ALTHAMMER & KILL

PRESSEMITTEILUNG

Cyber-Kriminalität bedroht Schutz der Daten
Was tun bei Hackerangriffen, Datenlecks & Co?

Hannover, 8. Oktober 2020. Im Fall von Datenklau und Datenlecks ist schnelles Handeln gefragt, sonst drohen empfindliche Bußgelder und Haftungsrisiken. Wie das auf Datenschutz, Informationssicherheit und IT- Compliance spezialisierte Unternehmen Althammer & Kill mitteilte, muss die Meldung zu einer Cyberattacke innerhalb von 72 Stunden bei der zuständigen Aufsichtsbehörde angezeigt werden. Zusätzlich besteht unter Umständen eine Informationspflicht gegenüber betroffenen Personen. „Wer Melde- und Eskalationsmechanismen verankert, klare Rollen und Verantwortlichkeiten zugeordnet sowie eine klare Kommunikations- und Krisenmanagementstrategie etabliert hat, der ist als Unternehmen oder Organisation gut gerüstet, um das Ausmaß des IT-Angriffes schnell abzuschätzen und einzudämmen“, weiß Thomas Althammer, Geschäftsführer von Althammer & Kill. Jedoch zeige die tägliche Praxis, dass gerade kleine und mittelständische Unternehmen sowie soziale Einrichtungen oft völlig unvorbereitet von Cyberattacken getroffen werden, so der Experte. Die Cyber-Kriminalität ist laut Bundeskriminalamt im vergangenen Jahr um 15 Prozent auf mehr als 100.500 Fälle gestiegen. Der Branchenverband Bitkom schätzt, dass solche Angriffe die deutsche Wirtschaft im vorigen Jahr insgesamt mehr als hundert Milliarden Euro gekostet haben.

Prävention: Infrastrukturen schaffen

Für den Fall eines Hackerangriffs, eines Datenlecks oder bei Erpressungsversuchen über Ransomware, sollte es in Unternehmen und Organisationen klare Strukturen und Maßnahmenpläne geben. Datenschutzbeauftragte müssen sich im Ernstfall schnell ein umfassendes und klares Bild über die Lage machen können, um die regulatorischen Vorschriften erfüllen zu können. Auch risikominimierende Maßnahmen zum Schutz der Betroffenen und zur Eindämmung des Schadens müssen unverzüglich umgesetzt werden. „Neben einem ganzheitlichen, organisationsweiten Krisenmanagementsystems spielt die Kommunikation zwischen den verschiedenen Fachbereichen eine entscheidende Rolle“, weiß Kristof Riecke, Bereichsleiter Compliance bei Althammer & Kill. „Wie kommuniziert die Organisation im Falle einer Cyber-Krise? Welche Maßnahmen wurden durch das Unternehmen adressiert und wie

unterstützt es Betroffenen? Antworten auf diese Fragen müssen schon im Vorfeld strukturiert und kommuniziert sein, nicht erst, wenn der Ernstfall eintritt." Wirksame Risikominimierungs- und Präventionsinstrumente sind immer organisationsweit zu betrachten und können nur umgesetzt werden, wenn alle relevanten Fachbereiche kooperieren und mitwirken. Das Ziel ist es, damit eine ganzheitlicher, übergreifender „Resilienz" gegen Attacken aus dem Cyberraum zu schaffen.

Die Maßnahmen, die im Falle einer Cyberattacke zu ergreifen sind, sind in der Datenschutzgrundverordnung (DSGVO), dem Bundesdatenschutzgesetz, dem Kirchengesetz über den Datenschutz der Evangelischen Kirchen oder dem Gesetz über den Kirchlichen Datenschutz geregelt.

Über Althammer & Kill:

Die Althammer & Kill GmbH & Co. KG hat sich als Beratungsunternehmen auf die Themen Datenschutz, Informationssicherheit und IT-Compliance spezialisiert. Zum 30-köpfigen Team gehören Juristen, IT-Berater, zertifizierte Datenschutzbeauftragte und IT-Sicherheitsspezialisten. Das Unternehmen ist von den Standorten Hannover, Düsseldorf und Mannheim aus bundesweit tätig, z. B. in der Funktion als externe Datenschutzbeauftragte oder Informationssicherheitsbeauftragte. Zu den weiteren Angeboten zählen die Bereiche Zertifizierung 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