Deutscher Bundestag **Drucksache 16/9160**

16. Wahlperiode 09. 05. 2008

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Gisela Piltz, Hans-Michael Goldmann, Dr. Max Stadler, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 16/8938 –

Identitätsdiebstahl

Vorbemerkung der Fragesteller

In letzter Zeit sind nach Presseangaben wieder verstärkt massenhafte Manipulationen von Computersystemen (so genannte Massenhacks) bei Internetusern zu beobachten. Computer werden mit Schadprogrammen infiziert, um diese dann unter die Kontrolle von Kriminellen zu bringen. Klassische Viren spielen aber nur noch eine untergeordnete Rolle. Professionell organisierte internationale Verbrecherbanden greifen vielmehr auf andere Programme zurück, um fremde Computer unter ihre Kontrolle („bösartige Bots“ oder ganze Bot-Netze) zu bringen. Anschließend werden dann von diesen „Zombie-Computern“ Spam verschickt, Daten ausgespäht und weitere Attacken auf andere Computer vorbereitet. Der rechtmäßige Nutzer des Computers bekommt dieses kriminelle Vorgehen gar nicht oder zu spät mit.

Zur Bekämpfung der Computerkriminalität wurden im Sommer 2007 durch die 41. Änderung des Strafgesetzbuches (BGBl. I 2007, 1786) im Hinblick auf das Ausspähen und Abfangen von Daten weitere Straftatbestände geschaffen.

Das Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV) führte im Februar 2008 die Konferenz „Sicherung der Identität in der digitalen Welt“ durch. Identitätsdiebstahl tritt aber in verschiedenen Formen auf und ist nicht nur auf die digitale Welt begrenzt.

Die USA haben im April 2007 nach Einberufung einer „Task Force“ durch den Präsidenten einen umfassenden Strategieplan zur Bekämpfung von Identitätsdiebstahl entwickelt, der neben Maßnahmen für den öffentlichen und privaten Sektor auch eine Öffentlichkeitskampagne vorsieht.

Vorbemerkung der Bundesregierung

Täuschungen über die Identität einer Person zu kriminellen Zwecken haben in den letzten Jahren eine erhebliche Größenordnung angenommen. Dies ist vor allem auf die modernen technischen Möglichkeiten zurückzuführen, die das Internet bietet. Täuschungen über die Identität sind zwar nicht erst durch das Internet entstanden, entsprechende kriminelle Praktiken haben sich allerdings besonders durch die modernen Kommunikationsmittel vervielfacht.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Justiz vom 8. Mai 2008 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Von der Nutzung des Internets zu Täuschungszwecken zu unterscheiden ist das kriminelle Geschehen im Zusammenhang mit der Nutzung dieses Mediums zur Durchführung von Angriffen auf ganze Computersysteme im Wege der illegalen Verwendung einer Vielzahl von zusammen geschalteten Computern (Bot-Netzen). Strafrechtliche Instrumente, um letztere Kriminalitätsform einschließlich des „Hackings“ zu bekämpfen, sind insbesondere die Straftatbestände der §§ 202a (Ausspähen von Daten), 202b (Abfangen von Daten) und 202c (Vorbereiten des Ausspähens und Abfangens von Daten) des Strafgesetzbuches (StGB) sowie der §§ 303a (Datenveränderung) und 303b (Computersabotage) StGB. Das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität vom 11. August 2007 (BGBl. I S. 1786) hat unter anderem dafür gesorgt, dass bisherige Lücken im bestehenden Computerstrafrecht vollständig geschlossen wurden, damit derartige Formen der Computerkriminalität im Einklang mit internationalen Rechtsinstrumenten auch in Deutschland umfassend bekämpft werden können.

1. Welche jährliche Kosten/Schäden entstehen der Wirtschaft durch Identitätsdiebstahl?

Zu Gesamtkosten/Schäden, die der deutschen Wirtschaft durch Täuschungen über die Identität entstehen, liegen der Bundesregierung keine Informationen vor. Die Schäden durch Computerbetrugsstraftaten im Zusammenhang mit Onlinebanking, bei denen Zugangsdaten zu den Konten mittels Phishing-Methoden ausgespäht wurden, gehen in der Regel zu Lasten der Bankkunden oder so genannter Financial Agents, bei denen die Banken Regress nehmen. Hierüber erteilt die Wirtschaft dem Bundeskriminalamt jedoch nur vereinzelt Auskunft. Es ist hier von einem erheblichen Dunkelfeld auszugehen.

2. Wie bewertet die Bundesregierung den Erfolg der Konferenz des Bundesministeriums für Ernährung, Landwirtschaft und Verbraucherschutz vor dem Hintergrund weiterer steigender Massenhacks?

Das Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz hat am 12. Februar 2008 gemeinsam mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) die Konferenz „Sicherung der Identität in der digitalen Welt“ durchgeführt. Die Konferenz mit Teilnehmern insbesondere aus Politik, Wirtschaft sowie Verbraucherschutz- und Datenschutzorganisationen hat zahlreiche Datenschutzprobleme bei IT-Anwendungen aus Verbraucher- und Unternehmenssicht beleuchtet, wie etwa den sorglosen Umgang mit privaten Daten im Internet oder die Risiken beim Onlinebanking. Die Bundesregierung bewertet den Kongress, der mögliche Lösungswege zum Schutz sensibler Daten im Internet und zur Vermeidung von Missbrauch dieser Daten diskutiert hat, als erfolgreichen Beitrag zur Aufklärung der Verbraucherinnen und Verbraucher und zur Sensibilisierung der IT-Branche – auch aufgrund der breiten Beteiligung der unterschiedlichen Akteure.

3. Hält die Bundesregierung ihre Rechtsauffassung aufrecht, dass das so genannte Phishing bereits nach geltendem Recht strafbar ist (Pressemitteilung des Bundesministeriums der Justiz (BMJ) vom 20. September 2006), und wenn ja, warum, und wenn nein, warum nicht?

„Phishing“ ist bereits nach geltendem Recht strafbar. Die in der genannten Pressemitteilung geäußerte Rechtsauffassung ist auch heute noch zutreffend. Unter Phishing versteht man das Ausspionieren persönlicher Daten im Internet.

Derjenige, der versucht den Empfänger einer E-Mail zu täuschen und zur Herausgabe von Zugangsdaten und Passwörtern für das Onlinebanking zu bewegen, kann sich auf Grund unterschiedlicher Tatbestände strafbar machen. Gibt der Empfänger die geforderten Daten auf der vermeintlichen Internetseite oder per E-Mail an, werden diese direkt an den „Phisher“ weitergeleitet, der mit den so erlangten Daten vermögensschädigende Transaktionen durchführt. Dann können die Straftatbestände des Ausspähens von Daten (§ 202a StGB), des Betrugs/Computerbetrugs (§ 263/§ 263a StGB), der Fälschung beweiserheblicher Daten (§ 269 StGB) und der unbefugten Datenerhebung und -verarbeitung (§§ 44, 43 des Bundesdatenschutzgesetzes, BDSG) einschlägig sein.

Im Gesetzgebungsverfahren für das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität hat die Bundesregierung in der Gegenäußerung auf die Stellungnahme des Bundesrates (Bundestagsdrucksache 16/3656) mitgeteilt, dass bereits bei der Erarbeitung des Gesetzentwurfs die Erforderlichkeit eines ausdrücklichen „Phishing“-Straftatbestandes in das Strafgesetzbuch geprüft wurde. Im Rahmen der Länderbeteiligung zum Referentenentwurf erfolgte eine Befragung der Strafverfolgungspraxis. Daraufhin hatten fast alle Landesjustizverwaltungen mitgeteilt, dass sie einen ausreichenden strafrechtlichen Schutz gegen „Phishing“-Angriffe nach geltendem Recht für gewährleistet hielten. Die Bundesregierung teilt diese Auffassung nach wie vor.

4. Worin liegt die Vermögensverfügung/Vermögensgefährdung beim Versenden einer „Phishing“-Mail im Rahmen der §§ 263, 263a des Strafgesetzbuches (StGB)?

Eine irrtumsbedingte Vermögensverfügung kann jedes Verhalten mit unmittelbar vermögensmindernder Wirkung sein. Der „Phisher“ zielt bei der Versendung der „Phishing“-E-Mail darauf ab, von dem Opfer Zugangsdaten zu Konten und Ähnlichem zu erhalten, um dann auf Vermögenswerte des Opfers zuzugreifen. Bis es jedoch zu der Vermögensverschiebung nach dem Versenden einer „Phishing“-E-Mail kommt, bedarf es weiterer Zwischenschritte, die durch das Opfer vorgenommen werden müssen. Die Strafbarkeit wegen Betrugs setzt nach ständiger Rechtsprechung und herrschender Ansicht voraus, dass das irrtumsbedingte Verhalten des Getäuschten die Vermögensverfügung auslöst, ohne dass dafür noch zusätzliche deliktische Zwischenhandlungen des Täters erforderlich sind. An dem Unmittelbarkeitserfordernis fehlt es, wenn der Getäuschte dem Täter lediglich die tatsächliche Möglichkeit gibt, den Vermögensschaden durch weitere selbstständige deliktische Schritte herbeizuführen (hier die Eingabe von Zugangsdaten).

Allerdings kann in Fällen des „Phishings“ eine schadensgleiche konkrete Vermögensgefährdung in Betracht kommen. Nach der Rechtsprechung des Bundesgerichtshofs (BGH) liegt eine betrugsrelevante Vermögensminderung nicht erst bei der Ausgliederung bestimmter Positionen aus dem Vermögen vor. Schon die konkrete Vermögensgefährdung steht der Vermögensminderung gleich, wenn sie bei wirtschaftlicher Betrachtung bereits eine Verschlechterung der gegenwärtigen Vermögenslage bedeutet (BGHSt 23, 300 ff.; 27, 342 ff.; 33, 244, 246 ff.).

In folgenden Fällen hat der BGH beispielsweise die Vollendung eines Betrugs bejaht:

- Aushändigung einer Kreditkarte, die in gleicher Weise wie ein Scheckheft einen Vermögenswert verkörpere, durch eine Bank an einen insolventen Kunden, der die Bank über eine Zahlungsfähigkeit getäuscht hat (BGH, Urteil vom 13. Juni 1985, BGHSt 33, 244, 246 ff.);

- Aushändigung der Schecks, der EC-Karte sowie der Kreditkarte an einen Kunden, der unter Vorlage eines gefälschten Personalausweises und Täuschung über seine Zahlungswilligkeit bei der Bank die Eröffnung eines Kontos erreicht (BGHSt 47, 160 ff.);
- Überlassung einer Geldautomatenkarte und PIN durch einen Kontoinhaber an den Täter, der dem Geschädigten vorgetäuscht hat, er wolle ihm eine Schuld zurückzahlen und benötige dazu dessen Geldautomatenkarte und PIN (BGH, Beschluss vom 17. Dezember 2002, Az.: 1 StR 412/02).

Geht man bei der täuschungsbedingten Erlangung der Daten des Geschädigten von einem Betrug aus, kommt für die bloße Versendung ein versuchter Betrug (§ 263 Abs. 2 StGB) in Betracht, wenn etwa der Empfänger die Phishing-E-Mail nicht öffnet, vernichtet, den mitübersandten Link nicht anklickt oder das gefälschte Onlineformular nicht ausfüllt.

Für die Verwirklichung des Tatbestandes des Computerbetrugs gemäß § 263a StGB gilt bezogen auf den Vermögensschaden das Gleiche wie für den Betrug gemäß § 263 StGB. Der in der Praxis häufig vorkommende Fall des Missbrauchs von Zahlungskarten oder Geldautomaten, bei dem der Täter mittels der meist auf illegale Weise erlangten PIN Geld vom Konto des Opfers abhebt, stellt eine solche Vermögensschädigung durch unbefugte Verwendung von Daten dar. Das Verschaffen des Zugangs zu einem geschützten Onlinekonto und die Überweisung von Geldbeträgen mittels durch „Phishing“ erlangter Zugangsdaten (PIN, TAN etc.) stellt lediglich eine etwas modernere Tatvariante dieses Kartenmissbrauchs dar. Eine abweichende Bewertung ist nicht geboten, so dass – ein tatsächlich entstandener Vermögensschaden beim Opfer vorausgesetzt – auch hier von einer Strafbarkeit wegen der unbefugten Verwendung von Daten nach § 263a StGB ausgegangen werden kann (Popp, NJW 2004, 3517 f.; Fischer, StGB, 55. Aufl. 2008, § 263a, Rn. 11a).

5. Ist für die Anwendbarkeit von §§ 263, 263a StGB danach zu unterscheiden, ob sich der Täter Zugang zu Kontodaten oder zu Internet- oder Auktionsportalen verschaffen will, wenn nein, warum nicht, wenn ja, warum?

Der Unterschied ist nicht darin zu sehen, ob der Täter sich Zugang zu Kontodaten oder Internet- oder Auktionsportalen verschaffen will, sondern es kommt allein darauf an, ob eine Vermögensverfügung einschließlich eines Vermögensschadens oder einer schadensgleichen konkreten Vermögensgefährdung Tatgegenstand ist. Ist Letzteres nicht der Fall, kommt eine Strafbarkeit nach § 263 StGB oder § 263a StGB nicht in Betracht.

6. Ist die Bundesregierung der Auffassung, dass das bloße Absenden einer „Phishing-Mail“ eine Strafbarkeit nach § 202c StGB begründen kann, wenn nein, sieht die Bundesregierung hier eine Strafbarkeitslücke, die geschlossen werden sollte?

Über den durch das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität eingeführten § 202c StGB (Vorbereiten des Ausspähens und Abfangens von Daten) sind bestimmte Vorbereitungshandlungen zu Computerstraftaten unter Strafe gestellt worden. Dieser Tatbestand dient allerdings nicht in erster Linie der Bekämpfung des „Phishings“. Das bloße Absenden einer Phishing-E-Mail fällt nicht unter § 202c Abs. 1 Nr. 1 StGB, da insoweit noch kein Verschaffen eines Passwortes oder sonstigen Sicherungscodes vorliegt und der Versuch des § 202c StGB nicht strafbar ist. Nach Auffassung der Bundesregierung liegt insoweit keine Strafbarkeitslücke vor, da das Absenden der Phishing-E-Mail bereits nach anderen Straftatbeständen strafbewehrt ist (siehe Antwort zu Frage 3).

7. Teilt die Bundesregierung die Auffassung, dass eine Strafbarkeit nach § 269 StGB wegen „Phishings“ in der Praxis häufig scheitert, weil die Erkennbarkeit des Absenders nicht gegeben ist und es daher an der „Garantiefunktion“ der digitalen Urkunde fehlt?

Ob eine Strafbarkeit gemäß § 269 StGB vorliegt, hängt davon ab, ob durch den Täter beweiserhebliche Daten so gespeichert oder verändert wurden, dass bei deren Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten durch den Täter gebraucht wurden, und dies zur Täuschung im Rechtsverkehr geschah.

Beim „Phishing“ wird der Anschein erweckt, die E-Mails seien von einer Bank, einem Internetauktionshaus oder anderen Unternehmen erstellt worden. Dabei handelt es sich folglich um den Aussteller kenntlich machender Daten im Sinne des § 269 StGB. Weiterhin müssen die Daten aber auch dazu geeignet und bestimmt sein, als Beweis für rechtlich relevante Handlungen zu dienen bzw. einen Aussagegehalt enthalten, der als eine von einem bestimmten Aussteller herrührende oder von ihm autorisierte Erklärung erscheint (Fischer, a. a. O., § 269, Rn. 4). Dies dürfte bei gefälschten „Phishing“-E-Mails der Fall sein, da sie den Adressaten dazu auffordern, dem Ersteller der E-Mail geschützte Zugangsdaten zu offenbaren. Folglich beinhalten sie eine (scheinbar) vom Aussteller herrührende und von diesem autorisierte Erklärung. Auch die gefälschte Webseite, die regelmäßig eine Eingabemaske zur Eingabe der geschützten Zugangsdaten enthält, hat einen Erklärungsgehalt, der im Rechtsverkehr hinreichend beweiserheblich ist. Denn die Webseite enthält die konkludente Erklärung, dass die geschützten Zugangsdaten an einen Berechtigten (z. B. die Bank) weitergeleitet werden.

Im Hinblick auf die Parallelität zum Urkundenbegriff des § 267 StGB muss weiterhin zur Erfüllung der Garantiefunktion im Fall der Wahrnehmung der Urkunde ein Aussteller erkennbar sein. Entsprechend der dazu vertretenen Geistigkeitstheorie erfordert dies, dass bei visueller Darstellung deutlich werden muss, wem die Daten ihrem geistigen Inhalt nach zuzurechnen sind.

Als Aussteller erscheint damit beim „Phishing“ in den meisten Fällen die Bank, deren Webseite täuschend ähnlich nachgemacht wurde. Wer Aussteller ist, ergibt sich aber letztlich aus den Umständen im Einzelfall. Die Garantiefunktion ist jedenfalls dann gegeben, wenn aus der übersandten Erklärung ein eindeutiger Aussteller hervorgeht. Die Garantiefunktion scheitert nicht schon daran, dass es sich um eine digitale Urkunde handelt.

Es ist anerkannt, dass die IP-Adresse eines Internetnutzers beweiserheblich im Sinne des § 269 StGB sein kann, da sie Aussagen über dessen Identität zulässt. Folglich können sich auch „Hacker“ gemäß der Vorschrift strafbar machen, die falsche IP-Adressen verwenden, um dem angegriffenen System eine falsche Identität vorzuspiegeln. Gleiches gilt bei „Phishing“ für die falschen Daten der E-Mail, die über die Identität des Absenders täuschen.

8. Plant die Bundesregierung ebenfalls einen Strategieplan zur Bekämpfung des Identitätsdiebstahls zu entwickeln?

Derartige Planungen gibt es bisher nicht. Ob der so genannte Identitätsdiebstahl durch bestimmte Strategien bekämpft werden kann und sollte, kann heute noch nicht beantwortet werden. Bei den Diskussionen auf europäischer Ebene zwischen den Mitgliedstaaten der Europäischen Union (EU) wurde die Frage offen gelassen, ob es sich tatsächlich um ein Phänomen handelt, dem nicht bereits durch herkömmliche rechtliche Rahmenbedingungen ausreichend begegnet werden kann. Was die deutsche Rechtslage angeht, wird auf die Antwort zu Frage 11 verwiesen.

9. Teilt die Bundesregierung die von dem Bundesvorsitzenden des Bundes Deutscher Kriminalbeamter Klaus Jansen auf dem Europäischen Polizeikongress in Berlin am 29. Januar 2008 gemachten Aussage, dass derzeit ca. 4 000 Internetfahnder fehlen?

Der Begriff „Internetfahnder“ wird in der Regel für Angehörige der polizeilichen Zentralstellen für anlassunabhängige Recherchen im Internet („Streife im Internet“) verwendet, deren Aufgabe die ständige, systematische, deliktsübergreifende, nicht extern initiierte Suche nach Gefahrenlagen im Internet und in Onlinediensten, einschließlich der Weiterverfolgung von dabei festgestellten, strafrechtlich relevanten Sachverhalten mit Beweissicherung bis zur Feststellung der Verantwortlichen und/oder der örtlichen Zuständigkeiten von Polizei und Justiz ist.

Seit 1999 wurden solche Zentralstellen für Internetrecherche beim Bundeskriminalamt, beim Zollkriminalamt sowie in einigen Bundesländern eingerichtet und personell entsprechend ausgestattet. Die Tätigkeiten dieser Zentralstellen werden in der „Koordinierungsgruppe anlassunabhängige Recherchen im Internet“ (KaRIn) koordiniert. Die Aussage, dass in diesem Bereich ca. 4 000 Internetfahnder fehlen, kann vor diesem Hintergrund nicht nachvollzogen werden.

10. Wie bewertet die Bundesregierung die Einrichtung von Schwerpunktstaatsanwaltschaften zur Verfolgung von Computerkriminalität?

Nach § 143 Abs. 4 des Gerichtsverfassungsgesetzes (GVG) kann den Beamten einer Staatsanwaltschaft für die Bezirke mehrerer Land- oder Oberlandesgerichte die Zuständigkeit für die Verfolgung bestimmter Arten von Strafsachen, die Strafvollstreckung in diesen Sachen sowie die Bearbeitung von Rechtshilfeersuchen von Stellen außerhalb des räumlichen Geltungsbereichs des Gerichtsverfassungsgesetzes zugewiesen werden, sofern dies für eine sachdienliche Förderung oder schnellere Erledigung der Verfahren zweckmäßig ist; in diesen Fällen erstreckt sich die örtliche Zuständigkeit der Beamten der Staatsanwaltschaft in den ihnen zugewiesenen Sachen auf alle Gerichte der Bezirke, für die ihnen diese Sachen zugewiesen sind. Die Bewertung, ob und ggf. inwieweit zentrale Zuständigkeitszuweisungen und die damit verbundene Bildung von Schwerpunktstaatsanwaltschaften für eine sachdienliche Förderung oder schnellere Erledigung der Verfahren zweckmäßig ist, obliegt den für die Verfolgung von Computerstraftaten zuständigen Ländern.

11. Hält die Bundesregierung die bestehenden Haftungsregelungen und die bestehende Haftungspraxis bei Eintritt eines Identitätsdiebstahls zwischen Täter, Verbraucher und Unternehmen für ausgewogen oder welchen Änderungsbedarf sieht die Bundesregierung?

Änderungsbedarf bei den Haftungsregelungen im Zusammenhang mit dem so genannten Identitätsdiebstahl besteht nach Auffassung der Bundesregierung nicht. Wenn der Täter den Namen des Opfers oder dessen Internetadresse, die aus seinem Namen oder seiner geschäftlichen Bezeichnung besteht, unbefugt verwendet, hat das Opfer gegen den Täter Unterlassungsansprüche nach § 12 des Bürgerlichen Gesetzbuchs (BGB). Auch bei der unbefugten Verwendung von Internetadressen, die nicht aus dem Namen oder einer Geschäftsbezeichnung bestehen, können Unterlassungsansprüche nach § 12 BGB bestehen, wenn der Internetadresse Namensfunktion zukommt. Das Namensrecht nach § 12 BGB ist ein absolutes Recht im Sinne des § 823 BGB. Wird das Namensrecht rechtswidrig und schuldhaft verletzt, können Schadenersatzansprüche bestehen.

Auch gegen einen Diensteanbieter, z. B. ein Internetauktionshaus, auf dessen Plattformen Namensrechte verletzt werden, können Unterlassungsansprüche nach § 12 BGB bestehen. Ein Diensteanbieter ist nach § 7 des Telemediengesetzes zwar nicht verpflichtet, die gespeicherten und ins Internet eingestellten Informationen auf Rechtsverletzungen hin zu überprüfen. Wurde der Diensteanbieter allerdings auf einen klaren Namensrechtsverstoß hingewiesen, muss er nicht nur die konkrete Namensrechtsverletzung unterbinden, sondern auch im Rahmen des Zumutbaren entsprechende Verstöße in der Zukunft verhindern (BGH, Urteil vom 10. April 2008, I ZR 227/05).

Darüber hinaus bieten die allgemeinen deliktsrechtlichen Vorschriften der §§ 823 ff. BGB für Schäden, die durch den Missbrauch ausgespähter Daten („Identitätsdiebstahl“) verursacht werden, eine ausgewogene Haftungsregelung. Gegenüber dem Täter besteht hierbei regelmäßig zumindest ein Anspruch nach § 826 BGB, wobei – je nach Fallkonstellation – entweder der Verbraucher oder das (Kredit-)Unternehmen Geschädigter und damit Anspruchsinhaber sein können. Unter Anwendung der allgemeinen deliktsrechtlichen Vorschriften hat sich eine verbraucherfreundliche Rechtsprechung herausgebildet; so wurde etwa mehrfach entschieden, dass Mittelsleute, denen keine konkrete Tatbeteiligung nachgewiesen werden kann, denen jedoch die deliktische Herkunft der transferierten Mittel bekannt sein musste, nach § 823 Abs. 2 BGB i. V. m. § 261 StGB haften (LG Ellwangen, ITRB 2007, 206 f.; LG Köln WM 2008, 354 ff.).

12. Gibt es europäische Programme zur Erforschung und/oder Maßnahmen zur Bekämpfung von Identitätsdiebstahl, und wenn ja, an welchen Programmen/Maßnahmen ist die Bundesrepublik Deutschland beteiligt?

Die Bundesregierung ist auf EU-Ebene im Rahmen der Arbeiten im Rat an der bisher offen geführten Diskussion zur Frage der Notwendigkeit der Schaffung EU-weit einheitlicher Vorschriften zur Regelung des „Identitätsdiebstahls“ beteiligt. Die EU-Kommission hatte in Ihrer Mitteilung „Eine allgemeine Politik zur Bekämpfung der Internetkriminalität“ an das Europäische Parlament, den Rat und den Ausschuss der Regionen vom 30. Mai 2007 erwähnt, dass der Bedarf für entsprechende einheitliche Regelungen durch die Kommission geprüft werden sollte. Die Mitgliedstaaten haben diesbezüglich bisher zurückhaltend reagiert. An einer Konferenz zu diesem Thema in Lissabon Anfang November 2007 nahmen nur wenige Mitgliedstaaten teil. Bei einer Konferenz der EU-Kommission vom 15. und 16. November 2007 in Brüssel, die sich mit der Internetkriminalität beschäftigte, wurde deutlich, dass von Seiten der EU-Mitgliedstaaten zurzeit Initiativen der EU-Kommission zur Schaffung von neuen Rechtsinstrumenten nicht für erforderlich gehalten werden. Teilnehmer der Konferenz waren sowohl Regierungsvertreter als auch Vertreter der Strafermittlungs- und Strafverfolgungspraxis und Vertreter von Internet-Service-Providern.

Im Schengener Informationssystem ist die Möglichkeit eines Missbrauchs der Identität bereits berücksichtigt. Entsprechende Informationen werden im System nachgehalten, um Opfer von Identitätsmissbrauch vor irrtümlich getroffenen Maßnahmen zu schützen. Diese Funktionalität wird in der Weiterentwicklung des Schengener Informationssystems zweiter Generation weiter ausgebaut.

Das Bundeskriminalamt nimmt regelmäßig an den internationalen Public-Private-Partnership-Initiativen „Digital Phish-Net“ sowie „Bot-Net Task-Force“ teil; hier werden auch „Best Practices“ für die Bekämpfung der beiden genannten Phänomene „Phishing“ und „Bot-Netze“ diskutiert und ausgetauscht.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) befasst sich mit der technischen Verfügbarkeit sicherer elektronischer Identitäten. Auf europäischer Ebene hat die EU-Kommission innerhalb ihres Rahmenprogramms „Wettbewerbsfähigkeit und Innovation“ einen Pilotversuch initiiert, der sich mit der Entwicklung und dem Einsatz von grenzüberschreitenden Anwendungen elektronischer Identitäten befasst (eID Large Scale Pilot). An dieser Initiative ist neben dem Bundesministerium des Innern und dem BSI auch die deutsche Industrie beteiligt.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln, Telefon (02 21) 97 66 83 40, Telefax (02 21) 97 66 83 44
ISSN 0722-8333