Education : 3 cyberattaques sur 4 dues Ã la compromission d'un compte.
Internet
PostÃ© par : JerryG
PubliÃ©e le : 1/9/2023 15:00:00

69 % des Ã©tablissements d'enseignement ont connu un incident de sÃ©curitÃ© au cours des 12 derniers moisÂ Netwrix, un fournisseur de cybersÃ©curitÃ© qui facilite la sÃ©curitÃ© des donnÃ©es, dÃ©voile des rÃ©sultats additionnels pour le secteur de l'Ã©ducation de son enquÃªte rÃ©alisÃ©e auprÃ¨s de 1 610 professionnels de l'informatique et de la sÃ©curitÃ© dans plus de 100 pays.Â Â Selon cette enquÃªte, 69 % des organisations du secteur de l'Ã©ducation ont subi une cyberattaque au cours des 12 derniers mois. L'hameÃ§onnage et la compromission de comptes utilisateurs sont les modes d'attaque les plus courants pour ces organisations ; contre le phishing et les logiciels malveillants (tels que les ranÃ§ongiciels) pour les autres secteurs verticaux.Â
De plus, 3 attaques sur 4 (75 %) dans le secteur de l'Ã©ducation sont associÃ©es Ã la compromission d'un compte utilisateur ou d'administrateur sur site, contre 48 % dans les autres secteurs.Â Â« Les organisations du secteur de l'Ã©ducation gÃ¨rent des comptes extrÃªmement divers - personnel, sous-traitants, Ã©ducateurs, Ã©tudiants, anciens Ã©lÃ¨ves - dont le taux de rotation est Ã©levÃ©. MÃªme si la gestion des identitÃ©s est automatisÃ©e, il est difficile de maintenir les utilisateurs formÃ©s aux meilleures pratiques de sÃ©curitÃ©, car il y a constamment de nouveaux arrivants, analyse Dmitry Sotnikov, VP of Product Management chez Netwrix.Â
En outre, les Ã©tudiants peuvent manquer d'expÃ©rience pour repÃ©rer les emails d'hameÃ§onnage ou les faux sites Web demandant leurs identifiants. Pour relever ces dÃ©fis, il est essentiel de fournir une formation obligatoire en matiÃ¨re de sÃ©curitÃ© au cours des premiÃ¨res semaines et de la rÃ©pÃ©ter rÃ©guliÃ¨rement. Â»Â Â« Pour permettre la recherche et la collaboration, les Ã©tablissements d'enseignement fournissent souvent aux utilisateurs une variÃ©tÃ© d'appareils et de systÃ¨mes partagÃ©s exposÃ©s Ã Internet, crÃ©ant une surface d'attaque massive, ajoute Dirk Schrader, VP of Security Research chez Netwrix.Â
Pour rÃ©duire les risques, il est crucial d'appliquer des politiques de mots de passe solides, qui empÃªchent l'utilisation dâ□□identifiants faibles et compromis, et qui obligent de mettre en Å□uvre l'authentification multifactorielle (MFA) et le dÃ©ploiement du principe du moindre privilÃ¨ge. En outre, les solutions de surveillance automatisÃ©e aident les Ã©quipes informatiques Ã dÃ©tecter et Ã rÃ©pondre Ã la compromission et Ã l'abus de comptes Ã temps. Â»Â Pour en savoir plus : netwrix.com/2023_hybrid_security_trends_report.html