10 Jahre
VERSICHERUNGSMONITOR

Lösegeld: „Wir verhandeln 80 bis 90 Prozent runter“

Posted By Christian Bellmann On 25. September 2023 In Abo,Allgemein,Industrieversicherung,Nachrichten,Top News,Versicherer | No Comments | Drucken

Es ist der Albtraum für ein Unternehmen: Hacker haben die Systeme verschlüsselt, drohen mit dem Löschen oder der Veröffentlichung von Daten – und fordern ein Lösegeld. Vor wenigen Jahren lagen die Forderungen noch oft im vierstelligen Bereich, inzwischen verlangen die Kriminellen sechs- oder siebenstellige Summen. Bei vielen Unternehmen haben sie damit auch Erfolg, moniert Manuel Hable von der Krisenberatung RiskWorkers. Firmen gehen Lösegeldverhandlungen seinen Beobachtungen zufolge oft völlig falsch an. Dabei können professionelle Verhandlungen die Schäden für Unternehmen und ihre Cyberversicherer erheblich reduzieren.

Manuel Hable ist Co-Gründer der Krisenberatung RiskWorkers GmbH in München

© Euroforum / Marc-André Hergenröder

Dilettantische Lösegeld-Verhandlungen nach einem Ransomware-Angriff treiben die Schadenkosten bei betroffenen Unternehmen massiv in die Höhe – beziehungsweise bei ihren Cyberversicherern, wenn die Lösegeldzahlung von der Police abgedeckt war. „Wenn ich erfahre, welche hohen Lösegelder inzwischen gezahlt werden, kann ich manchmal nur den Kopf schütteln“, sagte Manuel Hable von der Krisenberatung RiskWorkers am Rande der Jahrestagung Cyber Insurance von Euroforum. Das sei ein fataler Teufelskreis, denn so wird das „Geschäftsmodell“ für die Kriminellen immer lukrativer – und künftige Lösegeldforderungen fallen immer höher aus.

Das Problem aus seiner Sicht: Viele Unternehmen verzichten in einer solchen Situation auf die Hilfe von Experten . Sie wollen selbst mit den Kriminellen verhandeln und machen dabei einiges falsch. „Viele halten es auch für eine gute Idee, IT-Mitarbeiter die Verhandlungen führen zu lassen, weil man denkt, dass die mit den Hackern technisch auf Augenhöhe sprechen“, sagte er. Das bringe aber nichts.

Hohe Zahlungen sind die Folge – und dabei ist den Verantwortlichen gar nicht bewusst, wie viel Geld sie hätten sparen können. „Sie haben das Gefühl, sie hätten einen guten Deal gemacht, wenn sie mit den Hackern einen Rabatt von 10 Prozent ausgehandelt haben“, berichtete Hable. Dahinter stecke oft die Sorge, dass die Hacker bei einem zu niedrigen Gegenangebot die Verhandlungen abbrechen. „Dadurch machen die Unternehmen von Vornherein ein viel zu hohes

Gegenangebot."

Das genaue Schadenbild ist entscheidend

Hable geht anders vor. „Wir gehen gar nicht auf die geforderte Summe ein", sagte er. Grundlage für das Gegenangebot an die Kriminellen sollten vor allem die Fragen sein, welche Daten verschlüsselt sind und wieviel das Unternehmen für die Freigabe zahlen kann beziehungsweise zahlen will. Die Höhe hängt auch davon ab, ob das Unternehmen eine Cyberpolice mit Lösegelddeckung hat und wie schwer die Folgen der Verschlüsselung sind. Bei einem Logistikunternehmen, dessen gesamter Betrieb stillsteht, sei die Lage anders zu bewerten als etwa bei einer Firma, bei der lediglich Buchhaltungsdaten verschlüsselt sind, die Produktion aber unverändert weiterlaufen kann.

Drohen die Hacker mit der Veröffentlichung oder dem Löschen von Daten, die nicht besonders sensibel sind oder auf die das Unternehmen zur Not verzichten könnte, sei die Zahlung unter Umständen unnötig. „Das Unternehmen muss sich dann korrekt verhalten und die Veröffentlichung der Daten den Datenschutzbehörden melden, um nicht in Regress genommen zu werden", erläuterte er Hable. „Möglicherweise wird dann ein Bußgeld fällig, aber das war es dann auch."

In einigen Fällen gibt es kaum Alternativen zur Zahlung

Wenn die Hacker Systeme verschlüsselt und auch die Backups gelöscht haben oder wenn es keine funktionierenden Backups gibt, kommt es um die Lösegeldzahlung jedoch nur schwer herum. Hables Strategie besteht dann darin, mit dem Unternehmen die „Target Settlement Figure" zu ermitteln. Das ist der Betrag, den es maximal zahlen würde und außerdem schnell in Bitcoin umwandeln kann.

Von dem auf diese Weise festgelegten Betrag nennt Hable dann einen Bruchteil als Gegenangebot. Ein Beispiel: Wenn die Hacker 5 Mio. Euro fordern und das Unternehmen höchstens 1 Mio. Euro zahlen würde, bietet er 100.000 Euro an. Die Kriminellen zeigten sich dann in der Regel entrüstet, blieben aber dennoch am Ball und reduzierten ihre Forderung nicht selten direkt um die Hälfte, beobachtet der Experte immer wieder. „Wenn erst einmal 100.000 Euro auf dem Tisch liegen, läuft kein Hacker mehr weg."

Indem Hable das Gegenangebot um eine immer geringere Summe erhöht, versucht er, sich langsam dem definierten Maximalbetrag zu nähern – und im besten Fall am Ende leicht darunter zu bleiben. „Wenn wir dann doch 10.000 oder 20.000 Euro darüber auskommen, ist das auch okay, weil der Betrag dann immer noch ein Bruchteil der anfänglichen Forderung ist." Wenn Lösegeld geflossen ist, verhalten sich die Kriminellen nach Hables Erfahrung ausnahmslos zuverlässig. „Uns ist kein Fall bekannt, in dem gezahlt wurde und dann keine Entschlüsselung erfolgt ist", sagte er.

Manuel Hable startete seine Karriere in der Division Spezielle Operationen der Bundeswehr als Fallschirmjägeroffizier mit Schwerpunkt Evakuierungsoperationen. In dieser Zeit nahm er weltweit an zahlreichen Auslandseinsätzen und Übungen teil. Hable hat in Marburg ein Bachelor-Studium in Near and Middle East Studies absolviert und einen Masterabschluss in Sicherheitsmanagement von der Hochschule für Wirtschaft und Recht Berlin. Er ist vom Bundeskriminalamt als „Security Manager" zertifiziert und kann auf eine Reihe von gelösten Entführungsfällen im Ausland zurückblicken.

Wichtig sei allerdings, dass das Unternehmen keine Veränderung an den verschlüsselten Daten vornimmt, solange nicht klar ist, dass ein hundertprozentig funktionierendes Backup existiert. „Der Schlüssel passt immer nur auf die Datenstruktur zum Zeitpunkt der Verschlüsselung", erläuterte Hable. Daten, die auch nur marginal verändert wurden, können nicht mehr gerettet werden – daran können auch IT-Forensiker und selbst die Täter nichts mehr ändern. „Da reicht es schon, wenn man einen Ordner in einen anderen Ordner kopiert."

Lösegeldzahlungen sind hoch umstritten

Lösegeldzahlungen bei Cybervorfällen werden von vielen kritisch gesehen. Im vergangenen Jahr hatte sich eine Gruppe von IT-Experten in einem offenen Brief an die Bundesregierung explizit dagegen ausgesprochen. Sie forderten die Politik dazu auf, Anreize zu schaffen, die Lösegeldzahlungen bei Ransomware-Angriffen effektiv unterbinden, Lösegeldversicherungen zu verbieten und auch die steuerliche Absetzbarkeit von Ransomware-Lösegeldzahlungen nach Paragraph 33 EStG abzuschaffen.

Außerdem plädierten sie dafür, für Unternehmen ab einer bestimmten Größe eine Meldepflicht für Ransomware-Angriffe und Lösegeldzahlungen einzurichten und Versicherungen zu fördern, die die Umsatzeinbußen und Wiederherstellungsmaßnahmen absichern. Firmen, die durch Ransomware-Angriffe in finanzielle Notlage geraten, sollte der Staat „in angemessener Weise, beispielsweise

über einen Hilfsfonds" fördern, sodass diese nicht gezwungen seien, Lösegeld zu zahlen.

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Digitalverband Bitkom raten explizit von der Zahlung von Lösegeldern ab. „Nicht unwesentlich tragen auch Versicherungen zur Erhöhung der Lösegeldzahlungen bei", schreibt das Amt mit Blick auf die in den vergangenen Jahren rapide angestiegenen Forderungen. Der Versichererverband GDV ist anderer Ansicht: Ein Verbot der Zahlungen löse das Problem der Ransomware-Angriffe nicht, argumentiert er.

Cyberversicherer sollten auf Profi-Verhandler bestehen

Hable warnt davor, die Lösegeldzahlung zu verteufeln und zahlende Firmen ebenfalls in eine kriminelle Ecke zu rücken. Für viele Unternehmen sei sie der einzig praktikable Weg, um schnell wieder betriebsfähig zu werden und keine gravierende Schieflage oder sogar eine Pleite zu riskieren. „Das Geschäft ist für die Kriminellen nicht deshalb so lukrativ, weil die Firmen Lösegeld zahlen, sondern weil sie denken, dass man über die Höhe nicht verhandeln kann", sagte er. „Für mich ist die Zahlung eines professionell verhandelten Lösegeldes aber das einzige Mittel, mit dem der gesamte Markt auf einem stabilen Level gehalten werden kann."

In Deutschland ist es Versicherern erlaubt, Lösegelddeckungen anzubieten. In Ländern, in denen das verboten ist, etwa in Italien, ist zu beobachten, dass Unternehmen diese Deckungen bei Anbietern in anderen Ländern einkaufen. Auch deshalb hätte ein Verbot hierzulande nur eine begrenzte Wirkung.

Unverständlich findet Hable es allerdings, dass es immer noch Cyberversicherer gibt, die Unternehmen bei den Verhandlungen freie Hand lassen. „Ich verstehe nicht, wie man einem Kunden eine Lösegelddeckung verkaufen kann, ohne verpflichtend einen Krisenberater zur Seite zu stellen, der professionell das Lösegeld verhandelt." Bei Policen, die Lösegeld bei Entführungen absichern, sei der Einsatz solcher Experten obligatorisch. „Wenn der Kunde da selbst verhandelt will, entfällt die Deckung."

Mehr zum Thema:

- Ransomware-Schäden nehmen wieder zu [1]
- Cyberversicherer müssen Lösegeld zahlen [2]
- Cyber: Ransomware bleibt bedrohlichstes Risiko [3]

Das Umdenken bei den Versicherern habe langsam eingesetzt, sei aber schmerzhaft gewesen. „Die Versicherer haben sich hier in den vergangenen Jahren Schäden sehr sauer eingekauft", berichtete Hable. Dienstleister wie RiskWorkers seien zunehmend bei Lösegeldversicherern fest integriert. „Die Versicherer erkennen immer mehr, dass das in ihrem eigenen Interesse ist." Er spürt einen Anstieg der Anfragen von den Leitern der Schadenabteilungen. Sie wollen dringend etwas daran ändern, dass Unternehmen bei selbst organisierten Verhandlungen nicht selten die gesamte Deckungssumme ausschöpfen.

Christian Bellmann
