2573/AB XXIII. GP

Eingelangt am 29.01.2008

BM für Inneres

Anfragebeantwortung

Frau
Präsidentin des Nationalrates
Mag. Barbara Prammer
Parlament
1017 Wien

Die Abgeordneten zum Nationalrat Ing. Norbert Hofer, Kolleginnen und Kollegen haben am 29. November 2007 unter der Nummer PA 2427/J an mich eine schriftliche parlamentarische Anfrage betreffend „Internetkriminalität“ gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

Zu Frage 1:

Es erfolgt bei der Kriminalstatistik seit dem Jahr 2005 eine Aufgliederung nach den Fällen „Betrug bei Internetauktionen“. Eine Unterscheidung der vermeintlich angebotenen Waren wird allerdings nicht durchgeführt. Die Anzahl der Fälle mit Betrug bei Internetauktionen lag im Jahr 2005 bei 1.163 Anzeigen und im Jahr 2006 bei 2.612 Anzeigen.

Zu Frage 2:

Seitens der österreichischen Sicherheitsbehörden wurde die Zusammenarbeit mit Plattformen, welche Internetauktionen anbieten, verbessert. IP Adressen werden rückverfolgt und Täter können daher ausgeforscht werden. Geschädigte, welche noch keine Anzeige erstatteten, werden kontaktiert. Warnmitteilungen erfolgen an die Plattformen, welche verdächtige Angebote löschen. Dadurch kann weiterer Schaden abgewendet werden. Plattformen geben Sicherheitshinweise und weisen die User auf diese Erscheinungsformen des Betruges hin. Mit dem größten Auktionsanbieter erfolgt ein regelmäßiger Erfahrungsaustausch sowie Vorträge bei Schulungen.

Durch die laufenden Erhebungen und Fahndungserfolge in diesem Bereich wird von den Tätern das Bundesgebiet gemieden.

Zu Frage 3:

Betrugsdelikte werden im Internet in vielfältiger Weise begangen. Eine gesonderte Auswertung der Betrugsfälle im Internet wird nicht durchgeführt. Für sämtliche strafbare Handlungen ist eine Auswertung, bei der ein IT-Medium zur Tatbegehung verwendet wird oder wo das Tatobjekt ein IT-Medium ist, möglich. Die Kriminalstatistik zeigt hier folgendes Bild:

Angezeigte Fälle	Jahr 2002	Jahr 2003	Jahr 2004	Jahr 2005	Jahr 2006
Tatbegehung mittels IT-Medium	4.785	3.335	4.328	2.430	3.335
Tatbegehung mittels IT-Medium (Abhören von Daten-verkehr)	-	1	1	2	2
Tatbegehung mittels IT-Medium (Datenbezogene Wirtschaftsspionage)	-	2	1	-	-
Tatobjekt ist das IT-Medium (Hardware-Sabotage)	38	30	20	-	-
Tatobjekt ist das IT-Medium (Hacking)	11	-	-	-	13
Tatobjekt ist das IT-Medium (Trojanische Pferde)	4	-	-	-	2
Tatobjekt ist das IT-Medium (Viren)	10	-	-	-	1
Tatobjekt ist das IT-Medium (Software-Sabotage)	19	-	-	-	7
Tatobjekt ist das IT-Medium (Würmer)	2	-	-	-	-
Tatobjekt ist das IT-Medium (Telefon-Phreaking)	98	86	413	25	30

Zu Frage 4:

Es erfolgt seit dem Jahr 2005 eine Auswertung der Schadenssumme für Betrug bei Internetauktionen. Die Schadenssumme im Jahr 2005 ergab EUR 1.815.573,91 und im Jahr 2006 EUR 1.999.550,29.

Zu Frage 5:

Die Kooperation mit Betreibern von Internetportalen wurde intensiviert. Die Betreiber weisen auf die möglichen Gefahren hin und geben Sicherheitshinweise.

Auch werden in den Medien diese Betrugsdelikte thematisiert und die Bevölkerung gewarnt. Ferner werden die Polizeibediensteten in diesen Bereichen laufend geschult.

Es gibt eine enge Kooperation mit Bankinstituten hinsichtlich Phishing und eine Hotline wurde für die Banken für diesen Bereich eingerichtet. Die Zahl der Phishingfälle ist deshalb in Österreich, im Gegensatz zu anderen Ländern, sehr stark gesunken.

Zu Frage 6:

Die internationale Zusammenarbeit ist beim Internetbetrug als grenzüberschreitendes Delikt unerlässlich und es erfolgen Anfragen über die österr. Verbindungsbeamten oder über Interpol und Europol an die betroffenen Staaten. Vor allem im Bereich des Betrugs in Zusammenhang mit Internetauktionen werden Geschädigte, welche noch keine Anzeige erstattet haben, kontaktiert. IP Adressen werden rückverfolgt und die zuständigen Staaten kontaktiert.

Zu Frage 7:

Die Internetkriminialität tritt in verschiedensten Formen auf.

Bei echten Computerdelikten wird in die Software der User ohne deren Wissen eingegriffen oder es werden die Zugangsdaten von Usern herausgelockt und missbräuchlich verwendet. Beim Phishing wird versucht, den Empfänger mit einer E-Mail zur Herausgabe von Zugangsdaten und Passwörter zu bewegen. Meist erfolgt dies im Zusammenhang mit Online Banking. Zur Täuschung der Opfer werden Internetseiten von Bankinstitutionen täuschend ähnlich nachgemacht um den Geschädigten zur Bekanntgabe seiner Zugangsdaten zu bewegen. Die Täter verwenden auch Trojaner und Keylogger um an die Zugangsdaten und Passwörter zu gelangen. Beim Pharming erfolgt eine Manipulation der DNS-Anfragen und Internetnutzer werden dadurch auf gefälschte Webseiten, die den Original-Seiten oft täuschend ähnlich sehen, umgeleitet und unter Vortäuschung falscher Tatsachen dazu bewegt, ihre geheimen Online-Banking-Daten preiszugeben.

Bei DDos-Attacken werden Rechner oder Netzwerke mit dem Ziel angegriffen, die Verfügbarkeit dieser Rechner außer Kraft zu setzen. Der Angriff erfolgt unbewusst von Usern, deren Rechner durch Viren oder Hackerangriffe von den Tätern gesteuert werden.

Weiters dient das Internet nur als Mittel zum Zweck gerichtlich strafbarer Handlungen. Für diese unechten Computerdelikte werden beispielsweise angeführt:

Bei Betrug im Auktionshandel werden verschiedene handelsfähige Gegenstände (vor allem Kraftfahrzeug und Elektronikartikel) angeboten. Nach Bezahlung durch den potentiellen Käufer werden die Waren nicht dem Käufer zugestellt.

Auch Dienstleistungen werden im Internet in betrügerischer Weise angeboten. So werden beispielsweise Ratschläge für Arbeiten im Ausland oder Heimarbeiten gegen Entgelt angeboten und es erfolgt keine entsprechende Gegenleistung.

Von Betrügern werden ferner Hotelzimmer gebucht und im Voraus mit einem Scheck bezahlt. Anschließend erfolgt eine Stornierung mit dem Ersuchen, den Scheckbetrag abzüglich einer Stornogebühr zurück zu überweisen. In ähnlicher Weise werden überhöhte Schecks übermittelt und es wird ersucht, den Differenzbetrag ebenfalls zurück zu

überweisen. In beiden Fällen stellt sich der Scheck dann als Fälschung heraus oder ist nicht gedeckt.

Bei den „419 Briefen“ werden E-Mails versandt und vom Absender angegeben, über große Geldsummen zu verfügen. Das Opfer soll einen wesentlichen Teil dieser Geldsumme erhalten und wird um Unterstützung sowie um Überweisung von Geld für die Bezahlung von Rechtsanwälten, Gebühren usw. aufgefordert.

Für Anlagebetrügereien und Teilnahme an betrügerischen Gewinnlotterien wird ebenfalls per E-Mail geworben.

Über das Internet werden weiters kinderpornografische Darstellungen, ge- oder verfälschte Waren (Produktpiraterie), Waffen usw. abgesetzt sowie Urheberrechtsverletzungen begangen.

Zu Frage 8:

Angezeigte Fälle	Jahr 2002	Jahr 2003	Jahr 2004	Jahr 2005	Jahr 2006
§ 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem)	-	12	26	16	31
§ 119 StGB (Verletzung des Telekommunikationsgeheimnisses)	5	3	7	6	6
§ 119a StGB (Missbräuchliches Abfangen von Daten)	-	1	4	6	-
§ 126a StGB - Vergehen ALT (Datenbeschädigung)	54	-	-	-	-
§ 126a StGB - Vergehen (Datenbeschädigung)	7	30	45	81	40
§ 126a StGB - Verbrechen ALT (Datenbeschädigung)	5	-	-	-	-
§ 126a StGB - Verbrechen (Datenbeschädigung)	-	1	3	7	2
§ 126b StGB (Störung der Funktionsfähigkeit eines Computersystems)	-	4	11	6	5
§ 126c StGB (Missbrauch von Computerprogrammen oder Zugangsdaten)	-	8	32	26	45
§ 148a StGB – Vergehen (Betrügerischer Datenverarbeitungsmissbrauch)	167	103	78	86	210
§ 148a StGB - Verbrechen (Betrügerischer Datenverarbeitungsmissbrauch)	9	4	2	8	51
Missbrauch von Computer für herkömmliche Betrugshandlungen	7	37	28	35	79

Zu Frage 9:

Die Zusammenarbeit mit ausländischen Dienststellen wurde intensiviert und verbessert. Weiters wurden die Schulungen für Polizeibeamte über die Arten der Internetkriminalität sowie für die IT Beweissicherung durchgeführt. Täter der „419 Briefe“ meiden daher die persönliche Kontaktaufnahme im österr. Bundesgebiet. Dadurch kann eine große Präventivwirkung erzielt werden.

Zu Frage 10:

Die internationalen Aktivitäten erfolgen durch Zusammenarbeit im Rahmen von Interpol und Europol mit ausländischen Dienststellen. Durch die Anfragen und Auskunftserteilung können Geschädigte kontaktiert, E-Mails rückverfolgt und Tatverdächtige ausgehoben werden. Weitere Schadensfälle können dadurch rechtzeitig vermieden werden.