Cyberattaques dans le Cloud : Forte augmentation.
Internet
PostÃ© par : JulieM
PubliÃ©e le : 15/6/2022 15:00:00

Netwrix, fournisseur de cybersÃ©curitÃ© qui simplifie la sÃ©curitÃ© des donnÃ©es, annonce la publication de son rapport mondial 2022 sur la sÃ©curitÃ© du cloud. Celui-ci rÃ©vÃ¨le que plus de la moitiÃ© (53 %) des organisations ont subi une cyberattaque visant leur infrastructure cloud au cours des 12 derniers mois. Le phishing a reprÃ©sentÃ© le type dâ□□attaque le plus courant, puisque 73 % des rÃ©pondants y ont Ã©tÃ© confrontÃ©s.

Le rapport souligne Ã©galement que le dÃ©lai moyen de dÃ©tection de la plupart des types dâ□□attaques sâ□□est allongÃ© depuis 2020. Le ralentissement le plus important a Ã©tÃ© observÃ© du cÃ´tÃ© des compromissions de la supply chain : en 2020, 76 % des rÃ©pondants dÃ©tectaient ce type dâ□□attaque en quelques minutes ou en quelques heures, mais en 2022, seuls 47 % le dÃ©tectent aussi rapidement. Il est Ã©galement devenu plus difficile de repÃ©rer les ransomwares : 86 % des organisations avaient besoin de quelques minutes ou heures pour dÃ©tecter les ransomwares en 2020, contre 74 % en 2022.

Â« Les attaques Ã©voluent plus rapidement que lâ□□expertise, les outils et les processus de dÃ©fense utilisÃ©s pour les contrer. Les organisations dÃ©ploient davantage de contrÃ´les de sÃ©curitÃ© et dÃ©pensent plus dâ□□argent pour assurer leur sÃ©curitÃ© â□□ 49 % dâ□□entre elles ont confirmÃ© une hausse de leur budget de sÃ©curitÃ© du Cloud en 2022, analyse Dirk Schrader, vice-prÃ©sident de la recherche sur la sÃ©curitÃ© chez Netwrix.

Cependant, la multiplication des outils nâ□□est pas toujours synonyme de sÃ©curitÃ© accrue. Des solutions de diffÃ©rents fournisseurs fonctionnent de maniÃ¨re indÃ©pendante, offrent des fonctionnalitÃ©s qui se chevauchent ou sont contradictoires, et obligent les organisations Ã faire appel Ã plusieurs Ã©quipes dâ□□assistance.

Cette complexitÃ© est Ã lâ□□origine de lacunes en matiÃ¨re de sÃ©curitÃ©. Une faÃ§on de rÃ©soudre ce problÃ¨me consiste Ã Ã©laborer une architecture de sÃ©curitÃ© en collaboration avec un groupe restreint de fournisseurs de confiance qui dÃ©veloppent, proposent et prennent en charge un vaste portefeuille de solutions Â».

Le rapport indique en outre que les violations sont de plus en plus coÃ»teuses. Cette annÃ©e, 49 % des rÃ©pondants ont indiquÃ© avoir engagÃ© des dÃ©penses non planifiÃ©es pour combler les lacunes en matiÃ¨re de sÃ©curitÃ© Ã la suite dâ□□une attaque, contre 28 % en 2020. La proportion des organisations qui se sont vu infliger des amendes pour non-conformitÃ© a plus que doublÃ© (passant de 11 Ã 25 %), tout comme le nombre de celles qui ont vu la valeur de leur entreprise chuter (de 7 Ã 17 %).

Les trois principaux dÃ©fis en matiÃ¨re de sÃ©curitÃ© des donnÃ©es citÃ©s par les rÃ©pondants Ã lâ□□enquÃªte sont cependant restÃ©s les mÃªmes quâ□□en 2020 : le manque de personnel IT, le manque dâ□□expertise dans les environnements Cloud et le manque de budget. Ces derniers demeurent un problÃ¨me pour de nombreuses organisations, mais la proportion de celles qui sont aux prises avec ce problÃ¨me a chutÃ©, passant de 47 % en 2020 Ã 34 % en 2022.

Voici dâ□□autres conclusions de lâ□□enquÃªte :

â□¢ 80 % des organisations qui utilisent le Cloud y stockent des donnÃ©es sensibles ;

â¢ Plus de la moitiÃ© (53 %) des rÃ©pondants indiquent que lâamÃ©lioration de la sÃ©curitÃ© constitue leur principal objectif en termes dâadoption du Cloud ;
â¢ La majoritÃ© des organisations interrogÃ©es qui classifient leurs donnÃ©es ont Ã©tÃ© en mesure de dÃ©tecter une attaque en quelques minutes, alors que celles qui nâappliquent pas cette pratique ont gÃ©nÃ©ralement besoin de plusieurs heures, voire de plusieurs jours ;

â¢ Lâaudit de lâactivitÃ© des utilisateurs se rÃ©vÃ¨le particuliÃ¨rement efficace contre le phishing, les attaques par ransomware et la compromission de comptes, puisquâil a permis de rÃ©duire le dÃ©lai de dÃ©tection de plusieurs heures Ã quelques minutes.

Â« Le rapport nous apprend que lâadoption du Cloud bat son plein, ajoute M. Schrader. Les organisations signalent que 41 % de leurs charges de travail se trouvent dÃ©jÃ dans le Cloud, et elles prÃ©voient de porter cette part Ã 54 % dâici Ã la fin de 2023. Les Ã©quipes IT apprennent Ã utiliser le Cloud de maniÃ¨re efficace et sÃ©curisÃ©e, et elles forment leurs collÃ¨gues dans ce sens.

Il est temps de prÃªter une plus grande attention aux mesures de sÃ©curitÃ© qui amÃ©liorent la capacitÃ© dâidentifier les menaces, de sâen prÃ©munir, de les dÃ©tecter et dây rÃ©pondre, afin de rÃ©duire Ã la fois le risque de violation et ses consÃ©quences. Â»