PrÃ©dictions de Netskope pour 2024 : zero trust, IA et au-delÃ
Info
PostÃ© par : JerryG
PubliÃ©e le : 6/12/2023 13:00:00

Alors que 2024 approche Ã grands pas, les experts de Netskope prÃ©sentent les tendances et les thÃ©matiques qui devraient marquer lâ□□annÃ©e Ã venir, autour de quatre grands axes : intelligence artificielle, gÃ©opolitique, gouvernance dâ□□entreprise et compÃ©tences.

Intelligence artificielle

Lâ□□essor des groupes de menace assistÃ©s par lâ□□IA

Â« La facilitÃ© croissante avec laquelle les technologies dâ□□IA vont devenir accessibles permettra malheureusement aux cybercriminels de peaufiner leurs mÃ©thodes dâ□□attaque. Nous devons nous attendre Ã une utilisation de plus en plus pointue de lâ□□IA pour exploiter les vulnÃ©rabilitÃ©s encore plus rapidement et extraire de prÃ©cieuses informations de faÃ§on automatisÃ©e.

Les cybercriminels devraient Ã©galement faire appel Ã lâ□□IA gÃ©nÃ©rative pour Ã©laborer des rÃ©cits de phishing efficaces, ainsi que crÃ©er des sÃ©quences audio et vidÃ©o de type deepfake hautement rÃ©alistes dans lâ□□optique dâ□□amÃ©liorer leurs capacitÃ©s dâ□□ingÃ©nierie sociale. Face Ã la montÃ©e en puissance de cybermenaces toujours plus sophistiquÃ©es, les approches classiques Ã base de rÃ¨gles risquent de devenir inopÃ©rantes.

Nous pensons que de plus en plus dâ□□entreprises vont adopter lâ□□IA et des algorithmes de Machine Learning pour amÃ©liorer les renseignements sur les menaces, la prÃ©vention des tentatives de phishing et la dÃ©tection de schÃ©mas anormaux en temps rÃ©el Â», Yihua Liao, Head of Netskope AI Labs.

Les assistants dâ□□IA ont de beaux jours devant eux

Â« 2024 sera lâ□□annÃ©e des assistants dâ□□IA. Ã□ mesure que la demande en capacitÃ©s dâ□□intelligence artificielle augmentera et que les entreprises expÃ©rimenteront de nouveaux services, les employÃ©s exploiteront de plus en plus souvent leur propre assistant dâ□□IA, que ce soit pour simplifier des tÃ¢ches existantes ou pour soutenir et amÃ©liorer de nouveaux modes de travail.Â

En consÃ©quence, les entreprises devront concentrer leurs efforts Ã la fois sur la sÃ©curitÃ© et sur la confidentialitÃ© Â», Neil Thacker, CISO EMEA.

Lâ□□IA gÃ©nÃ©rative au service de lâ□□analyse et de la surveillance en continu

Â« Au cours de lâ□□annÃ©e Ã venir, lâ□□IA gÃ©nÃ©rative sera utilisÃ©e de faÃ§on croissante pour analyser les exigences rÃ©glementaires, le paysage des menaces et les rÃ¨gles qui existent dans les entreprises dans lâ□□optique de gÃ©nÃ©rer des politiques de sÃ©curitÃ© taillÃ©es sur mesure.Â

Je pense Ã©galement que lâ□□IA gÃ©nÃ©rative sera exploitÃ©e pour surveiller de faÃ§on continue le rÃ©seau et les systÃ¨mes des entreprises afin de dÃ©tecter toute compromission de ces politiques et de rÃ©agir automatiquement au moindre problÃ¨me Â», Mike Anderson, Chief Digital

and Information Officer.

GÃ©opolitique

Accords de cyberpaix en vue ?

Â« Pendant longtemps, les guerres se sont dÃ©roulÃ©es sur terre, en mer et dans les airs. Aujourdâ□□hui, le domaine numÃ©rique apparaÃ®t comme le dernier champ de bataille. Ã□ lâ□□aube de lâ□□annÃ©e 2024 â□□ et au-delÃ â□□, les grandes confrontations gÃ©opolitiques vont de plus en plus impliquer des Ã©lÃ©ments cyber, faisant de la sÃ©curitÃ© une prioritÃ© absolue pour les pays du monde entier.

De mÃªme que des traitÃ©s sont nÃ©gociÃ©s pour mettre un terme aux conflits classiques, des propositions dâ□□Â« accords de cyberpaix Â» entre nations pourraient voir le jour en 2024 Â», James Christiansen, vice-prÃ©sident, CSO - Cloud Security Transformation.

Vers une IA de plus en plus rÃ©glementÃ©e

Â« En 2024, des projets de rÃ©glementation concernant lâ□□IA seront Ã lâ□□Ã©tude. Dâ□□ores et dÃ©jÃ , des pays et des rÃ©gions entiÃ¨res proposent de nouvelles rÃ©glementations dâ□□IA pour contrer et tenter de contrÃ´ler de nouveaux services.Â

Â Mais assisterons-nous Ã lâ□□apparition et Ã la mise Ã jour de projets de rÃ©glementation capables dâ□□accompagner lâ□□innovation tout en prÃ©servant lâ□□Ã©thique et la confidentialitÃ© ?

Si tous les regards sont tournÃ©s vers les Ã□tats-Unis, lâ□□Europe et la Chine, il nâ□□est pas exclu que dâ□□autres pays tirent leur Ã©pingle du jeu en retardant leurs propres rÃ©glementations pour entrer dans la course aux armements en IA Â», Neil Thacker CISO EMEA.

ConsÃ©quences des incidents de sÃ©curitÃ© pour les conseils dâ□□administration

Â« Certains actionnaires risquent de poursuivre les entreprise pour ne pas avoir divulguÃ© des incidents de sÃ©curitÃ© importants comme lâ□□exigent les rÃ¨gles de la SEC (US Securities and Exchange Commission). Mais pourquoi des sous-dÃ©clarations ont-elles lieu ? Parce que les entreprises dÃ©finissent les "incidents matÃ©riels" selon leur propre perspective.

Or, les actionnaires ne sâ□□intÃ©ressent pas aux dÃ©finitions nuancÃ©es du terme "matÃ©riel", mais Ã ce quâ□□ils jugent important au moment dâ□□investir. La matÃ©rialitÃ© devrait Ãªtre dÃ©finie du point de vue des investisseurs, et non de lâ□□entreprise Â», Shamla Naidoo, Head of Cloud Strategy & Innovation.

Gouvernance dâ□□entreprise

Ã□tablir une confiance adaptative continue

Â« Alors que 2023 touche Ã sa fin, il convient de reconnaÃ®tre que les entreprises du monde entier ont adoptÃ© avec enthousiasme le concept du zero trust tout en recherchant un modÃ¨le appropriÃ© pour transformer leur approche de la cybersÃ©curitÃ©. En 2024 toutefois, il faut sâ□□attendre Ã ce que les entreprises exercent une pression croissante sur les fournisseurs pour quâ□□ils Ã©toffent quelque peu ce concept.

A titre dâ□□exemple, elles se demanderont concrÃ¨tement Ã quoi correspond effectivement le terme "zero" tout en recherchant une granularitÃ© toujours plus importante et des moyens dâ□□appliquer une "confiance zÃ©ro" capable de sâ□□adapter en permanence, chaque demande

Ã©tant traitÃ©e dÃ¨s quâ□□elle voit le jour indÃ©pendamment de son origine et de sa destination rÃ©elles Â», James Christiansen, VP, CSO â□□ Cloud Security Transformation.

Vers des obligations accrues pour les RSSI et les responsables de la cybersÃ©curitÃ©

Â« Le paysage rÃ©glementaire va sâ□□animer en ce qui concerne la responsabilitÃ© personnelle des RSSI et des responsables de la sÃ©curitÃ© des entreprises, comme nous lâ□□avons vu lorsque les responsables de la cybersÃ©curitÃ© de Solarwinds ont reÃ§u un avis Wells, ou que le ministÃ¨re amÃ©ricain de la Justice a intentÃ© un procÃ¨s Ã lâ□□encontre de Joe Sullivan, lâ□□ancien patron de la cybersÃ©curitÃ© dâ□□Uber.Â

Dans ce contexte, je prÃ©dis une responsabilisation plus importante que jamais en 2024 Â», David Fairman, CISO APAC.

CompÃ©tences

Le rÃ´le du RSSI va poursuivre sa mutation

Â« Au cours de lâ□□annÃ©e Ã venir, il faut sâ□□attendre Ã ce quâ□□un nombre croissant de RSSI abandonnent leur rÃ´le "technico-tactique" pour endosser celui de "souffleur" au sein du Conseil dâ□□administration, dâ□□influenceur transversal et de catalyseur de la transformation culturelle.Â

Les personnes qui disposent de ces nouveaux pouvoirs sont les leaders nÃ©cessaires pour mener Ã bien le programme de confiance numÃ©rique dont dÃ©pendent les stratÃ©gies organisationnelles Â», Ilona Simpson, CISO EMEA.

RedÃ©finir les attentes qui entourent le Â« dÃ©ficit de cybercompÃ©tences

Â« Je suis convaincu que nous allons assister Ã une Ã©volution du type de candidats que les entreprises souhaitent recruter en vue de pourvoir les postes vacants dans le domaine de la cybersÃ©curitÃ©.Â

Je ne crois pas Ã une pÃ©nurie de gÃ©nÃ©ralistes en sÃ©curitÃ©, mais bien Ã un manque dâ□□informaticiens, de dÃ©veloppeurs, dâ□□ingÃ©nieurs et de professionnels de la sÃ©curitÃ© de lâ□□information capables de coder et de comprendre la sÃ©curitÃ© technique et les architectures dâ□□entreprise ;Â

Ã un manque dâ□□experts en sÃ©curitÃ© des produits et des applications, dâ□□analystes disposant de compÃ©tences en chasse aux menaces et rÃ©ponse aux incidents, ainsi que de personnes qualifiÃ©es dans les domaines de la conception, de la maintenance et de lâ□□exploitation des rÃ©seaux.

Aucune de ces missions ne peut Ãªtre accomplie par un dÃ©butant formÃ© pendant six mois Ã la sÃ©curitÃ© de lâ□□information. Les entreprises vont commencer Ã rÃ©aliser quâ□□au lieu de rechercher la perle rare, elles doivent se concentrer sur la progression de carriÃ¨re et recruter des dÃ©butants avec lâ□□intention dâ□□investir dans leur dÃ©veloppement professionnel Â», Gerry Plaza Field CTO â□□ Head of Digital Transformation.