Cyberattaque : Les employÃ©s visÃ©s, maillon faible.
Internet
PostÃ© par : JulieM
PubliÃ©e le : 12/12/2022 13:00:00

Tanium, Ã©diteur de lâ□□unique solution de converged endpoint management (XEM) du marchÃ©, publie les rÃ©sultats dâ□□une enquÃªte rÃ©vÃ©lant que les attaques ciblant les employÃ©s sont principale cause dâ□□incidents Ã©vitables de cybersÃ©curitÃ©.

Lâ□□enquÃªte (Â« CybersÃ©curitÃ© : mieux vaut prÃ©venir que guÃ©rir Â») sâ□□intÃ©resse au temps et aux ressources investis par les organisations dans des mesures de cybersÃ©curitÃ© rÃ©actives ou prÃ©ventives, ainsi quâ□□aux raisonnements soutenant leurs dÃ©cisions.

Un Ã©chantillon de responsables informatiques dâ□□une variÃ©tÃ© de secteurs (secteur public, services financiers, santÃ© ou commerce de dÃ©tail) ont Ã©tÃ© interrogÃ©s dans le cadre de cette Ã©tude rÃ©alisÃ©e au Royaume-Uni. Selon les rÃ©sultats, 54 % des rÃ©pondants citent le fait que des employÃ©s cliquent sur des liens de phishing comme le problÃ¨me le plus frÃ©quemment Ã lâ□□origine de cyberattaques menÃ©es avec succÃ¨s.

Le rapport met Ã©galement en lumiÃ¨re les problÃ¨mes de cybersÃ©curitÃ© exacerbÃ©s par le passage Ã un modÃ¨le de travail hybride. Ainsi, 71 % des dirigeants et partenaires Ã©prouvent davantage de difficultÃ©s Ã se protÃ©ger des cybermenaces aujourdâ□□hui quâ□□avant la pandÃ©mie.

Â« Les rÃ©sultats de notre enquÃªte montrent clairement que de nombreuses organisations peinent Ã se protÃ©ger des cybermenaces planant sur lâ□□environnement hybride Â», dÃ©clare Chris Vaughan, vice-prÃ©sident de la gestion de compte technique pour lâ□□EMEA et lâ□□Asie du Sud chez Tanium.

Â« Pendant la pandÃ©mie, les organisations ont dÃ» mettre en Å□uvre de nouvelles technologies du jour au lendemain pour assurer leur continuitÃ© dâ□□activitÃ©. Ce mÃ©lange de solutions assemblÃ©es Ã la hÃ¢te a ouvert dâ□□importantes failles de sÃ©curitÃ©. Ces lacunes persistantes sont une des raisons pour lesquelles les responsables informatiques ont plus de mal Ã sÃ©curiser leurs environnements. Â»

Les principaux enseignements de lâ□□enquÃªte :

â□¢ Le phishing et les mauvaises configurations de sÃ©curitÃ© sont les principales prÃ©occupations des responsables informatiques. 64 % des rÃ©pondants du secteur public ont identifiÃ© des incidents Ã©vitables provoquÃ©s par des clics dâ□□employÃ©s sur des liens de phishing.

Les mauvaises configurations de sÃ©curitÃ©, comme le fait de ne pas protÃ©ger des donnÃ©es sensibles Ã lâ□□aide de mots de passe, reprÃ©senteraient la deuxiÃ¨me cause dâ□□incidents Ã©vitables (pour 50 % des personnes interrogÃ©es). Ce pourcentage passe Ã 57 % parmi les organisations de 250 Ã 500 employÃ©s.

â□¢ Les organisations nâ□□ont pas les technologies adÃ©quates pour protÃ©ger leurs parcs informatiques. La troisiÃ¨me principale cause dâ□□incidents Ã©vitables (47 % des rÃ©pondants) est lâ□□absence de logiciels permettant de prÃ©venir les cyberattaques.

Des outils de cybersÃ©curitÃ© figurant pourtant parmi les plus populaires ne sont pas utilisÃ©s par ces organisations, ou nâ□□ont Ã©tÃ© dÃ©ployÃ©s que rÃ©cemment. Par exemple, seuls 19 % des entreprises utilisent des outils dâ□□analyse des vulnÃ©rabilitÃ©s du web, seuls 17 % sâ□□appuient sur des logiciels de test dâ□□intrusion, et tout juste 11 % ont recours Ã des analyseurs de paquets depuis au moins 5 ans.

â□¢ Les prochains axes dâ□□investissement dans la cybersÃ©curitÃ©. 70 % des dirigeants dâ□□entreprises et des partenaires Ã©prouvent davantage de difficultÃ©s Ã se protÃ©ger des menaces quâ□□avant la pandÃ©mie.

Ce problÃ¨me les a poussÃ©s Ã effectuer de nouveaux investissements dans la cybersÃ©curitÃ©, et Ã faire de la dÃ©tection des menaces et de la sÃ©curitÃ© des endpoints les deux principaux domaines nÃ©cessitant davantage de dÃ©penses.

PrÃ¨s de la moitiÃ© (49 %) des rÃ©pondants comptent investir davantage dans la dÃ©tection des menaces lâ□□annÃ©e prochaine. En outre, les organisations ayant subi une cyberattaque ou une fuite de donnÃ©es au cours des six derniers mois sont Ã©galement plus susceptibles dâ□□investir pour corriger leurs lacunes sur ce plan.

La sÃ©curitÃ© des endpoints devrait Ãªtre le deuxiÃ¨me principal axe dâ□□investissement dans les 12 prochains mois â□□ 46 % des organisations comptent augmenter leurs dÃ©penses.

Le troisiÃ¨me axe dâ□□investissement concerne les outils de rÃ©cupÃ©ration et de sauvegarde de donnÃ©es, puisque 45 % de lâ□□ensemble des organisations ont prÃ©vu dâ□□augmenter leurs dÃ©penses dans de telles technologies.

Ce pourcentage atteint mÃªme les 58 % pour les entreprises ayant Ã©tÃ© victimes dâ□□une cyberattaque ou dâ□□une fuite de donnÃ©es au cours des six derniers mois. Les quatriÃ¨me et cinquiÃ¨me axes dâ□□investissement potentiel sont dâ□□abord la sensibilisation des employÃ©s (43 %), puis lâ□□acquisition de nouveaux endpoints (42 %).

Â« Les rÃ©sultats de cette enquÃªte montrent que les organisations peinent Ã prendre une longueur dâ□□avance sur les vulnÃ©rabilitÃ©s connues ou inconnues alors que leur surface dâ□□attaque est toujours plus Ã©tendue Â», dÃ©clare Jason English, analyste en chef chez Intellyx.

Â« Les Ã©quipes de sÃ©curitÃ© en sous-effectif et sous-Ã©quipÃ©es veulent adopter une approche plus proactive, mais attendent souvent quâ□□un incident se produise pour investir dans des contre-mesures.

Notre enquÃªte montre que 86 % des organisations compromises au cours des six derniers mois pensent quâ□□elles auraient pu minimiser ces incidents de sÃ©curitÃ© en investissant davantage dans des mesures prÃ©ventives, comme dans la formation de leur personnel, ou dans lâ□□acquisition dâ□□outils offrant une visibilitÃ© accrue sur leurs rÃ©seaux. Â»

Lâ□□enquÃªte a Ã©tÃ© rÃ©alisÃ©e par Arlington Research au Royaume-Uni auprÃ¨s de trois cents responsables des systÃ¨mes dâ□□information et de la cybersÃ©curitÃ© dâ□□organisations dâ□□au moins 250 employÃ©s. Les rÃ©pondants viennent dâ□□une variÃ©tÃ© de secteurs (secteur public, services bancaires et financiers, technologies, industrie manufacturiÃ¨re, commerce de dÃ©tail, tÃ©lÃ©communications, santÃ© et enseignement).

Â« Le nombre important de rÃ©pondants citant la sÃ©curitÃ© des endpoints comme une prioritÃ© parmi leurs futurs axes dâ□□investissement met en lumiÃ¨re les dÃ©fis que doivent relever les entreprisesÂ», poursuit Chris Vaughan.

Â« Il est difficile, voire impossible, de protÃ©ger les donnÃ©es et appareils sur lesquels les organisations nâ□□ont aucune visibilitÃ©. Il nâ□□y a donc rien de surprenant Ã ce quâ□□elles rÃ©affectent aujourdâ□□hui leurs ressources pour couvrir leurs angles morts. Dans cette optique, lâ□□abandon des outils monofonctionnels au profit dâ□□une plateforme complÃ¨te peut les aider Ã rÃ©duire le coÃ»t et la complexitÃ© de leurs parcs informatiques. Â»