Quatre étapes pour **gérer les cyber-risques dans l'enseignement supérieur**

L'augmentation spectaculaire des attaques par ransomware et autres atteintes à la cybersécurité crée un véritable ouragan pour les établissements d'enseignement supérieur, et les cyber-assureurs auprès desquels ils souscrivent pour se protéger.

Augmentation des risques et comment réagir

Le secteur de l'enseignement demeure ciblé de manière disproportionnée par les ransomwares et autres attaques.[1] Les établissements d'enseignement supérieur sont également confrontés à des défis informatiques spécifiques, notamment des exigences réglementaires uniques imposées par divers acteurs du monde universitaire, de l'administration, de la recherche et des soins de santé.

Parallèlement, les exigences financières plus élevées liées aux ransomwares, qui ont plus que doublé l'année dernière pour atteindre une moyenne de 2,2 millions de dollars par attaque[2], ont le même impact sur les cyber-assureurs que les catastrophes naturelles ont eu sur les autres assureurs. « À mesure que les conditions extrêmes se multiplient, qu'il s'agisse de conditions météorologiques ou de cyber-risques, une augmentation des primes sera inévitable », déclare Stephen Singh, responsable des fusions, acquisitions et cessions, du capital-investissement et du cyber-risque chez Zscaler.

Compte tenu de ces facteurs, les dirigeants de l'enseignement supérieur doivent améliorer la posture de cybersécurité de leurs établissements, gérer les cyber-risques et réduire la probabilité d'attaques menées à bien. Voici quatre étapes clés à suivre :

1. Appliquer une hygiène et des contrôles appropriés

Une première étape dans l'amélioration de votre cybersécurité, et ainsi devenir plus assurable, consiste à veiller à ce que votre institution suit les bonnes pratiques du secteur. Celles-ci vont de la sécurité du terminal et de l'autorisation multifacteur (MFA) à l'application de correctifs aux systèmes en place, en passant par la réalisation de sauvegardes et la protection contre la perte de données, ainsi que la formation des étudiants et du personnel.

Plusieurs études démontrent que de nombreuses entreprises n'ont pas adopté ces pratiques ou les ont appliquées de manière inappropriée.

« Ce niveau d'efficacité est incroyablement important, en particulier lorsque vous essayez de mesurer, de gérer et d'assurer des risques », explique Stephen Singh.

Documentez les contrôles et les stratégies mis en place, à la fois pour un usage interne et pour les fournisseurs de cyber-assurance. « Ne vous contentez pas de les déployer », ajoute Stephen Singh. « Déployez-les avec un niveau d'attribution significatif pour votre entreprise et pour ceux qui pourraient utiliser ces informations pour porter un jugement. »

2. Adopter le Zero Trust

La plupart des institutions ont créé « une carapace extérieure dure et un intérieur très moelleux » pour assurer leur cyber-défense, explique Stephen Singh. « Les acteurs malveillants peuvent se déplacer où ils le souhaitent une fois qu'ils ont franchi cette carapace renforcée. »

Les institutions devraient plutôt adopter le Zero Trust en tant que cadre de sécurité. Le Zero Trust, que Stephen Singh décrit comme « un parcours, et non pas un produit », est une approche qui vérifie en permanence l'identité de chaque utilisateur lorsqu'il navigue sur le réseau.

Le Zero Trust garantit que les utilisateurs n'ont accès qu'aux systèmes et aux données dont ils ont besoin, ce qui réduit considérablement le risque de compromission de systèmes ou de magasins de données entiers. « Une fois que vous avez réduit votre surface d'attaque, empêché la propagation latérale et stoppé la perte de données, vous avez éliminé une énorme quantité de risques de votre système », explique Stephen Singh.

Les architectures informatiques construites autour du Zero Trust fournissent également des données et des informations de télémétrie pour surveiller en permanence les comportements suspects et réagir automatiquement en fonction du risque potentiel. L'intelligence artificielle et l'apprentissage automatique (IA/AA) renforcent ces capacités, tout en fournissant des informations plus riches concernant les domaines dans lesquels les institutions devraient investir du temps et des ressources.

3. Faire appel à la quantification des cyber-risques

L'étape suivante exige un changement culturel de la façon dont les institutions envisagent le cyber-risque. La quantification des cyber-risques (ou CRQ pour « Cyber Risk Quantification ») change la donne en évaluant le risque en termes financiers. Les institutions utilisent des évaluations et des analyses de risques pour prévoir le coût potentiel d'une violation, qui se chiffre souvent en millions ou en dizaines de millions de dollars.

« Ce niveau de granularité vous permet d'avoir une bien meilleure idée de votre exposition réelle », explique Stephen Singh.

Sur cette base, les institutions peuvent déterminer à quel degré les investissements dans différentes stratégies de cybersécurité peuvent réduire ces pertes. « Chacune de ces stratégies permet de réduire les coûts en fonction de l'ampleur des pertes financières potentielles que les contrôles mis en place permettent d'atténuer », ajoute Stephen Singh.

En se concentrant sur les questions financières plutôt que sur la technologie, la CRQ permet aux dirigeants des institutions de discuter des stratégies dans une perspective commerciale. « Cela modifie le dialogue pour le rendre compréhensible par la direction et le conseil d'administration », explique Stephen Singh. « Le rééquilibrage de votre stratégie d'investissement dans le cyber-risque devient une discussion beaucoup plus constructive avec votre équipe de direction. »

Au cours de ces conversations éclairées par des données, les hauts dirigeants déterminent le montant du risque financier que l'institution est prête à accepter, à atténuer par des investissements dans des contrôles de cybersécurité ou à confier à des fournisseurs de cyber-assurance.

65 % des entreprises ne disposent toujours pas d'un plan de cyber-résilience ou de réponse aux incidents pour réagir aux attaques, des attaques que les responsables des institutions devraient considérer comme inévitables.

« Envisager une perte financière vous permettra de faire le meilleur choix plutôt que le premier choix. « Plus vous les atténuez, moins vous devez accepter les risques et moins vous devez les confier à un assureur », explique Stephen Singh. « Cela permet également de souscrire des polices de cyber-assurance plus avantageuses, car vous parlez désormais le même langage. »

4. Établir des partenariats avec des fournisseurs de cyber-assurance

Les fournisseurs de cyber-assurance font bien plus que proposer une couverture contre les violations et les attaques. Nombre d'entre eux proposent désormais une large gamme de services, notamment l'évaluation des risques et l'ingénierie, la réponse aux incidents et les services gérés. Certains proposent même des services juridiques et de relations publiques en cas de violation.

Envisager le pire, mais prévoir le meilleur

Surtout, soyez réaliste concernant menaces. Stephen Singh affirme que 65 % des entreprises ne disposent toujours pas d'un plan de cyber-résilience ou de réponse aux incidents pour réagir aux attaques, des attaques que les responsables des institutions devraient considérer comme inévitables.

« Toutes les entreprises devraient partir du principe qu'elles ont été ou seront compromises et disposer d'un plan d'action », déclare Stephen Singh. « Les menaces, les risques, les vulnérabilités, les violations et les extorsions n'ont jamais évolué aussi rapidement. Demandez-vous quel serait le bon modèle pour que votre budget limité génère le meilleur retour sur investissement pour l'ensemble de votre environnement. »

Notes de fin :
1. https://news.sophos.com/en-us/2023/07/20/the-state-of-ransomware-in-education-2023/
2. https://www.zdnet.com/article/ransomware-payments-heres-how-much-falling-victim-will-now-cost-you/

Cet article a été rédigé et produit par le Center for Digital Education Content Studio, avec les informations et les contributions de Zscaler.

Produit par :

CENTER FOR DIGITAL EDUCATION

Le Center for Digital Education est un institut national de recherche et de conseil spécialisé dans les tendances, les politiques et le financement des technologies de l'enseignement primaire, secondaire et supérieur. Le Center fournit aux leaders de l'enseignement et du secteur une aide à la prise de décision et des informations exploitables pour les aider à intégrer efficacement les nouvelles technologies au 21e siècle.

www.centerdigitaled.com

Sponsorisé par :

zscaler™ aws

Partenaire logiciel AWS de niveau Avancé, Zscaler est la plus grande plateforme cloud de sécurité inline au monde. Zscaler Zero Trust Exchange agit comme un standard téléphonique intelligent, connectant en toute sécurité les utilisateurs directement aux applications et aux workloads (jamais au réseau) depuis n'importe quel emplacement à l'aide de n'importe quel appareil, offrant une sécurité Zero Trust à la pointe du secteur. Zscaler réduit les risques commerciaux, améliore la productivité des utilisateurs et utilise des informations commerciales et cybernétiques de pointe optimisées par l'IA pour transformer les données en connaissances. La surveillance proactive de l'expérience numérique permet de maintenir la productivité des utilisateurs, tout en réduisant les appels au service d'assistance. Zscaler élimine également les coûts, la complexité et les risques de sécurité associés aux VPN, pare-feu et produits ponctuels traditionnels.

www.zscaler.fr

ADOBESTOCK.COM