La vulnÃ©rabilitÃ©, facteur de risque pour la Saint-Valentin
Internet
PostÃ© par : JerryG
PubliÃ©e le : 12/2/2024 13:00:00

Selon le rÃ©cent rapport "Year in Review" Cloud and Threat Report de Netskope, la maniÃ¨re la plus courante pour les cyberattaquants d'accÃ©der aux organisations en 2023 a Ã©tÃ© l'ingÃ©nierie sociale.

Bien qu'il s'agisse d'une des tactiques prÃ©fÃ©rÃ©es des cybercriminels, l'ingÃ©nierie sociale ne consiste pas Ã casser un code en Ã©tant penchÃ© sur un clavier lumineux. Elle s'appuie en effet sur la vulnÃ©rabilitÃ© humaine individuelle, en incitant les gens Ã ouvrir la porte Ã l'attaquant.

Selon Paolo Passeri, Cyber Intelligence Specialist chez Netskope, la Saint-Valentin reprÃ©sente une opportunitÃ© pour les cybercriminels qui vont chercher Ã profiter de la vulnÃ©rabilitÃ© de leurs cibles autour de cette date, et, in fine, atteindre les entreprises :

Â« Si la plupart des gens pensent qu'ils ne tomberont jamais dans le piÃ¨ge de telles attaques, la vÃ©ritÃ© est que nous pouvons tous en Ãªtre victimes. Toute personne en proie Ã des Ã©motions fortes peut facilement Ãªtre amenÃ©e Ã commettre des erreurs de sÃ©curitÃ©, Ã donner un accÃ¨s non autorisÃ© Ã des informations sensibles, voire Ã divulguer elle-mÃªme des informations sensibles.

La Saint-Valentin est un trÃ¨s bon exemple. Les escroqueries Ã la romance sont une affaire sÃ©rieuse, avec des pertes dÃ©clarÃ©es pour les victimes atteignant le chiffre de 1,3 milliard de dollars en 2022 aux Ã□tats-Unis, et 92,8 millions de livres sterling au Royaume-Uni en 2023. Les cas de fraude ne se limitent pas au 14 fÃ©vrier, mais c'est Ã ce moment-lÃ que les victimes sont les plus vulnÃ©rables.

Une personne Ã la recherche de l'amour peut Ãªtre suffisamment avisÃ©e pour ignorer les messages non sollicitÃ©s provenant d'un faux profil de rencontre 364 jours par an, mais si l'engouement pour la Saint-Valentin l'a amenÃ©e Ã se sentir particuliÃ¨rement seule, elle sera peut-Ãªtre plus encline Ã rÃ©pondre.

De mÃªme que les personnes dÃ©jÃ en couple peuvent Ãªtre dans un Ã©tat Ã©motif diffÃ©rent Ã l'approche de la Saint-Valentin, avec par exemple lâ□□impatience de cÃ©lÃ©brer une Ã©tape importante de leur relation ou de recevoir une surprise. Elles seront alors peut-Ãªtre plus susceptibles de cliquer sur une offre de carte-cadeau sans avoir vÃ©rifiÃ© au prÃ©alable qu'elle provient d'une source lÃ©gitime.

Les organisations peuvent se dÃ©fendre contre ces attaques de plusieurs maniÃ¨res. Le risque augmente inÃ©vitablement avec l'utilisation d'applications non professionnelles sur les appareils de l'entreprise, de sorte que certaines peuvent choisir des politiques qui bloquent complÃ¨tement l'accÃ¨s aux applications personnelles - telles que les applications de rencontres - sur les appareils professionnels.

L'essor rÃ©cent de l'IA, par exemple, a conduit de nombreuses entreprises Ã envisager de bloquer les outils tels que ChatGPT et d'IA gÃ©nÃ©rative sur leurs systÃ¨mes. Toutefois, le blocage pur et simple de toutes les applications non professionnelles peut crÃ©er des frustrations, limiter l'innovation et donner l'impression d'un manque de confiance dans le personnel.

Les entreprises peuvent au contraire mettre en Å□uvre une mÃ©thode moins radicale qui s'appuie sur des outils intelligents, ainsi que sur des Ã©quipes de sÃ©curitÃ© qui analysent rÃ©guliÃ¨rement le trafic HTTP/HTTPS, avec une approche plus agile qui se dÃ©place vers le cloud, ainsi que des contrÃ´les de sÃ©curitÃ© renforcÃ©s.

Elles doivent Ã©galement mettre l'accent sur l'Ã©ducation et la sensibilisation, en incitant les utilisateurs Ã Ãªtre vigilants avant de cliquer sur un lien ou d'accÃ©der Ã une application non autorisÃ©e. Pour aider les individus Ã comprendre leur vulnÃ©rabilitÃ© personnelle, il est important de mettre l'accent sur les risques personnels, et pas seulement sur l'impact sur l'entreprise.

L'utilisation d'exemples montrant comment les attaques peuvent avoir un impact - et dÃ©couler - de la vie personnelle des gens peut les aider Ã mieux comprendre comment ils peuvent Ãªtre ciblÃ©s.

Quoi qu'une organisation choisisse de faire, il est impossible d'empÃªcher les employÃ©s de cliquer sur un lien malveillant, et le plus grand risque est souvent lorsque les utilisateurs cachent les cyber-incidents, en particulier ceux qui rÃ©sultent d'attaques par ingÃ©nierie sociale oÃ¹ ils peuvent se sentir personnellement responsables.

En cas de compromission, il est essentiel de rÃ©duire le temps nÃ©cessaire Ã l'attÃ©nuation de l'attaque, c'est pourquoi il ne faut pas blÃ¢mer les victimes des attaques. L'essentiel est de favoriser une culture de collaboration dans laquelle le personnel fait partie du processus, plutÃ´t que d'instiller une culture de la peur.

La sensibilisation des employÃ©s dans un climat de partenariat peut grandement contribuer Ã rÃ©duire le risque que les cybercriminels profitent de la vulnÃ©rabilitÃ© humaine, autour notamment de la Saint-Valentin. Â»