverts. Leurs gains Ã©taient confortables, la police belge a saisi deux tonnes de cocaÃ¯ne et d'hÃ©roÃ¯ne et une valise bourrÃ©e de 1,7 million $.
MÃªme si elle avait Ã©tÃ© alertÃ©e de la disparition de quelques conteneurs, la police belge a pu interpeller les trafiquants uniquement Ã cause dâ□□une guerre des gangs sanglante. Sans cela, le hack du systÃ¨me industriel du port nâ□□aurait jamais Ã©tÃ© dÃ©couvert.

Un olÃ©oduc victime dâ□□une cyber explosion

Majoritairement dÃ©tenue par BP, l'olÃ©oduc Bakou-Tbilissi-Ceyhan a Ã©tÃ© construit pour Ãªtre l'un des plus sÃ»rs au monde. Ce pipeline gÃ©ant est Ã©quipÃ© de centaines de capteurs et de camÃ©ras pour surveiller les 1 800 kilomÃ¨tres. Ces systÃ¨mes de sÃ»retÃ© nâ□□ont pas permis dâ□□Ã©viter une explosion, projetant des flammes de 50 mÃ¨tres de haut et stoppant lâ□□exploitation du pipeline durant 3 semaines.

La communication autour de lâ□□incident a Ã©tÃ© chaotique. Le gouvernement turc parle dâ□□un accident mais les sÃ©paratistes kurdes ont revendiquÃ© une cyberattaque.
Les cyber attaquants ont pris le contrÃ´le du rÃ©seau de contrÃ´le commande. Ils ont volontairement leurrÃ© les systÃ¨mes dâ□□alarmes, coupÃ© les communications externes et augmentÃ© la pression de faÃ§on considÃ©rable au sein de lâ□□installation. VoilÃ pourquoi lâ□□explosion nâ□□a pu Ãªtre identifiÃ©e et pourquoi elle a causÃ© autant de dommages matÃ©riels.

Si lâ□□incident a Ã©tÃ© rendu public il y a quelques mois, les faits remontent Ã 2008.

Sortir de la posture du dÃ©ni

Face Ã ces menaces avÃ©rÃ©es, les responsables dâ□□installations industrielles doivent changer de comportement. Aujourdâ□□hui, ils sont dans la posture du dÃ©ni : â□□mon rÃ©seau est fermÃ©, rien ne peut mâ□□arriverâ□□. Face Ã une nouvelle classe de menaces qui nÃ©cessite des investissements consÃ©quents, câ□□est un mÃ©canisme de dÃ©fense naturel. Cette attitude empÃªche de dÃ©marrer les premiers projets de cybersÃ©curitÃ© nÃ©cessaires. Plus encore, elle met en danger la sÃ©curitÃ© des usagers et en pÃ©ril la propriÃ©tÃ© intellectuelle de leurs entreprises.

Les directions gÃ©nÃ©rales et leur unitÃ© opÃ©rationnels se doivent donc de penser rapidement Ã la cybersÃ©curitÃ© de lâ□□ensemble de leur systÃ¨mes industriels, quâ□□il sâ□□agisse de leur outils de production mais aussi de leur infrastructures (bÃ¢timents, datacenter, gestion dâ□□Ã©nergie) ou leur produit (conteneurs maritimes, voitures connectÃ©s, systÃ¨mes embarquÃ©s en gÃ©nÃ©ral).

Lâ□□arrivÃ©e sur le marchÃ© de solutions innovantes, conÃ§ues par des startups, devrait permettre dâ□□ouvrir les esprits. Une Ã©volution vers une approche plus pragmatique est attendue, centrÃ©e dâ□□abord sur la cartographie des flux du systÃ¨mes, lâ□□inventaire dÃ©taillÃ© et ainsi, la comprÃ©hension des dÃ©pendances et des faiblesses rÃ©siduelles. Câ□□est le point de dÃ©part Ã une gestion pÃ©renne de la cybersÃ©curitÃ© des systÃ¨mes industriels, affirme Laurent Hausermann, Directeur AssociÃ© de Sentryo.