Le Cloud Computing : quels sont ses risques ?
Internet
PostÃ© par : JulieM
PubliÃ©e le : 25/1/2023 13:00:00

De plus en plus dâentreprises migrent vers le cloud pour dÃ©crocher de nouvelles opportunitÃ©s et rÃ©pondre aux attentes croissantes du marchÃ© mondial, en dÃ©veloppant leur capacitÃ© dâinnovation.

Cette tendance se manifeste en particulier par une augmentation rapide des dÃ©penses sur ces types de services.Â

Selon une projection rÃ©cente dâIDC, le total des dÃ©penses mondiales dans les services cloud devrait dÃ©passer 1,3 milliard de dollars dâici 2025, avec un taux de croissance annuel composÃ© Ã©gal Ã 16,9 %.

Si le passage au cloud semble Ãªtre lâavenir de lâinformatique professionnelle, pour Philippe Alcoy, spÃ©cialiste de la sÃ©curitÃ© chez NETSCOUT, cette dÃ©pendance croissante soulÃ¨ve des problÃ¨mes inÃ©dits et prÃ©sente certains risques concrets en matiÃ¨re de cybersÃ©curitÃ©.

Â« Les entreprises qui adoptent le cloud computing doivent prendre des mesures spÃ©cifiques pour assurer leur sÃ©curitÃ©. Il est important dâexaminer chacun des risques prÃ©sentÃ©s afin de bien comprendre la meilleure faÃ§on dây faire face.Â

Le cloud apporte de nouvelles problÃ©matiques de cybersÃ©curitÃ© dans plusieurs domaines, de la violation de donnÃ©es au manque de visibilitÃ©, en passant par les piratages dâAPI ou encore les attaques DDoS :

â¢ Violations de donnÃ©es Ã grande Ã©chelle. Lorsque des donnÃ©es sensibles ou confidentielles sont stockÃ©es ou accessibles via le cloud, elles restent vulnÃ©rables, et le risque de vol demeure.Â

Face Ã la rÃ©currence de ce type dâattaques Ã grande Ã©chelle, souvent mÃ©diatisÃ©es, les entreprises doivent prendre toutes les prÃ©cautions nÃ©cessaires pour empÃªcher les cybercriminels dâavoir accÃ¨s Ã leurs informations, sous peine de consÃ©quences irrÃ©versibles, voire dÃ©vastatrices.

â¢ Manque de visibilitÃ©. La clÃ© dâune sÃ©curitÃ© efficace dans le cloud est la visibilitÃ©. Or, les ressources basÃ©es sur le cloud Ã©tant situÃ©es hors de lâinfrastructure de lâentreprise, la vision de bout en bout des rÃ©seaux sâen trouve limitÃ©e.Â

En effet, Ã©tant donnÃ© que les outils de suivi traditionnels ne peuvent pas garantir une visibilitÃ© complÃ¨te dans le cloud, la dÃ©tection et la lutte contre les cyberattaques sont alors impactÃ©es et les risques associÃ©s sâen trouvent augmentÃ©s.

â¢ Piratages dâAPI . Dans un environnement de plus en plus connectÃ© et automatisÃ©, les API (interfaces de programmation dâapplication) sont dÃ©sormais fondamentales pour la communication entre les services cloud.Â

Le fait quâelles soient gÃ©nÃ©ralement accessibles par des tiers, les rend plus vulnÃ©rables et augmente le risque dâexposer certaines donnÃ©es sensibles. Il est donc impÃ©ratif de les

protÃ©ger contre les cybermenaces.

â¢ Attaques DDoS. Les attaques par dÃ©ni de service distribuÃ© (DDoS) consistent Ã saturer un serveur Ã lâaide dâun trafic trop volumineux afin de le ralentir au point de le mettre hors service.Â

Â Lorsquâelles visent une infrastructure cloud, elles peuvent crÃ©er une perturbation gÃ©nÃ©ralisÃ©e pour toutes les organisations qui dÃ©pendent de ses services.

Dans certains cas, les cybercriminels utilisant lâapproche DDoS demandent une ranÃ§on pour mettre fin aux attaques et pour libÃ©rer les systÃ¨mes rendus indisponibles et rÃ©tablir lâaccÃ¨s aux donnÃ©es vitales de leurs victimes.

De fait, de nombreux groupes spÃ©cialisÃ©s dans le ransomware pratiquent dÃ©sormais une triple extorsion, ayant ajoutÃ© ces attaques DDoS Ã leurs techniques de menace de divulgation et de chiffrement visant les donnÃ©es hÃ©bergÃ©es dans le cloud.

Les entreprises sont confrontÃ©es Ã des risques de cybersÃ©curitÃ© propres au cloud computing, auxquelles elles peuvent faire face grÃ¢ce Ã une visibilitÃ© sur lâensemble du rÃ©seau. Elles ne peuvent effet pas sÃ©curiser ce quâelles ne voient pas.

Câest pourquoi des outils sont aujourdâhui Ã leur portÃ©e pour rÃ©pondre Ã leurs enjeux business tout en garantissant la protection de leurs actifs rÃ©seaux, et offrent aux entreprises une rÃ©ponse Ã tout lâarsenal des attaques DDoS et autres menaces informatiques actuelles.

Face aux risques permanents et en constante Ã©volution, les entreprises doivent continuer de prÃ©voir le pire afin de maintenir leur activitÃ©, rester compÃ©titive et assurer la protection de leurs donnÃ©es ; Ã lâheure oÃ¹ la sÃ©curitÃ© de la supply chain revient au cÅur du dÃ©bat, ces mesures permettront de protÃ©ger toute la chaÃ®ne, du fournisseur de service, en passant par lâentreprise pour aller jusquâau client final. Â»Â