Les assurances cyber sont-elles toujours viables en 2023
Info
PostÃ© par : JPilo
PubliÃ©e le : 25/1/2023 14:00:00

Alors que lâ□□annÃ©e 2020 Ã©tait fortement dÃ©ficitaire pour le micro-marchÃ© des assurances cyber, lâ□□AMRAE constate que la situation sâ□□est stabilisÃ©e en 2021, reprÃ©sentant dÃ©sormais 219 millions dâ□□euros. En cause, le taux des primes qui a doublÃ© et les conditions de versement devenues plus exigeantes.

Cette Ã©volution renforce le dÃ©bat autour de la pertinence des cyber assurance, portant notamment le doute sur leur efficacitÃ©, leur dÃ©ploiement et lâ□□Ã©tendue rÃ©elle de la couverture offerte.

Les experts juridiques de Cohesity ont en effet constatÃ©, aprÃ¨s avoir analysÃ© les principales assurances de ranÃ§ongiciel prÃ©sentes sur le marchÃ© Ã la fin de lâ□□annÃ©e 2022, que les garanties actuelles ne sont guÃ¨re plus que des limitations de responsabilitÃ© qui profitent aux fournisseurs â□□ et non aux clients.

Le PDG de Zurich Insurance dÃ©clarait dâ□□ailleurs dans une interview accordÃ©e au Financial Times que les cyberattaques deviendront bientÃ´t Â«â□□inassurablesâ□□Â», puisque lâ□□assurance et la prÃ©vention se sont communÃ©ment rÃ©vÃ©lÃ©es inefficaces aussi bien faces aux cyberattaques que pour la rÃ©cupÃ©ration effective des donnÃ©es.

Le risque cyber en France

La multiplication des attaques pose un risque considÃ©rable pour les entreprises, Ã lâ□□image de lâ□□Ã©diteur de logiciels Dedalus, sous-traitant des laboratoires mÃ©dicaux franÃ§ais qui sâ□□est vu infliger une amende Ã hauteur de 1,5 million dâ□□euros par la CNIL en avril dernier suite Ã plusieurs failles de sÃ©curitÃ© ayant conduit au vol de donnÃ©es de 500â□□000 patients franÃ§ais.

Le nombre dâ□□attaques nâ□□a fait quâ□□augmenter au cours des derniÃ¨res annÃ©es, si bien que le parquet de Paris, selon FranceInfo, a enregistrÃ© lâ□□ouverture de 600 enquÃªtes en 2022 (65 en 2021), dont la moitiÃ© concerne des attaques par ranÃ§ongiciels.

Lâ□□adoption rÃ©cente de la loi de programmation du ministÃ¨re de lâ□□IntÃ©rieur (LOPMI), soutenu par Bercy et les assureurs franÃ§ais, continue aussi dâ□□alimenter le dÃ©bat.

MÃªme si elle rend lÃ©gale lâ□□indemnisation des cyber ranÃ§ons payÃ©es par les entreprises, elle leur incombe tout dâ□□abord de dÃ©poser une plainte auprÃ¨s des autoritÃ©s compÃ©tentes, une condition dÃ©criÃ©e par beaucoup de par les consÃ©quences quâ□□elle impose pour la rÃ©putation de lâ□□entreprise ou de lâ□□organisme visÃ©.

Quelles alternatives Ã lâ□□assurance ?

Pour Jean-Baptiste Grandvallet, IngÃ©nieur SystÃ¨me chez Cohesity Â«â□□les organisations ont tout intÃ©rÃªt Ã concentrer leurs efforts sur la rÃ©cupÃ©ration des donnÃ©es en cas dâ□□attaques. Un dÃ©fi surmontable si de rÃ©elles mesures de prÃ©vention sont correctement mises en place. Â»

Les entreprises peuvent notamment conserver une copie isolÃ©e des donnÃ©es dans le cadre dâ□□une stratÃ©gie 3-2-1 et adopter une optique zÃ©ro-trust, afin que les donnÃ©es soient chiffrÃ©es aussi bien pendant les transferts que sur les espaces de stockage.

Pour Cohesity, lâ□□enjeux majeur en 2023 sera dâ□□atteindre la cyber-rÃ©silience en amÃ©liorant la collaboration entre les Ã©quipes IT et OT grÃ¢ce Ã une stratÃ©gie globale de sÃ©curitÃ©, pour leur permettre dâ□□Å□uvrer conjointement Ã la dÃ©tection et la prÃ©vention des attaques cyber.

Lâ□□ensemble de ces mesures pourraient non seulement avoir un impact positif direct sur la couverture des assurances cyber mais rÃ©duiront Ã©galement le risque dâ□□incidents et les Ã©ventuels dommages Ã la suite dâ□□une panne ou dâ□□une perte de donnÃ©es.