GEBÜHRENBETRUG

VERDEUTLICHUNG DER NOTWENDIGKEIT, DIE KOMMUNIKATIONSSYSTEME EINES UNTERNEHMENS ZU SCHÜTZEN

ANWENDUNGSHINWEIS

Alcatel·Lucent
Enterprise

INHALTSVERZEICHNIS

EINFÜHRUNG

Betrugsdelikte gegenüber Telekommunikationsdienstanbietern, Telefonisten, Teilnehmern und Unternehmen nehmen zu. Diese Zunahme ist darauf zurückzuführen, dass Betrüger aus dem Fehlen einer effektiven internationalen Telekommunikations-Regulierungsbehörde bzw. von Durchsetzungsmechanismen in Verbindung mit Sicherheitslücken in den Telekommunikationssystemen von Unternehmen Kapital schlagen können.

KUNDENSZENARIEN

1. Der IT-Manager eines Unternehmens entdeckt einen rapiden Anstieg bei internationalen Ferngesprächen in ein Land, mit dem gar keine Geschäftsbeziehungen bestehen – außerhalb der normalen Bürozeiten.

2. Der monatliche Abrechnungsbericht eines anderen Unternehmens zeigt ein erhebliches Anrufaufkommen an internationale Rufnummern – von ein und demselben internen Apparat.

3. Ein Geschäft mit 20 Mitarbeitern erhält eine monatliche Telefonrechnung, die so hoch ist wie die Rechnungen der letzten drei Jahre zusammen.

4. Ein Unternehmen erhält von seinem Telefonisten einen Betrugsalarm – gleichzeitig entdeckt man mehrere, regelmäßige kurze Anrufe bei einer Mehrwertnummer.

Verluste durch Betrug sind seit 2011 auf 15,4 % gestiegen

WAS IST PASSIERT?

Diese Szenarien sind Beispiele von Kunden, die Opfer eines Gebührenbetrugs geworden sind. Alle Unternehmen, von kleinen Büros bis hin zu multinationalen Unternehmen, sind potentielle Opfer, unabhängig von ihrem jeweiligen Kommunikationssystemanbieter. Und die Zahl der Angriffe steigt rapide.

Gebührenbetrug ist die nicht genehmigte Nutzung eines Kommunikationsdienstes durch unbekannte Dritte. Dabei kann es sich um Scammer handeln, die Gesprächsminuten zu Fernrufnummern über eine unverdächtige Instanz (beispielsweise eine kompromittierte TK-Anlage) weiterverkaufen. Ein weiteres Beispiel ist ein Mehrwertdienstbetrug, bei dem ein Kommunikationssystem oder -dienst ausgenutzt wird, um Anrufe an bestimmte internationale Servicerufnummern zu tätigen, die von dem betreffenden Teilnehmer Gebühren pro Minute oder pro Anruf erheben.

Geschätzte Verluste durch Betrug nach Hacken von TK-Anlagen im Jahr 2013:

4,4 Milliarden US-Dollar (USD)*

Betrug kann gewaltige finanzielle Verluste verursachen, bevor er entdeckt wird – im schlimmsten Fall kann ein voller Monat vergehen, bis der Abrechnungsbericht eingeht und der Betrug entdeckt wird. Betrug kann auch den Ruf eines Unternehmens schädigen: Es gibt Berichte von Fällen, in denen Kunden, die ihren persönlichen Berater anrufen wollten, stattdessen mit einem in keinem Zusammenhang damit stehenden – und möglicherweise verfänglichen – Mehrwertdienst verbunden wurden. Darüber hinaus können derartige Betrügereien durch Überlastung der Kommunikationsserverkapazitäten die Verfügbarkeit von Telefoniediensten beeinträchtigen und so möglicherweise zu einem vollständigen Dienstausfall führen.

Warum nimmt der Telekommunikationsbetrug zu?

Die Ausbreitung sozialer Netzwerke und sozialer Medien hat es extrem einfach gemacht, „Rezepte“ zu erstellen und zu verteilen – kurze Videoclips und Tutorials, die erklären, wie Kommunikationssysteme kompromittiert werden. Es sind nur sehr beschränkte Telekommunikationskenntnisse erforderlich, um auf nicht genehmigte Dienste zugreifen zu können und Geld aus Kommunikationsanwendungen zu schlagen, die eine anvisierte Unternehmensressource nutzen.

Darüber hinaus verfügen Kommunikationssysteme zwar über integrierte Schutzmechanismen, doch werden die Sicherheitsempfehlungen der Hersteller häufig nicht vollständig umgesetzt und Konfigurationen werden auf Grund eines mangelnden Gefahrenbewusstseins nicht optimiert. Diese Nachlässigkeiten bei der Sicherheit können das Hacken erleichtern.

Und schließlich sind Unternehmen mit alternden Systemen potentiell stärker durch diese Arten von Bedrohungen gefährdet.

Wie arbeiten Betrüger?

In der Regel erlangen Betrüger von außerhalb eines Unternehmens durch Sicherheitslücken unbefugten Zugriff auf ein Kommunikationssystem. In der Vergangenheit hackten sich Betrüger unter anderem direkt über die Wartungsschnittstelle in eine TK-Anlage, aber die Techniken haben sich weiterentwickelt und umfassen nun die Umleitung von Sprachanwendungen und das Austricksen von Endteilnehmern, was es schwierig macht, Anrufer zu verfolgen und zu ermitteln, da der betreffende Anruf von einer „vertrauenswürdigen Instanz“ statt von einem Betrüger zu kommen scheint.

Zu den gängigsten Methoden gehören:

Fernwartung

Hacker ermitteln ein an eine Wartungsschnittstelle angeschlossenes Modem und versuchen, sich mit dem Standardpasswort anzumelden, das Administratoren oft versäumen zu ändern. Einmal im System können die Hacker die Konfiguration sowie Anmeldenamen und Passwörter beliebig ändern.

Voicemail

Diese Methode zielt auf Voicemail ab, die durch Ausnutzung einer mangelhaften Passwortkontrolle gehackt wird. In der Regel zielt ein Angriff darauf ab, das Voicemail-System zum Tätigen abgehender Anrufe bei Mehrwert- oder Fernrufnummern zu nutzen. Telekonferenzbrücken mit Konferenzfunktionen für mehrere Leitungen stellen hier die primären Ziele dar.

Anrufsperre

Neben einer mangelhaften Passwortstrategie profitieren Hacker außerdem von laschen Anrufkontrollen, die ihrer Wardialer-Software einen Freibrief geben, unbegrenzt Anrufe bei Mehrwert- oder Fernrufnummern zu tätigen.

DISA (Direct Inward System Access)

Dieser für Telearbeiter gedachte Dienst ermöglicht Mitarbeitern von entfernten Standorten aus den Zugriff auf interne Telefondienste. Böswillige Benutzer können die TK-Funktionalität ganz oder teilweise remote nutzen, wenn der DISA-Dienst unzureichend geschützt ist (z. B. ein einziger Zugriffscode, keine Kontrolle der Anruferkennung).

Externe Übergabe, externe Weiterleitung

Externe Telefonfunktionsrechte bieten – wenn sie nicht ordnungsgemäß eingerichtet sind – Hackern die Möglichkeit, bequem Betrugsszenarien zu entwickeln. Einige Taten erfordern jedoch einen Komplizen innerhalb des betreffenden Unternehmens.

WAS MOTIVIERT BETRÜGER?

Zwar kann Gebührenbetrug genutzt werden, um die finanzielle Gesundheit eines Unternehmens oder den Ruf eines Mitbewerbers zu schädigen, in den meisten Fällen geht es jedoch um finanzielle Gewinne. Alcatel-Lucent hat Beispiele erlebt, bei denen Betrüger in vier Stunden 20.000 US-Dollar (USD) erbeutet haben – schnelles und leicht „verdientes“ Geld. Betrüger kann es auch in einem Unternehmen geben, beispielsweise unehrliche Mitarbeiter, die von der Aussicht gelockt werden, Unternehmensressourcen zur persönlichen Bereicherung umzulenken.

Zur beliebtesten Betrugsmethode hat sich das Hacken von TK-Anlagen entwickelt*

ERMITTLUNG DER SCHWACHSTELLEN EINES UNTERNEHMENS

Werden dieselben Systempasswörter seit mehr als einem Jahr benutzt?

Verwenden Endbenutzer ein standardmäßiges Voicemail-Passwort?

Sind Modems mit dem Kommunikationsserver verbunden?

Dürfen alle Endbenutzer auf internationale Rufnummern zugreifen?

Werden Benutzern außerhalb des Unternehmens Telefondienste zur Verfügung gestellt?

Hat es im Systemadministrationsteam vor Kurzem personelle Veränderungen gegeben?

KANN EINE DIESER FRAGEN MIT „JA“ BEANTWORTET WERDEN, DEUTET DAS AUF EIN MÖGLICHES RISIKO HIN.

SCHUTZ VON KOMMUNIKATIONSSYSTEMEN

Die Anwendung von Alcatel-Lucent-Schutzmechanismen und Best Practices auf Kommunikationssysteme hilft sowohl bei der Optimierung der Konfiguration als auch der Sicherheit und verhindert zahlreiche Gebührenbetrugsszenarien.

Ergreifen Sie angemessene Sicherheitsmaßnahmen

- Anrufsperre: Beschränken Sie abgehende Anrufe außerhalb der Geschäftszeiten, verlangen Sie die Eingabe von Passwörtern bei Ferngesprächen und untersagen Sie den Anruf von Mehrwertnummern.
- Überprüfen Sie die Passwortrichtlinien: Ändern Sie standardmäßige Systempasswörter und wiederholen Sie diesen Vorgang regelmäßig (z. B. monatlich).
- Implementieren Sie einen externen Übergabe- und Weiterleitungsschutz.
- Prüfen Sie Zuständigkeiten und Administratorrechte.
- Aktualisieren Sie die Systemdatenbank, indem Sie Daten ehemaliger Endbenutzer entfernen.

Stärken Sie das Bewusstsein im Unternehmen

- Unterrichten Sie Mitarbeiter über die grundlegenden Sicherheitsmaßnahmen und die entsprechenden Auswirkungen (z. B. rechtliche und finanzielle Risiken) sowie über ihre Rechte und Pflichten.
- Erinnern Sie Mitarbeiter an sinnvolle Verhaltensweisen hinsichtlich Vertraulichkeitsregeln, beispielsweise niemals unbekannten Anrufern technische Details über Daten- und Kommunikationssysteme mitzuteilen (z. B. persönliche Codes, Namen sowie Durchwahlnummern für IVR- und Voicemail-Dienste).
- Entwickeln Sie Kampagnen zur Betrugserkennung: Fordern Sie Ihre Mitarbeiter auf, ungewöhnliches Verhalten oder Aktivitäten bei Telefoniediensten zu melden, einschließlich seltsamer Nachrichten auf Voicemailboxen, besetzter Leitungen am frühen Morgen und Anrufprotokollen mit mehreren Ferngesprächen außerhalb der Geschäftszeiten.

Nutzen Sie die Fachkenntnisse Ihres Business Partners und von Alcatel-Lucent

- Halten Sie Softwareversionen auf dem neuesten Stand, um von den jüngsten Produktverbesserungen und Technologieentwicklungen zu profitieren.
- Stärken Sie Lösungen, indem Sie Best Practices für die Sicherheit implementieren.
- Installieren Sie die neuesten Sicherheits-Patches des Herstellers.
- Beurteilen Sie regelmäßig die Gefahr von Gebühren- und Mehrwertnummernbetrug für das Kommunikationssystem.

* Quelle: Communications Fraud Control Association, Studie für 2013

Alcatel·Lucent Enterprise