

## PRESSEMITTEILUNG

### Dreiviertel der Unternehmen zahlen Ransomware

*Delinea Research zeigt auch: Mittelständische Unternehmen werden zum bevorzugten Ziel, die Cloud wird zum anfälligsten Angriffsvektor*

München, 01. Februar 2024 – [Delinea](#), ein führender Anbieter von Lösungen, die das **Privileged Access Management (PAM)** nahtlos erweitern, zeigt in seinem jährlichen **State of Ransomware-Report** auf, dass Ransomware-Angriffe wieder zunehmen und einen Strategiewechsel der Cyberkriminellen erkennen lassen. Die bekannte Taktik, ein Unternehmen lahmzulegen und als Geisel zu nehmen, wurde durch neue Strategien ersetzt, bei denen private und sensible Daten heimlich exfiltriert werden. Cyberkriminelle drohen dann häufig damit, die Daten im Darknet an den Meistbietenden zu verkaufen oder sie zu nutzen, um eine stattliche Cyberversicherungszahlung zu erhalten.

Unter dem Titel „State of Ransomware 2024: Anticipating the Battle and Strengthening Your Defenses“ analysiert der Bericht Daten aus einer Umfrage unter mehr als 300 US-amerikanischen IT- und Sicherheitsentscheidern. Ziel der Analyse ist es, signifikante Veränderungen im Vergleich zu den Daten des Vorjahresberichts zu identifizieren und neue Trends aufzudecken. So zeigt sich vor allem, dass Ransomware wieder auf dem Vormarsch ist. Die Zahl der Unternehmen, die in den letzten zwölf Monaten Opfer von Ransomware geworden sind, hat sich seit dem letzten Jahr mehr als verdoppelt (von 25 auf 53 %), auch wenn sie nicht das Niveau von 2021 erreicht hat. Mittelständische Unternehmen scheinen am stärksten im Fadenkreuz der Cyberkriminellen zu stehen: 65 Prozent gaben an, Opfer von Ransomware geworden zu sein. Die Studie zeigt auch, dass Organisationen im Allgemeinen häufiger Lösegeld zahlen, nämlich 76 Prozent gegenüber 63 Prozent im Vorjahr.

#### Datenexfiltration als neues Hauptmotiv

Noch auffälliger sind jedoch die sich abzeichnenden Trends bei den Motivationen, Strategien und Taktiken. So verzeichnete die Datenexfiltration einen sprunghaften Anstieg um 39 Prozent. Während im letzten Jahr noch 46 Prozent der Befragten dies als häufigste Strategie angaben, sind es jetzt 64 Prozent. Damit wurde die Datenexfiltration zum bevorzugten Ziel der Angreifer, die nun die Kontrolle über ein Unternehmensnetzwerk erlangen, um sensible Daten herunterzuladen und im Darknet zu verkaufen. Dieser Trend zeigt sich auch darin, dass die traditionelle Geldgier als Hauptmotiv mit 34 Prozent gegenüber 69 Prozent im Vorjahr deutlich zurückgegangen ist.

„Ransomware scheint einen entscheidenden Wendepunkt erreicht zu haben. Es geht nicht mehr nur um die schnelle und einfache Auszahlung“, sagt Rick Hanson, Präsident von Delinea. „Selbst wenn Unternehmen mehr in Cyber-Versicherungen investieren, die oft

Ransomware-Auszahlungen in den Versicherungspolicen einschließen, stellen Cyber-Kriminelle fest, dass es für sie am erfolgversprechendsten ist, Stealth-Taktiken zu nutzen. So bleiben sie unter dem Radar und gelangen an sensible, wertvolle Informationen, um diese dann zu verkaufen."

Mit dem neuen Hauptfokus änderten die Cyberkriminellen auch ihre Taktik. So nutzten sie nicht mehr E-Mail als bevorzugten Angriffsvektor – deren Nutzung sank von 52 Prozent auf 37 Prozent. Stattdessen zielten sie auf die Cloud (44 Prozent) und kompromittierte Anwendungen (39 Prozent). Durch eine verdeckte Vorgehensweise können die Angreifer länger unerkannt bleiben und sich so kontinuierlich Zugang zu Systemen und Daten verschaffen. Dies versetzt sie in die Lage den Schaden jederzeit zu erhöhen, wenn sie es wünschen.

### **Führungskräfte häufig planlos**

Bei den Maßnahmen, die Unternehmen gegen Ransomware ergriffen haben, zeigten sich gegensätzliche Trends. Während 91 Prozent angaben, dass sie spezielle Budgets für Ransomware bereitstellen (gegenüber 68 % im Jahr 2022), nennen nur 61 Prozent (gegenüber 76 %), dass die Sicherheitsbudgets nach einem Angriff reduziert wurden, was auf wirtschaftliche Unsicherheit oder knappere Budgets zurückzuführen sein könnte. Obwohl die Befragten der Meinung sind, dass sie ihre Verteidigung durch höhere Ausgaben für kritische Bereiche wie Privileged Access Management (28 gegenüber 16 %) verstärken könnten, scheinen sie sich nicht im Klaren darüber zu sein, wie höhere Ausgaben zur Verbesserung der Sicherheit beitragen würden. Positiv zu vermerken ist, dass Führungskräfte und Vorstände nun zuhören: 76 Prozent gaben an, dass sich ihre Führungsriege Gedanken über Ransomware macht, wenn auch vielleicht erst nach einem Angriff.

„Die sich ändernden Strategien und Taktiken bei Ransomware-Angriffen erfordern einen mehrschichtigen Sicherheitsansatz, der das Risiko eines unbefugten Zugriffs mindert, selbst wenn die Zugangsdaten kompromittiert wurden“, sagt Joseph Carson, Advisory CISO und Chief Security Scientist bei Delinea. „Es zeigt auch die kritische Rolle, die der privilegierte Zugang in der gesamten Cybersicherheitsstrategie spielt.“

Ein kostenloses Exemplar des Berichts kann unter folgendem Link heruntergeladen werden <https://delinea.com/resources/ransomware-2024-research-report>.

### **Über Delinea**

Delinea ist ein führender Anbieter von Privileged-Access-Management (PAM)-Lösungen für moderne, hybride Unternehmen. Die Delinea Plattform erweitert PAM nahtlos, indem sie eine identitätsübergreifende Autorisierung bereitstellt und den Zugriff auf die kritischsten Hybrid-Cloud-Infrastrukturen sowie die sensibelsten Daten eines Unternehmens kontrolliert. Auf diese Weise werden Risiken reduziert, Compliance gewährleistet und die Sicherheit vereinfacht. Die Kundenbasis von Delinea umfasst Tausende Unternehmen weltweit und reicht von KMUs bis hin zu den größten Finanzinstituten und Unternehmen der kritischen Infrastruktur.

Weitere Infos unter: <http://delinea.com/de>

Erfahren Sie mehr über Delinea auf LinkedIn, Twitter und YouTube.

© Delinea Inc. (ehemals Centrifry Corporation) 2023. Delinea™ ist eine Marke von Delinea Inc. Alle anderen Marken sind Eigentum der jeweiligen Inhaber.

### **Pressekontakte:**

#### **Delinea DACH**

Claudia Specht, Senior Marketing Manager CEUR

[claudia.specht@delinea.com](mailto:claudia.specht@delinea.com)

**PR-Agentur: Weissenbach PR**

Felicitas Weller

T: +49 89 54 55 82 02

[delinea@weissenbach-pr.de](mailto:delinea@weissenbach-pr.de)

Web: [www.weissenbach-pr.de](http://www.weissenbach-pr.de)