expertenReport

Quelle: Redaktion experten.de / KI-generiert

Ransomware: Jedes fünfte betroffene Unternehmen hat schon Lösegeld gezahlt

Michael Fiedler

45 Prozent der deutschen Unternehmen waren innerhalb eines Jahres Ziel einer Ransomware-Attacke. Zwar bleibt die Mehrheit der Opfer hart, doch jedes fünfte betroffene Unternehmen hat bereits Lösegeld gezahlt – häufig fünf- oder sechsstellige Beträge. Eine aktuelle Bitkom-Erhebung zeigt zugleich eine überraschende Entwicklung bei der Zahl der Angriffe.

Ransomware-Angriffe gehen zurück

Bemerkenswert ist der Vergleich mit dem Vorjahr. Damals hatten noch 58 Prozent der Unternehmen von Ransomware-Angriffen berichtet. Bei 34 Prozent war ein Schaden entstanden, bei 24 Prozent nicht. Die Angriffsquote sank damit innerhalb eines Jahres um 13 Prozentpunkte. Auch der Anteil der Unternehmen, die tatsächlich einen Schaden erlitten, ging zurück. Entwarnung bedeutet das allerdings nicht. Fast jedes zweite Unternehmen bleibt betroffen – und sobald Angreifer erfolgreich sind, können die finanziellen Folgen erheblich werden.

Jedes fünfte betroffene Unternehmen hat bereits gezahlt

Die Mehrheit der Ransomware-Opfer verweigert die Zahlung. 66 Prozent der betroffenen Unternehmen geben an, den Erpressern kein Lösegeld überwiesen zu haben. 20 Prozent haben dagegen bereits gezahlt. Weitere 14 Prozent wollen oder können dazu keine Angabe machen. Bitkom-Präsident Dr. Ralf Wintergerst warnt ausdrücklich davor, auf die Forderungen der Täter einzugehen: „Jede Zahlung finanziert den nächsten Angriff.“ Hinzu kommt ein grundlegendes Problem: Eine Zahlung schafft keine Sicherheit. Unternehmen haben weder eine Garantie dafür, dass verschlüsselte Daten tatsächlich wieder freigegeben werden, noch dafür, dass gestohlene Informationen anschließend nicht doch veröffentlicht oder verkauft werden. Ransomware-Angriffe setzen deshalb zunehmend auf einen doppelten Hebel. Neben der Verschlüsselung von Systemen kann bereits der Abfluss sensibler Daten erheblichen Druck erzeugen. Selbst ein Unternehmen, das seine Systeme aus Backups wiederherstellen kann, ist damit nicht automatisch aus der Erpressungssituation befreit.

Lösegeld erreicht häufig sechsstellige Summen

Wer zahlt, muss mit erheblichen Forderungen rechnen. Von den Unternehmen, die bereits Lösegeld überwiesen haben, zahlten 37 Prozent zwischen 10.000 und 100.000 Euro. Bei fast jedem vierten zahlenden Unternehmen – 24 Prozent – lag die Summe zwischen 100.000 und 500.000 Euro. Weitere sechs Prozent überwiesen zwischen 500.000 Euro und einer Million Euro. Vier Prozent zahlten sogar mindestens eine Million Euro. 26 Prozent der zahlenden Unternehmen machten keine Angaben zur Höhe, drei Prozent konnten die Summe nicht beziffern. Die Zahlen zeigen damit auch eine Besonderheit des Ransomware-Risikos: Neben Kosten für Betriebsunterbrechung, Wiederherstellung, IT-Forensik und Krisenmanagement kann die Lösegeldforderung selbst eine erhebliche zusätzliche finanzielle Belastung darstellen.

Backups allein lösen das Problem nicht

Bitkom setzt bei der Prävention zunächst auf eine genaue Kenntnis der eigenen IT-Landschaft. Unternehmen müssen wissen, welche Systeme, Datenbestände, Zugänge und Schnittstellen vorhanden sind und voneinander abhängen. Ohne eine solche Übersicht lässt sich nach einem Angriff kaum zuverlässig feststellen, welche Bereiche betroffen sind. Eine zweite Säule sind Backups. Entscheidend ist dabei nicht allein, dass Sicherungskopien existieren. Sie sollten vom produktiven Netz getrennt aufbewahrt werden, damit Angreifer sie nicht ebenfalls verschlüsseln oder entwenden können. Zudem muss regelmäßig getestet werden, ob sich Systeme und Daten aus den Sicherungen tatsächlich wiederherstellen lassen. Damit wird allerdings nur ein Teil des Ransomware-Risikos beherrschbar. Sind Daten bereits abgeflossen, verhindert ein funktionierendes Backup nicht die Drohung mit ihrer Veröffentlichung.

Mehr-Faktor-Authentifizierung und Rechtemanagement schließen Einfallstore

Als weitere Schutzmaßnahme empfiehlt Bitkom eine konsequente Mehr-Faktor-Authentifizierung. Hinzu kommen ein restriktives Rechtemanagement und die Löschung nicht mehr benötigter Benutzerkonten. Von Bedeutung ist außerdem die frühzeitige Angriffserkennung. Werden Protokolldaten nicht kontinuierlich ausgewertet und verdächtige Vorgänge zu spät erkannt, können sich Angreifer länger unbemerkt in der IT-Infrastruktur bewegen. Unternehmen sollten deshalb nicht nur versuchen, Angriffe zu verhindern, sondern zugleich davon ausgehen, dass Schutzmechanismen überwunden werden können.

Der Ransomware-Ernstfall muss geübt werden

Der letzte Baustein ist organisatorischer Natur. Ein Notfallplan sollte Verantwortlichkeiten, Meldewege und Krisenkommunikation festlegen – und auch dann verfügbar sein, wenn die normale IT ausgefallen ist. Bitkom empfiehlt, diese Abläufe tatsächlich zu erproben. Im Ernstfall entscheidet nicht allein die technische Ausstattung darüber, wie lange ein Unternehmen stillsteht. Ebenso wichtig ist, ob Verantwortliche wissen, wer Entscheidungen trifft, welche Systeme zuerst wiederhergestellt werden müssen und wie intern und extern kommuniziert wird. Wintergerst fasst die Alternative zur Lösegeldzahlung deshalb mit Vorbereitung zusammen: Wer funktionierende Backups und erprobte Notfallpläne besitzt, verringert das Risiko, dass eine Verschlüsselung den Betrieb über längere Zeit lahmlegt.

Cyberversicherung trifft auf ein schwieriges Erpressungsrisiko

Für Unternehmen und ihre Versicherer ist Ransomware besonders anspruchsvoll, weil ein einziger Angriff verschiedene Schadenpositionen gleichzeitig auslösen kann. Neben Kosten für IT-Forensik und Wiederherstellung können Betriebsunterbrechungen, Haftungsfragen nach einem Datenabfluss und Aufwendungen für Krisenmanagement entstehen. Die Bitkom-Zahlen machen zugleich deutlich, warum Prävention für die Versicherbarkeit von Cyberrisiken entscheidend bleibt. Ein Unternehmen, das Systeme, Zugriffsrechte und Datenbestände nicht kennt, keine belastbaren Backups besitzt und keinen Notfallplan erprobt hat, erhöht nicht nur sein technisches Risiko. Im Schadenfall wird auch die Wiederherstellung erheblich schwieriger. Dass die Zahl der Ransomware-Angriffe gegenüber dem Vorjahr zurückgegangen ist, ist deshalb eine gute Nachricht. Bei einer Betroffenheit von 45 Prozent bleibt das Risiko jedoch weit davon entfernt, ein Randphänomen zu sein. Und die Lösegeldzahlungen zeigen, wie erfolgreich das Geschäftsmodell der Täter weiterhin sein kann: Schon wenn eine Minderheit der Opfer zahlt, können einzelne erfolgreiche Angriffe sechs- oder sogar siebenstellige Einnahmen bringen.

Methodik Grundlage der Angaben ist eine repräsentative Befragung von Bitkom Research im Auftrag des Digitalverbands Bitkom. Telefonisch befragt wurden 1.003 Unternehmen in Deutschland mit mindestens zehn Beschäftigten und einem Jahresumsatz von mindestens einer Million Euro. Die Erhebung fand von Kalenderwoche 16 bis

Kalenderwoche 23 des Jahres 2026 statt. Die Angaben zu Lösegeldzahlungen beziehen sich auf 452 von Ransomware-Angriffen betroffene Unternehmen. Zur Höhe der Zahlung wurden die 90 Unternehmen ausgewertet, die angegeben hatten, Lösegeld gezahlt zu haben.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4951728/Ransomware-Jedes-fuenfte-betroffene-Unternehmen-hat-schon-Loesegeld-gezahlt/