expertenReport

Hiscox: Ransomware und die Illusion der Wiederherstellbarkeit

Ute Pappelbaum

> „Selbst nach einer Zahlung bleiben Daten sehr häufig verloren, Systeme müssen neu aufgebaut werden und das Risiko weiterer Angriffe steigt."

Der operative Gegenentwurf liege daher in

> „starker Prävention, schneller Incident Response und professioneller technischer Hilfe im Ernstfall".

Ein Markt ohne Vertragssicherheit

Ökonomisch offenbart sich hier ein klassisches Informations- und Vertrauensproblem. Die Zahlungsentscheidung erfolgt unter maximaler Unsicherheit – Unternehmen kennen weder die tatsächliche Wiederherstellungsfähigkeit der Angreifer noch deren Anreizstruktur. Der Ransomware-Markt funktioniert asymmetrisch: Anbieter (Angreifer) verfügen über vollständige Kontrolle über den „Produktzugang" (Entschlüsselung), während Nachfrager (Unternehmen) im Ernstfall unter Zeitdruck und mit eingeschränkter Entscheidungsbasis agieren. Die Zahlung eines Lösegelds ist damit kein marktförmiger Austausch, sondern eine einseitige Risikoübernahme ohne Durchsetzungsmechanismus.

Individuelle Rationalität versus kollektives Risiko

Während Unternehmen kurzfristig zur Sicherung der Betriebsfähigkeit rational handeln, erzeugt jede Zahlung langfristig einen negativen externen Effekt. Sie stabilisiert das Geschäftsmodell der Angreifer, erhöht deren erwartete Rendite und senkt die Eintrittsbarrieren für weitere Attacken. Der individuelle Schadensminimierungsversuch kollidiert somit mit der kollektiven Risikodynamik.

Prävention ersetzt Reaktion

Die Argumentationslinie von Hiscox verweist auf einen Strategiewechsel: weg von reaktiven Zahlungen, hin zu präventiver Risikosteuerung und organisierter Krisenreaktion. Der eigentliche Wert einer Cyberversicherung liegt dabei weniger in der Kostenerstattung als im Zugang zu Forensik, Wiederherstellung und Entscheidungskoordination unter Zeitdruck. Versicherung wird damit Teil der operativen Sicherheitsarchitektur.

Versicherung als Steuerungsakteur

Für Versicherer entsteht daraus ein erweitertes Rollenverständnis. Cyberpolicen entwickeln sich vom passiven Risikoträger zum aktiven Steuerungsinstrument, das Mindeststandards erzwingt und Reaktionsfähigkeit organisiert. Gleichzeitig bleibt das moralische Risiko bestehen: Jede implizite Absicherung von Lösegeldzahlungen würde das Angreifermodell stabilisieren. Am Ende verschiebt sich die ökonomische Logik grundlegend: Ransomware ist kein Ausnahmeereignis mehr, sondern ein strukturelles Betriebsrisiko. Lösegeldzahlungen erscheinen kurzfristig als Ausweg – sind aber in Wirklichkeit ein Symptom

fehlender Resilienz. Wer zahlt, löst nicht das Problem, sondern verlängert seine systemische Ursache.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4949464/hiscox-ransomware-kmu-loesegeld/