Rubrik-Studie belegt durchlässige Netzwerke

Optimaler Schutz durch unveränderliche Daten und versteckte Backups

11.01.2022 | Von Matthias Breusch

150 europäische IT-Führungskräfte haben an einer Umfrage der Datenschutzspezialisten Rubrik teilgenommen. Die Ergebnisse lassen nur einen Schluss zu: Viele Unternehmen sollten dringend unveränderliche Backup-Modelle ausbauen, um Ransomware-Attacken zu begegnen.

Alptraum für Unternehmen: Cyberverbrecher verschlüsseln oder stehlen die Daten und fordern Lösegeld.
(Bild: © arrow - stock.adobe.com)

Die Studie „Immutable back-ups: Separating hype from reality“ entstand aus Informationen von Institutionen und Unternehmen unterschiedlicher Sektoren, darunter Technologiefirmen und Finanzdienstleister ebenso wie Bildungseinrichtungen und Behörden.

Laut einer anderen aktuellen Studie von Sophos, die von Rubrik zitiert wird <https://news.sophos.com/de-de/2021/04/27/ransomware-opfer-im-daten-nirvana-egal-wieviel-gezahlt-wird/> , sind deutschen Unternehmen bei Ransomware <https://www.security-insider.de/was-ist-ransomware-a-781385/> -Angriffen zuletzt durchschnittlich Kosten von annähernd einer Million Euro pro Datensanierung entstanden.

Die damit einhergehenden Lösegeldzahlungen beliefen sich durchschnittlich auf 115.000 Euro.

Rubriks Europadirektor Achim Freyer weist darauf hin <https://www.storage-insider.de/rubrik-erweitert-cloud-data-management-portfolio-a-1032254/> , dass selbst die fortschrittlichsten Anti-Malware <https://www.security-insider.de/was-ist-malware-a-578417/> -Lösungen Angriffe nicht zu hundert Prozent abwehren könnten, „vor allem nicht solche, die [...] auf sozialen Taktiken basieren, was immer häufiger der Fall ist". Nicht zuletzt die Umstellung auf Heimarbeitsplätze habe viele Unternehmen zu „weicheren" Zielen gemacht.

Mäßiges Vertrauen

43 Prozent der Befragten gaben an, die Zahl der Ransomware-Angriffe auf ihr Unternehmen habe infolge der Covid-19-Pandemie zugenommen, teilweise sogar deutlich. Dieser Wert kollidiert mit dem allenfalls mäßigen Vertrauen, das viele Entscheider in ihre eigene Datensicherung <https://www.security-insider.de/was-ist-backup-a-954035/> haben. Der Durchschnittswert der Antworten lag nur bei etwa 7 auf einer Skala von 1 bis 10.

Lediglich 16 Prozent stimmten der Aussage voll und ganz zu, sie seien sicher, dass ihre Backup-Daten „nicht durch einen Ransomware-Angriff gefährdet sind". 38 Prozent stimmten dem eingeschränkt zu; 46 Prozent sind demnach stark gefährdet.

Infektiöse Protokolle

58 Prozent verwendeten Standardprotokolle für ihre Backups, mehr als ein Drittel verfügte über *in-place*- statt *out-of-place*-schreibende Systeme. Dies bedeute: Infizierte Daten könnten weitere Daten gefährden. Nur etwas mehr als ein Drittel der Befragten verfügte über eine Datensicherungslösung, die eine sofortige Wiederherstellung ermöglichte.

Für 43 Prozent war die größte Schwierigkeit „die Geschwindigkeit der Wiederherstellung". Nur 18 Prozent der Befragten betrachteten dies als „ein leichtes Unterfangen". Bei der Mehrheit der befragten Unternehmen wäre der Geschäftsbetrieb für mehr als zwei Tage beeinträchtigt, bei 28 Prozent für länger als eine Woche.

Logische Lücke

Rubrik sieht die Antwort auf diese Problemzone in einer Architektur, „die nach dem Zero Trust Implementation Model von NIST modelliert ist". Das Prinzip ist so simpel wie effektiv: Niemand ist vertrauenswürdig – kein Nutzer, keine Anwendung, kein Gerät. Um

diesen Standard zu erfüllen, müssen die Daten von Haus aus unveränderlich sein, damit sie niemals durch Ransomware verändert, verschlüsselt oder gelöscht werden können.