CybersÃ©curitÃ© : Quatre tendances en 2023
Internet
PostÃ© par : JulieM
PubliÃ©e le : 9/12/2022 13:00:00

Netwrix, un fournisseur de cybersÃ©curitÃ© qui facilite la sÃ©curitÃ© des donnÃ©es, rÃ©vÃ¨le les principales tendances en matiÃ¨re de cybersÃ©curitÃ© qui affecteront les organisations franÃ§aises en 2023.

Cette analyse d'Anthony Moillic, Field CISO EMEA et APAC, et Pierre-Louis Lussan, Country Manager France et Directeur Europe du Sud-Ouest, est basÃ©e sur l'expÃ©rience de Netwrix en France dans un large Ã©ventail de secteurs verticaux, notamment la technologie, la finance, la fabrication, le gouvernement et la santÃ©.

Voici quatre tendances spÃ©cifiques pour 2023 dont les organisations doivent Ãªtre conscientes :

1. Les menaces internes vont continuer Ã augmenter.

Les Ã©quipes de sÃ©curitÃ© informatique se sont traditionnellement concentrÃ©es sur les menaces externes venant des cybercriminels. Mais l'explosion rÃ©cente du ransomware-as-a-service et l'Ã©volution rapide des logiciels malveillants permettent Ã des individus sans compÃ©tences techniques particuliÃ¨res de mener des cyberattaques.

Câ□□est pourquoi les entreprises doivent porter leur attention sur les attaques internes. Par exemple, un employÃ© ou un entrepreneur mÃ©content disposant d'un accÃ¨s lÃ©gitime peut dÃ©sormais causer des dommages importants Ã une organisation.

Par consÃ©quent, les organisations doivent contrÃ´ler Ã©troitement l'accÃ¨s aux donnÃ©es et aux systÃ¨mes sensibles pour rÃ©duire Ã la fois le risque d'une attaque dÃ©libÃ©rÃ©e mais aussi d'attÃ©nuer les consÃ©quences d'erreurs internes involontaires.

2. Les indemnisations des cyber-assurances vont devenir plus difficiles Ã obtenir.

La couverture du paiement des ranÃ§ons aprÃ¨s une attaque par ransomware dans le projet de loi d'orientation et de programmation (LOPMI) du ministÃ¨re de l'IntÃ©rieur est actuellement en dÃ©bat.

Les attaques Ã©tant de plus en plus courantes, les compagnies d'assurance ne paieront que dans des cas exceptionnels, avec des preuves substantielles de la part de la victime. Les organisations devront amÃ©liorer leur capacitÃ© Ã bloquer les menaces de maniÃ¨re proactive, Ã dÃ©tecter rapidement les attaques et Ã permettre une rÃ©cupÃ©ration rapide aprÃ¨s un incident.

3. Le rapport coÃ»t-efficacitÃ© dÃ©terminera les dÃ©cisions en matiÃ¨re de sÃ©curitÃ©.

Le climat Ã©conomique actuel obligera les organisations Ã contrÃ´ler plus Ã©troitement leurs dÃ©penses. En particulier, la nÃ©cessitÃ© d'assurer la cybersÃ©curitÃ© avec des Ã©quipes informatiques en sous-effectif conduira Ã une collaboration plus Ã©troite avec les Ã©diteurs de logiciels de sÃ©curitÃ© et les intÃ©grateurs spÃ©cialisÃ©s en cybersÃ©curitÃ©. Cette option permettra aux organisations de mieux gÃ©rer leurs coÃ»ts et de rÃ©pondre Ã leurs besoins de

flexibilitÃ©.

4. La poursuite de la migration vers le cloud rendra le pÃ©rimÃ¨tre de sÃ©curitÃ© encore moins dÃ©fini.

Selon le rÃ©cent rapport Netwrix sur la sÃ©curitÃ© du cloud, 51 % des charges de travail des entreprises franÃ§aises seront dans le Cloud d'ici fin 2023, contre 37 % en 2022.

Les Ã©quipes informatiques devront donc s'attaquer aux menaces qui pÃ¨sent sur les actifs sur site et dans le Cloud, y compris tous les terminaux utilisÃ©s par les travailleurs Ã distance. Avec ce pÃ©rimÃ¨tre informatique flou, l'audit complet de l'activitÃ© des utilisateurs deviendra encore plus crucial pour repÃ©rer les comportements anormaux Ã temps afin de prÃ©venir les incidents graves.

Â« Avec les cyberattaques, la question nâ□□est pas de savoir si mais quand elles se produiront, commente Anthony Moillic. Parce que les solutions ponctuelles fonctionnent sÃ©parÃ©ment, elles laissent des lacunes de sÃ©curitÃ© qui rendent difficile la dÃ©tection des acteurs de la menace dans l'environnement informatique.

Pour rÃ©duire ces lacunes, les organisations unifieront leurs architectures de sÃ©curitÃ© en faisant appel Ã un groupe restreint de fournisseurs de confiance disposant d'un vaste portefeuille de produits qui se complÃ¨tent. Â»