Neue Zürcher Zeitung

Wie ein Schweizer KMU ohne Lösegeld, dafür mit Militärtaktik einen Hackerangriff überlebt hat

Cyber-Attacken auf Unternehmen nehmen zu. Die meisten Opfer versuchen, nichts davon an die Öffentlichkeit dringen zu lassen. Beim Handelsunternehmen Offix ist das anders.

Christin Severin
10.7.2019, 06:00 Uhr

Der Hacker-Angriff auf den Bürobedarf-Grossisten Offix kommt aus dem Nichts. Zuerst leise, am Anfang unterschätzt. Dann trifft er das Unternehmen jedoch mit ungebremster Wucht. Für Offix geht es ums Überleben. Die Holding mit den Töchtern Ecomedia, Oridis und Papedis beliefert den Fach- und den Detailhandel mit Bürobedarfsartikeln.

Den Lebensnerv getroffen

An einem Donnerstagabend fängt es harmlos an. Die IT-Mitarbeiter entdecken Unregelmässigkeiten. Übermässig beunruhigt sind sie nicht, sie meinen, die Probleme bald wieder in den Griff zu bekommen. Über Nacht jedoch verschlechtert sich die Lage. Als die ersten Mitarbeiter morgens um 6 Uhr ins Büro kommen, haben sie keinen Zugang mehr zum Intranet. Um 6 Uhr 45 ist klar: Das IT-System liegt am Boden, kein Server ist sichtbar, die Mitarbeiter können ihre Arbeit nicht erledigen.

Im Laufe des Vormittags wütet das über Malware eingeschleuste Virus weiter. Gegen 10 Uhr ist Offix-CEO Martin Kelterborn klar, dass man IT-mässig «nichts mehr habe». Datenbanken sind gelöscht und zahlreiche Server auf Werkseinstellung gestellt. Noch schlimmer ist, dass viele Schnittstellen, über die Grosskunden ihre Bestellungen automatisch eingeben, ebenfalls gelöscht sind. Offix verliert die Übersicht über die Auftragseingänge und Verkäufe.

Hacker fordert hohes Lösegeld

Der anonyme Hacker stellt eine Lösegeldforderung: 45 Bitcoins (zu jenem Zeitpunkt umgerechnet rund 350 000 Fr.) soll das Unternehmen mit 230 Mitarbeitern und einem Jahresumsatz von 250 Mio. Fr. zahlen. Dafür, so verspricht der Hacker, würde er die Verschlüsselung wieder aufheben und den Zugang zu den Daten freigeben. Das Unternehmen befindet sich im Schockzustand. Kelterborn besinnt sich auf seine Zeit im Militär, das Reglement TF 95 (Taktische Führung) und schaltet auf Kriegszustand. Im Unternehmen werden ein «War Room», ein Kommandoposten und militärisches Vokabular etabliert.

Dem ehemaligen Oberleutnant bei den Panzergrenadieren und Stellvertretendem Kompaniekommandant Kelterborn wird klar, dass Offix die Sache nicht allein bewältigen kann. Er beauftragt einen externen Cybercrime-Spezialisten von InfoGuard, informiert die eidgenössische Melde- und Analysestelle Informationssicherung (Melani) und reicht Anzeige bei der Polizei ein. Am Freitag um 16 Uhr informiert Offix Kunden und Lieferanten über eine grössere technische Störung. Die Kunden werden mit Blick auf die Folgewoche gebeten, weitere Bestellungen via Telefon, Fax oder notfallmässig neu aufgesetzte Mail-Adressen aufzugeben. Anschliessend geht das ganze Unternehmen komplett offline.

Für das Kader und die IT ist das Wochenende abgesagt. Am Samstagmorgen kommen immer mehr schlechte Nachrichten von der IT. Das Virus steckt fast überall; alles ist infiziert, keine Datenbank ist mehr brauchbar. Das Krisenteam kauft 20 Laptops, die Geschäftsleitung setzt neue Mail-Adressen auf, und das Marketing baut unter Hochdruck eine neue Website. So gibt es wenigstens einen Kanal für die Kommunikation mit der Aussenwelt.

Zu diesem Zeitpunkt ist nicht klar, wie Offix mit der Lösegeldforderung umgehen will. Die Meldestelle des Bundes empfiehlt zwar, nicht auf die Erpressung einzugehen. Nur wenn die Hacker damit erfolgreich sind, lohnt sich ihr Geschäftsmodell. Gleichzeitig weiss man in der Fachstelle, dass viele Firmen doch zahlen. Grosse Unsicherheit herrscht aber auch deshalb, weil Offix nicht weiss, was das Unternehmen für das Lösegeld bekommen würde. Viele Applikationen sind zerstört. Daher hilft das Entschlüsseln der Daten-Back-ups alleine nicht viel.

Ein glücklicher Zufall

Am Ende eines harten Samstages realisieren die IT-Spezialisten, dass der Hacker einen Fehler gemacht hat. Anstatt alle Wege hinter sich zu zerstören, hat er, bildlich gesprochen, eine Brücke stehen lassen. Über diese gelingt es Offix, einen Teil der Daten wiederherzustellen. Zudem hat das Unternehmen Glück im Unglück: Ein IT-Spezialist hat nur wenige Wochen zuvor eine wichtige Applikation aus eigener Initiative auf einer externen Festplatte gespeichert. Diese Daten sind nun quasi Gold wert. Zum ersten Mal erwacht bei den Anwesenden die Hoffnung, dem Hacker vielleicht doch die Stirn bieten zu können. Für 22 Uhr ordnet Kelterborn Arbeitsschluss an. Abschalten ist angesagt.

Am Sonntagmorgen geht es weiter. Das Wichtigste ist jetzt, dass das Unternehmen am Montag in der Lage ist, wieder Ware zu verkaufen. «Der Verkauf ist unser Lebensnerv», sagt Sandra Hurter, Leiterin Marketing und Beschaffung. Der Markt ist hart umkämpft. Wer nicht Tag für Tag pünktlich liefert, hat keine Chance. Nach drei Wochen wären wohl auch die treusten Kunden weg und die Konventionalstrafen enorm. Das würde Offix erledigen oder zumindest um Jahre zurückbinden.

Am Montag bestellt Kelterborn per SMS alle Mitarbeitenden auf 7 Uhr zur «Befehlsausgabe». Der Geschäftsleiter macht den Ernst der Lage unmissverständlich klar: «Wir befinden uns im Krieg. Jemand will uns zerstören, aber wir holen uns unsere Firma zurück.» Der Einkauf erhält die Order, den Verkauf nach allen Kräften zu stützen. Die Mitarbeitenden rufen jeden einzelnen Kunden an und nehmen die Bestellungen auf. Der Ablauf ist weniger automatisiert, aber das Unternehmen ist am Markt und kämpft ums Überleben.

In den nächsten zwei Wochen pendeln Geschäftsleitung und Mitarbeiter zwischen Kommandostelle und den verschiedenen Firmensitzen hin und her und versuchen, «ihr» Unternehmen zu retten. Immer wieder gibt es Rückschläge zu verkraften.

Am Montag stellt Offix fest, dass die alten Faxnummern, die das Unternehmen an die Kunden geschickt hat, nicht mehr funktionieren. Die neuen Notfall-E-Mail-Adressen sind nicht für den Massenversand gemacht. Nach dem Verschicken der ersten 50er-Mail-Pakete wird Offix als Spammer eingestuft. Die Mails an die vielen Kunden müssen einzeln verschickt werden. Ein einfaches Microsoft-Zertifikat wurde nicht rechtzeitig erneuert, was zu einer Virenwarnung auf der Website eines Tochterunternehmens führte – alles Ereignisse, die in einer solchen Situation enorm stressig sind.

Nachdem die Systeme weitgehend durchgescannt sind, meldet die eidgenössische Meldestelle Melani, dass noch immer ein «bad guy» aus Offix herausfunke. Man überprüft, sucht und findet das Virus versteckt im Bereich Wareneingang auf einem alten Touchscreen-Computer. Von diesem aus hätte es in den Nächten zuvor zu seiner Sendezeit um 23 Uhr 45 mit dem Hacker Verbindung aufnehmen und Befehle entgegennehmen können. Die offene Flanke wird so schnell wie möglich isoliert und unschädlich gemacht.

Ein perfider Trick

Die IT entdeckt, wie das Virus vermutlich aktiviert wurde: Der Hacker hatte sich in einen realen E-Mail-Verkehr mit einem Kunden eingeklinkt und sich quasi vor den Kunden geschoben. Als vermeintlicher Kunde verwies er auf sein erhöhtes Sicherheitsprofil und forderte den Offix-Mitarbeiter zur Zertifizierung auf. Nur so könne er die von Offix geschickte Datei öffnen. Mit einem Klick auf einen Link kam der Mitarbeiter der Aufforderung nach und schleuste damit das Virus ein.

Kelterborn und sein Team versuchen, dem Hacker auf die Spur zu kommen. Diese verliert sich jedoch schnell. Die Lösegeldforderung wurde von einem Mail-Account von Proton verschickt, einem Schweizer Anbieter für sichere und verschlüsselte Mail-Kommunikation. Offenbar wurde dessen Dienstleistung vom Hacker missbraucht. Anders als Banken, wo die Anforderungen an die Compliance mittlerweile hoch sind, müssen Tech-Firmen ihre Kunden nicht kennen.

Täglich schreitet die Rekonstruktion des IT-Systems voran, sukzessive werden die Computer der Mitarbeiter wieder an das System angehängt. Nach gut drei Wochen schaltet die Firma auf die normale Organisation zurück. Ob der Hacker bewusst Offix angegriffen hat oder das KMU ein Zufallsopfer war, weiss man bis heute nicht. Sicher ist aber, wie Kelterborn erklärt, dass der Angriff, nachdem er erst einmal lanciert worden war, nicht automatisch ablief, sondern eine oder mehrere Personen gezielt Schaden anrichteten.

Viel gelernt

Von den Kunden habe Offix in der schwierigen Zeit eine enorme Solidarität erfahren, sagt Geschäftsleitungsmitglied Sandra Hurter. Anstatt abzuspringen, hätten sie weiterhin bestellt und damit das Unternehmen am Leben gehalten. Der Zusammenhalt der Mitarbeitenden gegen den äusseren Feind sei beeindruckend gewesen. Offix hat nach eigener Einschätzung viel aus dem Cyber-Angriff gelernt. «Wir dachten, unsere IT-Sicherheit sei in einem Topzustand», kommentiert Kelterborn. Diese Einschätzung sei falsch gewesen. Inzwischen plant das Unternehmen, sich selber anzugreifen, um Schwachstellen zu erkennen.

Es sei zudem ein Fehler gewesen, davon auszugehen, dass man als mittelständisches Handelsunternehmen kein Angriffsziel sei. Jeder könne ein Target sein, so Kelterborn. Anders als viele andere Unternehmen, die zum Ziel eines Hacker-Angriffs wurden, versteckt sich Offix heute nicht, sondern teilt die Erfahrungen und Erkenntnisse. Andere können daraus für sich ihre eigenen Schlüsse ziehen. Das Lösegeld hat Offix, wie Kelterborn sagt, übrigens nicht bezahlt. Durch seinen «Brücken-Fehler» und das externe Back-up hatte der Hacker ohnehin sein Faustpfand verloren.

Warum es sich für Firmen lohnen kann, Lösegeld an Cyber-Kriminelle zu zahlen

Schweizer Firmen geraten zunehmend ins Visier von Cyber-Kriminellen. Obwohl der Bund davon abrät, dürften sich zahlreiche von Ransomware betroffene Unternehmen auf Lösegeldforderungen einlassen.

Stefan Häberli / 17.6.2019, 16:49

Die Kriminalität im Internet nimmt zu – die Schweiz plant mehrere Cybercrime-Zentren

Cyberkriminalität nimmt in der Schweiz rasch zu. Die Täter attackieren in kurzer Zeit extrem viele Opfer im ganzen Land. Doch die Polizeistrukturen in der Schweiz stammen aus dem letzten Jahrhundert. Neue Kompetenzzentren sollen die Ermittler schneller und schlagkräftiger machen.

Daniel Gerny / 2.2.2018, 05:30