

Prof. Dieter Kempf, Präsident des BITKOM

**Statement zur PK „IT-Kriminalität in Deutschland“
Berlin, Bundespressekonferenz, 30. Juni 2011
Seite 1**

Sehr verehrte Damen und Herren,

ich begrüße Sie ebenfalls sehr herzlich zu unserer Pressekonferenz mit dem Bundeskriminalamt. Eine Veranstaltung mit einer gewissen Tradition, jedenfalls nach den Maßstäben unserer Branche. Zum vierten Mal informieren wir gemeinsam über die Entwicklung der Online-Kriminalität.

Wie in den Jahren zuvor haben wir die Bundesbürger befragt: nach ihrer technischen Ausstattung, ihren Ängsten und Erfahrungen, ihren Erwartungen an die Politik. Wir haben die Umfragen mit den Instituten Forsa und Aris gemacht; es wurden jeweils tausend Deutsche interviewt.

Das Hauptergebnis: Ängste und negative Erfahrungen der Internet-Nutzer haben deutlich zugenommen.

Zunächst zu den Ängsten: 85 Prozent der Internetnutzer fühlen sich mittlerweile von Kriminalität im Web bedroht. Das ist ein Anstieg um zehn Prozentpunkte gegenüber 2010. Über 60 Prozent haben Angst vor Viren oder anderen Schadprogrammen. Besonders stark gestiegen ist die Befürchtung, persönliche Daten könnten ausgespäht und missbraucht werden. Jeder achte Nutzer fürchtet sich vor Beleidigungen und Belästigungen im Internet, und jeder zehnte vor Mobbing.

Die Angst davor, Opfer zu werden, ist meist größer als das reale Risiko. Dennoch: Sieben von zehn Web-Nutzern haben bereits Erfahrungen

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstr. 10 A
10117 Berlin-Mitte
Tel. +49. 30. 27576-0
Fax +49. 30. 27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Marc Thylmann
Pressesprecher
Tel. +49. 30. 27576-111
Fax +49. 30. 27576-400
m.thylmann@bitkom.org

Präsident
Prof. Dieter Kempf

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Prof. Dieter Kempf**Statement zur PK „IT-Kriminalität in Deutschland“****Berlin, Bundespressekonferenz, 30. Juni 2011**

Seite 2

mit Kriminalität im Internet gemacht. In den meisten Fällen sind es klassische Virenangriffe. Das klingt harmloser als es ist. Denn diese Schadprogramme werden immer gefährlicher. Der Trend geht hin zum professionellen Ausspähen persönlicher Daten und Passwörter – und damit dem Diebstahl vollständiger digitaler Identitäten.

Die Umfrage ergab: Fast jeder Zweite hatte bereits einen Virus, Wurm oder ähnliches auf seinem Rechner, und bei jedem Siebten wurden Zugangsdaten ausspioniert. Absolut gesehen hat sich in diesem Bereich die Zahl der Betroffenen in einem Jahr fast verdoppelt, auf knapp 7 Millionen. Ähnlich viele Nutzer gaben an, schon einmal von einem Geschäftspartner im Netz betrogen worden zu sein. Hierzu gehören auch Personen, die bei Online-Auktionen falsche oder beschädigte Ware erhalten haben.

Stark zugenommen hat die Angst vor Betrug beim Online-Banking. Hier gibt es seit Jahren ein Katz- und Maus-Spiel zwischen Geldinstituten und Kriminellen. Bieten die Banken neue Technologien für die Online-Überweisung an, geht die Zahl der Fälle zunächst zurück, bis sich die Kriminellen darauf eingestellt haben – dann steigt sie wieder. Die derzeit rund 27 Millionen Nutzer von Online-Banking sollten daher stets frühzeitig auf neue Verfahren umsteigen, derzeit etwa chipTAN.

55 Prozent der Internet-Nutzer halten ihre persönlichen Daten im Allgemeinen für unsicher. Insbesondere die Jüngeren sind sehr skeptisch. Solche Ängste vor Kriminalität im Web haben konkrete Folgen für die Entwicklung der Online-Dienste: Drei Viertel der Nutzer verzichten wegen Sicherheits-Bedenken auf bestimmte Aktivitäten. 39 Prozent schicken wichtige Dokumente lieber per Post statt per Mail. Drei von zehn Nutzern machen kein Online-Banking – das sind über 14

Prof. Dieter Kempf

Statement zur PK „IT-Kriminalität in Deutschland“

Berlin, Bundespressekonferenz, 30. Juni 2011

Seite 3

Millionen Menschen. Und 15 Prozent, über 8 Millionen, nehmen gar keine Transaktionen im Netz vor. Das sind verschenkte Chancen.

Andererseits surft jeder Fünfte völlig ohne Virenschutz und Firewall. So gefährdet man nicht nur sich selbst, sondern auch andere, mit denen man Daten austauscht.

Unsere Branche hat hier reagiert. IT-Anbieter integrieren Sicherheits-Features direkt in bestehende Produkte. Bei neuen Betriebssystemen werden Virenschutz und Firewall den Käufern kostenlos mit angeboten. IT- und Internet-Sicherheit werden zudem immer häufiger als Service aus dem Netz bezogen. Schon jeder dritte User setzt ein Sicherheitspaket seines Internet-Dienstleisters ein.

Kommen wir nun zu den Trends in der IT-Kriminalität: Mittlerweile geht fast jeder vierte Internet-Nutzer unterwegs per Laptop oder Tablet-PC ins Netz, jeder fünfte per Mobiltelefon. Damit entstehen neue Angriffsflächen. Gerade bei mobilen Geräten wird derzeit kaum auf Sicherheit geachtet – obwohl sie besonders anfällig sind. Die Zahl neuer Schadprogramme für mobile Geräte steigt dramatisch an. Tablet-PCs und Smartphones können sich beim bloßen Surfen Viren einfangen.

Zudem greifen Nutzer mit ihren Handys immer häufiger auf Firmenserver zu und speichern sensible Daten. Aber nur jeder vierte Smartphone-Surfer hat derzeit einen Virenschutz und knapp jeder fünfte eine Firewall aufgespielt. Das ergab eine Studie im Auftrag der Deutschen Telekom. Wir empfehlen für mobile Geräte – neben Virenschutz und Firewall – grundsätzlich, alle Daten zu verschlüsseln.

Auch Unternehmen werden verstärkt Ziel der Online-Betrüger. Nach einer KPMG-Studie verzeichnete über die Hälfte aller Unternehmen, die

Prof. Dieter Kempf**Statement zur PK „IT-Kriminalität in Deutschland“****Berlin, Bundespressekonferenz, 30. Juni 2011**

Seite 4

2010 Opfer von Wirtschaftskriminalität wurden, Schäden durch ITK-Kriminalität. 2006 lag der Wert noch bei 23 Prozent. Insbesondere Mittelständler und kleinere Unternehmen haben oft Nachholbedarf bei der Organisation ihrer IT-Sicherheit. Das ergab eine aktuelle Umfrage von „Deutschland sicher im Netz“ unter fast 1.400 meist kleineren Unternehmen. Nur jedes vierte kleinere Unternehmen schult und informiert regelmäßig seine Mitarbeiter, nur jedes Dritte hat ein IT-Sicherheitskonzept, das von der Geschäftsleitung getragen wird. 37 Prozent sichern ihre geschäftlichen Daten nicht täglich, 7 Prozent sichern nie.

Neben der Mobilität ist ein zweiter Trend das so genannte Social Engineering. Soziale Netzwerke werden verstärkt für personalisierte Angriffe genutzt, um so persönliche Daten auszuspähen. Dies betrifft auch Mitarbeiter in Großkonzernen: Kriminelle versuchen sich Zugang zu sensiblen Informationen zu verschaffen, indem sie Beschäftigte unter Druck setzen oder ihre Hilfsbereitschaft ausnutzen. Daher sollten User persönliche Daten sparsam ins Netz stellen.

Der dritte Trend betrifft besonders produzierende Unternehmen. Moderne Maschinen und Anlagen kommen ohne vernetzte Komponenten nicht mehr aus. Durch diese Vernetzung, zum Teil über das Internet, entstehen ebenfalls neue Angriffspunkte.

Viele Unternehmen tun aber noch immer viel zu wenig für ihre IT-Sicherheit. Hier gibt es neue Lösungen, z.B. Sicherheitsdienste über das Web. Das Stichwort lautet „Security as a Service“. Wer aus Kostengründen oder aufgrund mangelnder eigener Kompetenz nicht in eigene Sicherheitstechnik und entsprechendes Personal investieren will, kann den maßgeschneiderten Service von einem spezialisierten Dienstleister hinzuziehen.

Prof. Dieter Kempf**Statement zur PK „IT-Kriminalität in Deutschland“****Berlin, Bundespressekonferenz, 30. Juni 2011**

Seite 5

Meine Damen und Herren, was folgt aus all diesen Trends und Zahlen?

Was erwarten die Nutzer von den Behörden und der Politik?

Die große Mehrheit der User fordert einen stärkeren staatlichen Schutz im Internet. Vier von fünf Surfern meinen, die Behörden sollten verstärkt eingreifen bei der Aufklärung und Verfolgung von Straftaten. So klar das Ja zur Strafverfolgung, so eindeutig das Nein zur Überwachung: Nicht einmal jeder Dritte befürwortet eine Speicherung von Internet-Verbindungsdaten. Unserer Meinung nach sind Eingriffe des Staates in die informationelle Selbstbestimmung nur bei schwerer Kriminalität oder Gefahr für Leib und Leben zu rechtfertigen.

Und was wünschen wir uns von der Politik? Wir wollen die Zusammenarbeit zwischen Staat und Wirtschaft weiter ausbauen, beispielsweise bei dem neu eröffneten Nationalen Cyber-Abwehrzentrum. Wir wünschen uns, dass auf staatlicher Seite das Know-how weiterentwickelt und insbesondere die Ausstattung verbessert wird. Dies betrifft natürlich weniger das BKA. Viele Polizeidienststellen jedoch könnten personell und technisch besser ausgestattet werden. Zudem setzen wir uns für spezialisierte Staatsanwaltschaften gegen IT-Kriminalität ein.

Die wichtigsten Mittel im Kampf gegen Cyber-Crime bleiben jedoch die Aufklärung und Sensibilisierung der Nutzer. Daher haben Vereine wie „Deutschland sicher im Netz“ eine wichtige Funktion. Dort gibt es kostenfreie Angebote, die zugeschnitten sind auf Zielgruppen wie Kinder, Eltern und Senioren oder mittelständische Firmen.

Sicherheit im Internet ist ein gemeinsames Interesse von Staat, Wirtschaft und Verbrauchern.

Vielen Dank.