11:11 Systems partage des conseils pour utiliser la réglementation pour renforcer la cyber-résilience

READING, UNITED KINGDOM, June 12, 2024 /EINPresswire.com/ -- Par Sean Tilley, directeur commercial senior chez 11:11 Systems

Dans le monde interconnecté actuel, la résilience opérationnelle, et notamment la cyber-résilience, sont au cœur des priorités des organisations. L'ère numérique multiplie les opportunités d'innovation et de croissance, mais aussi les dangers. Ces dangers peuvent prendre plusieurs formes, des logiciels rançon cyniques et des attaques de déni de service (DDoS) à l'usurpation d'identité et l'ingénierie sociale. De nouvelles attaques font régulièrement les gros titres, ce qui crée un sentiment d'insécurité diffus en raison des failles de données et des périodes d'arrêt contraint qui affaiblissent les organisations et entraînent des conséquences économiques graves.

Ces menaces sont amplifiées par la généralisation du télétravail et de l'accès à distance, car cela met en évidence des vulnérabilités dans des défenses numériques que l'on pensait robustes. Les cybercriminels sont désinhibés et font preuve d'ingéniosité pour exploiter les vulnérabilités, afin d'orchestrer des attaques d'ampleur, plus complexes et dévastatrices que jamais.

Dans ce contexte de menaces en évolution constante, les entreprises redoublent d'efforts pour se mettre en conformité avec la réglementation et renforcer la résilience opérationnelle, et notamment la cyber-résilience, pour atténuer les risques et assurer leur survie en cas d'attaque.

Les réglementations sont le fer de lance de la cyber-résilience

La cyber-résilience est une approche stratégique et globale qui permet aux organisations de mieux anticiper, prévenir, réagir et se rétablir en cas d'incidents ou d'attaques.

Le cadre législatif évolue pour tenter de créer les conditions d'une véritable résilience opérationnelle, intégrant la cyber-résilience, ainsi que la technologie, les personnes, les processus et les informations. Toutefois, cette législation est complexe et impose une approche stratégique pour comprendre les nuances des différentes lois, leurs implications et les délais d'application.

Des règlements tels que le RGPD, HIPAA et Sarbanes-Oxley (SOX) encadrent le mode de protection des données, mais de nouvelles propositions, comme NIS2, DORA et FCA CP19/32, esquissent une nouvelle approche de la sécurité des données, de la confidentialité et de la cybersécurité pour assurer la continuité du service au client en dépit des nouvelles menaces.

La mise en conformité avec la réglementation n'est pas une simple obligation légale, mais un impératif stratégique pour parvenir à la résilience opérationnelle, qui implique une approche globale et soigneusement planifiée de la cybersécurité. Les organisations ont tout à gagner en réévaluant, renforçant et revitalisant leur posture de cybersécurité, transformant ainsi la conformité réglementaire en avantage concurrentiel.

Coût de la « cyber-insécurité »

En 2023, le coût total moyen d'une violation des données a atteint 4,45 millions de dollars, soit le montant le plus élevé sur les 19 ans d'existence du rapport Cost of Data Breach publié par le Ponemon Institute et IBM. Cette trajectoire devrait rester ascendante, car les experts nous mettent en garde contre une augmentation de la fréquence et de la sophistication des cyberattaques.

La messagerie est au cœur de la communication dans les entreprises, mais est particulièrement vulnérable, car elle véhicule environ 94 % du total des logiciels malveillants et d'usurpation d'identité (phishing), une méthode qui mise sur les erreurs humaines, ainsi que la faible sensibilisation à la cybersécurité, et reste l'une des formes les plus répandues de cybercrime.

Des pertes financières et de clients à l'atteinte à l'image de marque et aux processus longs de remédiation, sans oublier les répercussions juridiques, l'impact de la cybercriminalité est profond et concerne tous les types et toutes les tailles d'entreprises. Selon Cybersecurity Ventures, la cybercriminalité devrait infliger 9,5 trillions de dollars de dommages cumulés en 2024 et 10,5 trillions annuellement d'ici 2025, alors que son impact n'était que de 3 trillions il y a à peine dix ans. Si la cybercriminalité était un État, elle formerait la troisième économie mondiale juste après les États-Unis et la Chine.

L'explosion des incidents de cybersécurité et de leurs coûts a entraîné la promulgation de nouvelles lois de cybersécurité et de protection des données.

Passer d'une stratégie réactive à une stratégie anticipatoire

Les États comme les organismes de réglementation du monde entier ont pris la mesure de l'importance de la fortification des infrastructures numériques face à l'évolution des cybermenaces, ainsi que des responsabilités découlant de produits d'intelligence artificielle (IA) défectueux ou malveillants. Le but n'est plus simplement de réagir aux incidents, mais de mettre en place un cadre proactif et résilient qui permet d'anticiper et de gérer les cybermenaces et leurs perturbations.

Toutefois, les implications des nouvelles réglementations sont profondes pour les entreprises. Elles imposent l'évolution des pratiques usuelles pour mettre en place des stratégies plus intégrées et globales qui recouvrent non seulement les solutions techniques, mais aussi la culture de l'entreprise, une planification minutieuse et la sensibilisation des employés à tous les niveaux.

La recrudescence des cybermenaces a fait de la cybersécurité une priorité des équipes de direction. Alors que les entreprises découvrent ce nouveau contexte, s'informer et rester agile sont essentiels, que ce soit pour se conformer aux nouvelles lois ou protéger leurs actifs numériques et leur futur en général. L'écart entre les intentions et l'état réel de préparation souligne l'importance d'une révolution stratégique de l'approche de la cybersécurité et de la cyber résilience.

Réglementations et cyber-résilience

Pour les entreprises, l'évolution du cadre réglementaire signifie que la cybesécurité et la protection des données ne sont plus simplement une question technique, mais bien un élément clé de la gouvernance et de la stratégie de l'entreprise. L'adaptation à ces lois implique une approche globale, associant la conformité à des pratiques de cybersécurité robustes pour la récupération des données, la formation du personnel et la surveillance du système, afin de créer un cadre opérationnel résilient à la hauteur des défis de l'économie numérique.

Destiny Gillbee
C8 Consulting Ltd.
11-11systems@c8consulting.co.uk
