Ce qui nous attend en 2024.
Info
PostÃ© par : JerryG
PubliÃ©e le : 26/1/2024 14:00:00

Multiplication des attaques par ransomware, tensions gÃ©opolitiques en Europe et au Moyen-Orient, incertitude Ã©conomique : lâ□□annÃ©e 2023 fut tumultueuse et marquÃ©e par une succession de crises protÃ©iformes.

Dans ce contexte, les organisations ont eu fort Ã faire pour prÃ©server lâ□□intÃ©gritÃ© de leur systÃ¨me dâ□□information, ou encore se prÃ©munir et remÃ©dier aux Ã©ventuelles cyberattaques. 2024 ne dÃ©rogera pas Ã la rÃ¨gle car ces dÃ©fis seront toujours dâ□□actualitÃ©. Pour aider les organisations Ã y faire face, voici un tour dâ□□horizon des grandes tendances cyber qui feront lâ□□annÃ©e 2024.

Une annÃ©e riche en Ã©vÃ©nements signifie autant dâ□□opportunitÃ©s pour les cybercriminels

Poursuite des diffÃ©rents conflits au Moyen-Orient et en Ukraine, Ã©lections prÃ©sidentielles aux Etats-Unis, Jeux Olympiques de Parisâ□¦ lâ□□annÃ©e 2024 est remplie dâ□□Ã©vÃ©nements qui vont malheureusement attirer les acteurs malveillants de toutes sortes.

MÃªme si, au vu de la nature de ces Ã©vÃ©nements, les organisations Ã©tatiques et supranationales seront la cible principale des attaquants, nâ□□importe quelle structure pourrait Ãªtre visÃ©e, quelle que soit sa taille. En effet, avec ce type de campagnes de cyberattaques, il existe toujours des dommages collatÃ©raux. Les secteurs de la dÃ©fense, de lâ□□Ã©nergie, de la santÃ© et de la banque seront trÃ¨s probablement les plus visÃ©s.

Les ETI rattrapent leur retard

Pendant longtemps, on a considÃ©rÃ© que les entreprises de taille moyenne Ã©taient en retard sur la sÃ©curitÃ©. Elles reprÃ©sentaient mÃªme un maillon faible pour les grands comptes, notamment parce quâ□□ils Ã©taient visÃ©s par des attaques indirectes qui ciblaient des partenaires de plus petite envergure - et donc moins protÃ©gÃ©s.

MÃªme si la sÃ©curitÃ© informatique est une quÃªte sans fin, on peut dire que les ETI ont fait des efforts importants pour combler le fossÃ© qui les sÃ©pare de leur partenaire grand compte. Et gÃ©nÃ©ralement, elles le font bien plus vite que leurs modÃ¨les car elles partent dâ□□une page blanche, et elles ont appris des erreurs des grands comptes, notamment en matiÃ¨re de rationalisation des outils cyber.

DÃ©sormais, elles sâ□□Ã©quipent directement de plateformes capables de couvrir une grande variÃ©tÃ© de besoins, tout en conservant la maÃ®trise de leurs coÃ»ts et de leurs ressources. En rÃ©sumÃ©, elles font plus avec moins.

RÃ©duction des coÃ»ts, consolidation des outils

AprÃ¨s les diffÃ©rents confinements, le retour en prÃ©sentiel signe la fin des investissements importants en informatique et en cyber. DÃ©sormais, les directions demandent aux DSI de justifier le moindre investissement, prÃ©sent ou passÃ©.

La consolidation des outils va donc sâ□□accentuer. Rien dâ□□Ã©tonnant lorsque lâ□□on sait que certaines organisations ont plus de 80 outils rien que pour la cyber ! Câ□□est la fin de lâ□□adage â□□un problÃ¨me = une nouvelle solutionâ□□ qui nâ□□a que trop durÃ©.

Nous allons voir les plateformes multi-usages se rÃ©pandre, offrant ainsi aux directions informatiques la possibilitÃ© de rÃ©duire le nombre dâ□□outils utilisÃ©s. Par consÃ©quent, elles pourront faire des optimisations sur les licences comme sur les ressources, humaines et matÃ©rielles, nÃ©cessaires Ã lâ□□utilisation et lâ□□entretien dâ□□un trop grand nombre dâ□□outils.

Il est important de noter Ã©galement que le mouvement qui tend Ã faire rentrer la cyber dans le giron des directions informatiques prend de lâ□□ampleur, alors quâ□□elles bÃ©nÃ©ficiaient jusque-lÃ d'une certaine autonomie.

La consolidation du marchÃ© complique lâ□□avenir des petits acteurs

Dans la suite logique de la rationalisation du nombre d'outils, les grands acteurs, tels que Microsoft, ServiceNow ou Palo Alto sont donc privilÃ©giÃ©s par les directions informatiques.

La conclusion Ã en tirer est que lâ□□annÃ©e 2024 sera compliquÃ©e pour les petits acteurs de la cyber, ceux qui ne sont pas encore bien Ã©tablis sur le marchÃ© ou ceux qui ne se sont pas encore associÃ©s Ã des grands noms de la cyber. Il leur faudra faire preuve de lâ□□excellence et de la plus value de leur solution technologique.

Lâ□□IAâ□¦va aider les acteurs historiques

Lâ□□intelligence artificielle continuera dâ□□avoir des rÃ©percussions majeures sur lâ□□Ã©cosystÃ¨me cyber, et ce nâ□□est pas prÃ¨s de s'arrÃªter. ChatGPT ne reprÃ©sente que la partie Ã©mergÃ©e de ces nouvelles technologies.

ConcrÃ¨tement, lâ□□IA accÃ©lÃ¨re grandement les cycles de dÃ©veloppement des solutions. Et contrairement Ã ce que lâ□□on pourrait croire, lâ□□IA sera dâ□□une grande aide pour les acteurs historiques. En effet, si pendant longtemps il y avait une prime Ã lâ□□innovation qui aidait les nouveaux acteurs, plus agiles, plus rapides Ã dÃ©velopper des nouvelles technologies, lâ□□IA va permettre aux acteurs historiques de devenir aussi rapides que les nouveaux entrants.

DÃ©sormais, avec lâ□□IA, dÃ©velopper des solutions est facilitÃ©. Cela implique deux consÃ©quences. PremiÃ¨rement, il y aura une multiplication des nouveaux acteurs qui vont vouloir se lancer. Mais avec un â□□Go to Marketâ□□, c'est-Ã -dire la capacitÃ© de passer de la conception Ã la commercialisation dâ□□un produit, toujours compliquÃ©.

Ensuite, les acteurs historiques vont proposer de plus en plus de solutions aussi innovantes que celles dÃ©veloppÃ©es par les startups. Dâ□□autant plus quâ□□ils disposent des moyens et de l'expÃ©rience pour rÃ©aliser un vrai â□□Go to Marketâ□□, ce qui leur confÃ¨rera un avantage important.

Mieux gÃ©rer et anticiper les cycles de vie et de support des OS Windows

Windows est lâ□□OS qui a accompagnÃ© l'explosion du nombre dâ□□assets Ã gÃ©rer au sein des organisations. Mais chaque version a une date de pÃ©remption si lâ□□on peut dire.

Cela veut dire que les directions informatiques doivent Ãªtre capables de savoir quels assets sont encore sous garantie Microsoft et lesquels ne le sont plus. Par exemple, depuis le 10 octobre de cette annÃ©e, Windows Server 2012 nâ□□est plus supportÃ©.

Ce qui veut dire que Microsoft ne fournit plus de mises Ã jour, notamment pour combler les failles dÃ©tectÃ©es. Les DSI doivent donc anticiper cela et mettre en place un plan de migration pour les machines concernÃ©es. Gare Ã la mauvaise gestion de lâ□□obsolescence !

Assurances cyber : la fin du dÃ©claratif et lâ□□arrivÃ©e de la cartographie

Lâ□□assurance du risque cyber est un problÃ¨me qui ne fait que prendre de lâ□□ampleur. DÃ©sormais, les assureurs savent quâ□□une attaque cyber peut avoir des consÃ©quences importantes sur une organisation et elles ont du mal Ã le qualifier de maniÃ¨re fiable.

Contrairement Ã ce qui se faisait avant, les assurances ne se contentent plus de dÃ©clarations de bonne foi des organisations. Les entreprises doivent sâ□□Ã©quiper de solutions afin de cartographier et quantifier le risque dâ□□origine cyber. Celles qui ne le feront pas risqueront dâ□□Ãªtre confrontÃ©es Ã une fin de non recevoir pour leur demande dâ□□assurance cyber.

Les entreprises qui ne pourront plus se faire assurer, que ce soit parce que cela leur sera refusÃ© ou en raison du coÃ»t de lâ□□assurance, devenu trop cher, devront Ã©lever significativement leur niveau de sÃ©curitÃ© pour rÃ©duire les consÃ©quences dâ□□une Ã©ventuelle attaque. Dans tous les cas, il va falloir investir, et rapidement !

2024 va Ãªtre une annÃ©e propice Ã la rÃ©ussite de beaux projets informatiques qui vont aider les entreprises Ã prospÃ©rer si elles prennent en compte les Ã©lÃ©ments clÃ©s que sont lâ□□Ã©valuation du niveau de la menace, la rÃ©duction des coÃ»ts et la consolidation du marchÃ©, lâ□□impact de lâ□□IA, la gestion de lâ□□obsolescence des OS Windows et la nÃ©cessitÃ© de cartographier le risque dâ□□origine cyber.

Alors que nous sommes proches de la fin du premier mois de 2024, il est urgent d'aller de l'avant et d'embrasser cette nouvelle annÃ©e avec la bonne approche.