CybersÃ©curitÃ© Industrielle, que doit-on craindre ?
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 27/11/2015 13:30:00

Quâ□□on les appellent Industries 4.0, Smart Grids ou BÃ¢timents Intelligents, tous les secteurs industriels construisent aujourd'hui leurs usines du futur. Plus quâ□□une rÃ©volution, câ□□est une Ã©volution, car depuis plusieurs annÃ©es, des systÃ¨mes numÃ©riques contrÃ´lent des environnements critiques.

Â
Quel serait l'impact une cyberattaque visant prÃ©cisÃ©ment ces systÃ¨mes industriels ? Perte d'exploitation, dÃ©sorganisation de lâ□□Etat Nation, risques mortels pour des individus sont aujourd'hui Ã portÃ©e de clics pour les acteurs malveillants. Tour d'horizon de ces impacts.

L'industrie, comme tous les autres secteurs Ã©conomiques, doit rÃ©ussir sa transformation digitale : plus de technologies numÃ©riques pour plus de services personnalisÃ©s et de meilleure qualitÃ©. Les initiatives tournÃ©es vers le numÃ©rique sont multiples dans l'industrie.

Â Lâ□□usine du futur se construit en utilisant le Big Data et en intÃ©grant verticalement tous les composants. Les professionnels du bÃ¢timent se tournent rÃ©solument vers les bÃ¢timents intelligents et les Smart Cities pour augmenter le niveau de service fourni aux usagers.

Le secteur de l'Ã©nergie cherche des solutions aux enjeux environnementaux et de veut rendre notre production, distribution et consommation dâ□□Ã©lectricitÃ© et de gaz plus intelligents au travers des rÃ©seaux et des compteurs intelligents. Les enjeux sont multiples : redynamiser lâ□□Ã©conomie europÃ©enne, stopper le rÃ©chauffement climatique ou encore doper lâ□□innovation.

Cette Ã©volution est en marche depuis plusieurs annÃ©es. Elle s'accÃ©lÃ¨re et passe par un usage massif de systÃ¨mes de contrÃ´le numÃ©rique. Ces derniers sont aujourdâ□□hui prÃ©sents au coeur mÃªme des procÃ©dÃ©s industriels qui contrÃ´lent notre monde rÃ©el.

Malheureusement, ce nÃ©cessaire renouveau pourrait Ãªtre anÃ©anti par le risque cyber. De nombreuses Ã©tudes ont dÃ©montrÃ© sa dangerositÃ©. La derniÃ¨re en date a Ã©tÃ© publiÃ©e en Septembre par le think tank britannique Chatham House. En particulier, elle se concentre sur le secteur nuclÃ©aire et montre combien certaines centrales, de part le monde, sont vulnÃ©rables.

Cette Ã©tude pointe aussi du doigt l'absence de culture de la cybersÃ©curitÃ© dans lâ□□industrie et le manque criant de budgets dÃ©diÃ©s Ã cette problÃ©matique au niveau mondial.

Pour mesurer l'impact que pourrait avoir une cyber-attaque sur un systÃ¨me industriel, analysons en dÃ©tail trois secteurs : lâ□□industrie manufacturiÃ¨re, les infrastructures de transport et la la production dâ□□Ã©nergie.

Tout dâ□□abord, lâ□□industrie manufacturiÃ¨re manipule des matiÃ¨res brutes, les transforme et gÃ©nÃ¨re des produits finis. Un criminel pourrait chercher Ã rÃ©aliser une extorsion de fonds auprÃ¨s d'un industriel par le biais d'un chantage. En effet, les cuves remplies de produits chimiques transformÃ©s valent chacune plusieurs dizaines de milliers d'euros.

Le criminel introduit dans le systÃ¨me pourrait dÃ©cider de mÃ©langer, et ainsi corrompre, ou de vider tout simplement la cuve. Lâ□□impact serait alors une perte d'exploitation massive. Elle se rÃ©pÃ©terait tant quâ□□une ranÃ§on ne serait pas payÃ©e. Dans le milieu de lâ□□entreprise, on a dÃ©jÃ vu des entreprises payer des maÃ®tres chanteurs qui avaient chiffrÃ© leurs ordinateurs

portables.

Dans le secteur des transports, l'impact est liÃ© Ã la disponibilitÃ© des infrastructures. Imaginez un tunnel routier au coeur d'une ville. Il est contrÃ´lÃ© par un systÃ¨me SCADA. Si un groupuscule aux sombres motivations, prenait le contrÃ´le du SCADA et coupait la ventilation, lâ□□Ã©clairage du tunnel et en changeait les feux rÃ©gulant le sens de la circulation, il provoquerait Ã coup sÃ»r une immense pagaille !

En 2006, des salariÃ©s mÃ©contents de la ville de Los Angeles ont rÃ©ussi Ã causer plusieurs jours de bouchons routiers en ayant uniquement modifiÃ© le programme de quatre feux tricolores. Ils ont reconnu sâ□□Ãªtre connectÃ©s depuis leur domicile durant une grÃ¨ve au rÃ©seau municipal. La disponibilitÃ© des routes, tunnels, ports, gares ou aÃ©roports est essentielle Ã notre vie de tous les jours. Leur rÃ©seaux industriels sont critiques.

Enfin, les impacts les plus Ã©vidents sont liÃ©s Ã la dangerositÃ© de certaines installations dans le domaine de l'Ã©nergie. Les industriels y manipulent des produits hautement rÃ©actifs ou inflammables qui peuvent exploser et provoquer des blessures graves ou causer la mort. Nous vivons tous Ã cÃ´tÃ© d'installations Seveso, de centrales nuclÃ©aires, de stockage de gaz.

DÃ©sormais, un terroriste cherchant Ã provoquer un chaos colossal se tournera sÃ»rement vers les rÃ©seaux industriels. Le FBI dÃ©clarait il y a peu que DAECH avait cherchÃ© Ã pirater le rÃ©seau Ã©lectrique amÃ©ricain. A priori, ses capacitÃ©s techniques sont aujourd'hui rÃ©duites et insuffisantes pour rÃ©ussir une telle attaque, mais il est Ã©vident que l'impact serait catastrophique et provoquerait des milliers de morts.

Face Ã tous ces risques, faut-il stopper la transition digitale de l'industrie europÃ©enne ?

Non, bien sÃ»r ! Mais des mesures doivent Ãªtre prises. La cybersÃ©curitÃ© doit dÃ©sormais s'intÃ©grer Ã l'ensemble des processus industriels. Elle doit Ãªtre prise en compte dÃ¨s la conception des systÃ¨mes. Plus urgent encore, les industriels eux-mÃªmes doivent entrer dans une posture de prÃ©vention et de surveillance : sortir du â□□Ã§a ne peut pas mâ□□arriverâ□□, ne plus se croire protÃ©gÃ©s et surtout veiller Ã la sÃ©curitÃ© de leurs installations.

Cela est impÃ©ratif pour la pÃ©rennitÃ© de leurs entreprises et la vie de leurs clients. Commente Laurent Hausermann - Co Founder de Sentryo