Bundeskriminalamt

8. Oktober 2009

Kernaussagen zur IuK-Kriminalität 2008

1 Daten

- Die Zahl der in der Polizeilichen Kriminalstatistik (PKS) erfassten Straftaten, die unter Ausnutzung moderner Informations- und Kommunikationstechnik oder gegen diese begangen werden − die so genannte IuK-Kriminalität im engeren Sinne − stieg in Deutschland von 2007 (34.180) zu 2008 erneut um etwa 11 % auf 37.900 Fälle. Ein großer Anteil der Fälle (17.006) war erneut dem Computerbetrug zuzuordnen; hier stieg das Aufkommen um 4,5 %.
- 2008 wurden zudem vor allem in den Bereichen Ausspähen/Abfangen von Daten (+60 %) und Datenfälschung/Täuschung bei der Datenverarbeitung (+30 %) erhebliche Steigerungen verzeichnet.
- Der im Jahr 2008 registrierte Schaden aller mit Schadenssummen erfassten Delikte der IuK-Kriminalität (im engeren Sinne) beläuft sich auf 37,2 Mio. Euro und ist somit gegenüber dem Vorjahr (31 Mio. Euro) um 20 % gestiegen.
- Im Jahr 2008 wurden in der PKS rund 167.000 Fälle registriert, in denen das Internet Tatmittel war – das ist gegenüber 2007 (179.026) ein Rückgang um 6,5 %. Dennoch bewegen sich die Zahlen weiterhin auf einem hohen Niveau. Im Fünf-Jahres-Vergleich stiegen die Fallzahlen (2004: 54.926 Fälle) sogar um rund 300 %.

2 Wesentliche Lageentwicklungen

- Die Fallzahlen der PKS spiegeln nicht die tatsächliche Lage der IuK-Kriminalität wider. Es ist von einem erheblich größeren Dunkelfeld auszugehen.
- Nach erstmals rückgängigen Zahlen im Jahr 2008 (ca. 1.800 Fälle wurden der Polizei bekannt) geht das BKA für das Jahr 2009 wieder von steigenden Phishing-Zahlen beim Onlinebanking aus, da sich die Täter veränderten technischen Gegebenheiten sehr schnell angepasst haben.
- Die Einführung des iTan-Verfahrens hat zunächst Wirkung gezeigt. Gleichwohl existieren mindestens drei Familien von Schadsoftware, die speziell auf den deutschen Bankenmarkt ausgerichtet sind und das iTAN-Verfahren erfolgreich durch so genannte „Man-In-The-Middle-Attacken“ angreifen können.
- Die Verwertungsmöglichkeiten der beim Onlinebanking abgephishten Daten entwickeln die Täter ständig fort. Nach wie vor werden Gelder illegal von Online-Bankkonten abgephisht; nur erwerben die Täter jetzt mit Hilfe nicht vom Geschädigten autorisierter Überweisungen Waren und lassen diese an so genannte Warenagenten liefern. Die Warenagenten haben die Aufgabe, die widerrechtlich erlangten Produkte an vorgegebene Adressen weiterzuleiten. Um die Rückverfolgung zu erschweren, erfolgen die Weiterleitungen teilweise über mehrere Packstationen, bis der Täter ohne das Risiko der Strafverfolgung die Waren übernehmen kann.
- Täter unternehmen große Anstrengungen, um neben den Onlinebanking-Daten die gesamte digitale Identität der Internetnutzer abzugreifen. Dazu gehören Zugangsdaten zu Social-Networking Plattformen, PayPal-Konten, Email-Accounts, Aktiendepots, Online-Vertriebsportalen, eigenen Webservern und Firmennetzwerken.
- In speziellen Foren der so genannten Underground Economy werden digitale Identitäten auf frei zugänglichen Internetseiten illegal zum Verkauf angeboten. Zusätzlich können dort Einzelkomponenten wie Falschpersonalien, Informationen über anonyme/verschlüsselte Kommunikationswege und Kreditkartendaten erworben werden.
- Die Underground Economy bietet eine Vielzahl krimineller Verwertungsmöglichkeiten zur Gewinnmaximierung. Beispiel hierfür sind das so genannte Carding on Demand, bei dem illegal erlangte Kreditkartendaten verwertet werden oder die Vermietung so genannter Bot-Netze, d. h. ferngesteuerter Netze zahlreicher, über einen Schadcode infizierter Computer, die ohne Wissen ihrer Besitzer gesteuert werden.

3 Handlungserfordernisse

- Die IuK-Kriminalität mit ihrem Brennpunkt Phishing besitzt ein hohes Gefährdungs- und Schadenspotenzial.
- Die Strafverfolgungsbehörden stehen vor der Aufgabe, Tathandlungen, die weltweit vernetzte Straftäter mit Hilfe technischer und logistischer Tricks zu verschleiern suchen, zeitnah zurückzuverfolgen und zu beweisen.
- Zunächst muss die Erkenntnislage zum Cybercrime weiter verbessert werden, um die Phänomene noch besser und schneller zu erkennen.
- Dies kann durch die Optimierung des Informationsaustausches sowohl der Polizeibehörden untereinander, als auch mit externen Partnern aus allen betroffenen Bereichen (Sicherheitsbehörden, Internet-Wirtschaft, Institute, Organisationen, Verbände und Vereine) erreicht werden.
- Die Wirtschaft als Anbieter und Entwickler von Internetdienstleistungen ist gefordert. Dienstleistungen und Produkte müssen verstärkt an bestehenden Sicherheitsanforderungen ausgerichtet werden.
- Die Anwender sind umfassend über die Risiken im Internet aufzuklären.