CybercriminalitÃ© : Attaques sur les informations comptables
Internet
PostÃ© par : JulieM
PubliÃ©e le : 15/3/2023 13:00:00

Tim Morris, Chief Security Advisor chez Tanium, Ã propos de lâ□□Ã©tude rÃ©alisÃ©e par Deloitte qui montre que les entreprises ne sont pas bien prÃ©parÃ©es Ã faire face Ã une augmentation des attaques visant des informations comptables et financiÃ¨res sensibles, mÃªme si la moitiÃ© des cadres interrogÃ©s ont dÃ©clarÃ© qu'ils s'attendaient Ã une augmentation de ces attaques :

Pourquoi une augmentation des cyberattaques visant les donnÃ©es comptables et financiÃ¨res est-elle prÃ©visible ?

Les donnÃ©es financiÃ¨res et comptables sont essentielles Ã la survie d'une entreprise. Comme le code source ou la propriÃ©tÃ© intellectuelle, les donnÃ©es financiÃ¨res sont inestimables, ce qui en fait une cible de grande valeur.

Pourquoi les Ã©quipes comptables et financiÃ¨res ne collaborent-elles pas plus Ã©troitement et de maniÃ¨re plus cohÃ©rente avec leurs homologues dans le domaine de la cybersÃ©curitÃ© ?

Les Ã©quipes comptables et financiÃ¨res sont des fonctions commerciales. L'informatique est souvent considÃ©rÃ©e comme un "mal nÃ©cessaire" et les Ã©quipes de sÃ©curitÃ© informatique comme le "dÃ©partement qui dit non". Ainsi, dans certaines organisations, les informaticiens qui gÃ¨rent les systÃ¨mes financiers peuvent Ãªtre des "informaticiens de l'ombre".

AprÃ¨s tout, le directeur financier signe gÃ©nÃ©ralement les chÃ¨ques et peut conserver une certaine autonomie par rapport aux Ã©quipes ITOps et CybersÃ©curitÃ© de l'entreprise. Toutefois, cela dÃ©pend de la taille de l'entreprise et de son organisation.

Ces derniÃ¨res annÃ©es, l'informatique et la sÃ©curitÃ© se sont efforcÃ©es de devenir des outils au service de l'entreprise, et non des points de friction. NÃ©anmoins, les systÃ¨mes financiers et comptables ne changent pas souvent, de sorte qu'il existe encore beaucoup de dettes technologiques et de systÃ¨mes hÃ©ritÃ©s qui sont nÃ©cessaires au fonctionnement de l'entreprise, par exemple "cette feuille de calcul est le Saint Graal de nos rapports mensuels".

Quelles mesures les responsables de la sÃ©curitÃ© informatique doivent-ils prendre pour remÃ©dier Ã cette situation ?

Comprendre ce qui doit Ãªtre protÃ©gÃ©. Travaillez avec les principaux dirigeants de l'entreprise, ainsi qu'avec toute Ã©quipe informatique, pour savoir quels actifs doivent Ãªtre protÃ©gÃ©s et quelles donnÃ©es doivent l'Ãªtre. Il est essentiel d'identifier les actifs et les donnÃ©es critiques. Il faut savoir oÃ¹ et comment les donnÃ©es sont transmises et stockÃ©es.

Quelles sont les cyberdÃ©fenses Ã mettre en Å□uvre pour mieux protÃ©ger les informations financiÃ¨res ?

C'est ce qui ressort de la rÃ©ponse prÃ©cÃ©dente. AprÃ¨s la dÃ©couverte et la classification des applications et des actifs, les mÃªmes programmes doivent Ãªtre mis en Å□uvre.

Pour l'authentification, il faut utiliser un systÃ¨me de gestion des accÃ¨s robuste (FIDO2 pour les donnÃ©es les plus critiques) et mettre en Å□uvre le principe du moindre privilÃ¨ge. Pour la

prÃ©vention, utiliser le programme de gestion des vulnÃ©rabilitÃ©s et patcher frÃ©quemment les actifs qui exÃ©cutent des applications financiÃ¨res et stockent des donnÃ©es.

Veillez Ã ce que les applications financiÃ¨res et les logiciels de comptabilitÃ©/fournisseurs fassent l'objet d'une Ã©valuation des vulnÃ©rabilitÃ©s. S'assurer que les donnÃ©es au repos sont chiffrÃ©es et que les donnÃ©es en mouvement transitent bien par des canaux sÃ©curisÃ©s.

VÃ©rifier que les contrÃ´les de sÃ©curitÃ© destinÃ©s Ã protÃ©ger les utilisateurs, les actifs et les donnÃ©es sont prÃ©sents, fonctionnels et efficaces (EDR, outils de gestion des systÃ¨mes, etc.). ProcÃ©der Ã une simulation ou Ã une Ã©mulation pour savoir Ã quoi ressemblent ces systÃ¨mes de lâextÃ©rieur, pour un attaquant ou un tiers. Sensibilisez et formez Ã©galement les utilisateurs.

Quels sont les risques de ne pas le faire ?

Les risques sont les mÃªmes pour la plupart des cyberattaques. Qu'il s'agisse d'un ransomware, d'une extorsion ou d'une destruction de donnÃ©es. Chacune d'entre elles perturbera les opÃ©rations, telles que le systÃ¨me de paiement des crÃ©ances, des fournisseurs et des salaires, ce qui entraÃ®nera une perte de revenus et une augmentation des dÃ©penses.

Il y a la menace des coÃ»ts monÃ©taires nÃ©cessaires pour payer les ranÃ§ons ou les extorsions, et il pourrait y avoir des amendes rÃ©glementaires. Tous ces Ã©lÃ©ments peuvent Ã©galement nuire Ã la rÃ©putation de l'entreprise et entraÃ®ner la perte de clients.