Bitkom e.V. | Presseinformation

Jedes fünfte Ransomware-Opfer hat schon einmal Lösegeld gezahlt

- **45 Prozent der Unternehmen waren in den vergangenen zwölf Monaten von Ransomware-Angriffen betroffen**
- **Wer zahlt, überweist häufig sechsstellige Summen**
- **Wintergerst: „Jede Zahlung finanziert den nächsten Angriff“**

Berlin, 04. September 2026 – Zahlen – oder personenbezogene Daten landen im Darknet: Vor dieser Entscheidung steht derzeit das Land Berlin. Zwei Millionen Euro fordern Cyberkriminelle, damit sie die bei einem Hackerangriff gestohlenen Daten nicht veröffentlichen. Was in Berlin für alle sichtbar verhandelt wird, erleben Unternehmen in Deutschland regelmäßig hinter verschlossenen Türen: Fast jedes zweite Unternehmen (45 Prozent) war in den vergangenen zwölf Monaten von einem Ransomware-Angriff betroffen, oft werden dabei auch die IT-Systeme der Opfer verschlüsselt und blockiert, wodurch der gesamte Betrieb stillstehen kann. Bei 25 Prozent ist dabei ein Schaden entstanden, bei 20 Prozent blieb der Angriff ohne Folgen. Gegenüber dem Vorjahr ist das ein Rückgang, damals waren 58 Prozent aller Unternehmen von Ransomware-Attacken betroffen (34 Prozent mit Schaden, 24 Prozent ohne).

Die große Mehrheit der betroffenen Unternehmen zahlt nicht: 66 Prozent haben den Erpressern nichts überwiesen. Jedes Fünfte (20 Prozent) hat aber schon Lösegeld gezahlt, 14 Prozent wollen oder können dazu keine Angabe machen. Das sind Ergebnisse einer repräsentativen Befragung von 1.003 Unternehmen ab 10 Beschäftigten in Deutschland im Auftrag des Digitalverbands Bitkom. „Der aktuelle Fall in Berlin zeigt, vor welch schwieriger Entscheidung Opfer von Ransomware-Angriffen stehen. Richtig wäre, nicht zu zahlen. Jede Zahlung finanziert den nächsten Angriff. Und selbst wer zahlt, erhält keine Garantie: Weder für die Entschlüsselung seiner Daten noch dafür, dass die Täter die Daten nicht doch veröffentlichen oder weiterverkaufen“, sagt Bitkom-Präsident Dr. Ralf Wintergerst. „Besser ist eine gute Vorbereitung auf den Ernstfall. Wer Backups besitzt und Notfallpläne aufgestellt hat, sorgt dafür, dass eine Verschlüsselung den Betrieb nicht über längere Zeit lahmlegt.“

Wer zahlt, zahlt meist sechsstellige Beträge

Wenn Unternehmen auf die Erpresser-Forderungen eingehen, geht es um erhebliche Summen. 37 Prozent der zahlenden Unternehmen überwiesen zwischen 10.000 und 100.000 Euro, 24 Prozent zwischen 100.000 und 500.000 Euro. 6 Prozent zahlten zwischen 500.000 Euro und einer Million und 4 Prozent sogar eine Million Euro oder mehr. 26 Prozent machen zur Höhe keine Angabe, 3 Prozent wissen es nicht.

Was Unternehmen tun können

Der Bitkom empfiehlt Unternehmen fünf Maßnahmen, um Ransomware-Angriffe abzuwehren und im Ernstfall handlungsfähig zu bleiben:

1. **Die eigene IT-Landschaft kennen**. Wer nicht weiß, welche Systeme, Datenbestände und Schnittstellen im Einsatz sind, hat keine Informationen zur eigenen Verwundbarkeit und kann nach einem Angriff die Betroffenheit nicht abschätzen. Eine aktuelle Übersicht über Systeme, Zugänge und Abhängigkeiten ist die Grundlage jeder Reaktion.
2. **Backups machen** – und offline halten. Viele Unternehmen haben gar keine oder nur unvollständige Sicherungen ihrer Daten, das spielt Erpressern, die Daten verschlüsseln und den Zugang kontrollieren, in die Hände. Wer Backups besitzt, sollte sie vom Netz getrennt aufbewahren, damit sie sich nicht mitverschlüsseln oder stehlen lassen. Und das Zurückspielen gehört regelmäßig geprobt, nicht erst im Schadensfall.
3. **Zugänge absichern**. Die konsequente Nutzung von Mehr-Faktor-Authentifizierung, ein striktes Rechtemanagement und die regelmäßige Löschung nicht mehr benötigter Konten schließen die

Einfallstore, die Angreifer am häufigsten nutzen.

4. **Angriffe früh erkennen**. Die unzureichende Erkennung von Sicherheitsvorfällen ist die häufigste Ursache dafür, dass aus einem Angriff ein Schaden wird. Protokolldaten müssen durchgängig ausgewertet und überwacht werden, um schnell reagieren zu können.
5. **Den Notfall üben.** Ein Notfallplan ist ein Muss, und zwar so, dass auf ihn beim Ausfall der IT auch zugegriffen werden kann. Darin müssen Verantwortlichkeiten, Meldewege und vorbereitete Krisenkommunikation enthalten sein. Geübte Abläufe entscheiden über Stunden oder Wochen Stillstand.

Kontakt

Andreas Streim
Pressesprecher
Telefon: +49 30 27576-112
E-Mail: a.streim@bitkom.org
Download Pressefoto

Felix Kuhlenkamp
Leiter Sicherheit
Download Pressefoto
Nachricht senden

Hinweis zur Methodik

Grundlage der Angaben ist eine Umfrage, die Bitkom Research im Auftrag des Digitalverbands Bitkom durchgeführt hat. Dabei wurden 1.003 Unternehmen ab 10 Beschäftigten und einem Jahresumsatz von mindestens 1 Mio. Euro in Deutschland telefonisch befragt. Die Befragung fand im Zeitraum von KW 16 bis KW 23 2026 statt. Die Umfrage ist repräsentativ. Die Angaben zu Lösegeldzahlungen beziehen sich auf die von Ransomware-Angriffen betroffenen Unternehmen (n=452), die Angaben zur Höhe der Zahlungen auf die Unternehmen, die Lösegeld gezahlt haben (n=90). Die Fragestellungen lauteten: „Welche der folgenden Arten von Cyberangriffen wurden innerhalb der letzten 12 Monate auf Ihr Unternehmen verübt und ist dabei ein Schaden entstanden?“, „Haben Sie bei Ransomware-Angriffen Lösegeld bezahlt?“ und „Wie hoch war die Summe, die Sie in den vergangenen 12 Monaten gezahlt haben?“

Direktlink: ***https://www.bitkom.org/Presse/Presseinformation/Jedes-fuenfte-Ransomware-Opfer-hat-Loesegeld-gezahlt***