Gezielt durchsuchen Cyber-Erpresser das Web: Sie erreichen mit ihren kriminellen Attacken nun auch den Oberpfälzer Mittelstand. Ein Unternehmen kommt nur mit der Zahlung von Lösegeld wieder zu seinen Daten.

Weiden. (cf) Standen bisher eher die prominenten Firmennamen aus Ostbayern im Fokus der Hacker, traf es nun einen mittelständischen Betrieb aus dem Raum Weiden. Der vom plötzlichen Cyber-Angriff völlig schockierte Firmeninhaber kämpfte wochenlang um seine Existenz, ehe er schrittweise – mit professioneller Hilfe – wieder die Keys (Schlüssel) für seine verschlüsselten Daten erhielt. Der materielle Schaden summiert sich auf einen hohen sechsstelligen Betrag. Noch viel schwerer wog die Ungewissheit um die Wiederherstellbarkeit der Firmendaten, an denen das wirtschaftliche Überleben hing. Über 15 000 Arbeitsstunden der Mitarbeiter „verbrannten".

Während sich die von Hackern betroffenen Unternehmen meist diskret in Schweigen hüllen, legt der Weidener Firmenchef in mehreren Gesprächen mit Oberpfalz-Medien die Chronologie und die Details der Cyber-Attacke offen: Damit sich die Oberpfälzer schützen können - und es ihnen nicht so ergeht wie ihm…

Ende April 2021 schaltet der IT-Fachmann des Mittelständlers um 6.01 Uhr das System an, kann aber nicht zugreifen. Der Administrator telefoniert mit seinem Chef: „Alle unsere Daten sind verschlüsselt." Der Inhaber informiert umgehend seine Cyber-Versicherung. Wenige Minuten später meldet sich ein IT-Forensiker aus Hamburg. Der Profi wird die nächsten Wochen zum ständigen Begleiter. Der Mittelständler informiert noch am gleichen Tag die zuständige Bundesbehörde und erstattet Anzeige bei der Kriminalpolizei Weiden.

Inzwischen rühren sich die Erpresser: „If you want your data back, sent an Email within six hours." Der Firmenchef kann die Situation immer noch nicht verstehen: „Ich habe an der IT-Sicherheit nicht gespart." Ironie der Geschichte: Als erstes schalteten die Cyber-Kriminellen den Viren-Scanner aus. „Wie Diebe in der Nacht schlichen sie unbemerkt in unser System, nisteten sich auf dem Server mit ihrer Schadstoff-Software ein und spionierten die Sicherheits-Komponenten aus." Nein, es war nicht wie in einem Krimi, „sondern viel schlimmer – und real". Der Unternehmer fühlte sich gegenüber den Hackern „nackt und bloß": „Ich kannte die Erpresser nicht, wusste nicht ob es sich um Nordkoreaner, Russen, Chinesen oder Amerikaner handelt. Umgekehrt wussten die Erpresser alles über mich und meine Firma."

Schon bald herrscht Klarheit: „Wenn wir nicht zahlen, erhalten wir keine Entschlüsselungs-Keys." Der Austausch mit den Hackern erfolgt über Email. Die Kriminellen bekunden ihren Wunsch nach Kommunikation stets mit einem schlichten „hello". Sonst nichts weiter. Der Mittelständler bietet eine Teilzahlung über die Kryptowährung Bitcoin für die ersten Entschlüsselungs-Sätze an. Nach einer Woche trudelt nur der „Schlüssel" für den Printserver ein: Der Nutzen ist zwar gleich Null, aber die Erkenntnis ist jetzt da, dass die Dekryptierung funktioniert. Ein weiterer „Schlüssel" folgt, es fehlen aber noch die Wichtigsten, um die Daten restlos wiederherzustellen.

Inzwischen will die Cyber-Versicherung nicht mehr für das geforderte Lösegeld aufkommen: „wegen mangelnder Erfolgsaussicht". Der Weidener erklärt sich zu finanziellen Eigenleistungen bereit – jenseits des Versicherungsvertrags. Am 21. Tag der Erpressung geht der letzte Bitcoin auf verschlungenen Netzpfaden in die digitale Geldbörse (wallet) der Erpresser. Nach Zahlungseingang erreichen die restlichen „Keys" die Nordoberpfalz. Am 31. Tag nach der Cyber-

Attacke können 79 Prozent der Daten zugeordnet werden. „Es ist vergleichbar mit Millionen losen Seiten, die dem jeweiligen Aktenordner zugeordnet werden müssen.“ Am 34. Tag nimmt der Betrieb wieder weitestgehend die Arbeit auf.

In der heiklen Phase, in der es schlicht um die Existenz der Firma geht, „stehen meine Mitarbeiter wie Ein-Mann hinter mir“. Die Betriebsversammlung geht - angesichts Corona – im Freien über die Bühne. Die bedrohliche Cyber-Attacke schweißt die Firma wie eine große Familie zusammen. Der Chef will im Juli für seine Mitarbeiter ein Fest ausrichten. Nach vier Wochen des Hoffens und Bangens fühlt sich der Unternehmer „völlig k.o.“ Er hat kaum eine Nacht geschlafen. „Jahrzehnte , schwerer Aufbauarbeit standen auf der Kippe. Ich war emotional am Tiefpunkt. Ich habe mir jede Nacht ausgemalt, was alles fehlen könnte. Ich wusste nicht, was am nächsten Tag passiert. Das macht dich emotional fertig.“ Die Kunden-Telefonate wurden auf das mobile Geräte umgeleitet. Zahlreiche Vorgänge müssen noch abgearbeitet werden.

„Das sind professionelle Erpresser, die offenbar aus dem Dunkel des Darknetzes heraus operieren“, meint der Mittelständler. „Man kann einen Cyber-Angriff zwar nicht verhindern, aber den Schaden minimieren, indem man einen ständigen Sicherheits-Dialog mit seinem IT-Betreuer führt und Worst-Case-Szenarien probt.“ Sonst steht man - wie er - „nackt und bloß“ da.

Kommentar

Die Wirtschaft spricht nicht gerne über dieses sensible Thema. Die gehackten Unternehmen fürchten um Ansehen und Ruf. Oft wird nur Anzeige erstattet, wenn die Entschlüsselung (Dekryptierung) der Firmendaten scheitert. Wie weit das Internet bereits von Kriminellen infiltriert ist, zeigen täglich weltweit die Hiobsbotschaften von digitalen „Einbrüchen“ bei börsennotierten Unternehmen, Kliniken, Meldungen von Softwarekonzernen über immer neue Sicherheitslücken oder Daten-Klau beim Banking.

Hackerattacken auf den Bundestag oder die US-Wahlen sind gewiss spektakulär. Aber für den Bürger weit weg. Die Cyberkriminellen entdecken die Provinz für ihre Beutezüge. Jetzt müssten endgültig die Alarmglocken schrillen. Hier dominieren die mittelständischen Familienbetriebe, hier wird die IT-Sicherheit oftmals noch unterschätzt. Es geht um Existenzen. Wirtschaftlich und emoti

Die Cybercrime-Software gilt inzwischen als so ausgefeilt, dass Ermittler vom „perfekten Verbrechen“ sprechen. Bisher scheint es technisch fast unmöglich, die digitalen Spuren der Erpresser zu verfolgen. Sie verlieren sich im Dunkel des Internets. Die Aufklärungsquote sinkt.

Die Zeit läuft davon. Es gibt zwar spezielle Kommissariate der Polizei für Cybercrime und Schwerpunkt-Staatsanwaltschaften. Doch sie müssen personell und technisch so ausgestattet werden, dass sie der digitalen Bedrohung wirkungsvoll und abschreckend begegnen.

Nachgefragt

Die Polizei hält sich aus „ermittlungstaktischen Gründen“ zum aktuellen Fall im Raum Weiden bedeckt. Die Pressestelle des Polizeipräsidiums Oberpfalz verweist auf ein laufendes Verfahren.

„Bei jeder Kriminalpolizeiinspektion des Polizeipräsidiums Oberpfalz gibt es ein eigenes Fachkommissariat zur Bekämpfung von Cybercrime. Die zuständige Generalstaatsanwaltschaft Bamberg – Zentralstelle für Cybercrime – betreut hierbei diese Strafverfahren“, teilt die Pressestelle auf Nachfrage von Oberpfalz-Medien mit. „Die Täter entwickeln hier immer neue Ideen, worauf die Oberpfälzer Polizei schnell reagieren muss. Durch das globale Computernetzwerk können die Täter weltweit verdeckt und anonymisiert – auch im Ausland - vorgehen. Hierbei sind intensive Ermittlungen in enger Abstimmung zwischen den Kriminalpolizeiinspektionen und der Staatsanwaltschaft – Zentralstelle für Cybercrime - notwendig, um Tatverdächtige ausfindig zu machen.“

Wie aus der Statistik des Bundeskriminalamts (BKA) hervorgeht verdreifachte sich von 2007 bis 2020 die (polizeilich erfasste) Cyber-Kriminalität von 34 180 auf 108 474 Fälle in Deutschland. Die Aufklärungsquote sinkt beziehungsweise stagniert. Bei der digitalen Erpressung kommt immer mehr sogenannte Ransom-Software zum Einsatz. Dazu schreibt das BKA in seinem „Bundeslage-Bild“ am 10. Mai 2021: „Ransomware verschlüsselt das System und erpresst damit das Opfer. Zur Entschlüsselung wird eine digitale Lösegeldsumme gefordert, die an die Täter gezahlt werden soll. (…) Laut IT-Sec-Dienstleister Coveware stiegen die durchschnittlichen Lösegeldforderungen 2020 weiter an. Ransomware verursacht einen Schaden im mindestens sechs- bis siebenstelligen Euro-Bereich. Darin nicht enthalten: Reputationsschäden und Folgeschäden durch den Abfluss sensibler Daten.

Laut Chainalysis ist der Profit, den Ransomware-Gruppierungen im Jahr 2020 in Form von Kryptowährungen erfolgreich erpresst haben, um 311 Prozent im Vergleich zum Vorjahr gestiegen.“ Die Hacker setzten Ransom-Software mutmaßlich auch im Weidener Fall ein.

Nach Recherchen von Oberpfalz-Medien bietet das Darknet inzwischen eine komfortable Liste für digitale Erpresser-Software und Daten-Diebstahl: sowohl für den Kauf, als auch zur monatlichen Miete. Ein Banking-Trojaner ist demnach für 1000 bis 10 000 Dollar zu haben. Die Preisspanne für die digitalen Spionage-Werkzeuge reicht in der Regel von wenigen Cents bis zu ein paar Hundert Dollar.

In der Corona-Pandemie entwickelte sich das schlecht gesicherte Homeoffice zur Alternative zum besser geschützten Arbeitsplatz. Die Video-Konferenz löste die Geschäftsreise ab. Dazu berichtet das BKA, dass bereits 2020 Cyberkriminelle die Login-Daten für den Videokonferenzdienst „Zoom“ errungen haben. Gemäß eigenen Angaben habe die IT-Sicherheitsfirma Cyble im Darknet und in einschlägigen Untergrundforen Hunderttausende ausgespähter Zugangsdaten-Sätze entdeckt, die dort zum Kauf angeboten wurden. (cf)