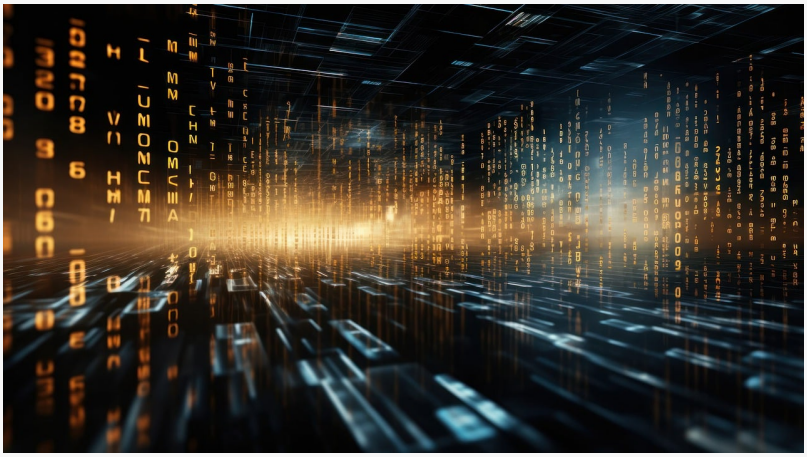
11:11 Systems gibt Tipps zur Nutzung von Vorschriften zur Stärkung der Cyber-Resilienz

LONDON, UK, June 12, 2024 /EINPresswire.com/ -- von Sean Tilley, Senior Director Sales bei 11:11 Systems



In unserer global vernetzten Welt haben operative Belastbarkeit und Cyberabwehr in Unternehmen höchste Priorität. Zwar schafft das digitale Zeitalter beispiellose Möglichkeiten für Innovation und Wachstum, jedoch nimmt auch die Zahl an Cyberbedrohungen ständig zu. Diese nehmen unterschiedliche Formen an, von gezielten Ransomware- und DDoS-Angriffen (Distributed Denial of Service) bis hin zu Phishing und Social Engineering. Angesichts immer neuer Schlagzeilen zu schweren Angriffen wird deutlich, wie sehr solche Vorfälle mit den daraus resultierenden Datenpannen und Systemausfällen Unternehmen in die Knie zwingen, ihren öffentlichen Ruf schädigen und erhebliche wirtschaftliche Verluste nach sich ziehen können.

Diese Bedrohungen werden durch die weiterhin wachsende Verbreitung von Homeoffice und Fernzugriff begünstigt, denn es ergeben sich Schwächen Abwehrsystemen, die bisher als ausreichend robust galten. Cyberkriminelle gehen immer verwegener und innovativer vor. Sie nutzen die neu aufgedeckten Schwachstellen aus, um Angriffe zu orchestrieren, die tiefgreifender, ausgefeilter und gefährlicher sind als je zuvor.

Die sich ständig weiterentwickelnde Bedrohungslandschaft verstärkt den Fokus auf gesetzlicher Compliance, operativer Belastbarkeit und Cyberabwehr, um die Risiken zu mindern und sicherzustellen, dass Unternehmen Angriffe überstehen können.

Gesetzesvorgaben fördern die Cyberabwehr

Cyberabwehr ist ein umfassendes Strategiekonzept, das Unternehmen nutzen können, um Cyberrisiken besser zu antizipieren, Vorfälle zu vermeiden und zu bekämpfen sowie die Wiederherstellung nach Angriffen zu optimieren.

Regierungs- und Regulierungsbehörden hoffen, mithilfe von regulatorischen Frameworks, die Technologie, Menschen, Prozesse und Informationen abdecken, eine hohe operative Belastbarkeit und robuste Cyberabwehr zu erreichen. Wer jedoch den Dschungel an Vorschriften und Bestimmungen erfolgreich navigieren will, muss strategisch vorgehen und sich ausführlich über die Nuancen jeder einzelnen Vorschrift, ihre Auswirkungen und den jeweiligen Compliance-Zeitrahmen informieren.

Bestimmungen wie DSGVO, HIPAA und Sarbanes-Oxley (SOX) haben bisher den Datenschutz in Unternehmen reguliert, jedoch ergeben sich durch neue Gesetze wie NIS 2, DORA und FCA CP19/32 Änderungen für Datensicherheit, Datenschutz und Cybersicherheit in Unternehmen, die trotz der zunehmenden Bedrohung für einen kontinuierlich hochwertigen Kundenservice sorgen sollen.

Gesetzliche Compliance ist nicht nur eine rechtliche Pflicht, sondern eine strategische Notwendigkeit für operative Belastbarkeit, die ein umfassendes, gut durchdachtes Cybersicherheitskonzept voraussetzt. Unternehmen profitieren von einer Neubewertung, Stabilisierung und Neubelebung ihrer Cybersicherheitsstrategien, sodass aus der Einhaltung von gesetzlichen Vorgaben ein Wettbewerbsvorteil wird.

Die Kosten mangelhafter Cybersicherheit

2023 stiegen die durchschnittlichen Gesamtkosten von Datenpannen auf 4,45 Millionen US-Dollar an. Das ist der höchste Wert seit der ersten Veröffentlichung des vom Ponemon Institute und IBM herausgegebenen Berichts „Cost of Data Breach“ vor 19 Jahren. Mit einer Stagnierung dieses Aufwärtstrends wird nicht gerechnet: Experten warnen vor einem kontinuierlichen Anstieg des Intervalls und der Professionalität von Cyberangriffen.

E-Mails, die vorrangige Kommunikationsmethode im Geschäftsumfeld, sind eine der größten Schwachstellen für Cyberkriminalität, über die heute etwa 94 % aller Malware- und Phishing-Angriffe stattfinden, da hier Bedienungsfehler und das fehlende Sicherheitsbewusstsein der Anwender ausgenutzt werden.

Von finanziellen Verlusten, Kundenabwanderung und Rufschädigung bis hin zu langwieriger Systemwiederherstellung und rechtlichen Konsequenzen hat Cyberkriminalität in jeder Branche schwerwiegende Folgen für Unternehmen jeder Größe. Laut Cybersecurity Ventures wird Cyberkriminalität 2024 Schäden in Höhe von insgesamt 9,5 Billionen US-Dollar anrichten und 2025 bereits in Höhe von 10,5 Billionen US-Dollar – vor nicht einmal zehn Jahren lag dieser Wert noch bei 3 Billionen US-Dollar. Würde man Cyberkriminalität als Nation betrachten, wäre sie die drittgrößte Volkswirtschaft nach den USA und China.

Der Anstieg bei Cybervorfällen und ihren Kosten führt zu neuen Gesetzen zur Regulierung von Cybersicherheit und Datenschutz.

Von reaktiven zu proaktiven Cyberstrategien

Regierungs- und Regulierungsbehörden weltweit sind sich der dringenden Notwendigkeit bewusst, digitale Infrastrukturen gegen immer neue Cyberbedrohungen, aber auch gegen rechtliche Folgen durch fehlerhafte oder böswillige KI-Produkte (künstliche Intelligenz) abzusichern. Dabei geht es darum, nicht nur auf Vorfälle zu reagieren, sondern stattdessen ein proaktives, resilientes Framework zu etablieren, mit dem sich Cyberbedrohungen und Störfaktoren antizipieren und abwehren lassen.

Allerdings ergeben sich durch die neue Gesetzgebung erhebliche Veränderungen für Unternehmen. Diese sind gezwungen, von einer herkömmlichen Cybersicherheitspraxis auf besser integrierte, umfassende Strategien umzustellen, die nicht nur technische Lösungen abdecken, sondern die gesamte Unternehmenskultur mit tief greifender Planung und Aufklärung von Mitarbeitern auf allen Ebenen.

Die Zunahme bei Cyberbedrohungen hat Cybersicherheit in den Führungsebenen in den Fokus gerückt. Unternehmen, die diese neue Situation erfolgreich meistern wollen, müssen informiert und agil vorgehen, um für Compliance mit den neuen Vorschriften sorgen und ihre digitalen Assets auch in Zukunft schützen zu können. Diese Lücke zwischen Bewusstsein und Bereitschaft unterstreicht die Notwendigkeit einer Revision der Unternehmensstrategie für Cybersicherheit und Cyberabwehr.

Gesetzesvorgaben und Cyberabwehr

Aufgrund all der gesetzlichen Veränderungen sind Cybersicherheit und Datenschutz für Unternehmen nicht mehr nur IT-Belange, sondern es sind entscheidende Themen für Governance und Unternehmensstrategie. Die Anpassung an diese Bestimmungen erfordert einen umfassenden Ansatz, der gesetzliche Compliance mit robusten Methoden für Cybersicherheit und Datenwiederherstellung, Mitarbeiterschulungen und Systemüberwachung kombiniert, um ein resilientes operatives Framework zu schaffen, das sich den Herausforderungen einer digitalisierten Ökonomie entgegenstellen kann.

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