Wie eine Firma durch einen Cyberangriff aus den Fugen gerät

Kriminalität im Internet Über Nacht verschlüsseln Hacker Daten eines Familienunternehmens in Meilen. Der Fall der Rolf Schlagenhauf AG zeigt, wie schnell eine Firma zum Opfer von Cyberkriminellen wird.

Nicola Ryser

Hatte nervenaufreibende Tage hinter sich: Rolf Schlagenhauf, Geschäftsführer der Rolf Schlagenhauf AG in Meilen. Foto: Manuela Matt

Noch vor dem «Zmorge» mit Gipfeli und Kaffee klingelt das Telefon. Rolf Schlagenhauf ahnt bereits, wer am anderen Ende der Leitung ist. Tags zuvor hat er gemerkt, dass die internen Computersysteme in seinem Unternehmen nicht mehr rundlaufen. Und darum Kontakt aufgenommen mit dem Provider, dem Systemanbieter seiner Firma. Als Schlagenhauf sich dann an diesem Samstagmorgen nicht mehr ins Mail einloggen kann, da befürchtet er Schlimmes.

Er nimmt den Anruf entgegen, der Provider ist dran. Nun ist klar, was die Probleme verursacht: ein Cyberangriff.

Die Rolf Schlagenhauf AG ist ein Familienunternehmen. Spezialisiert auf Malerarbeiten, Umbau, Fassaden und Bodenbeläge, befindet sich die Firma mit Rolf Schlagenhauf als Geschäftsführer in der dritten Generation. In Meilen ist seit 1934 der Hauptsitz, weitere Standorte sind unter anderem in Zürich, Winterthur und Zug. Die Digitalisierung hat in der Firma in den letzten Jahren Einzug gehalten, Kundenkontakt und Aufträge laufen vermehrt über IT-Systeme und das Internet.

Doch dann kommt der 26. Februar – und plötzlich funktioniert fast gar nichts mehr.

Beispiel in Meilen ist kein Einzelfall

E-Mails, Dokumente in Word oder Excel, Firmendaten werden über Nacht unzugänglich, sind mit Passwörtern versiegelt. Die Spezialisten des Providers reagieren rasch, fahren alle Systeme runter. Schlagenhauf kontaktiert derweil eine Cyber-Security-Firma.

Solche gibt es zahlreiche in der Schweiz, auch am Zürichsee. Eine davon ist die Oneconsult AG in Thalwil. Ihre Dienstleistungen: Sie berät Firmen bezüglich der IT-Sicherheit, simuliert Hackerangriffe als Tests und hilft bei Cyberattacken.

Tobias Ellenberger, Chief Operating Officer von Oneconsult, sieht im Beispiel von Meilen keinen Einzelfall. «Der Trend ist deutlich zunehmend, von überall aus der Schweiz werden wir wegen Cyberangriffen kontaktiert.» Gemäss Jahresbericht der polizeilichen Kriminalstatistik wurden im letzten Jahr landesweit 24'398 Straftaten im digitalen Bereich registriert. Ein Grossteil davon, fast 85 Prozent, wird der Cyber-Wirtschaftskriminalität zugeordnet.

Sei früher vor allem die Finanzindustrie von Cyberattacken betroffen gewesen, gerieten heute durch die Digitalisierung auch andere Branchen wie Industrie- oder Gesundheitsunternehmen ins Visier, erklärt Ellenberger. Opfer werden dabei nicht nur die grossen Betriebe mit Hunderten Mitarbeitern, sondern auch KMUs. «Vieles, wenn nicht alles – insbesondere geschäftskritische Prozesse – läuft bereits seit Jahren übers Internet und den Computer. Das macht verwundbar.»

Wenn dann eine Attacke erfolgt, wenn Computer- und Serversysteme nicht mehr funktionieren, sei es sinnvoll, neben dem IT-Dienstleister eine Cyber-Security-Firma zurate zu ziehen. «Wir sind dann wie die Feuerwehr. Wir erhalten einen Anruf, rücken bei Bedarf aus und helfen, das Chaos möglichst rasch unter Kontrolle zu bringen», erklärt Ellenberger. In der Regel wird dann, abhängig von der Art des Angriffs und der betroffenen Firma, eine Strategie festgelegt. Je nach Szenario versuchen die Spezialisten, den ursprünglichen Zustand wiederherzustellen. Oder sie begeben sich auf Spurensuche, beispielsweise indem sie falsche Fährten legen, um so die Urheber des Angriffs zu finden.

«Ich kann mir kaum vorstellen, dass die Angreifer jemals geschnappt werden. Die könnten irgendwo auf der Welt sein.»

Rolf Schlagenhauf
Geschäftsführer der Rolf Schlagenhauf AG

Stillstand an den ersten zwei Arbeitstagen

Im Meilemer Fall konsultiert Schlagenhauf eine Cyber-Firma in Zug. Innerhalb kurzer Zeit gehen deren Forensiker gemeinsam mit dem Provider dem Ursprung des Angriffs nach, verständigen die Cyber-Abteilung der Kantonspolizei und die zuständige Stelle des Bundes, das Nationale Zentrum für Cybersicherheit (NCSC).

Derweil herrscht in der Rolf Schlagenhauf AG fast Stillstand. Auf den Baustellen wird zwar normal gearbeitet. Die Administration aber kann nur eines: warten. Schlagenhauf kommuniziert intern mittels SMS, mit Kunden per Telefon. «Die Spezialisten liessen die Server langsam wieder hochfahren, aber an den ersten zwei Arbeitstagen lief bei uns im Backoffice gar nichts», erklärt Schlagenhauf. Erst am Mittwoch kann der Betrieb wieder vollständig aufgenommen werden. Fünf Tage, nachdem erste Symptome im Computersystem aufgetreten waren.

Unter anderem kann Schlagenhauf wieder auf seine Mails zugreifen. Sogleich fällt ihm eine Nachricht in seinem Posteingang auf. Es ist ein Erpressermail. «Auf Englisch verlangten die Erpresser 270'000 Dollar in Bitcoins.» Zahle Schlagenhauf das Lösegeld, würden alle Daten wieder zugänglich sein. Kooperiere er jedoch nicht, würden die Erpresser der Firma schaden.

Im Original: «We will damage your business as much as possible.»

Bei Erpressung: Reagieren oder ignorieren?

Dies sei das typische Businessmodell hinter solchen sogenannten Ransomware-Attacken, sagt Tobias Ellenberger von der Oneconsult AG. «Entweder drohen die Erpresser, die Daten verschlüsselt zu lassen oder abgezogene, empfindliche Daten zu veröffentlichen – oder gar beides.» In der Regel gelte für die Betroffenen die Empfehlung, nicht auf die Erpressung einzugehen.

Doch nicht immer ist die Antwort so simpel. Ellenberger relativiert: «Wenn Existenzprobleme in den Vordergrund rücken, beginnt man abzuwägen.» Insbesondere bei kleineren Unternehmen, die finanziell instabil sind. Denn auch eine Wiederherstellung aller Systeme und Daten durch Spezialisten koste Geld.

Wiederum solle man sich zweimal überlegen, das Lösegeld zu zahlen, drohten doch ethische oder juristische Konflikte. «Man will weder terroristische Gruppierungen finanzieren noch seinen eigenen Ruf schädigen.» So oder so sei es darum wichtig, einen IT-Partner oder die Polizei bei diesem Grundsatzentscheid miteinzubeziehen, sagt Ellenberger.

Die Spezialisten raten Schlagenhauf, nicht auf die Erpressung einzugehen. Auch weil keine sensitiven Daten auf dem Spiel stehen. Da die Firma täglich ein Back-up durchführt, also regelmässig ihre Daten sichert, sind nur Daten vom Tag des Angriffs verloren gegangen. «Das war für uns nicht so schlimm, dieses Risiko hatten wir vorab einkalkuliert», sagt Schlagenhauf.

Ohnehin hätte sich der Geschäftsführer nicht vorstellen können, Lösegeld an Kriminelle zu zahlen. Stattdessen erstattet er Anzeige. Denn die Spezialisten der Cyber-Firma und des Providers konnten im Verlauf der Woche eruieren, woher der Angriff mit grosser Wahrscheinlichkeit stammen könnte. Generell rät die Kantonspolizei, schon kleinere Vorfälle der zuständigen Kapo-Stelle sowie Anzeigen zu Cyberangriffen auf dem Polizeiposten zu melden.

Eine gute Vorbereitung ist alles

Die Krux: Die Angriffe erfolgen meist aus dem Ausland. So sind die Erfolgschancen einer Anzeige nicht allzu hoch. Das sieht auch Ellenberger von der Oneconsult AG. «Dahinter stecken nicht zwei Typen in einem Hoodie, sondern meist ganze Unternehmen. Das ist organisierte Kriminalität auf technologisch hohem Niveau.»

Schlagenhauf reicht bei der Kantonspolizei in Meilen Anzeige ein, die Staatsanwaltschaft wird mit der Causa beauftragt. Zuversichtlich ist jedoch auch Schlagenhauf nicht: «Ich kann mir kaum vorstellen, dass die Urheber jemals physisch geschnappt werden. Die könnten irgendwo auf der Welt sein.»

Am Ende ist dies für Schlagenhauf und seine Firma jedoch nur von geringer Bedeutung. Sie sind mit dem Verlust von wenigen Daten – die entstandenen Kosten sind noch nicht definiert – glimpflich davongekommen. Warum? «Wir waren zum Glück gut vorbereitet», sagt Rolf Schlagenhauf.

Durch die nervenaufreibenden Tage habe man einiges dazugelernt und plane dementsprechend, die eigene IT-Sicherheit weiter zu erhöhen. Nebst den täglichen Back-ups wolle man mehr Barrieren schaffen, beispielsweise mit der Einführung einer Anmeldung per Zwei-Faktor-Zertifizierung: Zuerst gibt man das Passwort am Computer ein, dann bestätigt man einen SMS-Code auf dem eigenen Handy. Der Geschäftsführer will zudem die Mitarbeitenden noch mehr auf die Thematik sensibilisieren, zum Beispiel im Umgang mit Phishingmails, also gefälschten Nachrichten von fingierten Firmen, deren Links man keinesfalls anklicken darf.

«Heute kann jede Firma oder Privatperson Opfer von Cyberangriffen werden», sagt Schlagenhauf. Vorbereitung sei darum alles. Man müsse wissen, was im Falle eines Angriffs zu tun ist und wen man kontaktieren soll. «Und sich die Frage stellen: Wie viel will ich investieren, beispielsweise in eine Versicherung, und wie viel bin ich bereit, in Kauf zu nehmen?»

Die Rolf Schlagenhauf AG war bereit, im Extremfall einen Tag an Daten zu verlieren. Nun ist genau das passiert.