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

Herausgeber: Swisscom

Band: 74 (1996)

Heft: 12

Artikel: Krimineller Missbrauch in Milliardenhöhe

Autor: Haag, Jürgen

DOI: https://doi.org/10.5169/seals-876805

KRIMINALITÄT IN TELEKOMMUNIKATIONSNETZEN

KRIMINELLER MISSBRAUCH IN MILLIARDENHÖHE

Foto H.R. Bramaz

Was vor einigen Jahren noch als Science-fiction abgetan wurde, ist heute bereits Realität geworden. Die Vernetzung unserer Umwelt mit Kommunikationssystemen ist mittlerweile so weit vorangeschritten, dass auch die Privathaushalte in zunehmendem Masse davon profitieren. Gleichzeitig ist eine neue Generation von Kriminellen entstanden, die ihr betrügerisches Vorgehen auf diese Bahnen gelenkt hat.

JÜRGEN HAAG, FRANKFURT

Der internationale Telekommunikationsmarkt dient diesen Kriminellen dabei als Betätigungsfeld. Durch ihre strafbaren Machenschaften und Betrügereien gelingt es ihnen, Gewinne in Millionenhöhe zu erzielen. Waren es anfangs jugendliche Hacker, die in die Netze der Telekommunikationsunternehmen einbrachen, um denen einmal zu zeigen, wozu sie fähig sind, sind es heute gewöhnliche Straftäter, die sich Leistungen auf Kosten anderer erschleichen wollen. Zunehmend verhärtet sich der Verdacht, dass sich auch die organisierte Kriminalität auf diesen Schauplätzen tummelt.

Telekommunikationsnetze

Das Telekommunikationsnetz gliedert sich in mehrere Bereiche. Bild 1 zeigt ein Übersichtsbild über mögliche Konfigurationen einer Telefonverbindung. Die aufgezeigten Bereiche unterliegen individuellen Risiken.

Die *Wohnung,* der Verantwortungsbereich des Telefonkunden, umfasst alle technischen Einrichtungen hinter der ersten Teilnehmeranschlusseinrichtung (TAE). Dritten ist in der Regel der Zugang zu Wohnungen verwehrt. Erhöhte Telefonrechnungen entstehen hier zumeist aus fehlendem Kostenbewusstsein der Kunden. Dazu trägt die Nutzung diverser Mehrwert- und Ansagedienste im In- und Ausland durch Personen aus dem familiären Umfeld nicht unerheblich bei. Auch sei auf die Gefahren unsicherer schnurloser Telefone, die zumeist nicht zugelassen sind, hingewiesen.

Das *Hausnetz* in Mehrfamilienhäusern liegt im Verantwortungsbereich Dritter. Es liegt zwischen der TAE, dem logischen Abschlusspunkt des Netzes und dem physikalischen Abschlusspunkt des Liniennetzes (APL). Zwischen der TAE und dem APL befindet sich in Mehrfamilienhäusern oft eine unübersichtliche, schlecht dokumentierte Hausinstallation. Frei zugängliche Punkte (z.B. Etagenverteiler) und Leitungsführungen durch andere Wohnungen ermöglichen relativ leicht den unerkannten kriminellen Missbrauch. Der technische Aufwand für das Eindringen in die fremde Anschlussleitung ist hier gering. Hausnetze sind damit ein Angriffsschwerpunkt für illegale Aufschaltungen.

Das *Anschlussleitungsnetz* zwischen APL und dem Hauptverteiler in der Vermittlungsstelle ist im Verantwortungsbereich der Telekom. Der Hauptverteiler befindet sich im erhöht gesicherten Betriebsgebäude, die Kabelverzweiger verfügen über ein Schliesssystem. Oberirdisch geführte Teile des Anschlussleitungsnetzes sind leicht einsehbar, wodurch missbräuchliche Aufschaltungen erschwert werden.

In *Vermittlungsstellen* ist der Schutz der Telefonverbindung im allgemeinen am besten gewährleistet. Ein möglicher Missbrauch durch eigene Mitarbeiter lässt sich allerdings trotz intensiver Sicherungsmassnahmen nicht völlig ausschliessen. Verfolgt man den Weg einer Verbindung weiter, leuchtet ein, dass ein gezielter Angriff auf eine bestimmte Anschlussleitung nach der Vermittlungsstelle praktisch unmöglich ist, da die Verbindungen immer wieder auf andere Verbindungsleitungen weitervermittelt werden.

Das *öffentliche Netz* in der Fernebene ist durch den hohen Digitalisierungsgrad nur mit grossem technischem Aufwand gezielt auf eine Telefonverbindung angreifbar.

Die *Gateway-Schnittstellen* zu anderen Netzen besitzen eine ähnlich hohe Sicherheit gegen Angriffe oder Missbrauch von Telefonverbindungen wie das öffentliche Fernnetz. Die digitalen Zeichengabenetze unterschiedlicher Netzbetreiber sind logisch getrennt und in ihrer Gateway-Funktionalität auf wesentliche Teile beschränkt, um Eingriffe von einem Netz ins andere zu unterbinden. Dennoch gibt es noch Risiken herkömmlicher Zeichengabeverfahren, wie zum Beispiel das sogenannte C5-Hacking, auf welches noch konkret eingegangen wird.

Schutzziele

Zur effektiven Prävention vor und zur Abwehr gegen missbräuchliche Nutzung des Telekommunikationsnetzes muss zunächst eine Definition von Schutzzielen erfolgen. Diese können sehr stark anwendungsorientiert sein und weit über die Schutzziele des öffentlichen Netzes hinausgehen. Alle Bereiche, ob Kunde, Dienstanbieter oder Netzbetreiber, haben ein grosses Interesse, die allgemeinen Schutzziele wie

- Integrität
- Vertraulichkeit
- Verfügbarkeit

zu gewährleisten. Diese Schutzziele werden durch Sicherheitsmerkmale charakterisiert, welche durch das jeweilige Schutzbedürfnis der individuellen Kommunikationspartner, Dienstanbieter oder Netzbetreiber umgesetzt werden:

- Authentifikation
- Anonymität
- Datenintegrität
- Urhebernachweis
- Zugangskontrolle
- Vertraulichkeit

Kriminalität in Telekommunikationsnetzen

Allein die Neugier der Menschen erweckte seit jeher den Wunsch, an Gesprächen anderer, gefragt oder unge-

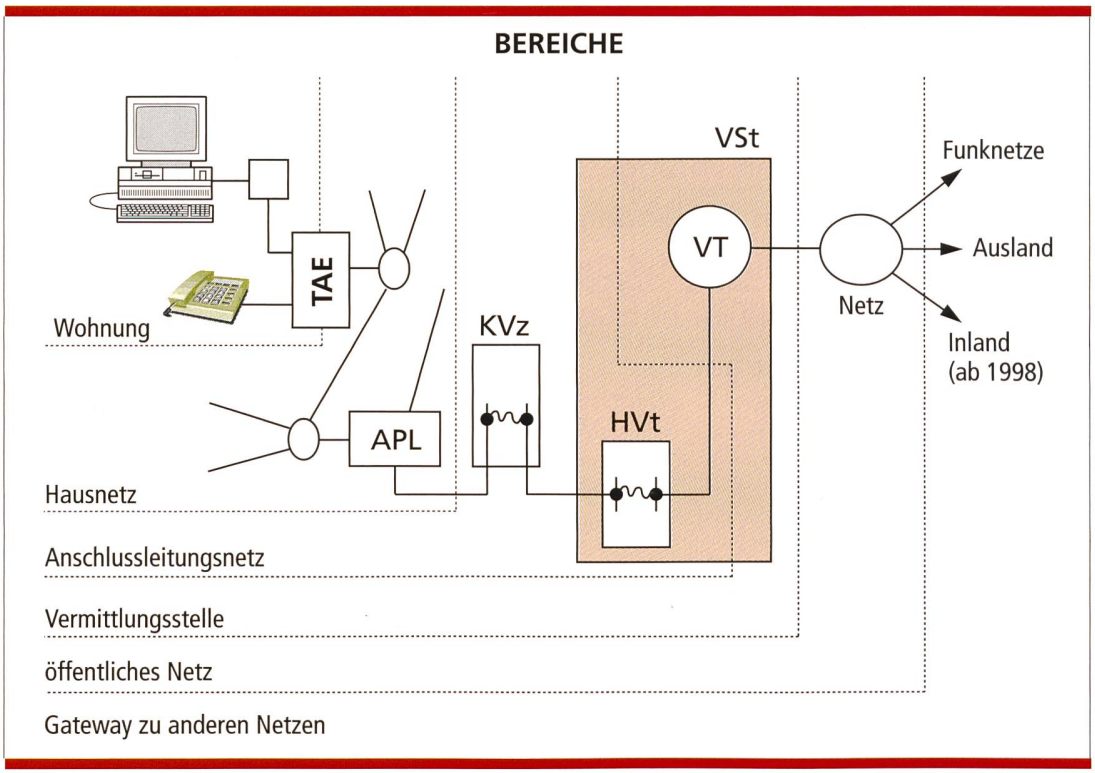

Bild 1. Die Telekommunikationsnetze gliedern sich in mehrere Bereiche.

fragt, teilzunehmen. Seit der Einführung des Telefons wuchs dieses Interesse und dehnte sich auch auf übertragene Gesprächsnachrichten aus. Computer werden heute sowohl im privaten als auch geschäftlichen Bereich von der Allgemeinheit genutzt. Auf ihre eigene PC-Tastatur «einhackende», dem Computer verfallene Hacker versuchen seitdem Einfluss auf Rechner anderer zu nehmen. Mit der Entwicklung der Telekommunikation als universelles Informationsmedium gesellten sich zu ihnen die «Phreaks», ein Akronym aus den Begriffen «telephone» und «freak». Beide Begriffe werden in der Praxis gleichermassen benutzt.

Das Telekommunikationsnetz wird von Schülern und Jugendlichen, die ihrem Drang und ihrer technischen Neugierde freien Lauf lassen, nach allen Regeln der Kunst auf Schwachstellen abgesucht. Ihre Erkenntnisse werden stolz an Gleichgesinnte weitergegeben. Hin und wieder verwischen sich dabei die Grenzen der Rechtmässigkeit insoweit, als die Erkenntnisse der Hacker von anderen kommerziell und unrechtmässig missbraucht werden. Dies führt dann letzten Endes zu strafrechtlicher Verfolgung und Kriminalisierung der beteiligten Personen.

Wunsch nach Machtausübung

War es in der Vergangenheit vorwiegend der Wunsch, unbemerkt Informationen und Nachrichten durch Abhören zu erlangen (Vertraulichkeit), so wird heute zusätzlich versucht, Informationen zu verfälschen (Integrität), sie zu Unbefugten fehlzuleiten, durch Maskerade einen anderen Benutzer vorzutäuschen, Abläufe von TK-Diensten zu verhindern oder zu missbrauchen und die Herkunft oder den Ursprung von Telekommunikationsteilnehmern zu verschleiern. Triebfeder all dieser Massnahmen ist der Wunsch nach Machtausübung, der sich oft im Erschleichen von Geld auswirkt.

Vorgehensweise

Mit steigender Komplexität der TK-Netze nehmen auch der Anreiz und die Möglichkeiten der Phreaks zu, ihre Angriffsmethoden subtiler zu gestalten. Dabei werden mitunter einzelne Manipulationsmethoden miteinander kombiniert. Die Vorgehensweise erfolgt in zwei Schritten. Zunächst versucht der Phreak, für ihn entgeltlos, das heisst aber auf Kosten anderer, in das TK-Netz einzudringen und dieses zu nutzen, um dann im zweiten Schritt das angestrebte Ziel, entweder Nachrichten über Daten- oder Telefonverbindungen austauschen zu können oder lediglich TK-Verkehr zu erzeugen, zu erreichen.

TIS-190 (Telekommunikations-Informations-Service 190)

Die Entgeltmodalitäten des TIS-190, im Ausland Audiotex-Service genannt, dienen oft als Ausgangspunkt für Missbrauch im TK-Netz. Zunächst sollen deshalb als Hintergrundinformation für die weiteren Erklärungen die Zusammenhänge der Entgeltabrechnung bei dem Mehrwertdienst TIS-190 erwähnt werden. Die Dienste privater Informationsanbieter (Information Provider, IP) können im öffentlichen Telefonnetz unter den Rufnummern der einzelnen Anbieter genutzt werden. Die Informationsanbieter haben die Möglichkeit, unter ihrer Rufnummer dem anrufenden Kunden bis zu 1000 – ab 1996 nur 40 – einzelne Programme anzubieten. Diensteanbieter schliessen auch Unterverträge mit (Unter-)Anbietern ab, wobei sie Teile ihrer 1000 Programmöglichkeiten an den (Unter-)Anbieter abtreten und ihm die

Nutzung überlassen. Die Abrechnung bezüglich dieser vermieteten Programmöglichkeiten muss dann zwischen dem privaten (Haupt-)Informationsanbieter und seinem (Unter-)Anbieter geregelt werden.
TIS-190 ist ein Mehrwertdienst. Der anrufende Kunde muss also nicht nur das für die Telefonverbindung entstehende Entgelt, sondern zusätzlich den Mehrwert dieses Dienstes bezahlen. Beide Entgeltanteile werden vom anrufenden Telefonkunden zusammen in Form eines erhöhten Tarifs an die Telekom entrichtet. Die Telekom erstattet dann einen Teil der Einnahmen an den (Haupt-)Informationsanbieter. Dies bedeutet, dass mit steigender Belegung des TIS-190-Anschlusses eines (Haupt-)Informationsanbieters auch dessen von der Deutschen Telekom erstatteter Anteil steigt.

Technische Manipulationsmöglichkeiten

Dialer

Als Dialer wird eine Wähleinrichtung bezeichnet, mit der zum Zwecke des Missbrauchs Telefonverbindungen im öffentlichen TK-Netz aufgebaut werden können. Dies kann sowohl manuell als auch automatisch gesteuert, zu einem vorgegebenen Zeitpunkt und sich zeitlich wiederholend geschehen. Der Netzmissbraucher verschafft sich im Netz Zugang zur Leitung eines Kunden. Häufig werden auch Leitungen benutzt, die zwar schon vorbereitend betriebsbereit mit der Vermittlungsstelle verbunden, aber den vorgesehenen Kunden noch nicht zugewiesen sind und somit dessen Konto nicht belasten. Hauptangriffspunkte sind Kabelverzweiger (mit Sonderschliesssystem gesichert) und andere Schaltstellen (Abschlusspunkt). Nach Einbringen des Dialers wählt dieser dann, oft nachts, im Inland oder auch im Ausland Audiotex-Rufnummern an, um Entgelteinheiten zu erzeugen, die dem angerufenen Informationsanbieter zugute kommen. Meistens bestehen geschäftliche Verbindungen zwischen dem Netzmissbraucher in Deutschland und dem angerufenen (ausländischen) IP, oft sind beide auch identisch. Auf diese Weise werden zusätzliche Gewinne mittels TIS-190 oder Audiotex-Service erschlichen.

TK-Anlagen-Missbrauch

Moderne TK-Anlagen bieten mannigfaltige Leistungsmerkmale, die immanent in Form der Anlagesoftware vorhanden sind. Für den Betrieb der TK-Anlage wird gewöhnlich nur ein geringer Teil aller Leistungsmerkmale freigegeben. Schutz- und Zugriffsfunktionen sind in der Regel firmenseitig mit vorgegebenen Grundvariablen (z. B. PIN = 0000) belegt; oft werden diese vom Anwender nicht entsprechend geändert. Für Phreaks ist es somit leicht, durch systematisches Ausprobieren (PIN-Hacking) innerhalb einer TK-Anlage Zugriffscodes zu erlangen. Da TK-Anlagen oft als S-130-Rufnummern (Toll-Free Service) von Anrufern entgeltfrei angewählt werden können, hat der Phreak beim PIN-Hacking ebenfalls kein Entgelt zu entrichten.
Bei aktivierter Durchwahlmöglichkeit (DISA) einer TK-Anlage kann diese nun vom Phreak, auch wenn sie PIN-geschützt ist – der ist ja bekannt – entgeltfrei zu Lasten des TK-Anlagen-Betreibers missbraucht werden. Oft werden dann beispielsweise teure Auslandsgespräche über die TK-Anlage abgewickelt.

Missbrauch von Inbandsignalisierung beim Zeichengabesystem

Toll-Free Services im Ausland, beispielsweise TK-Anlagen auch ohne Durchwahlmöglichkeit oder der Hei-

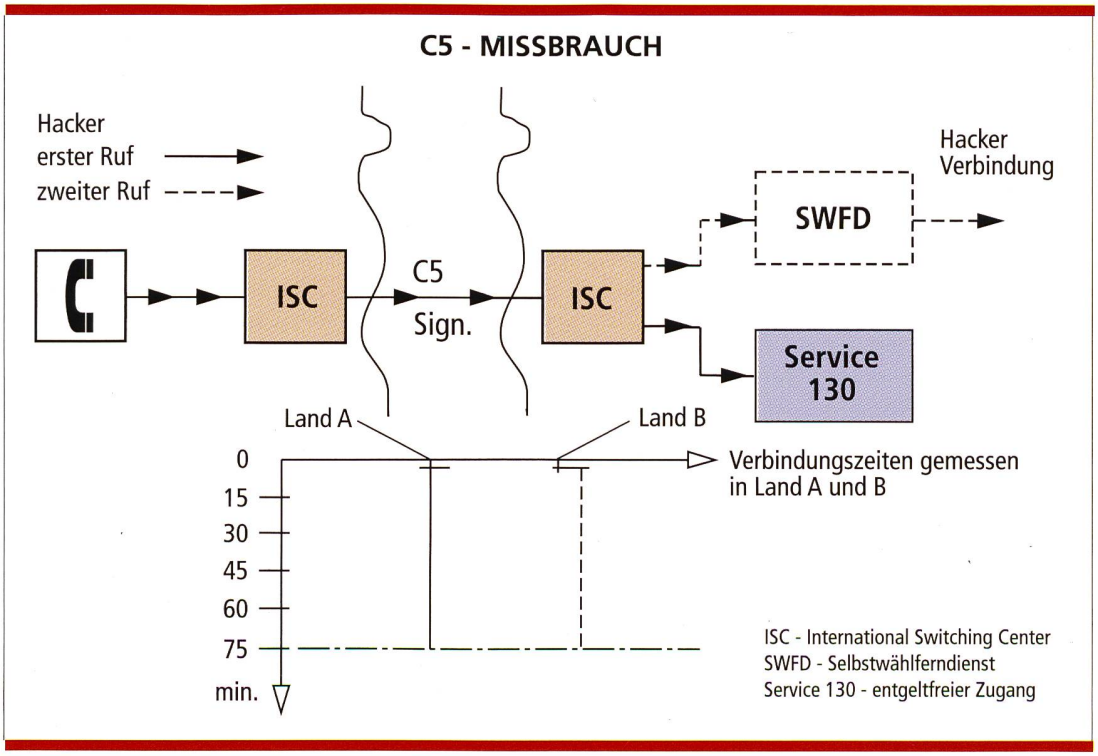

Bild 2. Toll-Free Services werden als Transitmöglichkeit missbraucht. ISC = International Switching Center, SWFD = Selbstwählferndienst, Service 130 = entgeltfreier Zugang.

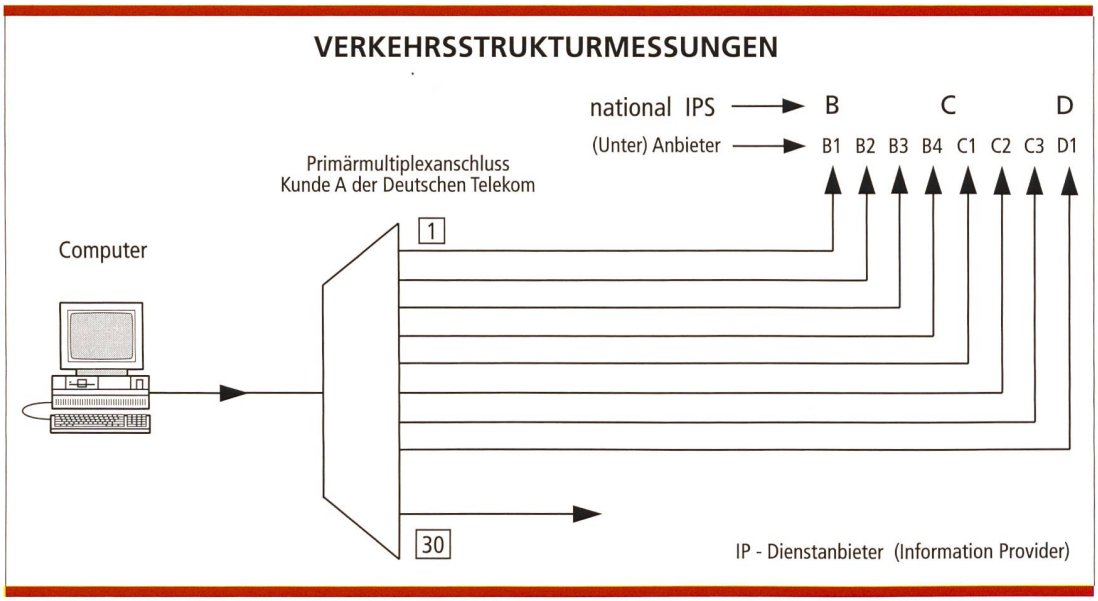

Bild 3. TIS-190-Informationsanbieter.

matdirektdienst (Country Direct Service), werden als Transitmöglichkeit missbraucht (Bild 2). Voraussetzung dafür ist, dass der Toll-Free Service über eine C5-gesteuerte Leitung mit dem Ursprungsland, in dem sich der Phreak befindet, verbunden ist. Zunächst wählt der Phreak den Toll-Free Service an, beeinflusst dann das C5-System durch Eingabe der genormten Zeichengabefrequenzen derart, dass der angewählte Toll-Free Service abgeschaltet wird, die Verbindung aber bis zu ihm bestehen bleibt. Durch Nachwahl kann der Phreak das von ihm gewünschte Ziel erreichen.

Kartenmissbrauch

Es gibt zwei grundsätzlich unterschiedliche Arten von Telefonkarten. Die Guthabenkarte (Prepaid Card) kann durch Vorauszahlung eines gewissen Betrags erworben werden, wobei durch die Nutzung der Karte das Guthaben entsprechend der geführten Telefongespräche abgebucht wird, bis der eingezahlte Betrag verbraucht ist. Bei der Guthabenkarte wird missbräuchlich versucht, «wiederaufladbare» oder auch unrechtmässig selbst hergestellte Karten in Umlauf zu bringen.
Mit (Kredit)-Telefonkarten, beispielsweise die T-Card mit Connect-Service, wahlweise zusätzlich auch mit Tele-Karten-Service der Deutschen Telekom, ist es dem Kunden möglich, ohne Vorauszahlung die angebotenen Dienste zu nutzen. Erst im nachhinein werden die entstandenen Entgelte mittels Kundenkonto abgerechnet. Der rechtmässige Eigentümer einer derartigen (Kredit-)Telefonkarte authentifiziert sich bei der Nutzung durch Eingabe seiner Kartennummer. Wird die Kartennummer Dritten bekannt, so können diese die Kartennummer missbrauchen und damit das Telefonkartenkonto des rechtmässigen Eigentümers belasten. Kredit-Telefonkarten werden im Ausland schon seit geraumer Zeit angeboten. Erfahrungen zeigen, dass regelrecht illegaler Handel mit gültigen Telefonkartennummern getrieben wird. Gültige Kartennummern können durch Ausspähen während der Nummerneingabe (Shoulder Surfing) oder auch durch Mitarbeitermissbrauch bekannt werden. Auch in Deutschland sind beispielsweise Calling Card Numbers (Country Direct Service) amerikanischer Gesellschaften illegal erhältlich.

Organisatorische Missbrauchspotentiale

Mitarbeitermissbrauch

Wartungsleute von TK-Gesellschaften, bauausführende Unternehmensmitarbeiter, haben als Folge ihrer Aufgaben Zugang zu den technischen Einrichtungen des TK-Netzes und somit die Möglichkeit, diese Einrichtungen auch (missbräuchlich) zu beeinflussen. Allerdings begrenzt die Deutsche Telekom diese Missbrauchsmöglichkeiten durch interne organisatorische und technische Massnahmen auf ein Minimum. So werden sporadisch grossangelegte, flächendeckende Überprüfungen und Kontrollen durchgeführt, die aber auch in kleinerem Umfang durch die Betriebssicherheitskräfte andauernd durchgeführt werden. Dazu kommen technische Massnahmen wie passwortgeschützte Zugangsprozeduren, Protokollierung der einzelnen Zugriffe und gebäudetechnische Schutzvorkehrungen bezüglich der Zugangsmöglichkeiten des Personals.

Kundenmissbrauch

Schon beim Einrichten eines Telefonanschlusses können vom Kunden vorbereitende Massnahmen ergriffen werden, die späterem Missbrauch dienen. Dies sind beispielsweise unrichtige Angaben bei der Adresse, Mieten von Appartements mit der Absicht, diese baldmöglichst zu verlassen, und Zahlungsverweigerung der ersten Telefonrechnung. Die Zeiträume zwischen den darauffolgenden Mahnungen werden dann genutzt, um das angemietete Appartement, begünstigt durch das anonyme Leben in Hochhäusern, ohne Begleichen der Telefonrechnung verlassen und aufgeben zu können.

Internationale TK-Kriminalität

Aufgrund der globalen Vernetzung von TK-Diensten und -Netzen müssen diese Entwicklungen weltweit betrachtet werden, das heisst, die Vorkommnisse beziehen sich nicht nur auf den nationalen Bereich. Gegenseitige enge Zusammenarbeit aller weltweit agierenden TK-Gesellschaften ist daher Voraussetzung, um dem TK-Missbrauch begegnen zu können.

Zwei Fallbeispiele

Inland

Als vorbereitende Massnahmen mietete sich ein Kunde ein Appartement und schloss einen Nutzervertrag als Unteranbieter mit einem TIS-190-Informationsanbieter. Danach wurde er Kunde der Deutschen Telekom. Es wurde für ihn ein Primärmultiplexanschluss eingerichtet, mit dem er die Möglichkeit hatte, gleichzeitig 30 Verbindungen im TK-Netz zu nutzen. Dies tat er auch, indem er seine eigenen gemieteten TIS-190-Rufnummern belegte, um dort mit steigender Belegungsdauer steigende Einnahmen zu erzielen. Computergesteuert wurden diese Verbindungen nach rund 12 Minuten abgebrochen und erneut hergestellt (Bild 3). Die Deutsche Telekom schaltet automatisch länger andauernde Belegungen bei TIS-190-Anschlüssen nach einer gewissen Zeit ab und versucht durch Verkehrsstrukturmessungen Missbrauch vorzubeugen. Durch die vorgenannten computergesteuerten Unterbrechungen der Belegungen wurden die präventiven Massnahmen der Deutschen Telekom teilweise umgangen.
Der Kunde zögerte die Zahlung der ersten Telefonrechnung hinaus. Durch Hinweise des (Haupt-)TIS-190-Informationsanbieters gelang es der Betriebssicherung, die betrügerischen Absichten des Kunden zu erkennen und die Strafverfolgungsbehörden rechtzeitig einzuschalten.

Ausland

Wie eine Reise in nur einigen Minuten um die Welt mutet der nachfolgend beschriebene Missbrauch, ebenfalls um Einnahmen mit TIS-190-Anschlüssen betrügerisch zu erhöhen, an (Bild 4). Von unterschiedlichen Telefonanschlüssen (A) aus wurden kostenfrei mit gestohlenen Telefonkartennummern der Country Direct Service im Ausland (D) benutzt und dort TK-Anlagen (E) mit Durchwahlfunktion und erhackten PINs angewählt. Zur Erhöhung der Effektivität vervielfachte man diese Verbindung (max. Faktor 15) durch Nutzung von Konferenzschaltungen und wählte nach Deutschland zurück. Hier wurden dann die eigenen TIS-190-Anschlüsse (H) über das Funknetz mit Anrufweiterschaltung geführt – denn der TIS-190 ist für vom Ausland ankommende Gespräche gesperrt –, angewählt und belegt. Durch eine Änderung der Tarifierung des C-Netzes konnte dieser Missbrauch unterbunden werden.

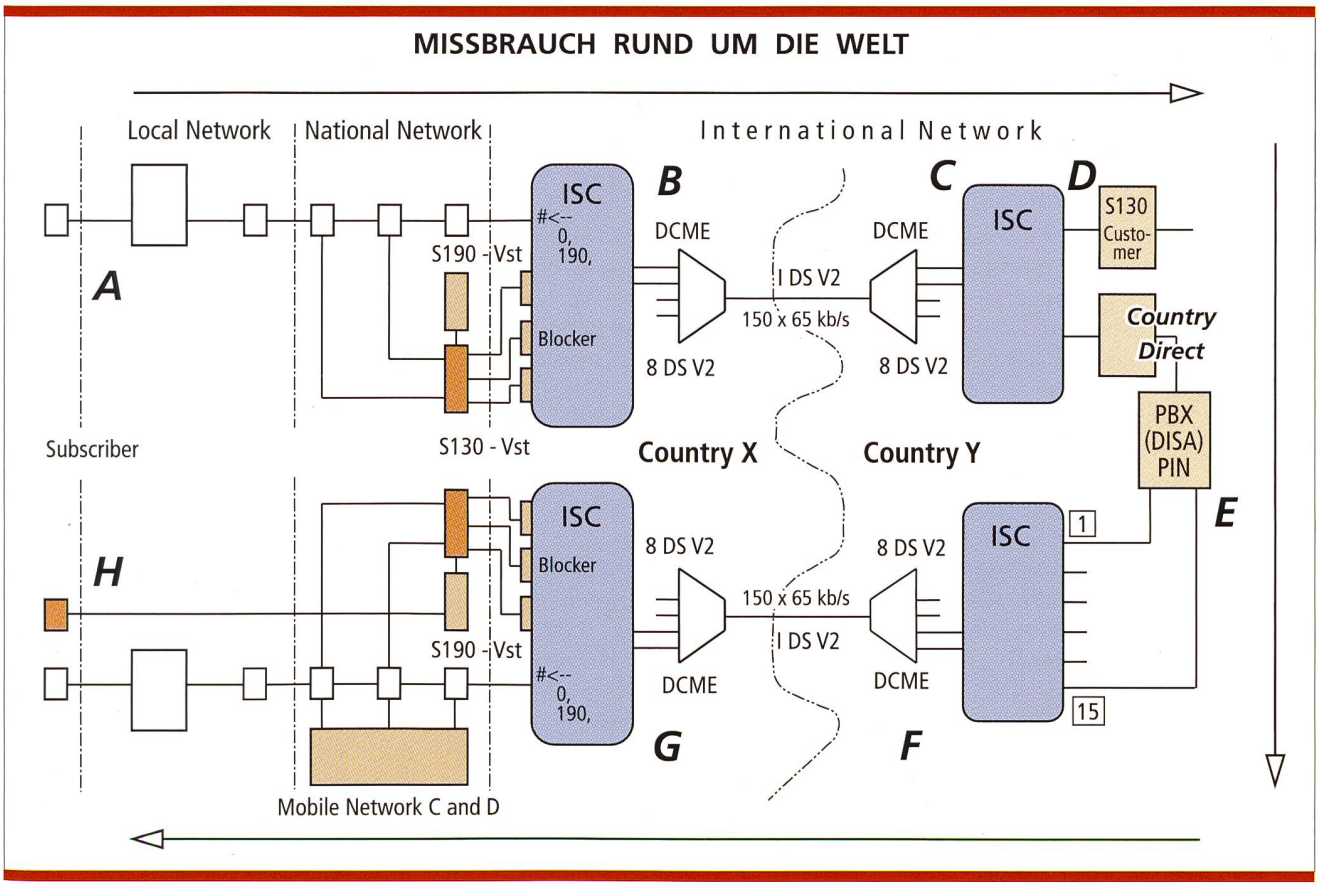

Bild 4. Kostenfreies Telefonieren mit gestohlenen Telefonkartennummern.

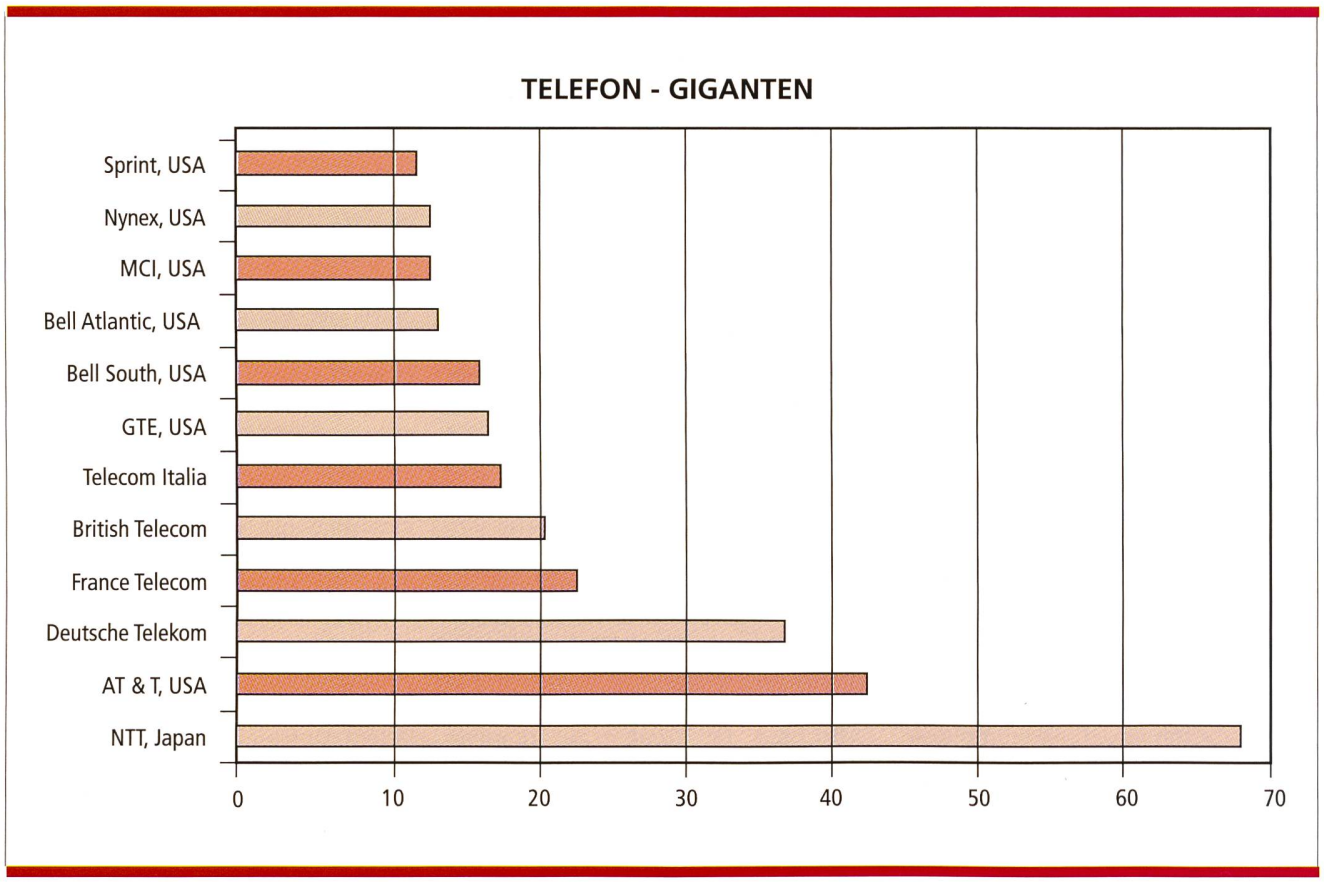

Bild 5. Grössenordnung des Telekommunikationsmarktes. Umsatz in Milliarden Dollar (ITU).

Verbreitung krimineller Informationsinhalte über das TK-Netz

Nicht nur der Missbrauch der technischen Einrichtungen, sondern auch der Inhalt der übertragenen Information kann einen Straftatbestand erfüllen.

Zurzeit wird von den Strafverfolgungsbehörden verstärkt darauf hingewiesen, dass Informationen mit pornographischem Inhalt über die Kommunikationsnetze, insbesondere über das Internet, verbreitet werden. Von der Gesellschaft als besonders verabscheuungswürdig werden dabei pornographische Inhalte mit Kindern und sonstigen Schutzbefohlenen empfunden.

Doch auch politische Gruppen mit extremen Ansichten nutzen die Kommunikationsnetze, um ihre rassistischen, volksverhetzenden und menschenverachtenden Inhalte zu verbreiten.

Die Anbieter von pornographischen oder volksverhetzenden Informationen fühlen sich bei ihren Aktivitäten durch die Anonymität der Übertragungswege ausreichend geschützt. Wie schwer es tatsächlich ist, ihrer habhaft zu werden, konnte erst in jüngster Zeit in den Medien verfolgt werden. Der Schritt von der Verhinderung von sich nicht mit der Rechtsordnung deckenden Texten und Bildern bis zur ungewollten Zensur ist sehr klein.

Um welchen Markt geht es?

Aus Bild 5 wird deutlich, welche Grössenordnung der Telekommunikationsmarkt heute schon hat. Wirtschaftsexperten sehen ein weiteres erhebliches Wachstum dieses Marktes voraus. Es ist also kein Wunder, dass gerade auch Straftäter versuchen, ihre kriminellen Aktivitäten auf diesen Markt zu verlagern. Zu befürchten ist, dass sich hier ähnliche Entwicklungen abspielen, wie wir sie heute im Automobilbereich vorfinden. Dort fordern Autodiebe und Schlepperbanden die Hersteller heraus, immer mehr und verbesserte Sicherheitsvorkehrungen gegen Diebstahl zu entwickeln.

Die bisher verursachten Schäden durch Hacker sind immens. Konkrete Zahlen können an dieser Stelle nicht genannt werden. Es soll jedoch darauf hingewiesen werden, dass sich in einigen aufgedeckten Fällen die Schadenssummen zwischen 200 000 und 10 Mio DM beliefen.

Schutzmassnahmen

Bei der Deutschen Telekom AG kommt als essentieller Bestandteil des Gesamtangebotes an Dienstequalität den Sicherheitsaspekten eine grosse Bedeutung zu. Vor allem vor dem Hintergrund aktueller Missbrauchsfälle war die Konzentration sicherheitsrelevanter Aufgaben in das Zentrum für Netzsicherheit ein grundlegender Vorstandsbeschluss für das Gesamtunternehmen. Unter anderem werden an

Sicherheitsfragen interessierten in- und ausländischen Gästen Unterstützung und Information zu Schutzmassnahmen der Basisinfrastruktur geboten.

Intern

Schulungsmassnahmen

Im Unternehmen werden zur Sensibilisierung der Mitarbeiter in zunehmendem Masse Schulungsmassnahmen organisiert. Wie wichtig die Information und der Umgang mit dem Thema Sicherheit sind, beweisen Untersuchungen des Bundeskriminalamtes, wonach 80 % der erkannten Computermissbräuche auf Innentäter zurückzuführen sind.

SIKO TMN

Bei der Deutschen Telekom erfolgt eine Vernetzung der administrativen und der Mehrwertdienstmanagement-Systeme der Kundenbereiche mit den Managementsystemen der Basisinfrastruktur. Damit werden die Geschäftsprozesse (schnelles Umbuchen und Bereitstellen von Anschlüssen und Übertragungswegen) optimiert. Für diese offene, auf internationalen Standards basierende Platfform werden erhöhte Sicherheitsanforderungen gestellt. Diesen wird durch das Projekt «Sicherheitskonzept Telecommunication Management Network» (SIKO TMN) Rechnung getragen. Bild 6 zeigt die Prinzipdarstellung für Netzelemente der Basisinfrastruktur.

National

Verlässliche Entgelterhebung

Den in der letzten Zeit immer häufiger auftretenden Streitfällen hinsichtlich der Entgelterhebung wurden von der Deutschen Telekom Massnahmen entgegengesetzt, welche unter anderem die Transparenz der Rechnungserstellung (z. B. Anbieten des Dienstmerkmals Einzelverbindungsnachweis) für den Kunden erhöhen. Es wurden Projekte mit verschiedenen unabhängigen Instituten ins Leben gerufen. Dabei ist das Ziel, neben der Transparenz die Glaubwürdigkeit durch Aufdeckung von Schwachstellen und durch Erarbeitung von Verbesserungen und Neuerungen zu unterstreichen. Untersuchungsobjekte sind:

- Entgelterfassung in der digitalen Vermittlungsstelle
- Entgeltdatenübertragung Vermittlungsstelle–Rechenzentrum
- Nachverarbeitung/Rechnungserstellung im Rechenzentrum
- Angriffsmöglichkeiten auf die Signalisierungsprotokolle (DSS1+ZGS Nr. 7)
- Qualitätskonzept zur SW-Erstellung für Module der Entgelterhebung

Monitorsystem

Die Deutsche Telekom setzt zur Erkennung von Missbrauchsfällen ein Monitorsystem ein, welches den internationalen Zeichengabeverkehr (Zeichengabesystem Nr. 7) auf bestimmte Kriterien hin auswertet. Der Zeichengabeverkehr mit anderen Netzen wird an wenigen Punkten konzentriert. Signalling Transfer Points (STP) – in diesem Fall Frankfurt und Düsseldorf – bieten den Zugang zu allen Nachrichten, die über die Netzgrenzen gehen. Zur Auswertung der erhaltenen Daten und zur Einleitung strafrechtlicher Verfolgung existieren in Düsseldorf

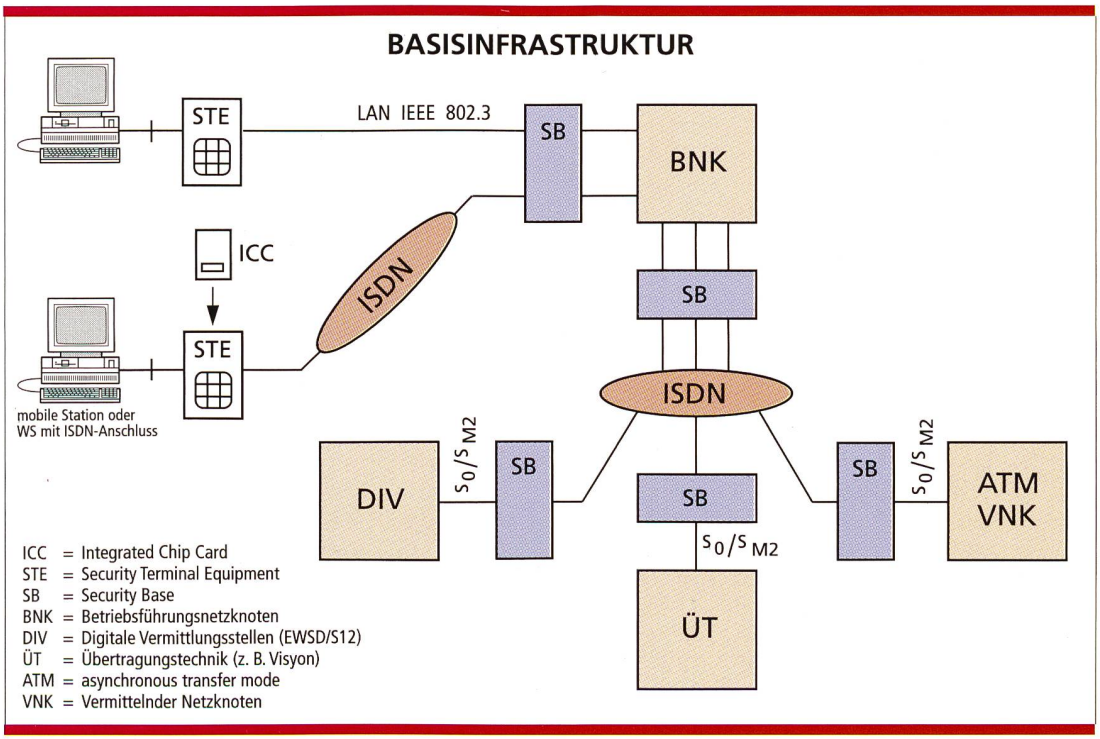

Bild 6. Prinzipdarstellung für Netzelemente der Basisinfrastruktur.

das Worldwide Network International Service Coordination Center (WN ISCC) und ein Fraud Investigation Team (FIT).

Grundsicherheit

Mit der Liberalisierung des Telekommunikationsmarktes werben neben der Deutschen Telekom auch andere Netzbetreiber um die Gunst der Kunden. Die gewährte Sicherheit kann je nach Auffassung der einzelnen Netzbetreiber unterschiedlich hohe Risiken für den Verbraucher (Kunden) bei der Abwicklung seines Verkehrsaufkommens bergen. Der Gesetzgeber hat daher zum Schutz des Verbrauchers ein grosses Interesse, ein gewisses Mass an Grundsicherheit für alle Netzbetreiber zu definieren und vorzuschreiben.

International

Der kriminelle Missbrauch von Telekommunikationsnetzen ist mittlerweile ein internationales Geschäft mit Umsätzen in Milliardenhöhe. Ohne die enge Zusammenarbeit der Netzbetreiber über Ländergrenzen hinaus lässt sich kein wirksamer Schutz gegen Angriffe des Netzes entwickeln. Die Deutsche Telekom arbeitet daher in verschiedenen internationalen Gremien wie zum Beispiel dem FIINA (Forum for International Irregular Network Access) mit. Über Kontaktlisten werden im Ernstfall schnell die Sicherheitsbeauftragten der jeweiligen Netzbetreiber erreicht. [1]

Quelle: Redigierter und leicht gekürzter Vortrag, gehalten anlässlich der 37. Post- und Fernmeldetechnischen Fachtagung des Verbandes der Ingenieure der Post und Telekommunikation e. V., CeBIT '96, Hannover.

Jürgen Haag
Dipl.-Ing., Deutsche Telekom AG

SUMMARY

Criminality in telecommunication networks

Technologies which a few years ago were still regarded as science fiction have now become reality. The networking of our environment with communication systems has in the meantime progressed so far that also private households are increasingly taking advantage of it. At the same time, a new generation of criminals is focusing their fraudulent behaviour in this direction. The international telecommunication market has become their field of activity. Their criminal and fraudulent action yields millions. In the beginning the network was cracked by youthful hackers, or phreaks, as they call themselves, in order to demonstrate their capability. Today the network is misused by criminals who take advantages of the services at the expense of others. There is growing suspicion that also organized syndicates are entering this field.