Die Kehrseite von All-IP

Hacker-Angriffe auf Telefonanlagen

Mit der All-IP-Umstellung wird das Telefon immer öfter zum Tatort. Hacker nutzen dabei zahlreiche Angriffsmuster und richten Schäden in Milliardenhöhe an.
Meist geschehen die Angriffe nachts, am Wochenende und an Feiertagen: Hacker dringen in die Telefonanlagen ein und verursachen durch Anrufe an kostenpflichtige Rufnummern Schäden, die häufig – wenn überhaupt – erst bei der nächsten Telefonrechnung bemerkt werden.
Dieser Voice Fraud genannte Gebührenbetrug ist beileibe nicht das einzige Angriffsszenario rund ums Telefon. Beim „Identity Fraud“ etwa telefonieren Hacker auf Kosten Dritter, beim „Call ID Spoofing“ nutzen sie eine bekannte Rufnummer, etwa die der IT-Abteilung, um beim Angerufenen Vertrauen zu erwecken und zu gutgläubigen Transaktionen zu bewegen. Das kann der Rückruf über eine hochpreisige Rufnummer sein, aber auch die Preisgabe von Firmengeheimnissen.
Beim „SIP Registration Spoofing“ melden Hacker im SIP-Registrar ein unberechtigtes Endgerät mit falscher Identität an, um es dann für weitere Attacken zu nutzen. Manchmal werden auch Fraud- und Spoofing-Methoden kombiniert.
Wie einträglich dieses Hacking sein kann, rechnet Achim Hager, CEO von HFO Telecom, vor: „Meist befindet sich die angerufene Servicenummer im Ausland, ein Anruf kostet zum Beispiel 4,00 Euro pro Minute. Der Hacker ist Inhaber der Nummer und bekommt ein Kick-Back von 2,50 bis 3,00 Euro pro Minute überwiesen – Fraud ist damit eine Lizenz zum Gelddrucken.“
Genaue Zahlen über die bei ihnen entstandenen Schäden wollen die Netzbetreiber nicht nennen. Ein Sprecher des Münchner Regio-Carriers M-net gibt allerdings einen Anhaltspunkt: „Voice Fraud verursacht bei uns einen nicht unbeträchtlichen Schaden. 2017 belief er sich auf eine Summe im sechsstelligen Bereich. Zu den monetären Schäden kommen natürlich noch die internen Aufwände für die Erkennung, Aufklärung und Lösung der Fraud-Fälle hinzu.“

Geschäftskunden und private Nutzer im Visier

Grundsätzlich sind von Fraud-Attacken sowohl gewerbliche Anschlussnutzer als auch Privatkunden betroffen – bei M-net hat man aber beobachtet, dass der Schaden im Privatkundenbereich vergangenes Jahr nahezu stagnierte, während er im Geschäftskundenumfeld deutlich angestiegen ist.
Weltweit entsteht der Telekommunikationsindustrie laut der Communication Fraud Control Association (CFCA) ein Schaden von rund 30 Milliarden Dollar. Die Dunkelziffer dürfte noch um einiges höher sein: Hacker-Angriffe, bei denen es über einen längeren Zeitraum nur zu kleineren Schäden kommt, werden oft erst spät oder überhaupt nicht bemerkt.
Entwarnung ist nicht in Sicht – im Gegenteil. Markus Schneider, Director Operation, Implementation & Customer Care bei Toplink, geht davon aus, dass durch die All-IP-Umstellung die Fraud-Attacken zunehmen. „Durch die öffentlich im Internet stehenden Systeme sind die in den Firmen oftmals nachlässig administrierten Anlagen und Sicherheitsmechanismen per Remote wesentlich leichter zu hacken als im klassischen ISDN-Telefonsystem“, betont er. Eine Meinung, die man bei der Telekom nicht teilt, obwohl auch die Bonner von einer Verlagerung der bisherigen Angriffe auf Routerhacking, Identitätsdiebstahl und Call ID Spoofing ausgehen.

Anomalien-Monitoring

Die Netzbetreiber arbeiten seit Jahren hart daran, die Schäden zu begrenzen. Im Zentrum stehen dabei Monitoring-Tools, mit denen der Datenverkehr gescannt und auf Anomalien überprüft wird. „Alarm wird zum Beispiel dann ausgelöst, wenn in gewissen Abständen immer wieder die gleichen Rufnummern in bestimmte Länder angewählt werden. Oder wenn innerhalb eines bestimmten Zeitraums eine außergewöhnlich hohe Summe für Telefongespräche überschritten wird“, erklärt Carina Panek, Leiterin Regulierung und Fraud Management bei der QSC AG. Dazu sind bei den meisten Netzbetreibern Expertenteams im Einsatz, die den Telekommunikationsverkehr ebenfalls auf Anomalien überprüfen.
Toplink entwickelt seit vielen Jahren im Rahmen von Forschungsprojekten gemeinsam mit der Hochschule Darmstadt Fraud-Erkennungssysteme auf Basis von Anomalien. Trusted Telephony, so der Name des ersten Projekts, ermöglicht das frühzeitige Erkennen und Abwehren von Fraud-Attacken. Allerdings ist der Einsatz von Trusted Telephony nur in Verbindung mit einem SIP-Trunk von Toplink möglich. Im zweiten Projekt – TrustCom – geht Toplink noch einen Schritt weiter: Die Lösung soll Fraud erkennen, noch bevor er stattfindet. Grundlage bilden Erkennungsmuster, die Anomalien
im Verbindungsaufbau schon wesentlich früher feststellen sollen.
QSC bietet Wiederverkäufern den Service Resale Fraud Control an. Damit können sie für ihre Kunden individuelle Kriterien wie etwa durchschnittliche Telefongebühren festlegen. Werden diese überschritten, wird ein Alarm ausgelöst, und QSC verspricht, den Anschluss in maximal zwei Stunden zu blockieren. Zwar haben die Hacker dann immer noch zwei Stunden Zeit, um ihre Ziele anzugreifen – aber zumindest kann der Schaden damit etwas begrenzt werden.
Mittel gegen Voice Fraud

- **Passwortschutz für die TK-Systeme:** Für persönliche Sprachboxen sollten vom Nutzer individuelle Passwörter vergeben werden – und die werksseitige Voreinstellung geändert werden. Sind im System DISA-Nebenstellen mit Durchwahlmöglichkeiten für Heimarbeitsplätze oder als Einwahlmöglichkeit vorhanden, so müssen diese ebenfalls geschützt werden.
- **Einrichten von Sperrlisten:** Mit sogenannten Blacklists können Zielrufnummern und Rufnummerngruppen – beispielsweise für kostenpflichtige Servicenummern oder für bestimmte Länder – gesperrt werden. Das kann entweder im TK-System geschehen oder auch beim Anschlussnetzbetreiber beantragt werden.
- **Warnzeichen erkennen:** Mit regelmäßigem Monitoring können Unternehmen erkennen, ob es Auffälligkeiten im Verbindungsaufkommen gibt.
- **Regelmäßige Updates:** Verbesserte Software-Versionen mit Sicherheitsbezug sollten möglichst zeitnah eingespielt werden.
- **Auch kleine Lücken schließen:** Hacker können Töne abfangen und so in ein System eindringen. Deshalb sollte auf die Ausgabe von Tönen bei der Eingabe eines Passworts oder einer PIN verzichtet werden.
- **Mitarbeiter sensibilisieren:** Ein Security-Guide sowie die Benennung eines Datenschutzbeauftragten sorgen für mehr Achtsamkeit bei den Mitarbeitern und erhöhen den Schutz.

Für HFO-Chef Achim Hager ein wichtiger Schritt, der aber nicht ausreicht – zumal nicht alle Netzbetreiber diesen Service anbieten. „Aktuell hat jeder Carrier eigene Maßnahmen zur Fraud-Bekämpfung entwickelt. Die Resultate dieser Analysen werden aber nicht immer schnell genug an die Wholesale-Partner weitergeleitet“, erklärt er. Die Folge: Da fast jeder Anbieter auch Leistungen von Wholesale-Partnern einkauft, entsteht die Gefahr, dass

Anomalien zwar erkannt, aber die Reseller nicht schnell genug über die Gefahr informiert werden – am Ende hat der Hacker mehr Zeit für seine Attacken, und die Schäden sind höher als eigentlich nötig.
HFO-Chef Hager, der vor knapp einem Jahr in den Vorstand des DVTM (Deutscher Verband für Telekommunikation und Medien) gewählt wurde, möchte deshalb über den Verband einen runden Tisch zum Thema Fraud ins Leben rufen. Ziel ist, so Hager, gemeinsam einen Kodex zu entwickeln, um Betrug zu bekämpfen. Und am Ende könnten sich die Netzbetreiber, aber auch Systemhäuser und Unternehmen, gegen Fraud versichern, wenn sie sich an den Kodex halten. Ob es je so weit kommt, ist aber offen. Bis dahin wird es bei den Insellösungen der Netzbetreiber bleiben – und Unternehmen und Systemhäuser tun gut daran, sich und ihre Kunden so weit wie möglich gegen das Hacken ihrer Telefonanlagen zu schützen. Die Instrumente sind bekannt, allerdings werden sie allzu oft ignoriert – bis ein Kunde zum Opfer wurde.