CybersÃ©curitÃ© : se dÃ©faire des idÃ©es reÃ§ues
Internet
PostÃ© par : JulieM
PubliÃ©e le : 7/10/2022 13:00:00

Octobre marque comme tous les ans le mois de la cybersÃ©curitÃ©. Lâ□□occasion de se pencher sur lâ□□Ã©volution des cybermenaces, les succÃ¨s de lâ□□annÃ©e Ã©coulÃ©e, mais aussi les causes des Ã©checs.Â

En effet, de nombreux prÃ©jugÃ©s, qui perdurent au sein des entreprises, continuent dâ□□alimenter des vulnÃ©rabilitÃ©s pouvant pourtant Ãªtre facilement gommÃ©es.

Selon Pierre-Louis Lussan, Country Manager Southern Europe chez Netwrix, il est urgent que les organisations dÃ©passent ces a priori et se montrent proactives en matiÃ¨re de cybersÃ©curitÃ© :

Â« Les donnÃ©es, aussi bien des employÃ©s que celles des clients, constituent les actifs dâ□□une organisation et sont, Ã ce titre, clÃ©s pour assurer la pÃ©rennitÃ© des activitÃ©s. Il est donc essentiel que les entreprises les sÃ©curisent en dÃ©passant trois idÃ©es reÃ§ues qui persistent.

IdÃ©e reÃ§ue nÂ°1 â□□ la cybersÃ©curitÃ©, câ□□est compliquÃ©

De mÃªme que la sÃ©curitÃ© physique, le principe de la cyberprotection repose sur contrÃ´ler qui fait quoi Ã tout moment, ainsi que savoir prÃ©cisÃ©ment oÃ¹ est chaque donnÃ©e.

Pour ce faire, les entreprises ont besoin dâ□□une traÃ§abilitÃ© complÃ¨te, pour hiÃ©rarchiser la sÃ©curisation des informations par ordre de criticitÃ©, alors que lâ□□adoption du travail hybride du fait de la pandÃ©mie a Ã©tendu la surface dâ□□attaque et accÃ©lÃ©rÃ© les risques.

Si gagner en visibilitÃ© et contrÃ´le semble ardu, il existe des outils technologiques automatisÃ©s Ã mÃªme de remplir ces fonctions, et qui notifient en temps rÃ©el les Ã©quipes IT en cas dâ□□activitÃ©s suspectes ou de modifications inadÃ©quates dans le systÃ¨me dâ□□information.

La classification automatisÃ©e des donnÃ©es et la surveillance de l'activitÃ© permettent de gagner un temps prÃ©cieux et n'impliquent l'Ã©quipe informatique que lorsque cela est nÃ©cessaire.Â

De plus, la cybersÃ©curitÃ© peut Ãªtre fournie en tant que service via un partenaire dÃ©diÃ©, lorsque l'organisation ne dispose pas de suffisamment de ressources internes pour assurer la protection de son environnement informatique.

IdÃ©e reÃ§ue nÂ°2 â□□ la menace vient de lâ□□extÃ©rieur

Traditionnellement, les organisations sont principalement prÃ©occupÃ©es par les acteurs externes, tels que les cybercriminels, mais les risques associÃ©s Ã leurs propres employÃ©s doivent Ã©galement Ãªtre pris en considÃ©ration.

Les comptes Ã privilÃ¨ges â□□ câ□□est-Ã -dire ceux possÃ©dant des droits dâ□□accÃ¨s Ã©levÃ©s â□□ sont particuliÃ¨rement visÃ©s par les cybercriminels. Si la menace vient alors de lâ□□extÃ©rieur, sa mise en Å□uvre est permise par des pratiques en interne.

En effet, des organisations ont adoptÃ© la stratÃ©gie du moindre privilÃ¨ge, en accordant le moins

de droits possible aux employÃ©s, afin que ces derniers ne puissent atteindre que les donnÃ©es nÃ©cessaires Ã la rÃ©alisation de leurs tÃ¢ches.

Cependant, cette limitation des droits nâ□□est pas une barriÃ¨re efficace contre les cybercriminels si les accÃ¨s sont accordÃ©s de faÃ§on permanente.Â

Il est ainsi conseillÃ© dâ□□adopter une politique plutÃ´t du Â« juste-Ã -temps Â», soit dâ□□octroyer des droits temporaires Ã chaque demande dâ□□accÃ¨s ; de sorte que si un cybercriminel compromet un compte utilisateur, il se retrouvera bloquÃ© et ne pourra donner suite Ã ses activitÃ©s suspicieuses car les droits dâ□□accÃ¨s ne lui seront alors pas accordÃ©s.

IdÃ©e reÃ§ue nÂ°3 â□□ Mes informations nâ□□intÃ©ressent pas les criminels

Encore aujourdâ□□hui, des organisations se pensent Ã lâ□□abri des hackers, en particulier les PME persuadÃ©es que les cybercriminels recherchent en prioritÃ© des donnÃ©es liÃ©es notamment Ã la propriÃ©tÃ© intellectuelle, telles que les brevets.

Or, toute information personnelle sur les employÃ©s et les clients est monnayable sur le Dark Net, et reprÃ©sente donc une cible pour les attaquants.Â

Â Ces derniers nâ□□ont en outre aucune Ã©thique et nâ□□hÃ©sitent pas Ã viser des organisations de santÃ©, comme les hÃ´pitaux, quitte Ã mettre la vie de patients en danger.

Alors que les cyberattaques sâ□□intensifient, les entreprises qui ne prennent pas mesure du danger et ne sâ□□arment pas en consÃ©quence risquent de prendre un retard, qui sera ensuite difficile de rattraper.

Lâ□□enjeu est pourtant de taille, car une protection des donnÃ©es innovantes, qui sâ□□adapte Ã lâ□□Ã©volution du paysage des menaces, est nÃ©cessaire pour parer toute tentative de compromission, mais aussi pour gagner la confiance de lâ□□ensemble de son Ã©cosystÃ¨me. Â»