Les PME franÃ§aises plus vulnÃ©rables aux cyberattaques.
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 24/5/2023 13:00:00

Dans un contexte oÃ¹ les pratiques cybercriminelles sâ□□industrialisent, Trellix, la sociÃ©tÃ© spÃ©cialiste de la cybersÃ©curitÃ© et pionniÃ¨re dans la dÃ©tection et la rÃ©ponse Ã©tendues (XDR), a interrogÃ© plus de 500 responsables de la sÃ©curitÃ© des systÃ¨mes dâ□□information travaillant dans des entreprises de plus de 1000 employÃ©s pour essayer de mieux comprendre la nature et lâ□□ampleur des attaques quâ□□ils subissent, les ressources quâ□□ils dÃ©dient Ã la cybersÃ©curitÃ© et le type de solutions quâ□□ils privilÃ©gient.

La France se distingue des autres pays dâ□□Europe en ce quâ□□elle demeure plus vulnÃ©rable aux attaques : un responsable sÃ©curitÃ© FranÃ§ais sur deux dÃ©clare en effet avoir eu Ã gÃ©rer Ã plus dâ□□une cyberattaque majeure dans sa carriÃ¨re.

Des ressources financiÃ¨res, technologiques et humaines parmi les plus limitÃ©es dâ□□Europe

Parmi les facteurs explicatifs possibles, on peut Ã©voquer le fait que la France est le pays dâ□□Europe qui consacre le plus petit pourcentage de son budget IT Ã la cybersÃ©curitÃ©.

En effet, 62% des rÃ©pondants franÃ§ais dÃ©clarent consacrer seulement 10 Ã 20% de leur budget IT Ã la cybersÃ©curitÃ©, tandis que la majoritÃ© des entreprises europÃ©ennes y consacrent entre 20 et 30%. De plus, la France dispose en moyenne du plus petit nombre de solutions de cybersÃ©curitÃ© par organisation : 40% d'entre elles disposent de moins de 10 solutions individuelles alors que ce pourcentage n'est que de 20% pour lâ□□ensemble des pays dâ□□Europe.

A cela sâ□□ajoute la pÃ©nurie de ressources humaines qui reste une prÃ©occupation majeure des responsables sÃ©curitÃ© : 1 sur 2 (48%) cite cette problÃ©matique comme son plus grand dÃ©fi, contre 39% pour lâ□□ensemble des pays dâ□□Europe.

Des solutions de sÃ©curitÃ© qui ne permettent pas de contrer efficacement les menaces

PrÃ¨s dâ□□1 responsable sÃ©curitÃ© franÃ§ais sur 2 dÃ©clare avoir eu Ã gÃ©rer plus dâ□□une cyberattaque majeure dans sa carriÃ¨re, contre seulement 4 pour 10 pour la moyenne europÃ©enne.

Si lâ□□on regarde plus en dÃ©tails les outils de protection dans lesquels les entreprises investissent en France vs. le reste de lâ□□Europe, on rÃ©alise que les investissements franÃ§ais sont principalement orientÃ©s vers la protection des terminaux (Endpoint protection) alors que la sÃ©curitÃ© du cloud arrive en dernier.

Par contraste, la plus grosse part du budget cybersÃ©curitÃ© des entreprises europÃ©ennes est aujourdâ□□hui dÃ©diÃ©e Ã la sÃ©curitÃ© du cloud. De plus, 84% des rÃ©pondants franÃ§ais estiment que les solutions de sÃ©curitÃ© mises en Å□uvre dans leur organisation nÃ©cessitent soit une importante amÃ©lioration soit dâ□□Ãªtre renouvelÃ©es, contre 77% pour la moyenne europÃ©enne.

Â« Face Ã des menaces de plus en plus complexes et en constante Ã©volution, les responsables sÃ©curitÃ© font face Ã un manque de ressources aussi bien matÃ©rielles que humaines, ce qui provoque un stress important chez les Ã©quipes de sÃ©curitÃ© opÃ©rationnelle en Europe Â», explique Fabien Rech, Senior Vice-PrÃ©sident EMEA chez Trellix.

Â« Les dirigeants doivent prendre conscience de ces points de friction et dÃ©bloquer des ressources qui permettront de soutenir les responsables sÃ©curitÃ© et leurs Ã©quipes, quâ□□il sâ□□agisse de l'embauche de plus de talents ou de l'acquisition de nouvelles technologies de sÃ©curitÃ© Â».

Lâ□□IA, une opportunitÃ© pour la cybersÃ©curitÃ© en France ?

Si les responsables sÃ©curitÃ© sâ□□identifient aujourdâ□□hui largement comme des visionnaires dont la motivation est de faire Ã©voluer la nature des dÃ©fis auxquels ils sont confrontÃ©s, 40% des rÃ©pondants franÃ§ais dÃ©clarent avoir souscrit Ã une solution de sÃ©curitÃ© pour leur organisation par obligation rÃ©glementaire, et afin dâ□□Ãªtre conforme aux normes de lâ□□industrie.

InterrogÃ©s sur la maniÃ¨re dont ces solutions de sÃ©curitÃ© de leur organisation doivent Ãªtre amÃ©liorÃ©es, les FranÃ§ais mentionnent en premier lieu le fait quâ□□elles doivent mieux travailler ensemble pour faire face aux attaques multi-vecteurs.

Ce nâ□□est toutefois pas leur unique prÃ©occupation puisquâ□□ils mentionnent Ã©galement et Ã la diffÃ©rence de leur homologues europÃ©ens le besoin de solutions plus automatisÃ©es et qui dÃ©tectent les vulnÃ©rabilitÃ©s plus rapidement, deux aspects sur lesquels lâ□□intelligence artificielle en matiÃ¨re de cybersÃ©curitÃ© a un rÃ´le important Ã jouer.