EUROPEAN-NEWS-AGENCY.COM

EUROPEAN NEWS AGENCY

International Press Service

Ressort: Internet und Technik

Ransomware : 90 Prozent würden Lösegeld bezahlen

Ingolstadt, 16.05.2022 [ENA]

88 Prozent der Unternehmen, die bereits Ziel eines Ransomware-Angriffes waren, würden bei einer erneuten Attacke Lösegeld zahlen, wie eine aktuelle Kaspersky-Studie zeigt. Firmen, die noch nicht von einem Ransomware-Angriff betroffen waren, wären hingegen lediglich 67 Prozent prinzipiell bereit dazu – sie wären jedoch weniger geneigt, dies sofort zu tun. Ist die Zahlung ein geeignetes Mittel zur Lösung des Problems?

Die Kaspersky-Studie zeigt, dass Ransomware nach wie vor eine große Bedrohung ist: so wurden bereits zwei Drittel (64 Prozent) der Unternehmen angegriffen. Des Weiteren hat sich die Zahl der Angriffe mit Ransomware allein im Jahr 2021 gegenüber dem Vorjahr fast verdoppelt. Die Tatsache, dass ein Unternehmen bereits einmal Lösegeld bezahlt hat, bedeutet nicht, dass dieses kein zweites Mal hierzu bereit wäre – im Gegenteil. So steigt sogar die Wahrscheinlichkeit, dass dies geschehen würde, im Falle eines neuen Angriffs. Fast jedes neunte (88 Prozent), bereits einmal kompromittierte, Unternehmen würde so verfahren, um den Zugriff auf die eigenen Daten zurückzuerlangen.

Zahlung ein effektiver Weg?

Diese Firmen neigen auch eher dazu, so schnell wie möglich zu zahlen, um sofortigen Zugang zu ihren Daten zu erhalten (33 Prozent der bereits angegriffenen Unternehmen gegenüber 15 Prozent der Unternehmen, die noch nie Opfer eines Angriffs waren), oder bereits nach ein paar Tagen erfolgloser Entschlüsselungsversuche zu zahlen (30 Prozent gegenüber 19 Prozent). Führungskräfte in Unternehmen, die bereits Lösegeld gezahlt haben, scheinen zu glauben, dass dies der effektivste Weg ist, um ihre Daten wiederzubekommen.

Diese Zahlungsbereitschaft könnte darauf zurückzuführen sein, dass sie kaum wissen, wie sie auf solche Bedrohungen reagieren sollen, oder dass die Wiederherstellung der Daten so lange dauert, da betroffene Unternehmen durch das Warten auf die Wiederherstellung der Daten mehr Geld verlieren könnten als durch die Zahlung des Lösegelds. Damit bleibt Ransomware eine echte Bedrohung für die Cybersicherheit.

Zwei Drittel (64 Prozent) der Unternehmen bestätigen, dass sie mit dieser Art von Vorfällen konfrontiert waren, und 66 Prozent gehen davon aus, dass es irgendwann zu solch einem Angriff auf ihre Organisation kommen wird. Wobei sie einen Ransomware-Angriff für wahrscheinlicher halten als andere gängige

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com

Haftungsausschluss:

Der Herausgeber übernimmt keine Haftung für die Richtigkeit oder Vollständigkeit der veröffentlichten Meldung, sondern stellt lediglich den Speicherplatz für die Bereitstellung und den Zugriff auf Inhalte Dritter zur Verfügung. Für den Inhalt der Meldung ist der allein jeweilige Autor verantwortlich.

Angriffsarten wie DDoS, Supply-Chain, APT, Cryptomining oder Cyberspionage.

„Ransomware ist zu einer ernsthaften Bedrohung für Unternehmen geworden, da regelmäßig neue Muster auftauchen und APT-Gruppen sie für fortgeschrittene Angriffe nutzen“, sagt Christian Milde, Geschäftsführer Central Europe bei Kaspersky. „Selbst eine versehentliche Infektion kann für ein Unternehmen zur Herausforderung werden. Da es hierbei oft um die Geschäftskontinuität geht, sehen sich Führungskräfte gezwungen, schwierige Entscheidungen hinsichtlich der Zahlung des Lösegelds zu treffen. Wir empfehlen jedoch grundsätzlich, Cyberkriminelle nicht zu bezahlen, da dies keine Garantie dafür bietet, dass die Daten tatsächlich wieder entschlüsselt werden; eine Zahlung ermutigt sie jedoch, ihre Vorgehensweise zu wiederholen.

Bei Kaspersky arbeiten wir mit zunehmenden Erfolg daran, Unternehmen dabei zu helfen, solche Folgen zu vermeiden. Für Firmen ist es wichtig, grundlegende Sicherheitsprinzipien zu befolgen und sich mit zuverlässigen Sicherheitslösungen zu befassen, um das Risiko eines Ransomware-Vorfalls zu minimieren. Der Anti-Ransomware-Tag bietet sich an, genau an diese wichtigen Praktiken zu erinnern.“

Führende IT-Sicherheitsexperte wie Kaspersky Kaspersky geben folgende Tipps für einen besseren Schutz von Unternehmen vor Ransomware:

• Die Software sollte auf allen genutzten Geräten stets auf dem neuesten Stand sein, um zu verhindern, dass Angreifer Schwachstellen ausnutzen und in das Netzwerk eindringen.

• Die Verteidigungsstrategie sollte auf die Erkennung von Seitwärtsbewegungen und die Datenexfiltration ins Internet fokussiert sein. Hierbei besonders auf den ausgehenden Datenverkehr achten, um Verbindungen von Cyberkriminellen zum eigenen Netzwerk zu erkennen.

• Einrichtung von Offline-Backups, die von Eindringlingen nicht manipuliert werden können und auf die im Notfall schnell zugegriffen werden kann.

• Aktivierung von Ransomware-Schutz für alle Endgeräte. Kaspersky Anti-Ransomware Tool for Business ist ein kostenloses Tool, das Computer und Server vor Ransomware und anderen Arten von Malware schützt und Exploits verhindert. Es ist mit bereits installierten Sicherheitslösungen kompatibel.

• Unternehmen sollten Anti-APT- und EDR-Lösungen für eine fortschrittliche Erkennung von Bedrohungen implementieren, die Untersuchung und zeitnahe Behebung von Vorfällen ermöglichen sowie den Zugriff auf die neuesten Bedrohungsdaten nutzen. Mithilfe eines MDR-Anbieters können fortgeschrittene Ransomware-Angriffe effektiv abgewehrt werden. All dies ist mit Kaspersky Expert

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com

Haftungsausschluss:

Der Herausgeber übernimmt keine Haftung für die Richtigkeit oder Vollständigkeit der veröffentlichten Meldung, sondern stellt lediglich den Speicherplatz für die Bereitstellung und den Zugriff auf Inhalte Dritter zur Verfügung. Für den Inhalt der Meldung ist der allein jeweilige Autor verantwortlich.



Security möglich.

• Wenn Unternehmen von einem Ransomware-Angriff betroffen sind, sollten sie niemals das geforderte Lösegeld zahlen. Denn es gibt keine Garantie, dass sie dadurch Daten zurückbekommen; es ermutigt Cyberkriminelle jedoch, ihre Geschäfte weiterzuführen. Ein Vorfall sollte stattdessen umgehend der örtlichen Polizeibehörde gemeldet werden. https://www.nomoreransom.org bietet Zugang zu Entschlüsselungsprogrammen.

Bericht online lesen:
https://www.en-a.de/internet_und_technik/ransomware__90_prozent_wuerden_loesegeld_bezahlen-83956/

Redaktion und Verantwortlichkeit:
V.i.S.d.P. und gem. § 6 MDStV: Heiko Schulz

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com

Haftungsausschluss:

Der Herausgeber übernimmt keine Haftung für die Richtigkeit oder Vollständigkeit der veröffentlichten Meldung, sondern stellt lediglich den Speicherplatz für die Bereitstellung und den Zugriff auf Inhalte Dritter zur Verfügung. Für den Inhalt der Meldung ist der allein jeweilige Autor verantwortlich.