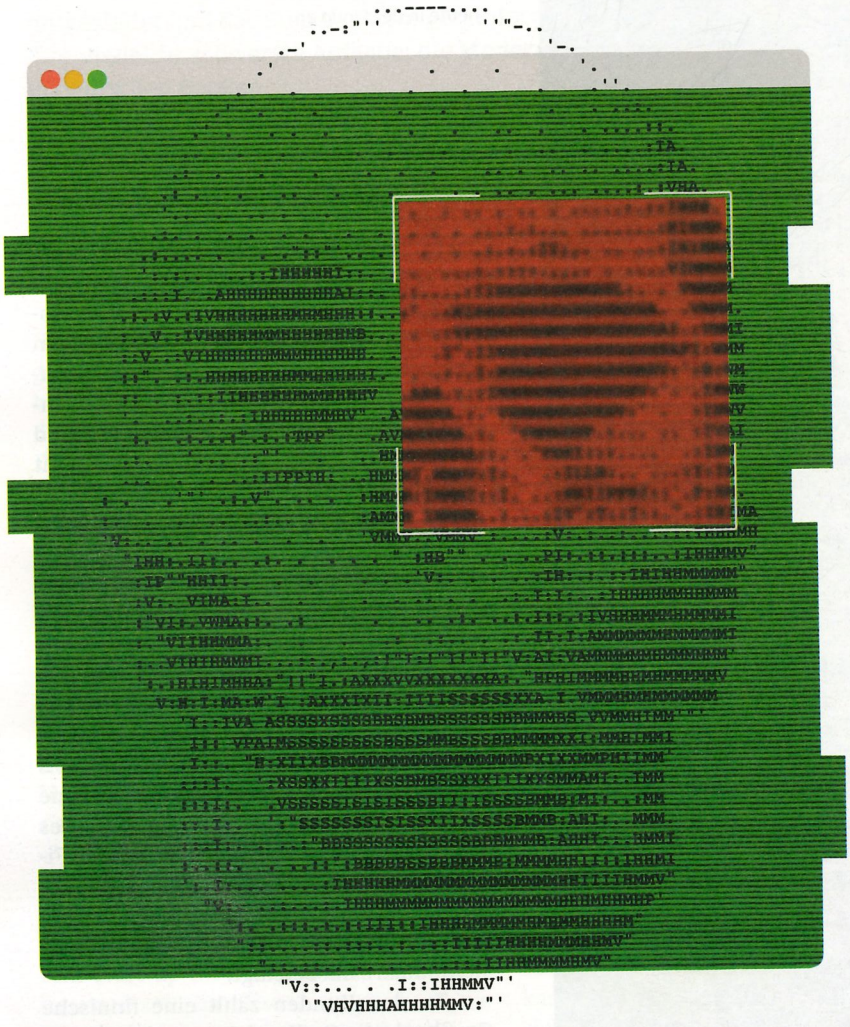
Spezial

Cybersecurity



Reden Sie nie darüber!

Pizza, Bluffs und Packpapier – mit welchen **Verhandlungstricks** Profis Lösegelder nach Cyberattacken drastisch reduzieren.

TEXT CLAUDIA TÖDTMANN

Wenn René Schumann einen Einsatz übernimmt, ist höchste Eile vonnöten und Diskretion oberstes Gebot. Sein erstes Mittel der Wahl: Packpapier. Damit klebt Schumann Fenster und Glastüren ab, sobald er den sogenannten War-Room bezieht, aus dem er Verhandlungen mit Erpressern führt. Weder Belegschaft noch Medien sollen erfahren, dass die Firmen, für die Schumann tätig wird, Opfer eines Hackerangriffs geworden sind. Meist schottet sich das Verhandlungsteam in einem Zimmer in der Vorstandsetage ab. Es kann Tage dauern, bis das Team aus externen Verhandlern, IT-Chef sowie dem Justiziar des Unternehmens den War-Room wieder verlässt.

Schumann, Dreitagebart, das dunkle Haar akkurat gescheitelt, leitete Verhandlungsteams etwa beim Autokonzern Daimler, bevor er sein Unternehmen Negotiation Advisory Group gründete. Heute wenden sich an ihn verzweifelte Manager aus allen möglichen Branchen, die nur der Grad an Verzweiflung eint. Nicht selten hängt das Überleben des Unternehmens von der Funktionsfähigkeit ihrer IT ab. Weil sie sonst nicht wieder lieferfähig sind, keine Rechnungen schreiben oder Aufträge annehmen können. Fast immer haben Hacker Daten gestohlen oder IT-Systeme verschlüsselt. Die Entsperrcodes gibt es nur gegen Lösegeld, oft in Millionenhöhe, zahlbar in Bitcoin oder anderen Kryptowährungen. „Verzweifelte Manager rufen fast immer zwischen 19 und 3 Uhr nachts an, wenn ihnen klar wird, dass sie nicht mehr weiterkommen“, erzählt Schumann. Er muss dann eine Einigung mit den Erpressern organisieren: zügig, unauffällig und so günstig wie eben möglich. Es ist ein Rennen gegen die Zeit, denn meist setzen die Angreifer kurze Fristen von 24, 48 oder 72 Stunden.

Eine Strategie gegen jeden Expertenrat

Nachdem sie sich lange auf Großunternehmen konzentriert hatten, attackieren die Hacker in letzter Zeit gezielt kleinere Opfer: Stadtverwaltungen, Krankenhäuser wie die Düsseldorfer Uniklinik oder Mittelständler wie den Farbenproduzenten Marabu. 2019 lag der Schaden durch Erpressungsprogramme, sogenannte Ransomware, laut IT-Verband Bitkom bundesweit bei rund 10,5 Milliarden Euro. Tendenz stark steigend. Das Bundeskriminalamt nennt „Ransomware die größte Bedrohung für Unternehmen und öffentliche Einrichtungen“.

Der Albtraum beginnt fast immer montagmorgens. Wenn im Büro erste Rechner streiken, sich Kundendatenbanken nicht mehr öffnen und Maschinen nicht mehr bedienen lassen, haben die Hacker das Wochenende genutzt, um die IT-Systeme ihrer Opfer zu verschlüsseln. Werde nicht gezahlt, so drohen die Cyberkriminellen, landen die erbeuteten Daten auf Marktplätzen im Darknet. Mal dauert es Stunden, manchmal Tage, doch irgendwann wird den Betroffenen klar, dass die Verschlüsselungen nicht auszuhebeln sind. Es schlägt die Stunde von Spezialisten wie René Schumann. Er übernimmt Aufgaben, die jedem Expertenrat widersprechen: Bei Erpressungen zu zahlen würde nur das Geschäft befeuern und neue Attacken nach sich ziehen, warnen Polizei und BKA. Bloß: Das mag für die gesamte Volkswirtschaft richtig sein, einem einzelnen Unternehmen, das plötzlich vor dem Ruin steht,

ILLUSTRATION: PATRICK ZEH FÜR WIRTSCHAFTSWOCHE

hilft diese Strategie wenig. Und so rufen sie lieber einen wie Schumann.

„Die Kommunikation mit den Chefs läuft über externe Dienste wie LinkedIn oder WhatsApp", sagt Schumann. „Sonst könnten Täter, die in die IT-Systeme eingedrungen sind, beim Austausch via Firmen-E-Mail mitlesen, was wir planen." Verhandelt wird meist schriftlich über Chatplattformen, die Sprache ist Englisch – und viel passiert nachts. Erpresserbanden agieren oft aus anderen Zeitzonen. Mitunter wird gar rund um die Uhr gerungen. Dann bleibt fürs Team oft nur ein Nickerchen auf der Liege im Erste-Hilfe-Raum der Firma. Essen gibt's vom Lieferservice.

Schumann gibt sich gegenüber Erpressern stets als Mitarbeiter des Unternehmens aus. „Wichtig ist, dass der Ton professionell und wertschätzend bleibt", betont Schumann, der im Chat nicht einmal Begriffe wie „Erpresser" oder „Lösegeld" benutzt. Keinesfalls will er die Gegenseite verärgern. Sonst bestehe die Gefahr, dass sich die Täter nach der Lösegeldzahlung rächen und Daten löschen. „Es gibt ja keine Sicherheit, dass sich die Täter an die Abmachung halten", sagt er. Am Ende sind auch Deals mit Erpressern Vertrauenssache.

Wie es gelingen kann, das Lösegeld zu drücken, hänge entscheidend davon ab, ob er es mit Einzeltätern oder einer Bande zu tun habe, so Schumann. Wenn auf der anderen Seite organisierte Erpressungsprofis sitzen, darf es bis zur Einigung nicht allzu rasch gehen. Akzeptiere ein Unternehmen die Forderungen zu schnell, „gleicht das einer Einladung an die Hacker, erneut Geld zu fordern". Also schindet der Profi bewusst Zeit. Mal erklärt er, man müsse noch mit der Bank verhandeln, oder es dauere noch, die Bitcoins zu besorgen. Einzeltäter hingegen wollten das Geld oft schnell, sie hätten weniger Durchhaltevermögen als arbeitsteilige Organisationen, so Schumann. „Einzelne Täter kann ich teils auf die halbe Summe herunterhandeln." Manchmal sogar noch deutlich weiter: Einem Angreifer, der zwei Millionen Euro forderte, schrieb der Experte, 50 000 Euro könne er sofort freigeben, alles andere müsse er sich erst von seinem Chefs genehmigen lassen. Kurz Zeit später bekam er die Entsperrcodes – und das Lösegeld war auf ein Vierzigstel gedrückt.

Für solche Deals, für Nachtschichten und Soforteinsätze berechnen die Verhandlungsprofis Tagessätze, manchmal zuzüglich Erfolgsprovision. Je nach Dauer der Fälle fließen 20 000 Euro bis 100 000 Euro, sagt Christian Schaaf. Er arbeitete früher als Experte für Wirtschaftskriminalität und als verdeckter Ermittler bei der Polizei. Heute übernimmt auch er als Chef der Sicherheitsberatung Corporate Trust Verhandlungsmandate für Erpressungsopfer. Und ganz zum Schluss, wenn die Entschlüsselung funktioniert, die IT wieder läuft und der War-Room geräumt ist, hat Experte Schaaf noch einen entscheidenden Rat für alle Unternehmen, damit sich der Albtraum nicht wiederholt: „Nie darüber reden, dass man gezahlt hat. Denn das lockt nur die nächsten Erpresser an." ■

10,5

Milliarden Euro
Schaden verursachten 2019 Angriffe mit Erpressungssoftware in Deutschland laut IT-Verband Bitkom