Cybercriminalité : Attaques sur les informations comptables

Internet

Posté par : JulieM

Publié le : 15/3/2023 13:00:00

Tim Morris, Chief Security Advisor chez Tanium, à propos de l'étude réalisée par Deloitte qui montre que les entreprises ne sont pas bien préparées à faire face à une augmentation des attaques visant des informations comptables et financières sensibles, même si la moitié des cadres interrogés ont déclaré qu'ils s'attendaient à une augmentation de ces attaques :

Pourquoi une augmentation des cyberattaques visant les données comptables et financières est-elle prévisible ?

Les données financières et comptables sont essentielles à la survie d'une entreprise. Comme le code source ou la propriété intellectuelle, les données financières sont inestimables, ce qui en fait une cible de grande valeur.

Pourquoi les équipes comptables et financières ne collaborent-elles pas plus étroitement et de manière plus cohérente avec leurs homologues dans le domaine de la cybersécurité ?

Les équipes comptables et financières sont des fonctions commerciales. L'informatique est souvent considérée comme un "mal nécessaire" et les équipes de sécurité informatique comme le "département qui dit non". Ainsi, dans certaines organisations, les informaticiens qui gèrent les systèmes financiers peuvent être des "informaticiens de l'ombre".

Après tout, le directeur financier signe généralement les chèques et peut conserver une certaine autonomie par rapport aux équipes IT Ops et Cybersécurité de l'entreprise. Toutefois, cela dépend de la taille de l'entreprise et de son organisation.

Ces dernières années, l'informatique et la sécurité se sont efforcées de devenir des outils au service de l'entreprise, et non des points de friction. Néanmoins, les systèmes financiers et comptables ne changent pas souvent, de sorte qu'il existe encore beaucoup de dettes technologiques et de systèmes hérités qui sont nécessaires 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 sécurité informatique doivent-ils prendre pour remédier à cette situation ?

Comprendre ce qui doit être protégé. Travaillez avec les principaux dirigeants de l'entreprise, ainsi qu'avec toute équipe informatique, pour savoir quels actifs doivent être protégés et quelles données doivent l'être. Il est essentiel d'identifier les actifs et les données critiques. Il faut savoir où et comment les données sont transmises et stockées.

Quelles sont les cyberdéfenses à mettre en œuvre pour mieux protéger les informations financières ?

C'est ce qui ressort de la réponse précédente. Après la découverte et la classification des applications et des actifs, les mêmes programmes doivent être mis en œuvre.

Pour l'authentification, il faut utiliser un système de gestion des accès robuste (FIDO2 pour les données les plus critiques) et mettre en œuvre le principe du moindre privilège. Pour la

prévention, utiliser le programme de gestion des vulnérabilités et patcher fréquemment les actifs qui exécutent des applications financières et stockent des données.

Veillez à ce que les applications financières et les logiciels de comptabilité/fournisseurs fassent l'objet d'une évaluation des vulnérabilités. S'assurer que les données au repos sont chiffrées et que les données en mouvement transitent bien par des canaux sécurisés.

Vérifier que les contrôles de sécurité destinés à protéger les utilisateurs, les actifs et les données sont présents, fonctionnels et efficaces (EDR, outils de gestion des systèmes, etc.). Procéder à une simulation ou à une émulation pour savoir à quoi ressemblent ces systèmes de l'extérieur, pour un attaquant ou un tiers. Sensibilisez et formez également les utilisateurs.

Quels sont les risques de ne pas le faire ?

Les risques sont les mêmes pour la plupart des cyberattaques. Qu'il s'agisse d'un ransomware, d'une extorsion ou d'une destruction de données. Chacune d'entre elles perturbera les opérations, telles que le système de paiement des créances, des fournisseurs et des salaires, ce qui entraînera une perte de revenus et une augmentation des dépenses.

Il y a la menace des coûts monétaires nécessaires pour payer les rançons ou les extorsions, et il pourrait y avoir des amendes réglementaires. Tous ces éléments peuvent également nuire à la réputation de l'entreprise et entraîner la perte de clients.