

Berlin hat nicht gezahlt

05.10.2026, 07:34 | IT, New Media & Software

Pressemitteilung von: *FAST LTA GmbH*



Rotes Rathaus - Berlin

Zwei Millionen Euro für das Schweigen

Zwischen dem 7. und 12. August 2026 hatten Angreifer unbemerkt Zugriff auf Teile des Berliner Landesnetzes. Am 14. August wurden die betroffenen Senatsverwaltungen vom Landesnetz isoliert. Rhysida verlangte 30 Bitcoin, rund zwei Millionen Euro, und bot die Daten ab Ende August im Darknet zur Versteigerung an. Der Senat lehnte ab. Nach eigenen Angaben haben die Täter knapp 5,8 Terabyte veröffentlicht.

Am selben 4. September veröffentlichte der Bitkom neue Zahlen. 45 Prozent der befragten Unternehmen waren in den vergangenen zwölf Monaten von Ransomware betroffen, im Vorjahr 58 Prozent. Von den Betroffenen haben 66 Prozent nichts gezahlt, 20 Prozent haben schon einmal Lösegeld überwiesen, 4 Prozent der Zahlenden eine Million Euro oder mehr. Bitkom-Präsident Ralf Wintergerst: „Jede Zahlung finanziert den nächsten Angriff.“

Verschlüsselung und Datenabfluss

Verschlüsselte Systeme legen den Betrieb still, abgeflossene Daten drohen öffentlich zu werden. Der Sophos-Report „The State of Ransomware 2026“ (2.158 befragte IT- und Sicherheitsverantwortliche, Erhebung Anfang 2026) beziffert beide Seiten. In 56 Prozent der Angriffe wurden Daten verschlüsselt, der erste Anstieg nach zwei Jahren Rückgang. Etwa jeder sechste Fall verband Verschlüsselung und Datenabfluss. Zwei Drittel der Opfer mit verschlüsselten Daten haben aus dem Backup wiederhergestellt, ein Jahr zuvor war es gut die Hälfte.

Gegen den Stillstand hilft ein funktionierendes Backup, gegen die Veröffentlichung abgeflossener Daten gibt es keine technische Antwort. Ein Unternehmen, das wiederherstellen kann, verhandelt im Ernstfall nur noch über den Datenabfluss. Ohne Restore kommt der Druck des stehenden Betriebs hinzu, und mit jedem Tag Stillstand wird das Lösegeld leichter zu rechtfertigen.

§ 30 und § 32 BSIG

Seit dem 6. Dezember 2025 gilt das NIS2-Umsetzungsgesetz, laut BSI für rund 29.500 Einrichtungen. § 30 Abs. 2 S. 2

Nr. 3 BSIG verlangt Maßnahmen zur „Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement“. Welche Technik dafür eingesetzt wird, lässt das Gesetz offen. Nach § 30 Abs. 1 müssen die Maßnahmen aber wirksam sein, und ein Backup, das sich im Notfall nicht zurückspielen lässt, ist das nicht.

Die Uhr läuft ab Kenntnis des Vorfalls. § 32 BSIG fordert eine frühe Erstmeldung binnen 24 Stunden, eine Meldung mit Erstbewertung binnen 72 Stunden und spätestens einen Monat danach eine Abschlussmeldung. Sind personenbezogene Daten abgeflossen, kommt Art. 33 DSGVO hinzu: Meldung an die Aufsichtsbehörde möglichst binnen 72 Stunden. Wer in diesen Tagen noch klären muss, ob das Backup überhaupt intakt ist, verliert die Zeit, die er für die Meldungen braucht.

Ein Backup im Netz ist ein Ziel

Der Bitkom empfiehlt in derselben Mitteilung, Backups „vom Netz getrennt aufbewahren, damit sie sich nicht mitverschlüsseln oder stehlen lassen“, und das Zurückspielen regelmäßig zu proben. Ein Backup enthält eine vollständige Kopie der Unternehmensdaten und kommt deshalb selbst als Quelle für einen Datenabfluss in Frage. Angreifer suchen es gezielt: Im Veeam Ransomware Trends Report 2025 gaben 89 Prozent der Betroffenen an, dass ihre Backup-Repositories angegriffen wurden.

Unveränderbare Speicherbereiche schützen gegen Löschen und Überschreiben, über das Netz lesbar bleibt das Backup trotzdem. Ein Offline-Backup, physisch oder galvanisch vom Netz getrennt (Air Gap), kann ein Angreifer weder verschlüsseln noch abziehen, auch wenn er Administratorrechte im Netz hat.

Air Gap im Silent Brick System

Silent Bricks sind ein Speichersystem für Backup und Restore, entwickelt in München und gefertigt in Deutschland. Es arbeitet mit den gängigen Backup-Lösungen wie Veeam, Commvault oder Veritas. Für den physischen Air Gap gibt es zwei Varianten.

Der Silent Brick Pro lässt sich aus dem Controller entnehmen und zum Beispiel im Tresor lagern. Der Silent Brick Max Air bleibt im Rack und trennt die Datenträger galvanisch, aufheben lässt sich die Trennung per Taste am Gerät. Mit der nächsten Softwareversion kommt eine zeitgesteuerte Reaktivierung über eine manipulationssichere Echtzeituhr hinzu. Zwei Max Air im Wechsel ergeben dann ein Offline-Backup, das jeweils 30 Tage vom Netz getrennt ist, ohne dass jemand Medien tauschen muss. Der Restore läuft lokal, ohne Internetverbindung und ohne Egress-Gebühren.

Vor der Lösegeldforderung

Ob ein Unternehmen zahlt, entscheidet sich selten am Tag der Forderung. Es hängt davon ab, ob der Restore erprobt ist und ob ein Offline-Backup existiert, das der Angreifer nicht erreicht hat. Beim Datenabfluss verschafft auch eine Zahlung keine Sicherheit. Wintergerst weist in der Bitkom-Mitteilung darauf hin, dass es weder eine Garantie für die Entschlüsselung gibt noch dafür, dass die Täter die Daten nicht doch veröffentlichen oder weiterverkaufen. Gegen den Abfluss helfen Maßnahmen, die vorher greifen, etwa Zugangsschutz und frühe Erkennung.

Ihr Backup schützt Sie vor Ransomware. Oder doch nicht?

Im Gespräch klären wir mit Ihnen, ob Sie ein Offline-Backup haben und wie lange ein vollständiger Restore bei Ihnen tatsächlich dauert. Gespräch vereinbaren oder das Silent Brick System auf der it-sa in Nürnberg live sehen: 27. bis 29. Oktober 2026, Halle 8, Stand 8-308.

FAST LTA

Tölzer Str. 1

81379 München
Deutschland

Marek Birkenhauer (Online Marketing Manager)

Marek.Birkenhauer@fast-lta.de

Portrait

FAST LTA ist der Spezialist für Datensicherheit und Data-Privacy in Enterprise Storage sowie für Systeme, die lokalen KI-Betrieb ermöglichen. Die Kombination aus langlebiger und wartungsarmer Hardware, integrierter Software und Wartungsverträgen mit bis zu zehn Jahren Laufzeit sorgt für langfristig kostengünstigen Betrieb – von der Archiv- und Backup-Speicherung bis zum lokalen KI-Einsatz. Die Lösungen für sichere Datenspeicherung Made in Germany und digitale Souveränität des Münchner Anbieters haben sich in über 3.500 Installationen bewährt, unter anderem in Healthcare, öffentlicher Verwaltung, Dienstleistung sowie Industrie & Handel. Weitere Informationen unter: www.fast-lta.de

News-ID: 1325531 • Views: 194 (Stand: 20.10.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/1325531/Berlin-hat-nicht-gezahlt.html>