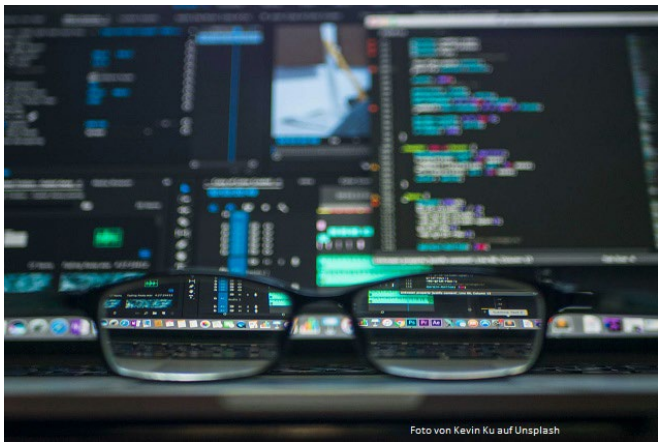
Cyber-Erpressung im Fokus: Gefahren, Folgen und Gegenmaßnahmen

Dr. Brigitta Schwarzer, 21.03.2024



Standen früher Entführungen mit Lösegeldforderungen im Zentrum der Aufmerksamkeit, sind im Zeitalter des Internets Erpressungen mit der Drohung, vermeintlich inkriminierende Informationen und Verhaltensweisen der Öffentlichkeit zugänglich zu machen, gang und gäbe.

Cyberkriminelle setzen heute zunehmend Schadsoftware - sogenannte Ransomware - als Mittel der digitalen Erpressung ein. Dabei werden Computer infiziert, Daten verschlüsselt und für deren Freigabe Lösegeld verlangt. Doch damit nicht genug: Vor der Verschlüsselung werden die Unternehmensdaten exfiltriert und das Unternehmen quasi doppelt erpresst: mit der Verschlüsselung und mit der Drohung, die Daten im Dark Web zu verkaufen oder anderweitig zu veröffentlichen.

Solche Vorfälle mit immer raffinierteren Methoden häufen sich in erschreckendem Ausmaß und sind mittlerweile zu einer der größten digitalen Bedrohungen weltweit geworden. Wenn Hacker verstärkt künstliche Intelligenz einsetzen werden, um Angriffsmuster zu standardisieren, wird sich das Bedrohungspotenzial weiter erhöhen.

So weit, so gut. Unternehmen, die auf solche Szenarien vorbereitet sind, einen Notfallplan in der Tasche haben sowie geschulte Mitarbeiter:innen, die nicht in Panik verfallen, sondern einen klaren Kopf behalten, wissen, was im Ernstfall zu tun ist.

Best-in-Class Unternehmen haben sich zusätzlich abgesichert und können in solchen Situationen auf einen spezialisierten Cyber-Dienstleister zurückgreifen, der rund um die Uhr erreichbar ist. So profitieren sie von externer Expertise mit langjähriger Erfahrung in ähnlichen Situationen. Das nimmt einerseits Druck von den Unternehmensverantwortlichen und bietet andererseits den Vorteil, dass eine externe und unabhängige Stelle direkt in die Aufarbeitung involviert ist bzw. einen Teil der einzelnen To-Dos übernehmen kann. Das können Verhandlungen mit den Cyberkriminellen sein, Unterstützung bei der Beschaffung

von Liquidität in Cryptowährungen für Lösegeldzahlungen oder Hilfestellung bei der Entscheidung, ob die verschlüsselten Daten reaktiviert oder neu generiert werden sollen.

Unternehmen, die all das nicht im Talon haben, tun sich im Ernstfall deutlich schwerer, die richtigen Maßnahmen zu ergreifen und Entscheidungen zu treffen. Ihr „Nutzen" besteht dann einzig und allein darin, eine Lernerfahrung gemacht zu haben und dadurch für ein nächstes Mal besser gerüstet zu sein.

Im Rahmen eines vierstündigen Webinars der **Internationalen Handelskammer / ICC Austria** am 13. März 2024 referierte **Michael Krausz** vor einem kompetenten und interessierten Publikum eindrucksvoll über alle Aspekte von Erpressungssoftware und deren Folgen. Sein großes Plus: Er konnte nicht nur mit seinem umfangreichen Wissen, sondern vor allem auch mit seiner allgemein verständlichen Sprache alle Teilnehmer:innen – die IT-Affinen, die Betriebswirte und die Juristen – abholen. Was ihm ebenfalls sehr gut gelang, war die ganzheitliche Betrachtung des Themas.

Insbesondere mit folgenden Kernaussagen brachte Krausz die komplexe Materie auf den Punkt:

- Cyber-Erpressungsversuche betreffen nicht nur öffentliche Stellen und Großunternehmen, sondern zunehmend auch den Mittelstand. Dieser wird eher nicht Opfer von gezielten Angriffen, sondern von „Massenversuchen". Hier sind die Lösegeldsummen zwar geringer, aber „auch Kleinvieh macht Mist".

- Oberstes Gebot bei Cybervorfällen ist absolute Vertraulichkeit. Jede Mitabeiterin und jeder Mitarbeiter muss wissen, was gegenüber Kunden, Lieferanten, Banken und sonstigen Geschäftspartnern kommuniziert werden darf. Besonders sensibel ist die Presse, hier muss es eine klare Regelung geben, „wer sagt was".

- Schutzmaßnahme Nr. 1: „Do not click on shit", ein falscher Tastendruck einer Person kann – je nach Umfang der Sicherheitsvorkehrungen – das ganze Unternehmen lahmlegen. Absolutes No-Go: Mitarbeiter:in schickt verdächtiges Mail am Privat-PC an die Firma, um es dort zu öffnen. Hier steht auch eine strafrechtliche Verantwortung im Raum.

- Ganz wichtig im Anlassfall ist die Entscheidung „Verhandeln auf Geld" oder „Verhandeln auf Zeit". Ob die eine oder die andere Strategie zielführender ist, hängt von den individuellen Gegebenheiten beim geschädigten Unternehmen ab.

- Krausz' Empfehlungen zur Verhandlungsführung zeugen von seiner langjährigen Erfahrung auf diesem Gebiet. Sein Appell: Betroffene sollten niemals selbst verhandeln, der Stresspegel wäre zu hoch und die gebotene kaufmännische Sorgfalt

würde darunter leiden. Außerdem sei es – im Gegensatz zu den Angreifern – nicht ihr Tagesgeschäft.

- Alle Unternehmen sind gut beraten, ihre Allgemeinen Geschäftsbedingungen „cyberfest“ zu machen, indem sie einen Passus aufnehmen, wonach Ransomware- und ähnliche Vorfälle im Hinblick auf Lieferverzögerungen als Höhere Gewalt bzw. nicht beeinflussbare Umstände zu werten sind.

- Last, but not least: Soll eine Cyberversicherung abgeschlossen werden und wenn ja, soll diese auch Lösegeldzahlungen abdecken? Laut Krausz gibt es gute und leistbare Produkte am Markt. Entscheidend für die richtige Auswahl sei eine gute Beratung.

Michael Krausz studierte Physik, Informatik und Rechtswissenschaften in Wien und den USA und ist ausgebildeter Berufsdedektiv und Buchautor zum Thema Security Incident Management sowie Kostenwahrheit bei Sicherheitsvorfällen. Im Rahmen seines 1998 gegründeten Unternehmens i.s.c. Group mit Büros in Wien, Coburg, London, Singapur und Salt Lake City und seit Gründung Projekten in 33 Ländern auf vier Kontinenten unterstützt er Unternehmen bei der Prävention und Bewältigung von schweren und schwersten extern oder intern ausgelöster Sicherheitsvorfällen. Seit 2002 widmet er sich insbesondere auch der Vorbeugung durch Informationssicherheits-Managementsysteme sowie der Verhandlungsführung und Unterstützung des Managements und der IT im Ernstfall.

Website ICC: www.icc-austria.org
Website Michael Krausz: www.iscgroup.co.at