International Working Group
on Data Protection
in Telecommunications

675.29.11 19. November 2004

Arbeitspapier
zu Mitteln und Verfahren der datenschutzfreundlichen Bekämpfung des Online-Betrugs

angenommen auf der 36. Sitzung am 18.-19. November 2004
in Berlin

- Übersetzung -

Wie in der realen Welt besteht Kriminalität zum größten Teil aus Eigentumsdelikten. Die am meisten verbreitete Form sind offenbar Betrug und Urheberrechtsverletzungen.

Das Zentrum für Beschwerden gegen Internetbetrug (Internet Fraud Complaint Center (IFCC)) nennt Internetbetrug in seinem Bericht für 2002 als wachsendes Problem[1]. Betrug bei Versteigerungen war das am häufigsten angezeigte Vergehen.

Der Ministerrat der OECD hat die „OECD Richtlinien zum Schutz der Verbraucher vor betrügerischen grenzüberschreitenden Handelspraktiken“ am 11. Juni 2003 beschlossen[2]. Viele Mittel wurden zur Bekämpfung der Cyberkriminalität/des Online-Betrugs vorgeschlagen. Die meisten davon betreffen verbesserte Formen der Strafverfolgung und verbesserte Zusammenarbeit zwischen den Regierungen. Auch wenn diese Mittel zweifellos nützlich sind, können sie auch zu Datenerhebungen und -übermittlungen Anlass geben, die Datenschutzprobleme aufwerfen.

Demgegenüber sind Mittel, die die Vorbeugung in den Vordergrund stellen, bisher offenbar weniger beachtet worden. Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation betont die positiven Wirkungen, die präventive Techniken auf die Senkung der Kriminalitätsrate im allgemeinen und die Sicherung von Aspekten des Datenschutzes bei der Strafverfolgung haben kön-

[1] www.ic3.gov/media/annualreport/2002_IFCCReport.pdf
[2] http://www.oecd.org/dataoecd/24/33/2956464.pdf

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.datenschutz-berlin.de

nen. Die Internationale Arbeitsgruppe zum Datenschutz bei der Telekommunikation hat sich mit diesem Fragenkreis bereits früher befasst[3].

Die folgenden Methoden und Techniken können zur datenschutzgerechten Bekämpfung des Online-Betrugs genutzt werden:

- **Digitale Signaturen** können dazu beitragen, die Geschäftspartner zu identifizieren;
- **Treuhanddienste** können den Austausch von Waren und Geld für beide Parteien durch den Einsatz von vertrauenswürdigen Dritten sicherer machen;
- **Auditierung und Gütesiegel** können den Kunden helfen, vertrauenswürdige Online-Händler zu erkennen;
- **Verbesserte Bezahlverfahren** sind weniger anfällig für Betrugsmanöver;
- **Besser informierte Kunden** werden seltener Opfer solcher Manöver;
- **Besser informierte Unternehmen** neigen eher dazu, Systeme zu nutzen, die besser gegen Betrug geschützt sind
- **Verbesserte Sicherheit** kann viele Formen betrügerischen Handelns verringern, das Computersysteme ins Visier nimmt oder deren Schwächen ausnutzt, um Menschen zu täuschen.

Die Erläuterungen zu diesem Dokument enthalten praktische Beispiele hierfür.

Schlussfolgerungen

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation empfiehlt, dass Behörden

- in erster Linie Mittel einsetzen sollten, die dem Online-Betrug vorbeugen, bevor sie Maßnahmen ergreifen, die derartige Straftaten nach ihrer Begehung bekämpfen sollen,
- Informationen und Beispiele der datenschutzfreundlichen Bekämpfung von Online-Betrug sammeln sollten,
- solche Informationen austauschen sollten,
- die Annahme datenschutzfreundlichen Verhaltensmaßregeln durch die Wirtschaft, insbesondere die Diensteanbieter, fördern sollten und
- die Öffentlichkeit und die Wirtschaft entsprechend informieren sollten.

[3] Gemeinsamer Standpunkt zur Missbrauchserkennung in der Telekommunikation, angenommen auf der 27.Sitzung der Arbeitsgruppe am 4./5.Mai 200 in Rethymnon/Kreta, http://www.datenschutz-berlin.de/attachments/231/fr_de.pdf

Erläuternder Bericht
zum Arbeitspapier zu Mitteln und Verfahren der datenschutzfreundlichen Bekämpfung des Online-Betrugs

Dieser erläuternde Bericht stellt detaillierter einige der Verfahren zusammen, die genutzt werden können, um Online-Betrug ohne Verletzung von Bürgerrechten zu bekämpfen. In diesem Bericht wird auf vorhandene Beispiele entsprechender Dienstleistungen und Produkte hingewiesen. Dies ist nicht als positive Bewertung durch die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation zu verstehen. Die Beispiele dienen lediglich als Anhaltspunkte für bereits vorhandene Lösungen. Die Informationen und Hyperlinks entsprechen dem Stand vom November 2004.

Digitale Signaturen
Digitale Signaturen können dazu beitragen, die Geschäftspartner zu identifizieren. Eine digitale Signatur ist eine von mehreren Möglichkeiten, um sich der Identität des Geschäftspartners zu vergewissern.

Digitale Signaturen sind nicht überall verfügbar und sie sind nicht perfekt. Es wird immer Mittel geben, um echte, aber irreführende Zertifikate zu erhalten oder um Menschen dazu zu verleiten, ohne digitale Signatur ein Geschäft abzuschließen, aber digitale Signaturen sind dennoch hilfreich.

Unternehmen können signierte Verkaufszertifikate ausstellen, die dem Käufer den Nachweis des Kauf ermöglichen.

Treuhandsysteme
Systeme, in denen der Kaufpreis nicht sofort an den Verkäufer ausgezahlt, sondern von einem vertrauenswürdigen Dritten treuhänderisch verwaltet wird („escrow service“ – Treuhanddienst), können Betrug bei der Lieferung verhindern, bei dem ein unehrlicher Verkäufer Vorauszahlung verlangt und dann nicht liefert. Diese Art des Betrugs ist besonders verbreitet bei Online-Auktionen. Der IFCC 2002 Internet Betrugsbericht nennt den Fall „Vereinigte Staaten gegen Teresa Smith“, in dem Frau Smith Computer auf Internet-Auktionsplattformen verkaufte, aber nicht lieferte. Sie betrog auf diese Weise mehr als 300 Opfer und erschlich mehr als $ 800.000.

Bei einem Treuhanddienst übergibt der Käufer den Kaufpreis dem Treuhänder. Der Verkäufer erhält eine Information vom Treuhänder, dass das Geld für ihn bereit liegt und nicht zurückgezogen werden kann, während der Käufer den Treuhänder anweist, das Geld auszuzahlen, wenn er den Kaufgegenstand erhalten hat. Im Streitfall bleibt das Geld beim Treuhänder hinterlegt, bis eine Einigung erzielt werden kann. Ein richtig eingesetzter Treuhanddienst kann Online-Betrug erheblich erschweren. Der Betrüger muss den Käufer oder den Treuhänder dazu verleiten, den Kaufpreis zu überweisen (z.B. indem er Gegenstände liefert, die ordnungsgemäß erscheinen, aber qualitativ minderwertig sind, oder indem er eine Auszahlungsanweisung fälscht). Alle diese Manöver sind allerdings für den Betrüger riskant und kostspielig.

Der Nachteil von Treuhanddiensten ist, dass sie für beide Parteien verfügbar und von ihnen akzeptiert sein müssen und dass sie Geld kosten. Personen, die an Geschäften mit legitimen, aber anstößigen Produkten (z.B. Pornographie) beteiligt sind, lehnen die Inanspruchnahme eines Treuhanddienstes möglicherweise aus Datenschutzgründen ab. Hochprofessionelle Betrüger können ihre eigenen Treuhanddienste anbieten. Andere Kriminelle können leichtgläubige Menschen davon abhalten, einen Treuhanddienst zu nutzen.

Ein zusätzlicher Vorteil aus Datenschutzsicht besteht darin, dass der Verkäufer vom Treuhänder die Information erhält, dass der vereinbarte Kaufpreis bereitliegt. Der Verkäufer muss nicht die Kreditwürdigkeit des Käufers überprüfen. Er muss nur dem Treuhänder vertrauen.

Ebay, ein populäres Internet-Auktionshaus, empfiehlt Treuhanddienste:
http://www.ebay.com/help/community/escrow.html

Verkäufer sollten ermutigt werden, mit Treuhanddiensten zusammenzuarbeiten und sie ihren Kunden zu empfehlen.

Auditierung und Gütesiegel
Wie kann man sich der Vertrauenswürdigkeit des Verkäufers versichern ? Um diese Frage zu beantworten, sind verschiedene Programme für Audits und Gütesiegel entwickelt worden.

Diese Programme mögen nicht perfekt sein, aber sie sind ein Unterscheidungsmerkmal zwischen einem Online-Shop, über den die Kunden keine Informationen haben, und einem Online-Shop, der von einer vertrauenswürdigen Stelle geprüft worden ist.

Verbesserte Bezahlverfahren
Ein großer Teil des Potentials für Missbrauch und Betrug liegt in technischen und organisatorischen Schwächen der Bezahlverfahren. Vor allem Kreditkarten sind besonders leicht zu missbrauchen. Viele Formen des Betrugs beziehen sich auf Kreditkartenzahlungen.

Die Behörden sollten prüfen, was zur Verbesserung der Bezahlungssysteme getan werden kann, so dass Betrüger weniger Möglichkeiten haben, um Sicherheitslücken auszunutzen.

Kundeninformation
Die beste Waffe gegen Betrug ist Information. Viele Länder haben bereits gute Kundeninformationsdienste, andere sollten nachziehen. In einigen Ländern bietet auch die Polizei Informationen an.

Es gibt genug Informationen (allerdings häufig auf Englisch). Die Bereitstellung und Verbreitung solcher Informationen in einer Sprache und Form, die den Bürgern entspricht, kann von großer Hilfe sein.

Informationen für Unternehmen
Sobald die Wirtschaft Systeme mit höherer Sicherheit einsetzt, die weniger anfällig für Manipulationen sind, dürfte dies die Betrugsfälle reduzieren.

Erhöhte Sicherheit
Betrug im Zusammenhang mit Angriffen auf Computersysteme wird häufig erleichtert durch unzureichende Sicherheitsmaßnahmen und unsicheren Programmen.

Betrug, der auf Computersysteme abzielt, ist eine verhältnismäßig neue Kriminalitätsform. Beim Computerbetrug ist das Hauptziel des Betrügers das Computersystem des Opfers. Der Kriminelle ist bestrebt, durch Manipulationen am Computer Zugriff auf finanzielle Mittel, Zugriffsrechte oder Ressourcen zu erhalten, die ihm nicht zugänglich sind oder die ihn Geld kosten würden. Einige Betrüger kopieren Kreditkarten-Daten, um Kreditkarten-Gesellschaften oder Banken zu betrügen[4]. Diese Betrugsart kann den Nutzer einbeziehen, allerdings nur zu einem bestimmten Grad, etwa indem jemand dazu verleitet wird, eine Programm herunterzuladen, das es dem Angreifer erlaubt, auf den Computer zuzugreifen („Trojanisches Pferd“).

Andere Kriminelle fälschen e-mails von Banken, um die Empfänger dazu zu veranlassen, Zugangsdaten für ihre Konten einzugeben (dies wird als „phishing“ bezeichnet). Phisher missbrauchen Sicherheitslücken in Browsern und e-mail-Programmen, um den fälschlichen Eindruck zu erwecken, jemand besuche die Website seiner Bank, während er in Wirklichkeit auf einer gefälschten Seite mit einer anderen Adresse ist.

[4] Dies wird häufig als „Identitätsdiebstahl“ bezeichnet.

Eine inzwischen verbreitete Angriffsart ist die heimliche Zweckentfremdung von Computern zur Versendung von unerwünschter Werbung (Spam). Dies ist zwar nicht Betrug im klassischen Sinn, es beruht aber auf Täuschung, um rechtswidrige Handlungen vorzunehmen. Darüber hinaus bieten viele Spam-Versender in betrügerischer Weise Güter und Dienstleistungen an. Weniger Spam bedeutet weniger Betrug.

Der beste Weg, solche Straftaten zu bekämpfen, ist die Verbesserung der Computersicherheit. Die Behörden können bessere Sicherheitsmaßnahmen, schnellere Reaktionen auf Sicherheitslücken und –bedrohungen und Rechtsbehelfe zum Schutz vor Schäden durch unsichere Systeme vorschlagen. Es ist möglich, die Bürger zum Einsatz von Technologie mit höherer Sicherheit aufzufordern.

Hersteller können dies ebenfalls unterstützen, indem sie die Vorteile von Hard- und Software-Lösungen mit höherer Sicherheit herausstellen, insbesondere beim Einsatz von Firewalls bei Breitbandverbindungen. Diese können die Angriffsmöglichkeiten reduzieren, indem sie unerkannte eingehende Verbindungsversuche blockieren.

Manchmal können sogar einfache Dinge wie ein gutes e-mail-Programm und ein gut gemachter Web-Browser hilfreich sein.