Pressemitteilung

VSE NET entwickelt in Kooperation mit 3M intelligenten Schutz für Telekommunikations-Netze

30.07.2015

Die Telekommunikationsnetze werden durch die Umstellung auf IP wirtschaftlicher und leistungsfähiger – aber auch anfälliger für IT-Sicherheitslücken, die bereits im großen Stil für Telefonie-Betrug ausgenutzt werden. Schutzmaßnahmen basieren bisher auf der nachträglichen Analyse solcher Angriffe. Anschließende Sperren betrügerischer Zielrufnummern sind allerdings zunehmend wirkungslos. Die VSE NET hat ein Fraud Mechanismus entwickelt, der Angriffsversuche in Echtzeit abwehren soll. In Kooperation mit 3M Services wird den Kunden damit ein innovativer Schutzansatz geboten.

Mit dem sogenannten „International Revenue-Share Fraud“ (IRSF) nutzen Angreifer Sicherheitslücken in den Netzen und Endgeräten. Spezielle IP- bzw. SIP-Scanner (Internet Protocol bzw. Session Initiation Protocol) durchsuchen die Netze nach verwundbaren Zugängen in IP-fähigen Geräten wie Nebenstellenanlagen (PBX), Gateways oder Teilnehmer-Endgeräten (CPE). Anschließend wird durch den Angreifer Telefonverkehr generiert und dieser über den Telefonanschluss des Geschädigten auf eigene oder gemietete internationale Rufnummern gelenkt. Die ahnungslosen -Kunden finden auf ihren Rechnungen dann teure Verbindungen beispielsweise zu internationalen Mehrwertdiensten (Revenue-Share). Die Carrier bleiben dann meistens auf den Kosten sitzen. Alle Versuche, die Täter zu ermitteln und die erbeuteten Rechnungsbeträge zurück zu erhalten, sind regelmäßig erfolglos.

Fraud wird sich vervielfältigen
„Bei den Angriffen auf IP- und TDM-Endgeräte stehen wir erst am Anfang und wir erwarten, dass sich die Fraud-Fälle vervielfältigen werden. Deshalb hat unsere Technik eine wirksame Anti-Fraud-Lösung entwickelt, um für die Zukunft gut gerüstet zu sein“, begründet Michael Leidinger, Geschäftsführer der VSE NET, sein Engagement. „Im Verbund mit dem Stromanbieter VSE AG und den RWE-Konzern gehört es bereits zu unseren Aufgaben, für höchste Datensicherheit und den Schutz von kritischen Infrastrukturen zu sorgen. Deshalb haben wir den Anspruch, durch Anwendung innovativer Technologien auch beim Fraud-Schutz Vorreiter zu sein“, so der Geschäftsführer.

Viele regionale oder Citycarrier setzen selbst erstellte Anti-Fraud-Lösungen ein und hoffen darauf, damit den Schaden in Grenzen halten zu können. Dabei werden die Kommunikationsdatensätze (Call Data Record, CDR) des eigenen Billingsystems auf mögliche Schadensfälle untersucht. Wird ein Missbrauch erkannt, kommt die Zielrufnummer auf eine Sperrliste und ist für künftige Angriffe nicht mehr nutzbar. Zu diesem Zeitpunkt ist der Schaden allerdings schon entstanden und die professionell organisierten Angreifer verwenden beim nächsten Mal bereits andere Zielrufnummern, um Rufnummernsperren und Schutzmechanismen für bestimmte Rufnummerngassen zu umgehen. Die Carrier sind mit dem CDR-Ansatz deshalb meistens einen Schritt zu spät.

Der bisherige Ansatz ist auch für viele Geschäftskunden problematisch. Globale Sperrungen von kompletten Rufnummerngassen oder ganzen Ländern können auch den normalen Geschäftsbetrieb behindern und führen zu großer Unzufriedenheit mit dem Service des Carriers.

Anti-Fraud-Schutz in Echtzeit
Die VSE NET, ein regionaler Telekommunikationsanbieter aus Saarbrücken, gehört zu den Innovatoren bei der Entwicklung neuer Schutzmechanismen gegen den Missbrauch von IP-Netzen. In Kooperation mit dem Dienstleister 3M Services wurde die von VSENET entwickelte Software, die ungewöhnliches Telefonieverhalten bereits während des Gesprächs erkennt, umgesetzt. „Der bisherige Schutz ist nicht mehr ausreichend. Wir brauchen eine proaktive Lösung, die Fraud erkennt, bevor die Calls bei teuren Zielrufnummern landen“, beschreibt der Geschäftsführer den neuen Ansatz. Zunächst wollte der Carrier die entwickelte Software als Add-on zum IN-System (Intelligentes Netz) einsetzen. „Die gemeinsame Lösung mit 3M Services hat deutliche

Vorteile, denn sie ist integraler Bestandteil der IN-Plattform. Dadurch vermeiden wir zusätzliche Schnittstellen und weiteres Equipment“, bestätigt Michael Leidinger.

Bei dem neuen Ansatz werden die Calls aus den drei EWSD- und zwei Softswitch-Telefonvermittlungssystemen der VSE NET über das IN-System des Carriers geleitet. Die Anti-Fraud-Lösung ist ein zusätzliches Software-Modul der intelligenten Netztechnik. Das Modul ist darauf ausgerichtet, ungewöhnliches Telefonieverhalten (Anomalien) in Echtzeit zu erkennen. Der Telefonverkehr wird dafür systematisch analysiert, um sowohl bereits identifizierte betrügerische Rufnummern als auch unbekannte Angriffe abzuwehren. Dazu wird der Telefonverkehr anhand statistischer Verfahren nach den typischen Merkmalen von Fraud-Angriffen untersucht.

Wichtige Anhaltspunkte zur Erkennung betrügerischer Angriffe sind beispielsweise eine Vielzahl von Anrufen in kurzer Zeit in einen bestimmten Rufnummernbereich und die Dauer dieser Gespräche. Mit der Anti-Fraud-Lösung werden für solche Szenarien Schwellwerte zu Anrufhäufigkeit und Anrufdauer festgelegt. Wenn das System ungewöhnliche Calls identifiziert, greifen die Schutzmechanismen des Anti-Fraud-Managements. Die als problematisch erkannten Rufnummernbereiche werden automatisch blockiert und der weitere Telefonverkehr in diese Bereiche verhindert. Dabei werden auch die verursachenden A-Rufnummern erkannt und von der Verwendung des Zielbereiches ausgeschlossen. Bei Bedarf können diese Sperren manuell wieder freigegeben werden. Als zusätzliche Maßnahme hat der Carrier die Software so eingestellt, dass bei individuell einstellbaren Schwellwerten pro Gasse das eigene Operating Center alarmiert wird, um ggf. Fehlalarme und irrtümliche Sperrungen zu vermeiden.

Fraud-Management als Kundenservice
Das neue Fraud-Management ist für die VSE NET auch ein individualisierbares Service-Produkt für Geschäftskunden. „Letztlich geht es beim Fraud-Schutz darum, Calls zeit- und ortsabhängig nach festgelegten Kriterien zu lenken und zu terminieren. Mit dem IN-System verfügen wir dafür über eine sehr leistungsfähige Plattform.“, erläutert der Geschäftsführer. So kann der Fraud-Schutz für jeden Geschäftskunden individuell als Kundenprofil konfiguriert und gespeichert werden. Schwellwerte für Auslandskontakte werden dann sehr eng an den tatsächlichen Erfordernissen des Unternehmens ausgerichtet. Bereits genutzte Zielrufnummern, die bisherige Anrufhäufigkeit und Anrufdauer des Unternehmens in einzelne Länder lassen sich individuell berücksichtigen. So können bei Unternehmen mit einem eigenen Software-Profil, Angriffe besser verhindert und globale Sperren von Rufnummerngassen vermieden werden.

Das Fraud-Management-System ist lernfähig
Das Fraud-Modul wird bei VSE NET schrittweise optimiert. Zunächst erfolgt eine sehr detaillierte Differenzierung nach Ländern und Zielrufnummerngassen. Nach der Auswertung des bisherigen Telefonieverhaltens wird ein Normalbetrieb definiert und mit den Merkmalen typischer Fraud-Angriffe werden Schwellwerte festgelegt. Im nächsten Schritt werden diese Grenzwerte in einem Testbetrieb überwacht und auf die Wirksamkeit hin überprüft. Es geht zunächst darum, Fehlalarme und unnötige Sperren zu vermeiden und zu hohe und zu niedrige Schwellwerte anzupassen. Erst anschließend kommt das Fraud-Management zum Echteinsatz. „Das Fraud-Software-Modul wird laufend nachjustiert und die Kriterien weiter verfeinert. Das System sammelt ständig neue Erfahrungen und wird dadurch laufend besser. Wir werden es den Angreifern immer schwerer machen“, zeigt sich der Geschäftsführer optimistisch.

Quelle: VSE NET