Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 78 (2000)

Heft: 9

Artikel: Bekämpfung von Betrug in Telekommunikationsnetzen

Autor: Nauer, Bernhard / Pfau, Alex / Ressenig, Alfred

DOI: https://doi.org/10.5169/seals-876481

Securitymanagement

Bekämpfung von Betrug in Telekommunikationsnetzen

Betrug ist in allen menschlichen Gesellschaftsformen anzutreffen. So tritt auch in der Telekommunikation immer häufiger der Fall ein, dass bei Nutzung öffentlicher Netze und Dienste anfallende Gebühren vorsätzlich nicht entrichtet werden. Beispiele hierfür sind die Nutzung falscher Identitäten bei der Subskription oder die Verwendung manipulierter Telefonkarten.

BERNHARD NAUER, AXEL PFAU, ALFRED RESSENIG, BERN

Eine weitere Betrugsvariante funktioniert auf Basis der Premium Rate Services (PRS) oder Mehrwertdienste. Dabei wird beispielsweise mit den 0190- oder den zukünftig eingesetzten 0900er-Nummern illegal «Geld verdient». Die Zeitschrift «Telecom & Network Security Review» (April 1997) schätzt, dass im Jahr 1997 durch Betrug in Telekommunikationsnetzen allein in den USA Schäden von rund 4 Mia. US-$ entstanden. Die Tendenz ist steigend. Die durchschnittliche Schadenshöhe eines Betreibers schätzt man auf rund 1 bis 3% des Gebührenaufkommens.

Betrug tritt nicht nur in öffentlichen Netzen, sondern zunehmend auch in privaten Netzen und Nebenstellenanlagen auf. In diesem Artikel geht es jedoch um Betrugsbekämpfung im Zusammenhang mit den öffentlichen Telekommunikationsnetzen.

Betrugsszenarien in öffentlichen Telekommunikationsnetzen

Exakte Zahlen über Betrug zu erhalten ist schwierig. Zum einen sind die Betreiber nicht daran interessiert, dieses Problem in der Öffentlichkeit zu diskutieren. Zum anderen fällt die Unterscheidung zwischen willentlichem Betrug – etwa, wenn Gebühren nicht entrichtet werden – und bestehenden Zahlungsschwierigkeiten schwer. Die Zahlen für das Betrugsaufkommen weichen daher je nach Einschätzung deutlich voneinander ab. Sie geben dennoch relativ guten Aufschluss über die grosse Schadenshöhe und deren beträchtliche Steigerungsrate.

Zwei Beispiele mögen dies veranschaulichen:

- Nach dem erwähnten Bericht in der Zeitschrift «Telecom & Network Security Review», stieg die Betragssumme in den Telekommunikationsnetzen der USA von 2 Mia. US-$ im Jahre 1994 auf geschätzte 4 Mia. US-$ im Jahre 1997 (Bild 1). Das bedeutet einen Anstieg der Schadenshöhe um 100%. Dies lässt sich dahingehend interpretieren, dass es in diesem Zeitraum verstärkt gelang, Schwachstellen zu erkennen und gezielt zu nutzen. Das Anwachsen des Betrugs ist zudem ein Zeichen dafür, dass entsprechende Gegenmassnahmen nicht oder in einem zu geringen Umfang ergriffen wurden. Möglicherweise verfehlten sie auch die gewünschte Wirkung.

Der Betrugsschwerpunkt liegt in den USA beim Fernverkehr, da aufgrund der existierenden Tarife in diesem Bereich für Betrüger die besten «Geschäftsmöglichkeiten» bestehen. Im Falle der Calling Cards lassen sich ebenfalls mangelnde Sicherheitsmassnahmen und ein zu geringes Kundensicherheitsbewusstsein als Ursachen für den hohen Verlustanteil feststellen.

Untersuchungen von Chorleywood Consulting Ltd. beschreiben Einnahmeverluste der Betreiber – aufgeschlüsselt nach Diensttypen und geografischen Regionen (Tabelle 1). Beim Vergleich der Regionen fallen die überproportional grossen Verluste im Mobilfunk Nordamerikas auf. Die Verluste lassen sich vor allem auf einen sehr hohen Anteil analoger Systeme mit zu geringen Sicherheitsstandards zurückführen.

Vergleicht man die Aufschlüsselung der Verluste für 1995 in Bild 1 mit Tabelle 1, dann stellt man fest:

- Die Grössenordnungen sind ähnlich. In Bild 1 werden für 1995 nur für die USA Gesamtverluste in Höhe von 3 Mia. US-$ angegeben. In Tabelle 1 sind es 5,2 Mia. US-$ für Nordamerika.
- Der einzige Unterschied besteht darin, dass in Bild 1 die Verluste in den USA durch Mobilfunk höher angegeben sind als die Verluste durch Calling Cards (420 Mio. US-$ gegenüber 360 Mio. US-$). In Tabelle 1 werden die Verluste durch Mobilfunk für Nordamerika niedriger eingestuft als die Verluste durch Calling Cards (720 Mio. US-$ gegenüber 1,3 Mia. US-$).

Öffentliche Betreiber nehmen den grossen Schaden immer weniger in Kauf und

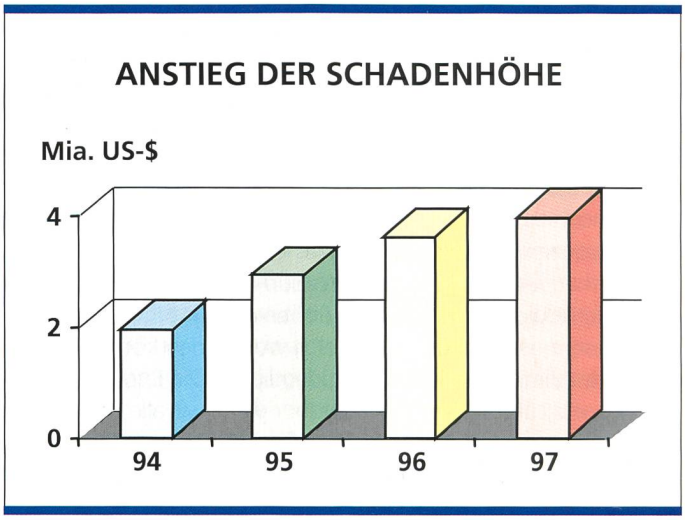


Bild 1. Zwischen 1994 und 1997 war beim Betrug in Telekommunikationsnetzen in den USA ein hundertprozentiger Anstieg der Schadenshöhe zu verzeichnen.

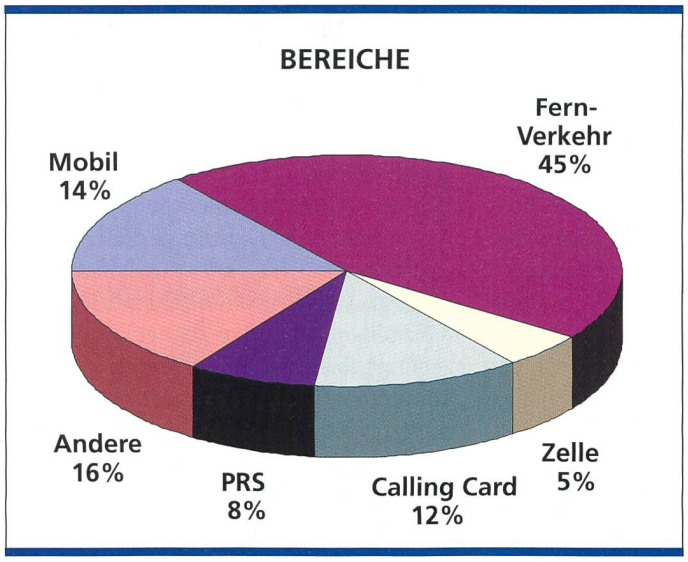


Bild 2. Der wachsende Markt für neue Netzdienste erhöht das Betrugspotenzial, insbesondere jenes des Missbrauchs von Managementaufgaben.

reagieren zunehmend auf diese Herausforderung. Dies lässt sich aus zwei wichtigen Indizien ableiten:

- Die Betreiber organisieren sich in verschiedenen nationalen und internationalen Foren zur Betrugsbekämpfung. Beispiele für solche Foren sind: TUFF, Telecommunications UK Fraud Forum, FIINA, Forum for International Irregular Network Access und CFCA, Communication Fraud Control Association.

Diese Foren erarbeiten in erster Linie Massnahmen gegen Betrug und koordinieren Aktivitäten verschiedener Betreiber.

- Die Nachfrage nach Betrugsmanagementsystemen (BMS) und nach qualifizierter Beratung und Unterstützung für ein richtiges Vorgehen bei der Betrugsbekämpfung wächst.

Typische Betrugsszenarien

Täter

Moderne Technologien eröffnen heute den Kriminellen vielfältige Möglichkeiten, Betrug zu begehen. Delikte können dabei von Innentätern, von Aussentätern oder in Zusammenarbeit dieser beiden Täterkreise begangen werden:

- Von Betrug durch *Innentäter* spricht man, wenn der Betrüger ein Angestellter des Betreibers ist und seine Kenntnisse und Rechte missbraucht. So kann ein hoher Schaden entstehen, denn Innentäter verfügen sehr häufig über detaillierte Kenntnisse von Netzkomponenten und Unternehmensprozessen. Zudem besitzt dieser Täterkreis häufig umfassende Zugangsrechte zu Räumen, in denen sich Netzkomponenten befinden, oder über Zugriffsrechte, die ihn zur Durchführung von Netzaktivitäten – insbesondere Managementoperationen – ermächtigen.
- Betrug durch *Aussentäter* meint, wenn der Täter kein Angesteller des Betreibers ist. Allgemein nutzen Aussentäter entweder Telekommunikationsdienste nicht vertragskonform oder missbrauchen ihre Kenntnisse. Sie verfügen mitunter über grosses Fachwissen – beispielsweise über die Architektur eines Telekommunikationsnetzes, über Abläufe von Diensten oder das Management von Diensten –, aber auch über Kenntnisse der internen Unternehmensprozesse. Sie haben insbesondere dann solche Kenntnisse, wenn sie einmal bei einem Netzbetreiber oder einem Systemlieferanten tätig waren.
- Kommt es zu einem Zusammenspiel von Innen- und Aussentätern, so bietet beispielsweise der Innentäter dem Aussentäter gegen Geld Fachwissen und «Dienste» an. Innen- und Aussentäter verstossen gemeinsam gegen das geltende Recht.

Von Betrug innerhalb der Telekommunikationsnetze kann jeder Betreiber oder Anbieter von Mehrwertdiensten und jeder Privat- oder Geschäftskunde betroffen sein.

Betrugskategorien

Fünf Betrugskategorien lassen sich differenzieren:

Dienstebetrug

In einem digitalen Telefonnetz bietet man den Teilnehmern verschiedene Dienste an, die in einer Vermittlungsstelle oder einem «intelligenten Netz» (IN) umgesetzt werden. Ein denkbares Szenario ist die Kreditkartentelefonie. Hier wird die Leitung erst nach Eingabe der PIN freigeschaltet. Spioniert nun ein Betrüger die Kreditkartennummer und die zugehörige PIN aus, kann er auf Kosten des Kreditkartenbesitzers beliebig viele Telefongespräche führen. Besonders hoch sind die Verluste, die durch Betrug mit den so genannten Premium Rate Services und mit Calling Cards entstehen. Diese Delikte sind daher in Statistiken oft gesondert ausgewiesen.

Signalisierungsbetrug

Bei der ss5-Signalisierung wird die Signalisierungsinformation über die Gesprächsleitung übertragen (so genanntes Inband Signalling). Einige Implementierungen des ss5-Protokolls reagieren jedoch auf fehlerhafte Signalisierungen nicht so, wie es die entsprechende ITU-Empfehlung (International Telecommunication Union) vorsieht. Dieser Implementierungsfehler wurde in der Vergangenheit häufig genutzt, um durch Einspeisen von spezifischen Signalen in die Gesprächsleitung Vermittlungsstellen zu täuschen und kostengünstige Gespräche zu führen. Diese Art des Betrugs wird auch als «blue boxing» bezeichnet. Seit der Einführung des ss7-Protokolls sind diese Schwächen beseitigt, da die Signalisierung über getrennte Kanäle übertragen wird.

Administrationsbetrug

Jedes Telekommunikationsnetz muss administriert werden. In öffentlichen Netzen wird zum Beispiel hierfür ein eigenes logisches Netz, das Telecommunication Management Network (TMN), verwendet. Der wachsende Markt für neue Netzdienste und Netzprodukte erfordert ein zunehmend automatisiertes und intelligentes Management. Hierdurch erhöht sich aber auch das Betrugspotenzial, insbesondere durch den Missbrauch von Managementaufgaben. So können beispielsweise durch Missbrauch von Zugriffsrechten Dienste für einen Teilnehmer eingerichtet werden, der diese auf Kosten des Betreibers nutzt (Bild 2).

Anschlussnetzbetrug

Jeder Teilnehmer eines Telekommunikationsnetzes ist über das Anschlussnetz mit seiner Vermittlungsstelle verbunden. Hierfür werden häufig Kupferleitungen eingesetzt. Ein Beispiel für Betrug im Anschlussnetz ist der so genannte «clip on fraud» auf Kupferleitungen. Der Betrüger «klemmt» dabei ein Telefon an die

Kupferleitung eines anderen Anschlussbesitzers und führt seine Gespräche auf dessen Kosten.

Teilnehmerbetrug
Kunden haben diverse Möglichkeiten, Betrug gegen den Betreiber zu begehen. Beim Subskriptionsbetrug melden sie einen Telefonanschluss an, ohne jemals die Absicht oder Möglichkeit zu haben, die Abrechnungen für diesen Telefonanschluss kontinuierlich zu bezahlen. Eine weitere Variante des Teilnehmerbetrugs ist die Manipulation von Telefonkarten oder von öffentlichen Münzfernsprechern.
Bei der am 24./25. Februar 1999 in London durchgeführten Konferenz «Detecting and Preventing Fraud in a Converging Telecoms Market» wurden Administrationsbetrug, Dienstebetrug (vor allem mit Calling Cards) und Teilnehmerbetrug (vor allem Subskriptionsbetrug) als häufigste Betrugsarten genannt. Die Häufigkeit und die Auswirkungen der Betrugsarten sind von der jeweiligen Region und vom Betreiber abhängig (Angebot der Dienste, Art der Organisation und der eingesetzten Technik, Tarifierung usw.). Deshalb kann für einzelne Betreiber das Betrugsspektrum verschieden aussehen.

Betrugsvorbeugung, Betrugsbekämpfung
Die Massnahmen zur Betrugsbekämpfung lassen sich in drei Kategorien einteilen:
– Betrugsvorbeugung
– Betrugserkennung
– Intervention
Es gibt mehrere Möglichkeiten, Betrug innerhalb eines Telekommunikationsnetzes bereits im Vorfeld zu verhindern.
Grundsätzlich müssen in jedem Fall zuerst die potenziellen Bedrohungen und Gefahren detailliert analysiert werden, die sich durch Betrug für das Telekommunikationsnetz ergeben können. Hieraus lassen sich netzspezifische Anforderungen an die Betrugsvorbeugung ableiten. Im nächsten Schritt müssen diese Anforderungen in Form von vorbeugenden Massnahmen umgesetzt werden. Diese lassen sich in drei Schritte unterteilen.

Organisatorisch-präventive Massnahmen
Eine grundlegende organisatorische Massnahme ist die Installation eines Antifraudteams. Das Antifraudteam ist für die Betrugsbekämpfung in einem Telekommunikationsnetz verantwortlich. Dazu gehört, konkrete Massnahmen für die Betrugsbekämpfung im Betreibernetz auszuarbeiten. Diese Massnahmen sind ständig an neue Betrugsszenarien und an Modifikationen des Betreibernetzes und der Dienste anzupassen. Schliesslich gilt es, alle Massnahmen durchzusetzen. Das Team ist in jedem Falle mit entsprechenden Kompetenzen auszustatten. Weitere organisatorisch-präventive Massnahmen sind beispielsweise die intensive Schulung des Personals, eine verstärkte Jobrotation des Personals oder die Einrichtung eines Fraudpreventionpools. Ein solcher Pool wurde für die Mobilfunkbetreiber in Deutschland eingeführt und dokumentiert die Taten «schwarzer Schafe» in der Mobiltelefonie.

Bauliche Massnahmen
Unter baulichen Massnahmen versteht man den Schutz von sensitiven Netzkomponenten, beispielsweise durch abschliessbare Gehäuse. PCs, die für Aufgaben des Netzmanagements verwendet werden, könnten ohne CD-ROM- und Floppy-Disk-Laufwerk ausgestattet sein. Hierdurch lässt sich unter anderem erschweren, dass Software zur Durchführung von Betrügereien manipuliert wird.

Technische Massnahmen
Unter technischen Massnahmen versteht man:
– *Sicherheitsdienste in den einzelnen Netzkomponenten*
  Dies sind Funktionen wie die Authentifizierung von Personen und Kommunikationspartnern, eine detaillierte Zugriffskontrolle auf Applikationen und Daten sowie ein umfangreiches Logging aller Aktivitäten.
– *Einschränkungen bei Nutzung der Dienste*
  Beispiele für die Einschränkungen bei der Nutzung von Diensten sind schwarze Listen, weisse Listen, Kreditlimiten, Vorauskasse oder auch Umstellen von speziellen Diensten auf Handvermittlung durch einen Operator.
– *Garantie für die Softwareintegrität*
  Um die Softwareintegrität zu gewährleisten, sollte bei der Entwicklung ein zertifizierter Entwicklungsprozess und bei der Auslieferung ein zertifizierter Auslieferungsprozess nach ISO durchlaufen werden. Darüber hinaus gilt es, geeignete Massnahmen zum Softwarekopierschutz zu treffen.

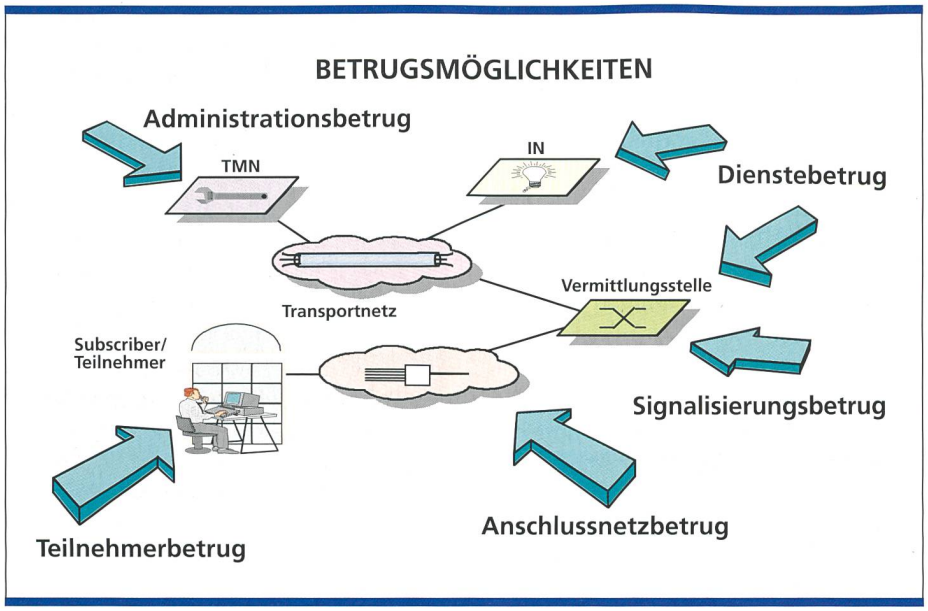
Betrugserkennung
Wenn trotz aller vorbeugenden Massnahmen dennoch Betrug begangen wird, muss ein Betreiber dies möglichst frühzeitig erkennen können.
Zwei methodische Ansätze existieren:
– Revision aller Aktivitäten im Netz
– Zuordnung aller Nutzer und Endteilnehmer eines Telekommunikationsnetzes zu Verhaltenskategorien bzw. Verhaltensmustern, um schnell auf Abweichungen reagieren zu können
Bei der Revision der Netzaktivitäten werden periodisch Logdateien, Statistiken und Verkehrsmessdaten mit Data Mining Tools auf Unstimmigkeiten ausgewertet. Eine solche Auswertung setzt seitens des Betreibers vor allem ein Konzept voraus. In diesem ist detailliert aufgeführt, wann und unter welchen Umständen ein bestimmtes Log ausgewertet werden soll, welche Statistiken zu analysieren sind, und welche Rückschlüsse man aus den Auswertungen ziehen kann.
Die zweite Methode basiert auf der Zuordnung und Analyse von Verhaltenskategorien bzw. Verhaltensmustern.
Ein Teilnehmer, der beispielsweise über Jahre hinweg niemals zwischen 22 Uhr und sieben Uhr telefoniert hat, und dann schlagartig in dieser Zeit extensive Telefongespräche führt, ändert sein Verhalten. Diese plötzliche Verhaltensänderung muss erkannt und als Hinweis auf einen möglichen Betrug untersucht werden. Hierzu werden Betrugsmanagementsysteme (BMS) verwendet, die mit einfachen Regelsätzen (beispielsweise Gebühren eines Teilnehmers müssen pro Tag geringer als ein bestimmter Wert sein), aber auch mit neueren Methoden wie beispielsweise neuronalen Netzen oder mit einer Kombination von Regeln und neuronalen Netzen arbeiten. Wesentliche Vorteile der neuronalen Netze sind deren Lernfähigkeit und die Berücksichtigung von «Ausnahmen einer Regel», Grenzfällen und abrupten Verhaltensänderungen eines Teilnehmers im Ergebnis. Die Analysen durch ein BMS basieren auf sämtlichen oder einem Teil der Daten, die von den Komponenten eines Telekommunikationsnetzes aufgezeichnet werden. Solche Daten sind unter anderem CDRs (Call Detail Records), Signalisierungsdaten, Logdaten, Statistikdaten oder Verkehrsmessdaten. Beim Einsatz eines BMS ist es wichtig, den Datenschutz zu beachten.

Intervention

Bezogen auf die Betrugsbekämpfung definiert man den Begriff «Intervention» als die Summe aller Massnahmen zur Betrugsverfolgung. Dazu zählen das Sammeln von Indizien, der Schutz der Endkunden und die Betrugsnachbearbeitung. Betrug ist ein kriminelles Vergehen und deshalb sollten Betrüger auch strafrechtlich verfolgt werden. Voraussetzung dafür ist, dass der Netzbetreiber bei einem Gerichtsverfahren Beweise für den begangenen Betrug vorlegen kann. Solche Beweise können auf Basis von Abrechnungsdaten der Vermittlungsstellen oder anderen Protokolldateien geführt werden – sofern lückenlose Aufzeichnungen auf ein fehlerfreies Funktionieren der Anlagen schliessen lassen. Auch hierbei ist besonders auf die Einhaltung des Datenschutzes zu achten. Die Zusammenarbeit mit Strafverfolgungsbehörden kann dazu beitragen, die Dauer von Gerichtsverfahren zu verkürzen, die Kosten zu reduzieren und die Erfolgsaussichten zu steigern. Neben der strafrechtlichen Verfolgung sollten Massnahmen zum Schutz der Endkunden ergriffen werden, beispielsweise:

- generelle Deaktivierung eines Dienstes
- Deaktivierung von Diensten für einen Teilnehmer
- Black Lists (Liste von Teilnehmern, die nicht berechtigt sind, einen bestimmten Dienst zu nutzen)
- White Lists (Liste von Teilnehmern, die berechtigt sind, einen bestimmten Dienst zu nutzen)
- ausgewählte Anrufbeschränkungen oder Sperrung des Anschlusses
- Kunden anrufen und zu den Vorgängen befragen
- schnelle Zuweisung einer neuen PIN
- Vor-Ort-Prüfung des Anschlusses.

Bei der Betrugsnachbearbeitung wird der Betrugsfall nochmals analysiert und der entstandene Schaden ermittelt. Zusätzlich sollen die vorbeugenden Massnahmen daraufhin überprüft werden, ob es Möglichkeiten gibt, gleichartige Betrugsfälle zukünftig im Vorfeld zu verhindern. Diese Prüfung muss vor allem dann durchgeführt werden, wenn sich bestimmte Betrugsarten häufen, eine neue Betrugsart erkannt oder ein hoher Schaden verursacht wurde.



Empfehlungen zur Betrugsbekämpfung

Folgende Fragen sind für einen Netzbetreiber bei der Betrugsbekämpfung wichtig: Was muss konkret unternommen werden, um einen ausreichenden Schutz gegen Betrug zu erreichen? Welche vorbeugenden, erkennenden und intervenierenden Massnahmen sollen umgesetzt werden? Wie spielen die Massnahmen zusammen?

Demnach gibt es auch unterschiedliche Anforderungen der Netzbetreiber an die Betrugsbekämpfung, Unterschiede bei den Netzrealisierungen, den Diensteportfolios, den Organisationsstrukturen und den Kundenprofilen. Es gibt keine Standardlösung für die Betrugsbekämpfung, weil in der Regel nur betreiberspezifische, massgeschneiderte Lösungen zum Erfolg führen.

Betrugsbekämpfung ist komplex und erfordert einen ganzheitlichen Ansatz. Für einen Netzbetreiber gibt es mehrere Möglichkeiten:

- alles in Eigenregie bewältigen
- sich mit anderen Netzbetreibern zusammenschliessen, um gemeinsam Lösungen zu erarbeiten und Erfahrungen auszutauschen
- sich an einschlägigen Arbeitskreisen beteiligen
- Unterstützung von einem spezialisierten Beratungsunternehmen in Anspruch nehmen

In jedem Fall sind jedoch folgende Aspekte bei der Beantwortung der oben aufgeführten Fragen zu berücksichtigen:

Agieren statt reagieren

Ein Netzbetreiber soll «proaktiv» gegen Betrug vorgehen. Es ist besser, zu agieren und nicht zu warten, bis Betrug begangen wird. Auch wenn durch Kosteneinsparungen kurzfristig ein besseres Ergebnis zu erzielen ist, werden langfristig die Verluste durch Betrug und die Folgekosten für Schadensbehebung ein beträchtliches Ausmass annehmen. Es ist ausgesprochen wichtig, dass sich Netzbetreiber rechtzeitig auf die Möglichkeit eines Betruges vorbereiten.

Zusammenhänge erkennen

Primäres Ziel muss sein, Betrug so weit möglich und wirtschaftlich vertretbar zu verhindern. Den vorbeugenden Massnahmen muss daher ein entsprechend hoher Stellenwert beigemessen werden (z.B. Bonitätsprüfungen bei der Subskription). Allerdings kann man nicht alle Betrugsarten durch vorbeugende Massnahmen abwehren. Die Kreativität von Betrügern ist sehr hoch und die technische Entwicklung, die auch Kriminellen neue Nischen offeriert, schreitet schnell voran. Betrugsfälle, die durch vorbeugende Massnahmen nicht zu verhindern waren, müssen schnellstmöglich erkannt, analysiert und auf eine wirtschaftlich vertretbare Weise bekämpft werden. Als besonders geeignet erwiesen sich hierbei die Betrugsmanagementsysteme. Die erforderlichen Investitionen für ein BMS amortisieren sich häufig bereits nach wenigen Monaten. Das BMS liefert Daten, die aufgrund auffallender Abweichungen von vordefinierten Werten Anlass zum Betrugsverdacht geben. Spezialisten werten die Daten anschliessend aus und überprüfen ihre Stichhaltigkeit. Erkannte Betrugsfälle erfordern dann angemessene Gegenmassnahmen. Auch diese Massnah-

men müssen sorgfältig überlegt und in Form eines Aktionsplanes präzise vorbereitet werden.
Vorbeugende, erkennende und intervenierende Massnahmen stehen in einem engen Zusammenhang. Zum einen erzeugen effiziente, erkennende und intervenierende Massnahmen eine abschreckende Wirkung und tragen zur Vorbeugung bei. Zum anderen sollen bei der Intervention vorbeugende und erkennende Massnahmen überprüft und gegebenenfalls angepasst werden. Tabelle 2 beschreibt das Ziel einer aufeinander abgestimmten Kombination von vorbeugenden, erkennenden und intervenierenden Massnahmen.

	Nordamerika	Europa	Asien/Pazifik	Andere	Global
Mobil analog	650	200	200	150	1200
Mobil digital	20	130	260	50	460
Mobil andere	50	40	50	20	160
Total mobil	720	370	510	220	1820
Fernverkehr	2300	1500	1400	500	5700
Zelle	100	100	200	80	480
Calling Cards	1300	100	100	50	1550
International	200	300	300	100	900
PRS	450	300	100	100	950
Andere	200	300	300	200	1000
Total Festnetz	4550	2600	2400	1030	10580
Total	5270	2970	2910	1250	12400

Tabelle 1. Betrugsverluste 1995 in Mio. US-$, weltweit, nach Diensttypen (Chorleywood Consulting Ltd.

Betrugsbekämpfungsphase	Massnahme
Vorbeugung	Festlegen von Schwellenwerten für die Nutzung von Diensten
Erkennung	Überprüfung der Schwellenwerte durch Einsatz eines BMS
Intervention	Sammeln von Indizien durch das BMS zur Vorlage bei Gerichtsverfahren, unter Berücksichtigung der Datenschutzbestimmungen

Tabelle 2. Beispiel einer abgestimmten Kombination von Massnahmen.

Wirtschaftlichkeitsberechnungen durchführen

Bei der Auswahl von konkreten Massnahmen sind Wirtschaftlichkeitsberechnungen sehr hilfreich. Die Kosten werden hierbei dem wahrscheinlichen Nutzen gegenübergestellt. Jede Massnahme wird dahingehend überprüft, ob der Nutzen in einem wirtschaftlich vernünftigen Verhältnis zu den Aufwendungen steht.
In einer Wirtschaftlichkeitsberechnung zu Beginn der Betrugsbekämpfung werden folgende Faktoren überprüft:
- Quantifizierung des Verlustes durch Betrug

Ist der Umfang vom Netzbetreiber nicht zu ermitteln, können als Richtwert 1 bis 3% des Gebührenaufkommens herangezogen werden.
- Auflistung von möglichen, vorbeugenden, erkennenden und intervenierenden Massnahmen
- Abschätzung über die voraussichtlichen Kosten einer Massnahme

Es sollen die technischen, baulichen und organisatorischen sowie die erstmaligen und laufenden Kosten einfliessen.
- Abschätzung über den voraussichtlichen Nutzen der Massnahmen

Im Verlauf der Zeit ergeben sich neue Erfahrungen und verlässliche Zahlen. Mit fundierten Zahlen lassen sich neue Wirtschaftlichkeitsberechnungen durchführen. Es lässt sich die Wirksamkeit von Massnahmen überprüfen und die Notwendigkeit für entsprechende Anpassungen erkennen.

Betrugsbekämpfungskonzept erstellen

Wichtiger Bestandteil jeder erfolgreichen Betrugsbekämpfung ist ein umfassendes Betrugsbekämpfungskonzept. Dies beschreibt alle Aspekte der Betrugsbekämpfung und dient den Spezialisten als Nachschlagewerk und neuen Mitarbeitern zur Einarbeitung. Das Konzept zur Betrugsbekämpfung ermöglicht erst ein abgestimmtes, koordiniertes Vorgehen gegen den Betrug. Entsprechend wichtig ist es, dass dieses Dokument ständig aktualisiert und auf dem neusten Stand gehalten wird.
Das Konzept sollte Folgendes beinhalten:
- Die Betrugsbekämpfungspolitik legt die Zielvorgaben, die wesentlichen Anforderungen und die Grundsätze fest.
- Es zeichnet die relevanten Betrugsszenarien mit Aussagen zum erforderlichen Wissen und zur Ausrüstung der Betrüger, zum potenziellen Schaden und zur Betrugswahrscheinlichkeit auf.
- Es enthält alle Massnahmen zur Betrugsvorbeugung und bei Betrugserkennung jene zur Intervention.
- Es beschreibt die Schnittstellen der Bedienung.
- Es enthält ein Betreiberkonzept zur Organisation, zu Rollen und Verantwortlichkeiten.
- Wenn neue Betrugsformen auftreten, werden neue Hinweise und Verhaltensregeln mit einbezogen.

Wirksames Berichtswesen einführen

Erfolgreiche Betrugsbekämpfung erfordert, dass zur richtigen Zeit die richtigen Massnahmen ergriffen werden. Eine Voraussetzung dafür ist, dass das tatsächliche Ausmass des Betrugs jederzeit überblickt werden kann. Dies erreicht man mit einem gut funktionierenden Berichtswesen. Netzbetreiber können in einer Datenbank die erkannten Betrugsfälle mit Detailinfos zur Betrugsentwicklung, zum Schadensausmass und zur erfolgten Betrugsbehandlung sammeln. Das Berichtswesen lässt sich so gestalten, dass jederzeit beweiskräftige Unterlagen für eine gerichtliche Verfolgung von Betrügern abrufbar sind.

Beratungsleistung in Anspruch nehmen

Nur wenige Netzbetreiber nehmen selbst alle beschriebenen Aufgaben wahr. Mit Unterstützung eines renommierten Beratungsunternehmens bewältigen sie die anstehenden Aufgaben häufig mit besseren Ergebnissen, in kürzerer Zeit und kostengünstiger. Neben anderen verfügt Siemens in diesem Bereich über ein breit gefächertes Know-how und bietet im Rahmen der Telco Security Services™ eine umfassende Unterstützung zur Betrugsbekämpfung. Das Spektrum reicht von einführenden

Informationsveranstaltungen über die Detailanalyse von spezifischen Betrugsszenarien bis zum vollständigen Erstellen von Betrugsbekämpfungskonzepten.

Ausblick

Weil durch intensiven Wettbewerb und damit verbundene Gebührensenkungen die Gewinnmargen der Betreiber abnehmen, wird es immer wichtiger, geeignete Massnahmen zur Betrugsbekämpfung einzusetzen. Heute gewinnt deshalb die Betrugsbekämpfung zunehmend an Bedeutung und stellt eine Herausforderung für alle Beteiligten in der Telekommunikation dar. Betreiber haben darauf reagiert und organisatorische und technische Massnahmen ergriffen. Durch die Veränderungen im Telekommunikationsmarkt, hervorgerufen durch Deregulierung, Konvergenz von Techniken und Diensten sowie die wachsende Bedeutung des Internets, ergeben sich laufend weitere Herausforderungen. Dies betrifft beispielsweise völlig neue Arten von Betrug beim E-Commerce oder die rasche Verbreitung von Anleitungen zum Betrug – etwa über das Internet. Betrugsbekämpfung ist deshalb kein einmaliger Vorgang, sondern muss kontinuierlich an die neuen Herausforderungen und Gegebenheiten im Wettlauf gegen die Betrüger und deren Methoden angepasst werden.

Für Siemens ist das Thema Betrugsbekämpfung sehr wichtig. Das umfangreiche Portfolio von Dienstleistungspaketen, welches zur gezielten Beratung und Unterstützung von Netzbetreibern und Diensteanbietern entwickelt wurde, verdeutlicht dies. Gerade das Zusammenspiel von Betreibern, Herstellern, Endkunden und Sicherheitsbehörden verspricht die grössten Erfolgsaussichten hinsichtlich des gemeinsamen Ziels, Betrugsprobleme und Schäden auf ein akzeptables Ausmass zu reduzieren. [7]

Bernhard Nauer, *Director, Bereich Communication on Air, Abteilung Chief Technical Office, Technology and Network Strategies, Siemens AG.*

Axel Pfau, *Marketing für Trusted Networks and Applications, Bereich ICN, Siemens AG.*

Alfred Ressenig, *Unterstützung bei Betrugsbekämpfung, Bereich ICN, Siemens AG.*

Summary

Combating fraud in telecommunication centres

Modern technologies open up a multitude of new possibilities for criminals to commit fraud. Crimes may be committed by insiders (people working within a company), outsiders (people working outside an organization) or a combination of the two. Measures to combat fraud can be divided into three categories: Fraud prevention, fraud recognition and intervention. Combating fraud is therefore gaining in importance today and presents a challenge to all participants in telecommunications. Operators have reacted to fraud and taken organizational and technical action. Deregulation, convergence of technologies and services, and growth in the importance of the Internet have introduced changes to the telecommunications market. These changes are continually presenting new challenges.

Color Line Service

« Clear-Channel-Gbit-Service »

Die Idee von Color Line ist, neue Netzlösungen für Kunden mit hoch komplexem Datenverkehr anzubieten. Die Leistungsfähigkeit des Kommunikationssystems eines Unternehmens ist für den kommerziellen Erfolg entscheidend.

Mit bis zu 32 protokollunabhängigen Channels transportiert Swisscom Daten bis 80 Gbit/s im Vollduplexverfahren innerhalb der Rechenzentren, Serverfarmen und LANs. Mit der Color Line werden die Kunden-IT-Systeme leistungsfähiger. Um zeitkritische Daten jederzeit und überall für die Kundenbetreuung verfügbar zu haben, verbindet Swisscom firmeninterne Netze bis zu einer Distanz von 50 km mit einem «full through put» Gbit Ethernet Channel.

Data Center Services

Mit dem Color Line Service ermöglicht Swisscom die Vernetzung von Serverfarmen und Taperobotern. Damit verbindet der Service redundante Mainframes mit ESCON Directors bzw. deren Discs in Synchronapplikation. Swisscom arbeitet für die Kunden fehlertolerante, hoch verfügbare Netzlösungen für Disaster-Scenarios aus. Denn eine unterbruchslose Verfügbarkeit von Daten, auch im Katastrophenfall, ist Erfolg bestimmend für ein Unternehmen.

Die Konvergenz der Transporttechnologie

Der neue, auf Dense-Wavelenght-Division-Multiplexer (DWDM) basierende Service Color Line von Swisscom ermöglicht die Konvergenz der optischen Transporttechnologien höchster Bandbreite. Mit Color Line verfügt der Kunde bis zu 32 Clear Channels, womit er Daten für die verschiedensten Applikationen transportieren kann:

- im LAN-Service-Bereich
- im Data-Center-Bereich
- im Switched-Data-Service-Bereich
- im Synchronous-Transmission-Service-Bereich

Color Line Services ist seit dem 14. Juli 2000 in der ESCON-Applikation über 38 km erfolgreich im Betrieb.

Info Homepage:
www.swisscom.com/business-solutions