Hackerangriff ließ Telefonkosten von 200 auf 10.000 Euro steigen

Ein kleines österreichisches Unternehmen wurde vom Internet-Dienstleister nach einer Cyber-Attacke heftig zur Kasse geben. Das Höchstgericht spielte dabei aber nicht mit.

STEPHAN KLIEMSTEIN

In den meisten österreichischen Betrieben wird heute im Festnetz über das Internet telefoniert, ohne es zu wissen.

BILD: SN/GAJUS - FOTOLIA

„Phreaking" wird das Hacken von Telefonanlagen genannt. Kriminelle verschaffen sich dabei Zugang in das System der Telefonanlage und wählen – meistens unbemerkt in den Nachtstunden – kostenpflichtige Mehrwertnummern an, die sie zuvor im Ausland installiert haben. Während bei den gehackten Unternehmen die Telefonkosten in die Höhe schießen, ist es für Betrüger ein höchst lukratives Geschäft.

Auch ein österreichisches Unternehmen, das Dienstleistungen im Bereich Schülernachhilfe und Studentenkurse anbietet, wurde Opfer einer solchen Attacke. Durchschnittlich betrugen die Rechnungen für Grundentgelte und Verbindungsentgelte im Monat 210 Euro, wobei eine Gebührenanzeige über die aktuellen Kosten auf den IP-Telefonen nicht vorhanden war.

2014 wurde die Telefonanlage der Firma über eine ägyptische IP-Adresse gehackt. Überwiegend nachts und in den frühen Morgenstunden wurden Verbindungen ins Ausland getätigt – nach Grönland, Thailand, Eritrea, Elfenbeinküste, Bosnien-Herzegowina, Serbien, Burkina Faso, Zentralafrika, Mali, Benin und Kuba. Entdeckt wurde der Betrug erst mit der Monatsabrechnung, die allein für den Zeitraum Jänner 10.160,14 Euro betrug. Nachdem das Unternehmen die Rechnung nicht bezahlte, wurde die Sache gerichtsanhängig.

Im Verfahren behauptete die Klägerin (das ist der Internet-Dienstleister) nebenvertragliche Schutz- und Sorgfaltspflichten. Das heißt, der Kunde habe die Pflicht, die Entwicklung der Telefongebühren zu überwachen. Diese Aufgabe würde den IT-Dienstleister überfordern, weil dieser nicht „Beherrscher der Gefahr" sei. Eine Warnung vom vorliegenden Hackerangriff gab es nicht und auch eine Sicherheitssperre wurde vom Provider nicht errichtet, weil man hierzu nicht verpflichtet sei.

Die Klägerin stellte der Beklagten Festnetz- und Internetverbindungen (ISDN-Anschlüsse) für ihre Telefonanlage zur Verfügung. Das geklagte Unternehmen verwendet eine Telefonanlage, die über zwei Netzwerkanschlüsse, eine integrierte Firewall, zwei analoge Anschlüsse für ein portables Funktelefon und ein Fax sowie über die Möglichkeit zur Errichtung eines virtuellen privaten Netzwerks verfügt.

Der Oberste Gerichtshof (OGH) stellte nun fest: Der Abschluss eines Vertrags lasse nicht bloß Haupt-, sondern auch Nebenpflichten entstehen, nämlich insbesondere Schutz- und Sorgfaltspflichten. Auf diese Weise soll eine möglichst reibungslose Abwicklung des Vertragsverhältnisses gewährleistet werden. Nach Ansicht des OGH war die Gefahr eines Hackerzugriffs für den IT-Dienstleister insofern beherrschbar, als es ihm sowohl personell als auch technisch leicht möglich gewesen wäre, durch Gebührenmonitoring und eine entsprechende Warnung die Folgen des Angriffs zu verhindern. Solche Schutzmaßnahmen könnten inzwischen vollautomatisiert und ohne Personaleinsatz vorgenommen werden. Das betroffene Unternehmen hingegen hatte keine Möglichkeit, die Gefahr einer Cyber-Attacke durch interne Vorkehrungen abzuwenden, denn die Basiseinstellungen an der Telefonanlage, die ein Drittunternehmen installiert hatte, ließen sich nicht verändern.

Im Ergebnis hält der OGH technisch leicht umsetzbare Maßnahmen zur Abwehr von Hackerangriffen für durchaus zumutbar. Es überspanne die Schutz- und Sorgfaltspflichten keineswegs, derartige Sicherheitsmaßnahmen zu ergreifen. Im Gegenteil: Eine Verletzung dieser Verpflichtungen macht den Provider unter Umständen sogar schadenersatzpflichtig.

Zudem sind Leistungen nicht zu vergüten, wenn, wie im vorliegenden Fall, Schutz- und Sorgfaltspflichten verletzt werden. Hätte man gebotene Sorgfalt eingehalten, wären die Telefonkosten, die durch den Hackerangriff verursacht wurden, nicht angefallen, betonten die Höchstrichter.

Obwohl der Internetanbieter den Hackerangriff wesentlich früher wahrgenommen hat oder jedenfalls hätte er ihn früher als die Kundin wahrnehmen können, hat er es unterlassen, den Angriff abzuwehren. Auch wurde nicht rechtzeitig gewarnt. Die eingeklagte Rechnung musste daher nicht bezahlt werden.

Stephan Kliemstein ist Rechtsanwalt in Salzburg (Zumtobel Kronberger Rechtsanwälte)

Daten & Fakten
Wie wir über Internet telefonieren

Schon jetzt telefonieren Millionen Österreicher über das Internet. Und das oft ohne es zu wissen. Laut A1 basiert ein Großteil der Telefonanlagen österreichischer Firmen auf IP-Telefonie, also auf Anrufen, die über Computernetzwerke und nicht über die Telefonleitungen funktionieren. Der Nutzer selbst merkt davon nur wenig, da meist nur die Anlage und nicht das Telefongerät selbst ausgetauscht wird.

Die sogenannte IP-Telefonie ist beispielsweise im A1-Festnetz mittlerweile Standard. „ Jeder A1-Festnetzkunde telefoniert also inzwischen (indirekt) per Internet.