Renforcer la cybersÃ©curitÃ© des acteurs de lâ□□Ã©nergie.
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 26/4/2023 13:00:00

Les entreprises du secteur de lâ□□Ã©nergie, de lâ□□eau et dâ□□autres infrastructures critiques sont quotidiennement confrontÃ©es Ã des cyberattaques. Les services publics sont lâ□□un des secteurs les plus ciblÃ©s dans tous les pays. Pourquoi ? En raison des ravages potentiels quâ□□une intrusion peut causer chez ces acteurs.

Les menaces Ã©voluent plus vite que la cybersÃ©curitÃ© ne peut le faire. Que veulent les pirates informatiques ? Voler des donnÃ©es confidentielles appartenant Ã lâ□□organisation visÃ©e, Ã ses clients et ses fournisseurs, et envahir les systÃ¨mes de contrÃ´le.

Souvent, une attaque peut provenir dâ□□un Ã©lÃ©ment aussi petit et apparemment inoffensif quâ□□une clÃ© USB. Le tristement cÃ©lÃ¨bre virus Stuxnet qui a infiltrÃ© une centrale nuclÃ©aire iranienne en 2010 provenait dâ□□une clÃ© USB utilisÃ©e par un ingÃ©nieur sur son ordinateur personnel.

Sâ□□adapter Ã lâ□□organisation et aux spÃ©cificitÃ©s des Ã©quipes

Une main-dâ□□Å□uvre de plus en plus mobile implique des risques encore plus Ã©levÃ©s, et plus de la moitiÃ© des entreprises du secteur de lâ□□Ã©nergie et des services publics craignent dÃ©jÃ que leurs collaborateurs Ã distance aient Ã©tÃ© piratÃ©s.

Avec la montÃ©e en puissance du BYOD, une cyberattaque est dÃ©sormais inÃ©vitable. Les clients de Peopleâ□□s Energy se sont vu voler leurs coordonnÃ©es lors dâ□□une importante attaque en 2020, lorsquâ□□un tiers non autorisÃ© a eu accÃ¨s Ã ses systÃ¨mes de stockage de donnÃ©es. Et en 2018, un vol de donnÃ©es par un tiers sur une vanne de rÃ©gulation intelligente a presque dÃ©truit une usine chimique dâ□□Arabie saoudite.

Mais le pÃ©rimÃ¨tre ne concerne pas seulement les collaborateurs des professionnels de lâ□□Ã©nergie. Comment Ãªtre sÃ»r que les fournisseurs et les partenaires de la chaÃ®ne dâ□□approvisionnement prennent la cybersÃ©curitÃ© au sÃ©rieux ? En 2018, une grande entreprise de services publics a Ã©tÃ© condamnÃ©e Ã une amende de 2,7 millions de dollars pour un vol de donnÃ©es par un tiers.

Les services publics dâ□□Ã©lectricitÃ© comptent parmi les moins performants en matiÃ¨re de correction de la catastrophique vulnÃ©rabilitÃ© BlueKeep, Ã laquelle de nombreux services publics sont encore exposÃ©s. Il faut donc offrir Ã chaque employÃ©, fournisseur et client une tranquillitÃ© dâ□□esprit totale. En ce sens, prendre en considÃ©ration les menaces liÃ©es aux pÃ©riphÃ©riques USB personnels et Ã ceux appartenant Ã lâ□□entreprise est aujourdâ□□hui un impÃ©ratif.

Lâ□□objectif est de rÃ©duire les risques que des logiciels malveillants sâ□□introduisent dans les rÃ©seaux IT par lâ□□intermÃ©diaire de collaborateurs Ã distance, indÃ©pendamment de ce que le propriÃ©taire a accidentellement tÃ©lÃ©chargÃ©. Sur ce point, au final il sera alors possible de ne plus subir de cyberattaques coÃ»teuses, de perte de rÃ©putation et dâ□□amendes rÃ©glementaires.

Christophe BOUREL, CEO de TYREX