ALTHAMMER & KILL

PRESSEMITTEILUNG

Cyber- und Informationssicherheit: Budgets & Ressourcen im Sozial- und Gesundheitswesen fehlen

Hannover, 23. März 2023. Die steigenden Risiken durch Datenverlust oder -missbrauch haben die meisten Unternehmen und Organisationen erkannt – bei der Umsetzung ist allerdings noch viel Luft nach oben. Das hat die aktuelle Studie „Global Future of Cyber Survey 2023" von Deloitte gezeigt, teilte das auf Beratung im Bereich Datenschutz, Informationssicherheit, Cloud- & Cyber-Security und Compliance spezialisierte Unternehmen Althammer & Kill mit. 38 Prozent der Organisationen weisen noch einen niedrigen Reifegrad ihrer Maßnahmen auf, 41 Prozent einen mittleren und 21 Prozent einen hohen. „Das sehen wir auch in unserer täglichen Praxis", sagt Thomas Althammer, Geschäftsführer der Althammer & Kill GmbH & Co. KG. „Gerade Organisationen aus dem Sozial- und Gesundheitsbereich besitzen zwar enorm viele sensible Daten, haben aber nicht die Budgets und Ressourcen, eine ganzheitliche Cyber- und Informationssicherheitsstrategie zu implementieren und nachzuhalten. Das ist eine Krux." Dabei spielt der Umgang mit digitalen Anwendungen eine wichtige Rolle für Unternehmen auf dem Weg in die digitale Transformation. Besonders im Hinblick auf die Themen Cloud-Computing, Datenanalytik, operative Betriebstechnik und Steuerungssysteme sowie künstliche Intelligenz.

KRITIS-Einrichtungen müssen sich auf EU-NIS-2 und B3S einstellen

Die wichtigen kritischen Infrastrukturen hat die EU inzwischen mit der EU-NIS-2-Richtlinie in den Blick genommen und fordert höhere Mindeststandards bei Cyber-Sicherheit und Risiko-Management – sie muss nun bis Oktober 2024 in nationales Recht umgesetzt werden und betrifft schon mittlere Unternehmen mit 50-250 Beschäftigten und einem Umsatz von 10 bis 50 Millionen Euro. Reguliert werden außerdem Betreiber digitaler Infrastruktur, Einrichtungen der öffentlichen Verwaltung, Zentral- und Regionalregierungen. Auch für die branchenspezifischen Sicherheitsstandards für die Gesundheitsversorgung im Krankenhaus (B3S) liegt inzwischen eine konkretisierende Fassung vor und diese rückt besonders das Thema Cyber-Angriffserkennung in den Fokus. Hinsichtlich KRITIS-Prüfungen sollten Krankenhäuser und Kliniken auf die

neuen Anforderungen vorbereitet sein. Aber auch kleinere Unternehmen und Organisationen kommen um das Thema IT-Sicherheit nicht mehr herum.

Ganzheitliche Informationssicherheitsstrategien für Organisationen und Unternehmen

Der Deloitte-Studie zufolge melden 91 Prozent der globalen Organisationen im Befragungszeitraum mindestens einen Cybervorfall oder eine Sicherheitsverletzung. Die Unterbrechung des Geschäftsbetriebs durch Cybervorfälle ist dabei das ungünstigste Szenario. „Die fehlenden personellen Ressourcen im IT-Bereich hemmen oft den Aufbau sinniger Informationssicherheitsstrategien. Es gibt inzwischen aber auch die Möglichkeit, sich externe Experten als Informationssicherheitsbeauftragte heranzuziehen“, so Althammer. Um das Thema stärker in den Organisationen zu verankern, beschreibt er fünf Handlungsfelder:

1. Strategische und konzeptionelle Beratung wahrnehmen. Diese sollte Analysen des Status Quo und des Gefahrenpotenzials enthalten, gesetzliche Vorgaben berücksichtigen, sowie interne und externe Audits.
2. Mitarbeitende schulen und sensibilisieren
3. Ein Informationssicherheits-Managementsystem aufbauen
4. Ggf. nach ISO 27001 auditieren und zertifizieren
5. Einen Informationssicherheitsbeauftragten etablieren

Cyber- und Informationssicherheit ist keine Modeerscheinung, sondern wird Unternehmen aller Branchen auf dem Weg durch die digitale Transformation weiter beschäftigen. Die Ausgaben für Cybersicherheit lagen im letzten Jahr bei geschätzten 7,8 Milliarden Euro in Deutschland. Im laufenden Jahr soll dieser Posten auf 8,5 Milliarden und bis 2025 auf 10,3 Milliarden Euro anwachsen (Quelle: Marktforschungsinstituts Canalys / Statista). „Budgetschwache Branchen wie das Sozial- und Gesundheitswesen, das unter Personalmangel und Investitionsabbau leidet, dürfen wir dabei nicht vergessen“, mahnt Althammer.

Über Althammer & Kill:

Die Althammer & Kill GmbH & Co. KG hat sich als Beratungsunternehmen auf die Themen Datenschutz, Informationssicherheit, Cloud- & Cyber-Security und Compliance spezialisiert. Es

bietet pragmatische Lösungskonzepte und berät Unternehmen und Organisationen bundesweit. Zum 40-köpfigen Team gehören Juristen, IT-Berater, zertifizierte Datenschutzbeauftragte und IT-Sicherheitsspezialisten. Das Unternehmen ist von den Standorten Hannover, Düsseldorf und Mannheim aus bundesweit für mehr als 500 Kunden unterschiedlichste Branchen tätig, z. B. in den Funktionen als externe Datenschutzbeauftragte, Informationssicherheit- und IT-Experten. Zu den weiteren Angeboten zählen die Bereiche Security Awareness und die Durchführung von (IT-)Sicherheitsanalysen/Penetrationstests.

Kontakt:

Susanne Maack
Pressereferentin
Mail: sm@althammer-kill.de
Mobil: 0170 933 17 52

Althammer & Kill GmbH & Co. KG
Roscherstraße 7
30161 Hannover