Data-Breach-Response

Banken wappnen sich gegen Hacker-Angriffe

Finanzdienstleister stehen immer häufiger im Fokus von Cyber-Attacken. Das Ausmaß möglicher Schäden nimmt dabei erheblich zu. Viele Banken haben die Ernsthaftigkeit der Bedrohung erkannt und überprüfen deshalb die bestehenden Strategien für das Risikomanagement und ihre Data-Breach-Response-Mechanismen.

Das ist auch deshalb wichtig, weil Banken als Konsequenz von Datenschutzverletzungen aufgrund einer Cyber-Attacke in umfangreiche Gerichtsverfahren verwickelt werden können – abhängig von Faktoren wie der Dimension des Angriffs, von betroffenen Unternehmen und Kunden, sowie von der Art und Tragweite des dadurch entstandenen Schadens. Kommt es zu einem Prozess, kann eine eDisclosure die effiziente Erfassung, Bearbeitung und Überprüfung relevanter Daten für die Beweisführung ermöglichen. Moderne Technologien können automatisierte Suchen innerhalb von Datensätzen durchführen und ermöglichen so die Bestimmung der tatsächlichen Relevanz der vorliegenden Informationen. Die Nutzung solcher Technologien beschleunigt nicht nur die eDisclosure, sondern spart darüber hinaus Kosten. Im Fall einer Datenschutzverletzung durch Cyber-Kriminalität müssen betroffene Organisationen nachweisen können, dass sie angemessene Schutzmechanismen gegen den Datenraub implementiert hatten. Sie müssen zeigen, dass sie zum Zeitpunkt des Vorfalls über klare Unternehmensrichtlinien zur Prävention und damit in Verbindung stehenden Prüfungsverfahren verfügten. Auch muss nachgewiesen werden, dass es zuvor keine Anzeichen für eine bevorstehende Attacke gab und nach dem Vorfall in angemessener Weise verfahren wurde. Dokumentenprüfung ist ein wesentlicher Bestandteil der Beweisführung und schließt die eingehende Bewertung der erfolgten Kommunikation mit ein. Das kann insbesondere dann eine große Herausforderung darstellen, wenn große Mengen an Dokumenten auf ihre Relevanz hin beurteilt und dann von Experten innerhalb kurzer Zeit gesichtet werden müssen. Banken müssen die Kontrolle über den gesamten Prozess in Zusammenhang mit Datenverlusten behalten. Experten für Informationsmanagement können bei einem proaktiven Ansatz für Prävention ebenso unterstützend tätig werden wie im Rahmen der ganzheitlichen Aufdeckungsarbeit.

Autor: Brookes Taney, Epiq Systems.