Le Cloud hybride Ã lâ□□Ã©preuve des cybermenaces
Internet
PostÃ© par : JulieM
PubliÃ©e le : 8/7/2022 13:00:00

Selon lâ□□ANSSI, les intrusions avÃ©rÃ©es dans des systÃ¨mes d'information ont augmentÃ© de 37 % en 2021 par rapport Ã 2020. Les cybercriminels ont notamment profitÃ© de lâ□□accÃ©lÃ©ration de la transformation digitale au sein des entreprises, souvent mal maÃ®trisÃ©e, y compris lâ□□usage du cloud.

La nÃ©cessitÃ© d'une adoption rapide a ainsi entraÃ®nÃ© des failles de sÃ©curitÃ© et encouragÃ© les acteurs malveillants Ã tirer parti de la moindre vulnÃ©rabilitÃ©. Dâ□□aprÃ¨s les estimations de Gartner, les dÃ©penses en services de cloud public devraient atteindre plus de 480 milliards de dollars cette annÃ©e, en raison notamment du dÃ©veloppement des environnements hybrides, multicloud et edge, qui ouvrent la voie Ã de nouveaux modÃ¨les de cloud.

Selon Anthony Moillic, Director of Solutions Engineering EMEA et APAC chez Netwrix, les organisations recherchent la flexibilitÃ©, le contrÃ´le des coÃ»ts et l'agilitÃ© du cloud tout en Ã©tant assurÃ©es de stocker leurs donnÃ©es sensibles en toute sÃ©curitÃ© :

Â« Le cloud hybride continue de gagner en popularitÃ© parmi les entreprises de tous secteurs, au niveau mondial, allant de la finance au dÃ©veloppement de jeux vidÃ©o, par exemple. L'adoption d'une approche hybride signifie que le paysage informatique de lâ□□organisation contient Ã la fois des services de cloud public et privÃ©, qui peuvent Ãªtre accompagnÃ©s de centres de donnÃ©es traditionnels sur site.

En plus d'offrir un plus haut degrÃ© de flexibilitÃ© entre les services, les avantages supplÃ©mentaires d'un tel modÃ¨le incluent la possibilitÃ© de sÃ©parer les diffÃ©rentes charges de travail pour obtenir une meilleure rentabilitÃ©. Par exemple, les donnÃ©es les plus critiques peuvent Ãªtre conservÃ©es dans un cloud privÃ©, tandis que les informations non sensibles peuvent Ãªtre stockÃ©es sÃ©parÃ©ment dans un cloud public.

Le stockage de diffÃ©rentes formes de donnÃ©es de cette maniÃ¨re peut contribuer Ã rÃ©duire les coÃ»ts, Ã optimiser la disponibilitÃ© du stockage, Ã rÃ©pondre aux exigences rÃ©glementaires et Ã attÃ©nuer les cyber-risques Ã©mergents, le tout en mÃªme temps.

Notre rÃ©cente Ã©tude sur la sÃ©curitÃ© des donnÃ©es dans le cloud a rÃ©vÃ©lÃ© l'ampleur des dÃ©fis auxquels les entreprises sont confrontÃ©es en matiÃ¨re de protection des environnements dans le cloud. En effet, 80 % des organisations stockent des donnÃ©es sensibles dans le cloud et 53 % ont subi des cyberattaques sur leur infrastructure cloud au cours des 12 derniers mois. Dans ce contexte, la majoritÃ© des entreprises dÃ©signe l'amÃ©lioration de la sÃ©curitÃ© comme leur principal objectif d'adoption du cloud.

Pour relever ce dÃ©fi, la sÃ©curitÃ© du cloud hybride doit Ãªtre abordÃ©e Ã plusieurs niveaux : administratif, physique et technique. La premiÃ¨re consiste Ã dÃ©finir des procÃ©dures claires et Ã les documenter. La deuxiÃ¨me couche concerne le contrÃ´le de l'accÃ¨s physique aux centres de donnÃ©es.

Les couches techniques comprennent gÃ©nÃ©ralement le chiffrement, les VPN et d'autres mesures de sÃ©curitÃ©. L'un des principaux dÃ©fis est le manque de clartÃ© quant aux domaines de responsabilitÃ© de l'Ã©quipe informatique interne et du fournisseur de services cloud. Pour y

parvenir, les charges de travail doivent Ãªtre clairement attribuÃ©es et chacune doit avoir son propre plan de rÃ©ponse aux incidents.

Une solution de cloud hybride peut offrir aux entreprises le meilleur des deux mondes : la commoditÃ© et la rentabilitÃ© d'un service de cloud public, associÃ©es Ã la sÃ©curitÃ© et Ã la flexibilitÃ© d'un environnement de cloud privÃ©. Toutefois, pour en tirer le meilleur parti, il est crucial de prÃªter attention aux menaces de sÃ©curitÃ© uniques auxquelles le cloud hybride est confrontÃ©, et de suivre les rÃ¨gles Ã©prouvÃ©es pour assurer la sÃ©curitÃ© des donnÃ©es. Â»