CybercriminalitÃ© : 5 tendances.
Internet
PostÃ© par : JerryG
PubliÃ©e le : 4/12/2023 13:00:00

En cette saison de prÃ©dictions pour lâ□□annÃ©e Ã venir, nous vous proposons un regard sur les tendances cyber 2024, Ã travers lâ□□analyse de Patrick Joyce, RSSI Global chez Proofpoint, sociÃ©tÃ© leader en matiÃ¨re de cybersÃ©curitÃ© et de conformitÃ©.

Lâ□□annÃ©e 2023 a une nouvelle fois Ã©tÃ© marquÃ©e par une recrudescence des cyberattaques â□□ en France, les collectivitÃ©s territoriales et le secteur hospitalier continuent dâ□□Ãªtre des cibles privilÃ©giÃ©es des criminels, en atteste lâ□□attaque menÃ©e contre le Centre Hospitalier Vosgien en octobre dernier. Les acteurs de la menace ne cessent dâ□□aiguiser leurs modes opÃ©ratoires, faisant appel Ã des technologies avancÃ©es et Ã©largissant les points dâ□□entrÃ©es pour mieux compromettre leur cible finale.

Pour Patrick Joyce, 2024 sera une annÃ©e difficile pour les cyber-dÃ©fenseurs qui devront faire face Ã des cybercriminels plus prÃ©cis, qui chercheront Ã affiner leurs stratÃ©gies pour exploiter davantage les faiblesses du tout un chacun. Un dÃ©fi de taille pour les entreprises qui devront prendre en compte cinq grandes tendances :

â□¢ La chaÃ®ne d'approvisionnement reste une porte grande ouverte : Les cybercriminels vont continuer de cibler les fournisseurs des grandes entreprises quâ□□ils tentent dâ□□escroquer. Moins Ã©quipÃ©s pour se protÃ©ger, et bÃ©nÃ©ficiant dâ□□accÃ¨s privilÃ©giÃ©s aux systÃ¨mes internes de leurs clients, les fournisseurs de services sont une proie bien identifiÃ©e des criminels â□□ en attestent les attaques menÃ©es contre PÃ´le Emploi par le biais de son fournisseur de CRM Majorel et la fuite de donnÃ©es personnelles dâ□□environ 10 millions de demandeurs dâ□□emploi en France.

â□¢ Lâ□□IA gÃ©nÃ©rative en catalyse : Lâ□□intelligence artificielle et les grands modÃ¨les de langage seront de plus en plus intÃ©grÃ©s aux produits des fournisseurs pour renforcer leurs offres de sÃ©curitÃ© entraÃ®nant la nÃ©cessaire Ã©mergence de politiques d'IA responsable adjoint Ã de potentiels Ã©checs. Dans le mÃªme temps, cette technologie permet dâ□□accÃ©lÃ©rer et dâ□□amÃ©liorer la sophistication des attaques par hameÃ§onnage, se rapprochant toujours plus de la rÃ©alitÃ© vÃ©cue par les victimes visÃ©es â□□ augmentant ainsi leur propension Ã cliquer sur un mail piÃ©gÃ©.

â□¢ Lâ□□accÃ¨s gÃ©nÃ©ralisÃ© aux logiciels malveillants : La dÃ©mocratisation des logiciels open-sources et de l'IA gÃ©nÃ©rative a rendu la programmation avancÃ©e accessibles Ã un public. Une tendance qui devrait perdurer, et faire baisser davantage la barriÃ¨re Ã lâ□□entrÃ©e pour les dÃ©veloppeurs moins qualifiÃ©s.

â□¢ La multiplication des attaques multicanales : Les campagnes d'ingÃ©nierie sociale multi-touch toucheront de plus en plus les utilisateurs sur leurs appareils mobiles. Au-delÃ des attaques maintenant bien connues par SMS (pour recharger une carte vitale qui ne sâ□□Ã©puise jamais, oÃ¹ rÃ©ceptionner un colis que lâ□□on nâ□□avait jamais commandÃ©), se sont dÃ©sormais la mise en place de QR codes ou dâ□□appels vocaux frauduleux qui deviendront les canaux dâ□□attaque privilÃ©giÃ©s par les cybercriminels.

â□¢ La compromission dâ□□identitÃ©, talon d'Achille des entreprises : Bien que les CVE reste un vecteur dâ□□attaques puissant, les identitÃ©s seront en ligne de mire des cybercriminelles

en 2024 et les recherches montrent que les criminels ont dÃ©sormais dÃ©ployÃ© des techniques permettant de contourner lâ□□authentification multifactorielle (MFA). Les entreprises ne peuvent se contenter de protÃ©ger uniquement leur infrastructure, mais doivent Ãªtre en mesure de sÃ©curiser les informations d'identification, les cookies, les clÃ©s d'accÃ¨s ainsi que remÃ©dier aux erreurs de configuration, notamment lorsquâ□□il sâ□□agit de comptes Ã privilÃ¨ges.

Les prÃ©dictions 2024 de Proofpoint.