

2.2 Rückruftrick

Mit der digitalen Telefonie unter dem ISDN-Protokoll²⁹ wurden seit 2002 intelligente Telefonnetze möglich, in denen besondere Angebote wie Mehrwert-, Auskunft- und Dienste mit Kostenteilung angeboten werden konnten³⁰. Sie haben dazu geführt, dass telefonische und andere Kommunikationsdienste im Zusammenhang mit dem Internet miteinander verwachsen sind und sich vor allem nur noch durch ihre Protokolle unterscheiden (Konvergenz). Der Rückruftrick konzentriert sich auf den Missbrauch von Mehrwertdiensten und hat damit einen festen Platz in der IuK-Kriminalität im weiteren Sinne.

2.2.1 Mehrwertdienste und Regulierung

Hinter den Mehrwertdiensten (auch: Premium Rate) steckt die Vorstellung, dass der Zugangsprovider nicht nur eine TK-Verbindung herstellt, sondern *darüber hinaus eine weitere Dienstleistung erbracht wird, die gegenüber dem Anrufer gemeinsam mit der Telekommunikationsdienstleistung abgerechnet wird*³¹. Dafür war zunächst der Nummernkreis (0)190 reserviert, wobei die Rufnummerngruppe (0)19 00 frei tarifierbar war³². Dazu bedurfte es nur einer Vereinbarung zwischen dem Zugangsprovider und dem Anschlussinhaber. Schnell folgten Missbräuche von Premium Rate-Diensten, die die betroffenen Kunden mit immensen Kostenforderungen überraschten. Die Methoden waren immer dieselben: Täuschung über die Tatsache, dass ein solcher Dienst angerufen wird, kostenpflichtige Warteschleifen, Schlechtleistung und untergeschobene Dialer³³.

²⁹  [Integrated Services Digital Network - ISDN](#)

³⁰ [CF, intelligente Nummernverwaltung](#), 21.11.2008

³¹ [BNA, Nummernverwaltung. 0900](#)

³² [CF, 1900-Nummern. Abrechnung. Missbrauch](#), 21.11.2008

³³ Dialer sind automatische Einwahllösungen, die vor allem dadurch bekannt geworden sind, dass sie die Internetzugänge von PCs auf teure Mehrwertdienstenummer „umgebogen“ haben. Sie stellen eine frühe Form der Malware dar, auf die noch näher eingegangen wird.

2003 reagierte der Gesetzgeber mit einer erfolgreichen Regulierung³⁴. Er schuf den Nummernkreis (0)190 ab, führte dafür den neuen Nummernkreis (0)900 ein, deckelte den dabei abrechnungsfähigen Mehrwertanteil (§ 66d TKG) und führte eine Meldepflicht für Mehrwertdienste und Dialer ein. Dazu wurden bei der Bundesnetzagentur – BNA – drei Datenbanken mit den Betreiberdaten eingerichtet. Bei Missbräuchen kann die BNA Rufnummern entziehen, sperren und den Anschlussinhabern die Rechnungslegung untersagen (§ 67 Abs. 1 TKG). Das hat zur Folge, dass die Betreiber ihre vorgeblichen Forderungen nicht mehr gerichtlich durchsetzen können. Die in § 149 TKG aufgeführten Ordnungswidrigkeiten zeigen die Ferkeleien, die im Zusammenhang mit den Mehrwertdiensten stattgefunden haben und noch immer gelegentlich probiert werden³⁵. Dazu werden jetzt häufig teure Auslandsnummern verwendet³⁶, die keine strikte Regulierung wie hierzulande kennen.

2.2.2 automatisierter Rückruftrick

Eine besonders dreiste Form des Rückruftricks wurde 2002 publik und kann sich jederzeit wiederholen³⁷. Der Inhaber von mehreren Mehrwertdienstnummern startete auf seinem Computer ein Programm, das den D1-Nummernkreis systematisch anwählte und die Verbindung sofort wieder unterbrach. Das reicht aber für die Meldung "Anruf in Abwesenheit" auf dem Handy. Nur wenige der Empfänger wählten den Anrufer an und bekamen das Freizeichen zu hören, so als wenn keine Verbindung zustande gekommen wäre. Das Freizeichen stammte jedoch vom Tonband und der Gebührenzähler lief. Sehr lukrativ. Der Täter

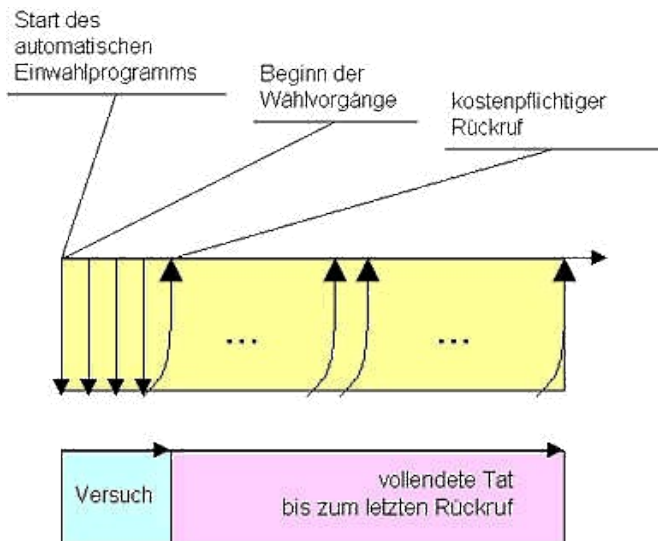
Siehe: [CF, rechtliche Handhabung](#), 21.11.2008.

³⁴ [Gesetz zur Bekämpfung des Missbrauchs von 0190er-/0900er-Mehrwertdiensternummern](#), 09.08.2003

³⁵ [CF, Regelungen im TKG](#), 21.11.2008

³⁶ [CF, Auslandsvorwahlnummern](#), 21.11.2008

³⁷ [0190-Betrug: Jetzt mit "gefälschten" Freizeichen](#), Heise online 07.08.2002



wurde später wegen Betrug zu Freiheitsstrafe verurteilt³⁸.

Materiell handelt es sich tatsächlich um einen Betrug im Sinne von § 263 StGB. Der Täter nutzt zwar die technischen Möglichkeiten, die ihm die mobile Telefonie (Anzeige eines Anrufes in Abwesenheit) und die Computertechnik bieten (automatisches Wählen in Verbindung mit einer Telefonanlage), wählt aber den angesprochenen Nummernkreis selber und startet auch den technischen Vorgang. Dabei hofft er darauf, dass das Opfer unbedacht die Rückruf-Taste seines Handys drückt und dabei nicht vor Augen hat, dass die Verbindung zu einem Mehrwertdienst erfolgt. Das gewählte Beispiel ist deshalb besonders infam, weil die Verbindung tatsächlich aufgebaut und aufrecht erhalten bleibt, während der Anrufer arglos nur ein Freizeichen hört und sich die Gebühren summieren.

Mit dem Start des Einwahlprogramms setzt der Täter nach seiner eigenen Vorstellung von der Tat unmittelbar zur Verwirklichung des Tatbestandes an (Versuch: § 22 StGB). Mit der Auswahl des Nummernkreises hat er die mögliche Zahl und die persönlichen Merkmale der Betroffenen eingegrenzt (Anschlussinhaber unter dem Nummernkreis von D1) und muss keine Handlungen mehr beitragen, um einen Taterfolg herbeizuführen. Alle weiteren Handlungen können nur von dem Opfer selber ausgeführt werden, das mit dem Rückruf den automatischen Gebührenabrechnungsmecha-

nismus anstößt. Der geforderte Irrtum besteht in der Person der Anrufers, der nicht damit rechnet, eine Mehrwertdienstnummer anzurufen, und auch nicht damit, mit einem Tonband oder einem anderen Wiedergabegerät recht einseitig zu kommunizieren. Dabei wird keine technische Einrichtung manipuliert, sondern allein auf die Arglosigkeit des Opfers spekuliert. Dessen Schaden besteht in dem Mehrwertanteil des abgerechneten Entgeltes, der am Ende an den Täter abgeführt wird. Der beträchtliche Technikaufwand, die Einrichtung mehrerer Mehrwertdienstnummern und der auf mehrere Monate ausgerichtete Betrieb der Technik legen einen gewerbsmäßigen Betrug im Sinne von § 263 Abs. 3 Nr. 1 StGB nahe.



Der Tatablauf ist prinzipiell der gleiche, der auch für den Massenversand von Spam- und Phishing-Mails gilt: Der Täter handelt nur **einmal**, indem er den Versand von Nachrichten startet. Die potentiellen Opfer sind aber breit in der Fläche verstreut. Wenn sie mit einer Verzögerung von mehreren Wochen mit ihrer Telefonrechnung zu ihrer örtlichen Polizei gehen³⁹, wird die wahrscheinlich den Inhaber der Mehrwertdienstnummer ermitteln und die Akten an die örtlich zuständige Staatsanwaltschaft abgeben.

Der überschaubare Schaden, den der einzelne Anzeigerstatter erlitten hat, könnte den zuständigen Staatsanwalt dazu veranlassen, das Ermittlungsverfahren gegen eine geringe Geldauflage vorläufig gemäß § 153a StPO einzustellen. Zahlt der Täter die Buße, dann tritt wegen aller anderen Geschädigten Strafklageverbrauch ein (Art 103 Abs. 3 GG⁴⁰), weil alle Schadensereignisse auf das einmalige Handeln des Täters beim Start des Computerprogramms zurück gehen. Sie sind Teil einer einheitlichen prozessualen Tat (§ 264 Abs. 1

³⁹ Ich spreche deshalb häufig von dem „Wäh“, also von dem Menschen, der sich mit seiner Telefonrechnung bewaffnet bei der Polizei über Betrug beschwert.
Zuletzt: CF, der "Wäh!", 01.02.2011

⁴⁰ Dasselbe gilt für Strafbefehle, sobald sie rechtskräftig, und für Anklagen, sobald sie zur Hauptverhandlung zugelassen sind.

³⁸ Die Textpassage stammt aus: CF, Rückruftrick, 2007

StPO).

Das Beispiel lehrt, dass sich auch in Strafanzeigen wegen kleinerer Schäden Teile einer groß angelegten Straftat verbergen können, die nur dann angemessen beurteilt werden kann, wenn ihre Teilakte im Rahmen der Strafverfolgung zusammen geführt werden. Die dazu nötigen Mechanismen, vor allem Melde- und Analysedienste, sind bis heute unvollständig. Allerdings ist die Sensibilität bei den polizeilichen Fachbehörden erheblich gestiegen, so dass jedenfalls erwartet werden kann, dass der klassische Rückruftrick angemessen bearbeitet wird.

2.3 Hacking und Malware

Im Vorgriff auf die besonderen Erscheinungsformen der IuK-Kriminalität müssen die Phänomene und Methoden grundsätzlich betrachtet werden, weil sie in Varianten immer wieder auftauchen.

Noch heute währt eine ideologische Auseinandersetzung über die vor 50 Jahren entstandene Hackerkultur an, wobei sich die Hackerszene von den bedenkenlosen Skript-Kiddies, die unbedacht und skrupellos mit zerstörerischen Werkzeugen hantieren, ohne sie selber entwickelt zu haben oder sie zu beherrschen, von den Crackern, die vor allem Zugangssicherungen zu Programmen und Systemen durchbrechen, um kostenpflichtige Programme oder Dienste ohne Entgelt nutzbar zu machen, und von den Kriminellen abgrenzt, die mit Profitinteresse Malware herstellen, verkaufen und pflegen, Botnetze betreiben, Phishing und andere Formen des Identitätsdiebstahls⁴¹ praktizieren. Darin kommt ein gutes Teil Hilflosigkeit zum Vorschein, weil alle, die „Guten“ wie die „Bösen“, dieselben Methoden, Werkzeuge und Angriffsziele verwenden und sich allenfalls im Motiv unterscheiden. Das zeigt ganz besonders die Auseinandersetzung um das Hackerkollektiv Anonymous⁴².

Hacking und Malware stellen die beiden grundlegenden Strategien dar, mit denen die Penetration bei der IuK-Kriminalität betrieben wird. Beim Hacking erfolgt ein individuell gesteuerter Angriff gegen informationsverarbeitende Systeme mit dem Ziel, in sie einzudringen und zu penetrieren. Der nähere Zweck der Einflussnahme orientiert sich an den Motiven des Hackers und kann wegen des technischen Vorgehens offen bleiben.

Die Spannweite der Akteure und ihrer Motive reicht von berechtigten Auftragsarbeiten von Sicherheitsunternehmen über wohlmeinende, sich aufdrängende Experten bis hin zu Datendieben, Industriespionen und zerstörungswütigen Vanda-

⁴¹ Siehe: Identitätsdiebstahl und Phishing, in: [Dieter Kochheim, Cybercrime](#), 24.06.2010, S. 45.

⁴² [CF, IT-Söldner im Kampfeinsatz](#), 15.02.2011; [Dieter Kochheim, Eskalationen](#), 20.02.2011.