Teufelskreis Ransomware: Das Wirtschaftssystem hinter der Daten-Geiselnahme

Durch die enorme Professionalisierung der Vertriebswege wie Ransomware-as-a-Service (RaaS), benötigen Angreifer nicht mehr zwingend tiefgreifende technische Fähigkeiten, sondern vielmehr unternehmerisches Talent, um hohe Summen von ihren Opfern zu erpressen. Die Entwickler des GandCrab-RaaS rühmten sich, 2,5 Millionen US-Dollar pro Woche einzunehmen. Aktuelle Angriffe mit dem polymorphen Emotet-Virus, der den TrickBot-Trojaner einführt, daraufhin Daten stiehlt und die Ryuk-Ransomware herunterlädt, können ebenso effektiv wie profitabel sein.

Neues Druckmittel: Victim-Outing von Unternehmen, die kein Lösegeld bezahlen
Darüber hinaus greifen Cyberkriminelle zu neuen Mitteln, um den Druck auf ihre Opfer weiter zu erhöhen. Die Angreifer hinter der Ransomware-Variante Maze haben begonnen, öffentlich bekanntzumachen, wenn Unternehmen sich weigern, Lösegeld zu zahlen. Auf einer Website gaben die Kriminellen kürzlich Namen, Websites und sogar gestohlene Daten von Opferfirmen weiter.

Ransomware bleibt nicht nur eine ernsthafte Bedrohung, weil sie für Cyberkriminelle eine effektive Einnahmequelle ist. Das florierende Geschäft der Daten-Geiselnahme wird auch durch weitere Akteure zusätzlich angefacht:

Ransomware-Broker zur Abwicklung der Lösegeldzahlungen

Versicherungsanbieter: Teilweise Ermutigung zur Zahlung von Lösegeldern

Traditionell ermöglichen Anbieter, die auf Cyber-Versicherungen spezialisiert sind, eine Deckung für Verluste, die durch eine Ransomware-Infektion entstehen. Wie die Non-Profit-Nachrichtenseite ProPublica vor kurzem herausfand, haben einige Versicherer dazu ermutigt, Lösegelder zu zahlen, wenn es wahrscheinlich ist, dass die Kosten durch eine schnelle Wiederherstellung des Geschäftsbetriebs minimiert werden können. Dies ermöglicht es den betroffenen Unternehmen zwar, schneller einen Decryption-Key zu erhalten, doch durch Lösegeldzahlungen an die Erpresser wird das Problem nur noch weiter verschärft.

Nicht jede Organisation, die von Ransomware betroffen ist, ist mit den treuhänderischen Forderungen der Angreifer vertraut; dazu gehört auch, wie Krypto-Währungen wie Bitcoin funktionieren. Hierfür gibt es mittlerweile Vermittlerservices, die von Unternehmen oder deren Rechtsberatung beauftragt werden können, um eine Reduzierung der geforderten Summe auszuhandeln oder den Prozess der Lösegeldzahlung abzuwickeln. Zu diesen Dienstleistern zählt etwa die Firma Coveware, die sich selbst als „Ransomware Recovery First Responder" bezeichnet und Unternehmen bei der Erleichterung von Zahlungen, aber auch bei der Erhebung und Weitergabe von Daten hilft, die sie mit Strafverfolgungsbehörden und Sicherheitsforschern austauscht. Eine Handvoll anderer Firmen wie Gemini Advisory und Cytelligence sind in letzter Zeit ebenfalls entstanden.

Grundlegende Best Practices gegen Ransomware

1. Aufklärung: Eine effektive Ransomware-Abwehr fußt maßgeblich auf der umfangreichen
Die Einhaltung grundlegender Best Practices bleiben der Schlüssel zur Minimierung von Schäden durch Ransomware. Zu den wichtigsten Sicherheitspraktiken zählen:

Mitarbeiterschulung. Zu den häufigen Infektions- oder Angriffsvektoren gehören:
• E-Mail-Anhänge: Eine der gängigsten Methoden zur Verbreitung von Ransomware ist die Versendung bösartiger E-Mail-Anhänge durch Phishing-Attacken, beispielsweise als gefälschte Rechnungen oder Bewerbungsunterlagen.
• Social Media: Ein weiteres Mittel der Täuschung ist ein Angriff über Social Media. Einer der bekanntesten Kanäle ist der Facebook Messenger: Kriminelle erstellen Konten, die die aktuellen Kontakte eines Benutzers nachahmen und Nachrichten mit bösartigen Dateien oder Links versenden.
• Online-Popups: Ein älterer, gängiger Angriffsvektor sind Online-Popups, die häufig verwendete Software nachahmen und Nutzer dazu bringen wollen, auf das gefälschte Fenster zu klicken, um die Malware herunterzuladen.
• Gefälschte Apps: Im Bereich der mobilen Ransomware zählen gefälschte Apps zu den häufigsten Infektionsvektoren. Apps sollten daher nur von vertrauenswürdigen Quellen bezogen werden.

2. Häufige und getestete Backups: Die Sicherung aller wichtigen Dateien und Systeme ist eine der stärksten Abwehrmaßnahmen gegen Ransomware. Backups sollten regelmäßig getestet werden, um sicherzustellen, dass die Daten vollständig und nicht beschädigt sind.

3. Strukturierte, regelmäßige Updates: Die meiste Software, die Unternehmen verwenden, aktualisiert der Softwarehersteller regelmäßig. Diese Updates können Patches beinhalten, um die Software vor bekannten Bedrohungen zu schützen. Jedes Unternehmen sollte einen Verantwortlichen benennen, der die Software aktualisiert.

4. Korrekte Verfolgung von Berechtigungen: Jeder Mitarbeiter, der Zugang zu Systemen erhält, schafft eine potenzielle Schwachstelle für Ransomware. Fehlende Aktualisierung von Passwörtern und unzulässige Nutzerberechtigungen können zu noch höheren Angriffswahrscheinlichkeiten führen.

5. Weitere Security-Technologien und -Services: Darüber hinaus können zusätzliche Security-as-a-Service-Dienste wie etwa Managed Detection and Response (MDR) Unternehmen durch externe Sicherheitsexperten dabei unterstützen, Bedrohungen zu jagen, zu erkennen und in Echtzeit auf Angriffe zu reagieren, um Ransomware-Angriffe und andere Advanced Threats zu stoppen, bevor sensible Unternehmensdaten gefährdet werden.

Prävention bleibt die beste Verteidigung. Mit einem mehrschichtigen Sicherheitsansatz aus Mitarbeiteraufklärung, kontinuierlichen Update- und Backup-Praktiken sowie Sicherheitstechnologien lässt sich das Risiko eines Ransomware-Angriffs deutlich verringern.