Perspective sur la cybersÃ©curitÃ© 2023 : 5 prÃ©dictions
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 5/4/2023 13:00:00

Au-delÃ des vulnÃ©rabilitÃ©s qui vont submerger les organisations en 2023, les responsables de la cybersÃ©curitÃ© devront se concentrer sur cinq risques majeurs dans l'annÃ©e Ã venir. De la rÃ©cession Ã©conomique aux consolidation sectorielles, examinons ainsi les dÃ©fis et les opportunitÃ©s qui nous attendent dixit Pierre Samson, Chief Revenue Officer Hackuity

Accessoire ou indispensable ?

Si vous ne faites pas partie d'un process critique (comme le VM), attendez-vous Ã Ãªtre dÃ©priorisÃ©.

Consolidation des fournisseurs

Optimisez le ROI de vos outils actuels. Les directions seront Ã la recherche dâ□□une vue consolidÃ©e pour booster lâ□□efficacitÃ© de leur arsenal cyber grÃ¢ce Ã un cockpit unique. Simplification et automatisation, ainsi que renforcement du ROI de vos investissements, câ□□est faire dâ□□une pierre, deux coups.

TolÃ©rance au risque et automatisation

dans le contexte de ressources plus limitÃ©es, de lâ□□augmentation des charges de travail, voire de situations burn-out, les entreprises auront deux choix: (1) automatiser massivement pour suivre le rythme des attaques (de plus en plus facilitÃ©es par lâ□□Ã©largissement de la surface dâ□□attaque) OU (2) avoir lâ□□accord de leur direction pour tolÃ©rer le risque dâ□□Ãªtre victime dâ□□attaques (qui auraient pu facilement Ãªtre Ã©vitÃ©es grÃ¢ce Ã une hygiÃ¨ne de cybersÃ©curitÃ© plus rigoureuse).

Gain de productivitÃ©, automatisation et ROI

Vos actions sont surveillÃ©es de prÃ¨s par la DAF. Des critÃ¨res plus stricts pour les projets et surtout un retour sur investissement plus court seront attendus (par rapport au ROI classique de 3 Ã 5 ans des gros investissements dans lâ□□infra). Automatiser les tÃ¢ches manuelles et libÃ©rer de la bande passante pour vos ETPs grÃ¢ce Ã une plateforme spÃ©cialisÃ©e clÃ©-en-main (ne nÃ©cessitant donc pas de personnalisation ni coÃ»t important de mise en place) deviendra une Ã©vidence.

CybersÃ©curitÃ© = protection des emplois

Quâ□□est ce qui empÃªche les DSI de dormir paisiblement (et le reste de lâ□□Ã©quipe pour Ãªtre honnÃªte) ? Bienvenue en rÃ©cession, oÃ¹ une mauvaise dÃ©cision peut signifier un licenciement. Personne ne souhaite exposer son entreprise au risques cyber et voir son poste passer sur un siÃ¨ge Ã©jectable ni connaÃ®tre un â□□cyber burnoutâ□□ de plus en plus rÃ©pandu chez les praticiens de la cybersÃ©curitÃ©.

Il sera ainsi nÃ©cessaire de (1) continuer Ã renforcer vos dÃ©fenses tout en (2) estimant avec plus de prÃ©caution les nouveaux projets. Les Ã©quipes opteront pour les projets Ã faible risque et Ã faible friction. Les fournisseurs de cybersÃ©curitÃ© (plateforme & service) devront rÃ©duire

le risque projet afin de rÃ©duire le FOMU (â□□Fear Of Messing upâ□□) plutÃ´t que de vendre des â□□fonctionnalitÃ©s tape Ã lâ□□oeilâ□□ qui sâ□□appuient sur le FOMO (â□□Fear Of Missing Outâ□□).

La dÃ©cision reviendra comme souvent Ã un choix Make vs Buy. Le DIY est souvent plus coÃ»teux, mais selon les budgets disponibles (qui peuvent Ã©voluer avec les coupes budgÃ©taires), certains seront malgrÃ© tout tentÃ©s de privilÃ©gier des dÃ©veloppements internes.

De faÃ§on ironique, câ□□est en suivant cette voie quâ□□ils risquent de commettre des â□□erreursâ□□, car leurs effectifs seront dÃ©jÃ sous pression. Sâ□□appuyer sur un partenaire externe en sÃ©curisant un budget dÃ©diÃ© demeure la bonne pratique du secteur qui a fait ses preuves. Les pÃ©riodes difficiles deviennent souvent des moments de rupture, et particuliÃ¨rement lorsquâ□□on prend de faux raccourcis. Une crise est souvent le meilleur moment pour se redÃ©finir.