

Berlin, 20. September 2006

Besserer Schutz vor Hackern, Datenklau und Computersabotage

Das Bundeskabinett hat heute den Regierungsentwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität beschlossen. Der Entwurf schließt Regelungslücken vor allem im Bereich des „Hacking“, d.h. dem „Knacken“ von Computersicherheitssystemen, und der Computersabotage. „Deutschland verfügt bereits über ein weitreichendes Computerstrafrecht. Mit den Straftatbeständen des Computerbetrugs, der Fälschung beweisbarer Daten und der Datenveränderung existieren Vorschriften, die dem internationalen Standard vollständig entsprechen. Die rasante Entwicklung der Informationstechnologie führt jedoch immer wieder zu neuen kriminellen Gefahren und Missbrauchsmöglichkeiten. Straftäter greifen moderne Informationssysteme mit Computerviren, Würmern und Denial-of-Service-Attacken an und verursachen weltweit erhebliche Schäden. Letzte Lücken im deutschen Strafrecht schließt der heutige Gesetzentwurf“, sagte Bundesjustizministerin Brigitte Zypries.

Auch das so genannte "Phishing" ist bereits nach geltendem Recht strafbar. Darunter versteht man das Ausspionieren persönlicher Daten im Internet. Dabei wird per E-Mail versucht, den Empfänger irre zu führen und zur Herausgabe von Zugangsdaten und Passwörtern für das Online-Banking zu bewegen. 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. Hier kommen die Straftatbestände des Ausspähsens von Daten (§ 202a StGB), des Betrugs/Computerbetrugs (§ 263/§ 263a StGB), der Fälschung beweisbarer Daten (§ 269 StGB) und der unbefugten Datenerhebung und -verarbeitung (§§ 44, 43 BDSG) in Betracht.

Der heutige Regierungsentwurf setzt den EU-Rahmenbeschluss über Angriffe auf Informationssysteme sowie das Europarat-Übereinkommen über Computerkriminalität in nationales Recht um:

- Künftig soll bereits der unbefugte Zugang zu besonders gesicherten Daten unter Überwindung von Sicherheitsvorkehrungen unter Strafe gestellt werden (§ 202a StGB). Ein Verschaffen von Daten wird nicht mehr erforderlich sein. Damit wird klargestellt, dass „Hacking“ strafbar ist.
- Computersabotage ist bisher nur bei Angriffen gegen Betriebe, Unternehmen und Behörden strafbar (§ 303b StGB). Künftig sollen auch private Datenverarbeitungen geschützt werden. Ferner werden Störungen durch unbefugtes Eingeben und Übermitteln von Computerdaten unter Strafe gestellt, um „DoS-Attacken“ erfassen zu können, bei denen die Dienste eines Servers durch eine Vielzahl von Anfragen so belastet werden, dass dessen Kapazitäten nicht ausreichen und der Zugang für berechtigte Kontaktaufnahmen mit dem Server blockiert oder erschwert wird. Besonders schwere Fälle der Computersabotage können künftig mit Freiheitsstrafe bis zu zehn Jahren bestraft werden.
- Das Sichverschaffen von Daten aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage soll unter Strafe gestellt werden (§ 202b StGB neu).
- Besonders gefährliche Vorbereitungshandlungen zu Computerstraftaten werden künftig strafbar sein. Sanktioniert wird insbesondere das Herstellen, Überlassen, Verbreiten oder Verschaffen von „Hacker-Tools“, die bereits nach Art und Weise ihres Aufbaus darauf angelegt sind, illegalen Zwecken zu dienen (§ 202c StGB neu).