Und täglich grüsst das Murmeltier …

von Andreas Wisler

Der Super-GAU: alle Daten sind verschlüsselt, auf dem Bildschirm steht eine Meldung, dass nur gegen Bezahlung eines Lösegelds die Daten wieder hergestellt werden können. Die Gefahr, Opfer von einem solchen Angriff zu werden, ist zu einem ständigen Begleiter geworden. Fast täglich kann von einem erfolgreichen Angriff gelesen werden.

Ransomware, eine Form von Malware (Kurzform für malicious software, jegliche Art von unerwünschter Software), die Daten zuerst stiehlt, danach verschlüsselt und Lösegeld für deren Freigabe fordert, breitet sich zunehmend aus und stellt eine ernsthafte Bedrohung für Unternehmen weltweit dar. In der heutigen vernetzten Welt, in der Daten oft das wertvollste Gut eines Unternehmens sind, kann ein Ransomware-Angriff katastrophale Folgen haben. Viele Firmen aller Grössen und Branchen sind bereits betroffen, und die Zahl der Vorfälle steigt stetig.

Hatten Hacker früher noch einen Ehrenkodex und haben beispielsweise keine Spitäler angegriffen, ist heute jedes Ziel lohnenswert. Im Januar traf es mehrere Hilfsorganisationen, im Februar konnte gelesen werden: «Angreifer konnten auf IT-Systeme vom KaDeWe, der Landeskirche Hannover, von Schneider Electric und Thyssenkrupp zugreifen. Dabei sind zum Teil Daten abgeflossen.» Und im März wurde der Klinikverbund im deutschen Kreis Soest gestört, um nur einige wenige Beispiele aus dem ersten Quartal 2024 zu nennen. Gleichzeitig hat der Landkreis Anhalt-Bitterfeld Mitte März bekanntgegeben, dass die Bereinigung nach dem Ransomware-Vorfall 2.5 Millionen Euro gekostet hat.

Die Entscheidung, ob das geforderte Lösegeld bezahlt werden soll, ist komplex und wird kontrovers diskutiert. Auf der einen Seite kann die Zahlung als schnellster Weg zur Wiederherstellung der Daten erscheinen, insbesondere wenn kritische Geschäftsprozesse zum Stillstand gekommen sind. Doch zahlen bedeutet auch, die kriminellen Aktivitäten zu unterstützen und möglicherweise zur Zielgruppe für zukünftige Angriffe zu werden. Experten und Strafverfolgungsbehörden raten in der Regel davon ab, das Lösegeld zu bezahlen. Stattdessen sollten Unternehmen ihre Bemühungen auf die Prävention, Erkennung und schnelle Reaktion auf solche Angriffe konzentrieren.

Bei einem Ransomware-Angriff ist es wichtig, sofort zu handeln und die richtigen Stellen zu informieren. Das betroffene System muss umgehend isoliert werden. Auch schon das Netzwerkkabel auszustecken, hilft, die Ausbreitung zu stoppen. Umgehend ist die IT-Abteilung zu informieren. Diese kann erste Schritte zur Identifikation einleiten und bei Bedarf externe Unterstützung hinzuziehen. Zusätzlich kann es sinnvoll sein, eine Anzeige bei der Polizei zu erstatten, um rechtliche Schritte gegen die Angreifer einzuleiten.

Von grosser Bedeutung ist die Prävention von Ransomware-Angriffen. Diese erfordert eine mehrschichtige Sicherheitsstrategie. Dazu gehören als wichtigster Punkt regelmässige Sicherheitsupdates für alle Systeme und Anwendungen, um bekannte Sicherheitslücken zu schliessen. Neue Schwachstellen werden immer schneller von Hackern ausgenutzt. Über Suchmaschinen können gefährdete Systeme innert Sekunden gefunden werden. Auch auf Schwachstellen spezialisierte Websites helfen, verwundbare Systeme schnell zu finden. Weiterhin ist eine umfassende Schulung der Mitarbeitenden erforderlich, um sie über die Gefahren von Phishing-Angriffen und anderen Methoden, die zur Verbreitung von Ransomware genutzt werden, aufzuklären. Als Lebensversicherung für jedes Unternehmen sind regelmässige Back-ups unerlässlich. Diese sollten immer getrennt vom Netzwerk gespeichert werden, um im Falle eines Angriffs eine schnelle Wiederherstellung der Daten zu ermöglichen.

Zu den Vorbeugungsmassnahmen gehört die Implementierung von «Endpoint Detection and Response (EDR)»-Lösungen und die Nutzung von Anti-Malware-Software, die speziell darauf ausgelegt ist, Ransomware zu erkennen und zu blockieren. Netzwerksegmentierung kann ebenfalls hilfreich sein, um die Ausbreitung der Malware im Falle eines Angriffs zu begrenzen. Darüber hinaus sollten Unternehmen einen Incident-Response-Plan entwickeln und regelmässig üben, um im Falle eines Angriffs schnell und effektiv reagieren zu können.

Ransomware stellt eine ernstzunehmende Bedrohung dar, die proaktive Massnahmen zur Prävention und Vorbereitung erfordert. Obwohl die Entscheidung, das Lösegeld zu bezahlen, von den spezifischen Umständen des Einzelfalls abhängt, ist es generell ratsam, sich auf Prävention, Vorbereitung und die Zusammenarbeit mit Behörden zu konzentrieren. Durch die Implementierung einer robusten Sicherheitsstrategie, die regelmässige Schulungen, Back-ups, die Aktualisierung von Software und die Vorbereitung auf Sicherheitsvorfälle umfasst, können Unternehmen ihre Resilienz gegen Ransomware-Angriffe stärken und ihre Daten und Ressourcen schützen.

Andreas Wisler
ist Inhaber und Senior Security Consultant der goSecurity AG
ISO 27001, 27701 und 22301 Lead Auditor

www.goSecurity.ch | www.27001.blog
www.angriffslustig.ch