Les entreprises paient des millions en ranÃ§ons,
Info
PostÃ© par : JerryG
PubliÃ©e le : 9/2/2024 13:00:00

93 % des entreprises seraient incapables de restaurer leurs donnÃ©es et de rÃ©tablir leurs processus opÃ©rationnels dans les trois jours. Une Ã©tude commanditÃ©e par Cohesity, lâ□□un des leaders de la gestion et de la sÃ©curisation des donnÃ©es augmentÃ©e par lâ□□IA, rÃ©vÃ¨le que lâ□□omniprÃ©sence des cyberattaques obligerait la majoritÃ© des entreprises Ã payer des ranÃ§ons, enfreignant leur propre politique de Â«â□□non-paiementâ□□Â».

Ce phÃ©nomÃ¨ne serait par ailleurs accentuÃ© par des lacunes rÃ©currentes en matiÃ¨re de restauration des donnÃ©es. Lâ□□Ã©tude menÃ©e auprÃ¨s de plus de 900 dÃ©cideurs IT et sÃ©curitÃ© montre que les entreprises ne se posent plus la question de savoir Â«â□□siâ□□Â», mais Â«â□□quandâ□□Â» elles se feront attaquer.

Lâ□□Ã©tude rÃ©vÃ¨le Ã©galement que la plupart des entreprises ont payÃ© une ranÃ§on au cours des deux derniÃ¨res annÃ©es, et quâ□□une majoritÃ© sâ□□attend Ã ce que la menace cyber augmente considÃ©rablement en 2024.

Fait alarmant, prÃ¨s de 8 rÃ©pondants sur 10 (79 %) ont dÃ©clarÃ© que leur entreprise avait Ã©tÃ© victime dâ□□une attaque par ransomware entre juin et dÃ©cembre. Le paysage de la menace cyber devrait encore sâ□□aggraver en 2024, 96 % des personnes interrogÃ©es affirmant que la menace des cyberattaques pour leur secteur dâ□□activitÃ© augmentera cette annÃ©e, et plus de 7 sur 10 prÃ©voyant une augmentation de plus de 50 %.

La surface dâ□□attaque dâ□□une organisation est dÃ©finie par la taille, la complexitÃ© et la portÃ©e de ses environnements de gestion des donnÃ©es. 78 % des rÃ©pondants ont dÃ©clarÃ© que les risques liÃ©s Ã la sÃ©curitÃ© des donnÃ©es ont augmentÃ© plus rapidement que la croissance des donnÃ©es elles-mÃªmes.

Les personnes interrogÃ©es estiment Ã©galement que leurs stratÃ©gies de cyber-rÃ©silience et de sÃ©curitÃ© des donnÃ©es ne sont plus adaptÃ©es au paysage actuel des menaces, 21 % seulement ayant pleinement confiance dans la stratÃ©gie de cyber-rÃ©silience de leur entreprise et dans sa capacitÃ© Ã Â«â□□faire face Ã lâ□□Ã©volution des dÃ©fis liÃ©s aux menaces cyberâ□□Â»

La lenteur de la restauration des donnÃ©es et le manque de cyber-rÃ©silience entraÃ®nent le paiement de ranÃ§ons

La cyber-rÃ©silience est devenue lâ□□Ã©pine dorsale de la continuitÃ© des activitÃ©s. Elle dÃ©finit la capacitÃ© des entreprises Ã restaurer leurs donnÃ©es et Ã rÃ©tablir leurs processus opÃ©rationnels lorsquâ□□elles sont victimes dâ□□une cyberattaque ou dâ□□un incident.

Lâ□□Ã©tude souligne lâ□□ampleur des dÃ©fis en matiÃ¨re de cyber-rÃ©silience :

â□¢ Tous les rÃ©pondants de lâ□□Ã©tude ont dÃ©clarÃ© avoir besoin de plus de 24 heures pour restaurer leurs donnÃ©es et rÃ©tablir leurs processus mÃ©tier.
â□¢ Seulement 7 % ont dÃ©clarÃ© que leur entreprise pouvait restaurer les donnÃ©es et rÃ©tablir les processus opÃ©rationnels dans un dÃ©lai de 1 Ã 3 jours.
â□¢ 35 % ont dÃ©clarÃ© pouvoir restaurer en 4 Ã 6 jours, et 34 % ont besoin de 1 Ã 2 semaines

pour le faire.
â¢ De maniÃ¨re alarmante, prÃ¨s dâ une entreprise sur quatre (23 %) a besoin de plus de 3 semaines pour restaurer ses donnÃ©es et rÃ©tablir ses processus mÃ©tier.

Preuve supplÃ©mentaire des lacunes en matiÃ¨re de cyber-rÃ©silience, Ã peine 12 % ont dÃ©clarÃ© que leur entreprise avait procÃ©dÃ© Ã des tests de rÃ©sistance de leurs processus ou solutions de sÃ©curitÃ©, de gestion et de restauration des donnÃ©es au cours des six mois prÃ©cÃ©dant lâenquÃªte, et 46 % nâont pas testÃ© leurs processus ou solutions depuis plus de 12 mois.

A la lumiÃ¨re de ce constat, il apparaÃ®t finalement peu surprenant que 94 % des rÃ©pondants dÃ©clarent que leur entreprise paierait une ranÃ§on pour restaurer les donnÃ©es et rÃ©tablir les processus opÃ©rationnels en cas dâattaque rÃ©ussieâ; 5 % ont rÃ©pondu Â«âpeut-Ãªtre, en fonction du montant de la ranÃ§onâÂ».

Plus de 2 rÃ©pondants sur 3 (67 %) ont dÃ©clarÃ© que leur entreprise serait prÃªte Ã payer plus de 3 millions de dollars de ranÃ§on pour restaurer leurs donnÃ©es et rÃ©cupÃ©rer leurs processus opÃ©rationnels, et 35 % plus de 5 millions de dollars.

Lâ Ã©tude souligne par ailleurs un paradoxe important : 9 rÃ©pondants sur 10 ont dÃ©clarÃ© que leur entreprise avait payÃ© une ranÃ§on au cours des deux annÃ©es prÃ©cÃ©dentes, alors que 84 % dâentre elles avaient mis en place une politique de Â«ânon-paiementâÂ».

Â«âLes organisations ne peuvent pas contrÃ´ler lâaugmentation du volume, de la frÃ©quence ou de la sophistication des cyberattaques telles que les ransomwares.

Ce quâelles peuvent contrÃ´ler, câest leur cyber-rÃ©silience, câest-Ã -dire leur capacitÃ© Ã rÃ©agir rapidement et Ã se remettre dâune cyberattaque ou dâune panne informatique, en adoptant des capacitÃ©s avancÃ©es de sÃ©curisation des donnÃ©esâÂ», a dÃ©clarÃ© Brian Spanswick, RSSI et directeur de lâIT chez Cohesity.

Â«âIl nâest pas surprenant que la majoritÃ© des entreprises aient Ã©tÃ© touchÃ©es par des cyberattaques telles que les ransomwares. Ce qui est alarmant, câest que 90 % dâentre elles ont payÃ© une ranÃ§on, enfreignant ainsi leur propre politique de non-paiement, et que la plupart sont prÃªtes Ã payer jusquâÃ 3 millions de dollars de ranÃ§on parce quâelles ne peuvent pas rÃ©cupÃ©rer leurs donnÃ©es, ou ne peuvent pas le faire assez rapidement.âÂ»

La direction gÃ©nÃ©rale devrait porter la responsabilitÃ© des risques liÃ©s Ã la sÃ©curitÃ© des donnÃ©es

Lâ Ã©tude rÃ©vÃ¨le deux axes dâamÃ©lioration possibles : la sensibilisation et la responsabilisation des dirigeants en matiÃ¨re de sÃ©curitÃ© des donnÃ©es, puisque seulement 35 % des rÃ©pondants dÃ©clarent que leurs supÃ©rieurs et dirigeants comprennent parfaitement Â«âla gravitÃ© des risques et les dÃ©fis quotidiens liÃ©s Ã la protection, Ã la sÃ©curisation, Ã la gestion, Ã la sauvegarde et Ã la restauration des donnÃ©esâÂ».

Quatre rÃ©pondants sur cinq ont dÃ©clarÃ© que la direction gÃ©nÃ©rale et les conseils dâadministration devraient partager la responsabilitÃ© de la stratÃ©gie de sÃ©curitÃ© des donnÃ©es de leur entreprise, tandis que 67 % ont dÃ©clarÃ© que le DSI et le RSSI de leur entreprise pourraient Ãªtre mieux alignÃ©s.

Les plus grandes inquiÃ©tudes concernant les consÃ©quences dâune violation de donnÃ©es ou dâune cyberattaque rÃ©ussie sont, par ordre dâimportance : une atteinte Ã la rÃ©putation de la marque (34 %), une baisse du cours de lâaction, des investissements ou de la rentabilitÃ© (31 %), un impact direct sur le chiffre dâaffaires (30 %) et une perte de confiance de la part des

parties prenantes (30 %).

A la question de savoir qui est le plus touchÃ© par une violation de donnÃ©es ou une cyberattaque, les personnes interrogÃ©es ont rÃ©pondu que les clients existants (29 %), lâ□□Ã©quipe de sÃ©curitÃ© (29 %), lâ□□Ã©quipe informatique (28 %), les employÃ©s (28 %) et leurs partenaires tiers (27 %) Ã©taient les plus touchÃ©s.

Â«***â□□La cyber-rÃ©silience*** et la sÃ©curitÃ© des donnÃ©es devraient Ãªtre une prioritÃ© organisationnelle holistique, car chaque fonction et chaque employÃ© utilise les donnÃ©es et les systÃ¨mes dâ□□information.

Les graves consÃ©quences dâ□□une cyberattaque rÃ©ussie ou dâ□□une violation de donnÃ©es sur la continuitÃ© de lâ□□activitÃ©, le chiffre dâ□□affaires, la rÃ©putation et la confiance suffisent Ã empÃªcher les dirigeants dâ□□entreprise, les responsables informatiques et les responsables de la sÃ©curitÃ© de dormirâ□□Â», a dÃ©clarÃ© Sanjay Poonen, PDG de Cohesity.

Â«â□□Pour rÃ©pondre rapidement aux cyberattaques, les organisations ont besoin de solutions de sÃ©curitÃ© et de gestion des donnÃ©es alimentÃ©es par lâ□□IA, qui protÃ¨gent leurs donnÃ©es, dÃ©tectent lorsquâ□□elles sont attaquÃ©es et les restaurent le plus rapidement possible pour rÃ©tablir leurs processus opÃ©rationnels.â□□Â»

La rÃ©glementation nâ□□incite pas les entreprises Ã adopter de meilleures pratiques en matiÃ¨re de sÃ©curitÃ© des donnÃ©es

MalgrÃ© les efforts constants des gouvernements et des institutions publiques pour encourager les meilleures pratiques en matiÃ¨re de cybersÃ©curitÃ© et de gestion des donnÃ©es, seulement 46 % des personnes interrogÃ©es dÃ©clarent que les rÃ©glementations stimulent les initiatives de leur entreprise en matiÃ¨re de sÃ©curitÃ©, de gestion ou de restauration des donnÃ©es.Â