International Working Group
on Data Protection
in Telecommunications

Gemeinsamer Standpunkt

zur Missbrauchserkennung in der Telekommunikation

angenommen auf der 27. Sitzung der Arbeitsgruppe am 4./5. Mai 2000 in Rethhymnon/Kreta

- Übersetzung -

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation weist auf Probleme des Datenschutzes im Zusammenhang mit der Erkennung von Missbrauch in der Telekommunikation hin, insbesondere im Hinblick auf die Verarbeitung von Verbindungsdaten durch die Anbieter von Telekommunikationsdiensten.

Der Begriff Missbrauch wird hier im Sinne von „betrügerischer Inanspruchnahme von Telekommunikationsdiensten“ gebraucht, statt im Sinne von missbräuchlichen Aktivitäten unter Nutzung von Telekommunikationsnetzen (hacking etc.)“. Die Arten des Missbrauchs, die hier behandelt werden, schädigen die Anbieter von Telekommunikationsdiensten, weil diese Dienste anbieten, die nicht oder nur teilweise bezahlt werden, was zu einem Gewinnverlust führt.

Der Umfang des Missbrauchsphänomens in Hinsicht auf finanzielle Verluste der Anbieter ist schwer abzuschätzen. Weltweit werden Zahlen zwischen drei und sechs Prozent genannt. Es ist offensichtlich, dass ein Ansteigen des Missbrauchs zur Besorgnis bei vielen Anbietern führt, besonders weil die Margen für Telekommunikationsdienste in den liberalisierten Märkten schrumpfen. Das liegt im ureigenen Interesse der Anbieter von Telekommunikationsdiensten, diese Arten des Missbrauchs zu begrenzen.

Allgemeine Arten des Missbrauchs

Zwei allgemeine Arten des Missbrauchs sind:

Weiterverkaufs-/Gebührenbetrug. Der Weiterverkauf von Verbindungen an Dritte, ohne den Anbieter für die Verbindungen zu bezahlen. Verschiedene Konstruktionen sind möglich, oft unter Nutzung von „Telefon-Läden“ („phone houses“), Durchwahl-Konstruktionen oder mobilen Endgeräten.

Mehrwertdienstebetrug. Dieser umfasst verschiedene Typen des Missbrauchs kostenintensiver, spezieller Anschlüsse (typischerweise 09-Nummern). In einigen Fällen wird der Anschluss in der Art genutzt, dass Anrufe über manipulierte Telefone zu einem Mehrwertdiensteanschluss getätigt werden. Ein weiterer Ansatz besteht darin, unter Zuhilfenahme von Mittätern Verbindungen zu solchen Mehrwertdiensten aufzubauen, z. B. nach Geschäftsschluss in Büros. Eine weitere Möglichkeit besteht darin, Nutzer, ohne dass diese sich darüber klar sind, zum Anruf bei kostenintensiven Anschlüssen zu verführen. Der Betrüger streicht dabei den Gewinn aus diesen Aktivitäten ein.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

Methoden des Betrugs

Die hauptsächlichen Methoden zum Begehen eines Betrugs sind:

Betrug durch den Teilnehmer. Ein Anschluss wird durch den normalen Anmeldeprozess unter einer falschen oder gestohlenen Identität erlangt. Es ist auch möglich, dass Angestellte von Telekommunikationsdiensteanbietern bei dieser Art des Betrugs mitwirken, z. B. indem sie absichtlich Prozeduren außer Acht lassen, die zur Feststellung der Identität eines neuen Kunden dienen.

„Surfing". Diese Methode schließt verschiedene Formen der unautorisierten Nutzung von Einrichtungen ein:

- Duplizierung von Endeinrichtungen. Identitäten, Telefone oder andere Attribute werden dupliziert.

- Betrug mit „Calling-Cards". Dies schließt den Diebstahl oder den Betrug mit PIN-Codes und wiederaufladbaren Karten ein.

- Missbrauch von Hardware. Dies schließt verschiedene Möglichkeiten zum Eindringen in Telekommunikationsnetzwerke ein.

Wenn dieses „Hacking" einmal erfolgreich war, wird das Netzwerk benutzt, ohne dafür zu zahlen. Zugang zu dem Netzwerk kann erlangt werden durch Service-Einrichtungen in Vermittlungsstellen oder Nebenstellenanlagen, Einwahlnummern, Voice-Mail-Systeme etc.

- Das Anzapfen eines anderen Anschlusses durch physikalische Verbindungen mit diesem Anschluss.

Betrug in der Mobilkommunikation. Die Mobilkommunikation eröffnet verschiedene neue Möglichkeiten zum Betrug. Spezifische Typen des Betrugs, die unter Nutzung von Mobiltelefonen begangen werden, sind die folgenden: Die einfachste Form besteht in dem einfachen Diebstahl von Mobiltelefonen. „Roaming"-Betrug ist eine andere Form; kostenintensive Gespräche werden vom Ausland aus geführt, unter Nutzung der Verzögerung, die bei der Abrechnung solcher Gespräche in dem Land entsteht, wo das Telefon registriert ist. Es wird auch über das Wiederaufladen oder Kopieren vorausbezahlter Karten berichtet. Darüber hinaus existieren auch verschiedene Arten des Betrugs im Zusammenhang mit Anrufweiterschaltung.

Betrugserkennung: Methoden

Die Bekämpfung von Betrug impliziert dessen Entdeckung. In diesem Abschnitt werden einige Hinweise gegeben, wie die Erkennung von Betrug funktioniert und welche Daten als Basis für die angewendeten Techniken genutzt werden.

Der größte Teil der für die Betrugserkennung genutzten Daten sind entweder Einzelverbindungsdatensätze (Call Detail Record - CDRs) oder Abrechnungsdaten. CDRs bestehen aus einer Sammlung von Daten, die durch das Signalisierungssystem durch das Netzwerk übertragen werden. Diese Verbindungsdaten enthalten die anrufende und die angerufene Nummer, die Zeit, die Dauer und andere für die Kommunikation notwendige Daten. In dem Abrechnungssystem werden die CDRs ausgewertet und die Rechnungen für die einzelnen Kunden erzeugt.

Systeme zur Missbrauchserkennung können grob wie folgt zusammengefasst werden:

- Analyse von auf Verbindungsdaten (CDRs) und Abrechnungsdaten basierenden Auswertungen. Dies bedeutet die Analyse der Auswertung und die Suche nach Auffälligkeiten.

- Automatisierte Werkzeuge zur Analyse von CDRs, die auf einem festen voreingestellten Regelsystem basieren. Dies kann während der Kommunikationsvorgänge oder nach deren Abschluss erfolgen. Diese Methode ermöglicht mehr Flexibilität als die einfache Analyse, mit der Möglichkeit, die entsprechenden Regeln anzupassen. Diese Systeme sind typischerweise „Expertensysteme".

- Komplexe automatisierte Systeme mit einer gewissen Lernfähigkeit und der Fähigkeit, selbst neue Regeln zur Erkennung zu entwickeln. Die hierbei gebräuchlichen Techniken sind neuronale Netze, genetische Algorithmen und Data-Warehouse-/Data-Mining-Techniken.

Zur Missbrauchserkennung genutzte Daten

Verschiedene Datenarten werden für die Missbrauchserkennung genutzt. Eine unvollständige Zusammenfassung der in diesem Prozess genutzten Daten schließt ein:

- hohe Nutzungsfrequenz,
- ansteigende Nutzungsfrequenz,
- verdächtige Nutzung, wie der plötzliche Anstieg der Nutzung von Mehrwertdiensten,
- langdauernde Verbindung, z. B. länger als acht Stunden,
- verdächtige Verbindungsziele im Ausland, die als anfällig für Betrug bekannt sind,
- Nutzung kostenintensiver Angebote, die als anfällig für Missbrauch bekannt sind,
- Nutzerprofile, die im Allgemeinen in verschiedene Risikoklassen aufgeteilt sind,
- individuelle Anrufgewohnheiten.

Es wird angeführt, dass Missbrauchserkennungssysteme dataillierte Daten über lange Zeiträume sammeln müssen, um „lernen" zu können. In der Tat wird berichtet, dass die Qualität der Missbrauchserkennung mit fortschreitender Zeit ansteigt, wenn „Data Mining"-Verfahren und andere vergleichbare Techniken angewandt werden. Dies setzt die Aufbewahrung der gesamten zurückliegenden Verbindungsdaten voraus. Generell nehmen der Umfang der gesammelten Daten und der Zeitraum, in dem diese Daten für Analysezwecke aufbewahrt werden, mit der Komplexität und Anpassungsfähigkeit der Betrugserkennungssysteme zu.

Datenschutzaspekte

Die Missbrauchserkennung birgt verschiedene Datenschutzrisiken. Unschuldige Bürger können als potenzielle Betrüger behandelt werden, es gibt ein Risiko für falsche Entscheidungen; Daten, die für den Zweck der Missbrauchserkennung verarbeitet werden, können ihrerseits missbraucht werden und die Übermittlung und Nutzung dieser Daten an Dritte (Polizei, Geheimdienste) kann außerhalb der Kontrolle der Betreiber liegen.

Was sind die gesetzlichen Rahmenbedingungen im Hinblick auf die Aktivitäten der Telekommunikationsdiensteanbieter zur Missbrauchserkennung? Die Erkennungsmethoden stützen sich auf die Analyse von Verkehrsdaten, die in einem allgemeinen Sinne als personenbezogene Daten anzusehen sind. Die Verarbeitung von Verbindungsdaten sollte daher den Datenschutzbestimmungen genügen.

Von der Perspektive der Telekommunikationsanbieter aus gesehen eröffnet die Formulierung in den anwendbaren Gesetzen einen Interpretationsspielraum im Hinblick darauf, welche Daten sie rechtmäßig erheben, verarbeiten und speichern können. Dasselbe gilt für die Zeitdauer, für die die Daten gespeichert werden.

Empfehlungen der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation

1. Methoden zur Begrenzung des finanziellen Risikos wie Systeme mit vorheriger Bezahlung, die Verkürzung von Abrechnungszeiträumen oder garantierte Zahlungen sind generell den Methoden zur nachträglichen Überwachung oder Analyse des persönlichen Verhaltens vorzuziehen.

2. Die Anwendung von Missbrauchserkennungssystemen sollte auf diejenigen Fälle begrenzt werden, in denen präventive Maßnahmen zur Minimierung des Risikos erwiesenermaßen gescheitert sind. Generell ist die umfassende Aufbewahrung von Verbindungsdaten für verlängerte Zeiträume zum Zwecke der Missbrauchserkennung nicht zu rechtfertigen.

3. Systeme zur Missbrauchserkennung existieren in verschiedener Ausprägung und die Daten, von denen behauptet wird, dass sie für die Missbrauchserkennung erforderlich sind, differieren stark, abhängig von der Art des Betrugs und den für die Betrugserkennung eingesetzten Technologien. Jede Art des Betrugs sollte in der Art behandelt werden, die den Datenschutz am wenigsten einschränkt; z. B. sollte der Betrug durch Kunden durch die Verbesserung von Verfahren zur Überprüfung der Kreditwürdigkeit der Anschlussinhaber begrenzt werden.

In Fällen, in denen Missbrauchserkennungssysteme automatisierte Entscheidungen treffen, sollten die Betroffenen darüber informiert werden und Möglichkeiten des Rechtsschutzes erhalten.