Bild: shutterstock/Ar_TH

Peter Marwan
speicherguide.de

Immutability für den Mittelstand

FÜRS UNERWARTETE GEWAPPNET SEIN

Keine Branche ist vor Ransomware-Angriffen gefeit. Den Mittelstand macht die Kombination aus Fachkräftemangel, knappen Budgets und rasch komplexer werdender IT-Infrastruktur besonders anfällig. Benötigt werden nicht nur unkomplizierte und den Anforderungen gewachsene Lösungen, sondern auch moderne Bezahlmöglichkeiten, wie Pay-per-Use.

Dem aktuellen Bundeslagebild Cybercrime zufolge steigt das Bedrohungspotenzial durch Ransomware weiterhin stark an. »Ransomware bleibt der Modus Operandi mit dem höchsten Schadenspotenzial im Bereich Cybercrime«, teilte das *Bundeskriminalamt* (BKA) bei der Vorstellung seines Berichts mit. Betroffen sind Unternehmen jeder Branche sowie Behörden, Kommunen und Bildungseinrichtungen.

Die Schäden liegen in Milliardenhöhe. Konkret spricht das BKA für 2021 (für 2022 liegen die Daten noch nicht vor) von 24,3 Milliarden Euro alleine durch Erpressung mit gestohlenen oder verschlüsselten Daten in Deutschland. Besserung ist nicht in Sicht: Die Allianz-Tochter *Allianz Global Coporate & Specialty* (AGCS) nennt Zahlen, wonach Unternehmen bis Ende 2023 durch Ransomware weltweit mit Schäden in Höhe von 30 Milliarden US-Dollar rechnen müssen.

Die Bandbreite der genannten Werte erklärt sich durch unterschiedliche Definitionen und Schadensbewertungen – die Tendenz ist aber klar: Sie zeigt nach oben.

Die vom BKA genannten Zahlen zu den Profiten der Ransomware-Gruppierungen basieren auf Untersuchungen von *Chanalysis* und scheinen mit 602 Millionen Dollar dagegen fast gering. Sie zeigen dennoch, dass es sich um ein profitables Geschäft in großem Stil handelt. Auch der durchschnittliche Lösegeldbetrag nimmt immer weiter zu. Er stieg von 169.446 Dollar 2020 auf 204.695 Dollar im Jahr 2021 an.

Lösegeldforderung nur ein kleiner Teil des Problems

Der Vergleich der Zahlen macht auch deutlich, dass die Lösegeldzahlung für Unternehmen das kleinere Problem ist. Viel schwerer wiegen die Einbußen durch den Stillstand des Unternehmens, der Verlust von Geschäftsbeziehungen und die Kosten zur Wiederherstellung. Denn die Schadenssumme ist um den Faktor 40 höher als die Einnahmen der Cyberkriminellen.

Grafik: Cristie

Die wichtigsten Kriterien einer modernen Backup- und Disaster-Recovery-Lösung im Überblick.

Bild: Cristie

Schlüsselfertige Hard- und Software-Kombi: Die Rubrik RCDM-Software mit Dell Poweredge-Server als Pay-per-Use-Lösung.

Kein Wunder also, dass zum Beispiel *Mario Greco*, Chef des Versicherungskonzerns *Zurich*, im Dezember in einem Interview erklärte, dass Cyberangriffe bald »unversicherbar« werden könnten. Womöglich als Reaktion darauf berichteten Sicherheitsforscher kurz darauf von einer Ransomware-Gruppe, die ihre Opfer nach Details ihrer Cyberversicherung befragt und verspricht, die Lösegeldforderung der Deckungssumme anzupassen. Offenbar will man die Kuh nicht schlachten, die sich so gut melken lässt.

Angriffe sind kaum zu vermeiden

Das alte Credo der IT-Security-Branche – »100-prozentige Sicherheit gibt es nicht«, gilt auch für Ransomware-Angriffe. Bei ihnen gelangt die Malware oft über E-Mail- Phishing-Angriffe oder Social-Engineering ins Unternehmen – also Methoden, bei denen Unachtsamkeit oder Unwissen der Beschäftigten ausgenutzt werden. Die sind zwar aufwändig, aber die Angreifer suchen sich ihre Opfer gut aus und spekulieren auf hohe Gewinne.

Eine im Februar 2023 veröffentlichte Sonderauswertung des Mittelstandspanels der Staatsbank KfW zeigt, dass in Deutschland besonders Unternehmen mit mehr als hundert Beschäftigten und von denen solche mit besonders ausgeprägten Digitalisierungsaktivitäten ins Visier der Angreifer geraten. So wurden etwa 43 Prozent der Unternehmen attackiert, die im Jahr 2020 mehr als 10.000 Euro für Digitalisierungsprojekte ausgegeben hatten. Bei Unternehmen ohne derartige Investitionen lag der Anteil der angegriffenen Firmen dagegen bei 23 Prozent. Was zunächst paradox klingt, hat Methode: Offenbar rechnen die Angreifer damit, dass für Firmen, die Digitalisierung aktiv betreiben, Daten einen hohen Wert haben und sie daher auch eher bereit sind, das geforderte Lösegeld zu bezahlen.

Business-Continuity muss das Ziel sein

Nach einem Ransomware-Angriff haben Unternehmen in der Regel mit weitreichenden operativen und logistischen Problemen zu kämpfen. Ohne externe Spezialisten lassen sich die nicht meistern. Zum Beispiel muss erst einmal festgestellt werden, wann das letzte saubere Backup erfolgte. Keine triviale Aufgabe, da die Angreifer im Schnitt 45 Tage im Netzwerk verbrachten, bevor sie zuschlagen. In der Zeit durchleuchten sie die gesamte Netzstruktur inklusive der Backup-Prozesse, versuchen, auch die Back-

Cyber-Recovery im Detail

Für weitere Kopien und Archivierung der Daten bieten Rubrik und Cristie vielfältige Optionen:

- Replication to Rubrik ist eine Backup-basierte, WAN-optimierter Replikation
- Archive to S3 – lokal oder nachhaltig bei Cristie im Windrad als Sicherungs-, Replikations- und Archivierungsziel für die Sicherungsprozesse.
- Archive to NFS ermöglicht niedrigere RTOs von Archivspeichern und macht regelmäßige, vollständige Snapshots unnötig, was auch die Storage-Kosten reduziert.
- Archive to Tape unterstützt Kunden, für die die Archivierung auf Band eine unvermeidliche gesetzliche oder Compliance-Anforderung ist
- Archive to Cloud rationalisiert die Archivierung in privaten und öffentlichen Clouds (wo möglich und erwünscht) und reduziert so Kosten bei gleichzeitig hoher Verfügbarkeit.

ups zu infizieren und ziehen oft noch Daten ab, um mit deren Veröffentlichung zu drohen. Ausfälle von bis zu drei Wochen sind keine Seltenheit. Das können sich die meisten Firmen nicht leisten.

Daher rückt der Begriff Business-Continuity immer mehr in den Vordergrund. Dabei geht es einerseits darum, die Relevanz einzelner Anwendungen für das Geschäft festzulegen und Maßnahmen zu ergreifen, die auch nach einem Totalausfall gewährleisten, dass die unverzichtbaren Prozesse möglich schnell wieder laufen. Andererseits geht es aber auch darum, das Backup als aktiv nutzbare Ressource in einer breit angelegten Cyber-Security-Strategie zu sehen, als letzte Verteidigungslinie und gleichzeitig Startpunkt für die Wiederherstellung. Experten empfehlen dafür per Air-Gap getrennte, unveränderliche, zugriffsgesicherte Backups. Sie schützen auch davor, dass Angreifer gezielt Backups verschlüsseln, um ihre Forderungen durchzusetzen. In Großunternehmen hat sich dafür unter anderem **Rubrik** als Anbieter etabliert.

Pay-per-Use: Bedarfsgerecht bezahlen

Mussten Backup-und-Recovery-Lösungen bisher komplett oder zumindest in Raten bezahlt werden, kommen nun bedarfsgerechte Bezahlmodelle hinzu. **Cristie Data** bringt die Rubrik-Lösung für Daten-, Ransomware- und Disaster-Recovery als *Cristie Cyber Recovery powered by Rubrik* nun auch im deutschsprachigen Raum als mittelstandstaugliches »True Opex«-Pay-per-Use-Angebot. Zusammen mit *Cristie Nordic* bietet Cristie das Modell schon länger an und versetzt auch Service-Provider in die Lage, Backup- und Recovery-Services anzubieten. Dafür werden auch Partner in der DACH-Region gesucht.

»Aus Sicht des Mittelstands attraktiv sind neben den Pay-per-Use-Modellen sowie den mit MSP-Partnern angebotenen SaaS-basierten Nutzungsmodellen auch die zusätzlich enthaltenen Dienste und Mehrwertfunktionen«, erklärt Cristie-Geschäftsführer **Volker Wester**. »Denn Pay-per-Use macht die Enterprise-Lösung von Rubrik für den Mittelstand erst nutzbar und bezahlbar. Die Kosteneinsparungen liegen zwischen 20 und 30 Prozent. Mit Tools zur Vorhersage der möglichen Einsparungen führen wir mit Unternehmen gerne gemeinsam eine erste Berechnung durch.«

Die Services und Mehrwertfunktionen basieren unter anderem auf dem Status von Cristie als einer der wenigen Rubrik-Partner mit der *Velocity ELITE*-Zertifizierung und dem Status als autorisierter Support-Partner. »Dadurch ist auch Support auf Deutsch gewährleistet«, sagt Wester. »Außerdem beraten und unterstützen wir vom Design über die Implementierung bis zur Wartung und Betrieb sowie bei der Auswahl der Verbrauchsmodelle, Compliance-Fragen und dem Lizenzmanagement.«

Rubrik hat zusammen mit *Dell* die Software *Rubrik Cloud Data Management* (RCDM) auf *Dell PowerEdge*-Servern validiert. Cristie bietet die Lösung als Kombination von Hard- und Software an. Da die Hardware mit dem monatlichen Pay-per-Use-Modell ebenfalls bereits abgedeckt ist, bleibt das Gesamtpaket für Firmen kalkulierbar und sind die Kosten transparent.

Schnelles Disaster-Recovery & effizienter Backup-Betrieb

Im Normalbetrieb unterstützt Rubrik Unternehmen beim umfassenden Data-Management. »Durch SLA-Automatisierung lassen sich zahllose Sicherungsjobs durch wenige Policies ersetzen, die auf alle Workloads angewendet werden«, erläutert Wester. Die Funktion *Rapid Recovery* helfe, einzelne Dateien oder Objekt schnell zu finden und wiederherzustellen. Dank der umfangreichen APIs kann jede Aktion skriptgesteuert und automatisiert ausgeführt sowie in Tools integriert werden, die Unternehmen bereits nutzen und mit denen ihre Administratoren vertraut sind.

»Im Ernstfall bietet *Cristie Recovery Assurance* durch Automatisierungs- und Orchestrierungsfunktionen für die Notfallwiederherstellung sowie die Möglichkeit, Systeme in einer Sandbox-Umgebung wiederherzustellen«, sagt Wester. »So lassen sich Anomalien feststellen und das letzte gute Backup schnell identifizieren. Dadurch reduzieren sich Wiederherstellungsprozesse von üblicherweise mehreren Wochen auf maximal wenige Tage und lassen sich kurze RTO-Ziele definieren. Das hilft Unternehmen auch bei Gesprächen mit Banken oder Cyberversicherungen.«

Bezahlbare Absicherung nach dem Stand der Technik

Selbst mit hohem technischen und administrativen Aufwand können Unternehmen nicht sicherstellen, dass sie gegen Ransomware-Angriffe immun sind. Dennoch müssen sie sich entsprechend »dem Stand der Technik« absichern, um Compliance-Anforderungen zu entsprechen. Eine wesentliche Komponente ist dabei eine moderne Backup- und Disaster-Recovery-Lösung.

»Finanziell erschwinglich und administrativ beherrschbar werden Mittelstandslösung durch Zusatz-Services und Pay-per-Use-Modelle«, meint Cristie-Chef Wester. »Sie erlauben Unternehmen die bestmögliche Vorbereitung auf einen Ransomware-Angriff und helfen ihnen im Normalbetrieb, ihre Daten unternehmensweit und unabhängig vom Speicherort weitgehend automatisiert zu verwalten.« ■

Weiterführende Links:

➔ Mehr zu Cristie Cyber Recovery und der Initiative Expect the Unexpected