von Rechtsanwalt **Arndt Joachim Nagel**

Vorsicht strafbare Handlung: Ein Gesetzentwurf löst Diskussionen aus

Seit dem 20. September 2006 liegt der Regierungsentwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität vor. Das Gesetz dient der Umsetzung des Übereinkommens des Europarats über Computerkriminalität und der Umsetzung des Rahmenbeschlusses 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme. Die geplanten Gesetzesänderungen bringen einige erwähnenswerte Änderungen mit sich, über die in der Fachwelt schon jetzt intensiv diskutiert wird. Der folgende Beitrag soll einen kleinen Überblick über die geplanten Änderungen verschaffen.

1. Ausspähen von Daten (§ 202a Abs. 1 StGB-E) - Erweiterter Schutz vor Hacking

Nach der aktuellen Gesetzeslage macht sich wegen Ausspähens von Daten strafbar, wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderem verschafft. In der neuen Regelung des § 202a Abs. 1 StGB-E wird die Tathandlung des Sichverschaffens von Daten durch ein Zugangsverschaffen zu Daten ersetzt. Die Strafbarkeit wird hierdurch bereits auf den Moment vorverlagert, in dem der Hacker erfolgreich in ein fremdes System eindringt. Nach geltender Gesetzeslage muss er zudem auch noch von den Daten Kenntnis nehmen. Der bloße Zugriff auf ein fremdes System ohne Kenntnisnahme reicht nach heutiger Gesetzeslage noch nicht für eine Strafbarkeit wegen Ausspähens von Daten. Die geplante Gesetzesänderung hätte demnach zur Folge, dass sich auch derjenige strafbar macht, der aus reiner Experimentierfreude unbefugt in fremde Systeme eindringt. Davon wäre beispielsweise auch ein sog. "White-Hat"-Hacker betroffen, der ohne Auftrag in ein Bankensystem eindringt, um eine Sicherheitslücke im System aufzudecken. Hacken im Auftrag des Berechtigten zur Überprüfung der Systemsicherheit bliebe dagegen auch nach der geplanten Gesetzesänderung straflos, da sich der Hacker in diesem Fall nicht unbefugt Zugang zu Daten verschafft.

2. Abfangen von Daten (§ 202b StGB-E) - Schutz vor Phishing

Nach dem geplanten § 202b StGB-E macht sich strafbar, wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft. Mit der geplanten Neuregelung soll eine bestehende Strafbarkeitslücke geschlossen werden. Nach geltendem Recht ist nämlich das sog. Fremd-Sniffen bzw. Mitschneiden von Netztraffic grundsätzlich straflos, da es an der für § 202a Abs. 1 erforderlichen "besonderen Sicherung" fehlt. Nur dann, wenn die mitgeschnittenen Daten zuvor verschlüsselt wurden und die Originaldaten nach dem Abfangen wieder erfolgreich entschlüsselt werden, kommt eine Strafbarkeit nach geltendem Recht in Betracht. Der neue § 202b StGB soll nun dafür sorgen, dass auch unverschlüsselte Datenpakete geschützt werden. Allerdings wird der Tatbestand insoweit eingegrenzt, als nur die nichtöffentliche Datenübertragung geschützt wird. Nichtöffentlich dürften nur solche Datenübertragungen sein, die sich auf ein bestimmtes Ziel zur Entgegennahme der Daten richten, ohne dabei der Allgemeinheit einen freien Zugriff gewähren zu wollen. Die neue Regelung eignet sich beispielsweise zur Bestrafung von Phishing mittels Trojanern oder gefälschter Bank-Websites, die als technische Mittel im Sinne von § 202b StGB-E in Frage kommen. Darüber hinaus könnte unter die geplante Regelung aber auch der Fall zu fassen sein, dass jemand sich mit seiner W-LAN-Karte unbefugt in ein fremdes unverschlüsseltes Netzwerk einwählt, um so auf Fremdkosten im Internet zu surfen. Dieser Fall dürfte jedoch nur dann strafbar sein, wenn der Fremdsurfer dabei auch vorsätzlich Kenntnis von den fremden Daten erlangt. Insoweit besteht noch Klärungsbedarf.

3. Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB-E)

Nach dem geplanten § 202c StGB macht sich strafbar, wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

- Passworte oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
- Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht.

a) Schutz vor Phishing-Versuchen

Die Regelung unterscheidet zwischen zwei Fällen. § 202c Nr. 1 StGB-E soll Phishing-Versuche unter Strafe stellen. Danach sollen Fälle bestraft werden, in denen sich Phisher Passwörter oder ähnliches verschaffen, mit deren Hilfe sie auf Daten zugreifen können, die gesichert und nicht für sie bestimmt sind. Darunter fallen beispielsweise Zugriffe auf Konten via Online-Banking.

b) Schutz vor Hacker-Tools

Nach § 202c Nr. 2 StGB-E soll künftig das Herstellen, Verschaffen, Verkaufen, Überlassen, Verbreiten oder Zugänglichmachen sog. Hacker-Tools strafbar sein. Ob hierdurch auch ein konkreter Erfolg erzielt wird, ist für die Strafbarkeit unerheblich. Dies ist insoweit bedenklich, als sich die Strafbarkeit auch auf solche Programme erstrecken kann, die zwar nicht für die Begehung von Computerstraftaten konzipiert sind, die aber potentiell gefährliche Funktionen als zusätzliche Features beinhalten. Danach könnte sich beispielsweise ein IT-Sicherheitsexperte, der ein entsprechendes Schadprogramm aus dem Internet herunterlädt und ausprobiert, der Strafbarkeit nach § 202c Nr. 2 StGB-E ausgesetzt sehen. Insoweit besteht also ebenfalls noch Klärungsbedarf.

3. Datenveränderung (§ 303a Abs. 3 StGB-E) - Schutz vor Vorbereitung einer Datenveränderung

Nach dem heute bereits geltenden § 303a StGB macht sich strafbar, wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert. Der Gesetzentwurf der Bundesregierung sieht nun einen Abs. 3 vor, der die Vorbereitung einer solchen Straftat unter Strafe stellt. Danach soll es auch insoweit nicht mehr auf den Eintritt eines konkreten Erfolgs ankommen. Da es bei § 303a StGB-E noch schwieriger werden dürfte, taugliche Abgrenzungskriterien für Programme mit Missbrauchspotential zu finden, gelten die zu § 202c Nr. 2 StGB-E geäußerten Bedenken hier erst recht. Schließlich ließe sich jeder herkömmliche Dateimanager für eine rechtswidrige Datenveränderung missbrauchen.

4. Computersabotage (§ 303b StGB-E) - Schutz vor Störung von Datenverarbeitungsvorgängen (jetzt auch für Privatpersonen)

Nach § 303b StGB kann sich nach heutiger Rechtslage wegen Computersabotage nur strafbar machen, wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, stört. Nach der neuen Regelung soll sich der Schutzbereich des § 303b StGB auch auf Privatpersonen beziehen. Dadurch wird der Schutzbereich der Norm erheblich ausgeweitet. Außerdem wurden einige neue Tatbestandsmerkmale in die Norm aufgenommen, die den Geltungsbereich der Norm wieder etwas einschränken bzw. konkretisieren sollen.

Fazit

Der Gesetzentwurf enthält einige sinnvolle Änderungen, durch die das deutsche Strafrecht an die neuen Herausforderungen im Bereich der Computerkriminalität angepasst wird. Gerade im Hinblick auf die Schreckgespenster Hacking und Phishing wird der strafrechtliche Schutz erheblich ausgeweitet. Dies führt jedoch - wie oben gezeigt - in einzelnen Fällen auch zu unbilligen Ergebnissen. Der Gesetzgeber sollte den Entwurf daher an einigen Stellen noch etwas nachbessern, um sich nicht dem Vorwurf der Überkriminalisierung ausgesetzt zu sehen.

Autor:
RA Arndt Joachim Nagel
Rechtsanwalt und Fachanwalt für Informationstechnologierecht