



POSTANSCHRIFT Bundesministerium der Justiz, 11015 Berlin

Herrn Alexander N. Benner

alexander.benner@googlemail.com

HAUSANSCHRIFT Mohrenstraße 37, 10117 Berlin

POSTANSCHRIFT 11015 Berlin

BEARBEITET VON StA Dr. Merz

REFERAT IIA4

TEL +49 1888 580 9241

FAX +49 1888 580 9242

E-MAIL merz-ma@bmj.bund.de

AKTENZEICHEN 7036 - 10 II - 23 683/2006

DATUM Berlin, 06. Oktober 2006

BETREFF: Entwurf eines ... Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität

BEZUG: Ihre E-Mail vom 26. September 2006

Sehr geehrter Herr Benner,

vielen Dank für Ihre E-Mail vom 26. September 2006, in der Sie um eine Erläuterung des in dem Entwurf eines ... Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität vorgeschlagenen Straftatbestandes gegen bestimmte Vorbereitungshandlungen zu Computerstraftaten bitten. Sie befürchten, dass durch den neuen Straftatbestand ein Schutz von Computersystemen nicht mehr im ausreichenden Maße möglich sei.

Das aber ist nicht der Fall. Der Entwurf eines ... Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität sieht mit seinem neuen § 202c StGB-E eine Strafvorschrift vor, die bestimmte besonders gefährliche Vorbereitungshandlungen zu Computerstraftaten unter Strafe stellt. Strafbar soll sein, wer eine Computerstraftat (§§ 202a, 202b, 303a, 303b StGB) vorbereitet, indem er Passworte oder sonstige Sicherungscodes, die den Zugang zu Daten ermöglichen (Nr. 1) oder Computerprogramme, deren Zweck die Begehung einer solchen Tat ist (Nr. 2), herstellt, sich verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht.

Bereits für die Erfüllung des objektiven Tatbestandes müssen insbesondere zwei Merkmale vorliegen. Einerseits muss es sich objektiv um ein Schadprogramm handeln und andererseits muss sich die Tathandlung - also das Herstellen, Verschaffen, Verkaufen, Überlassen, Verbreiten oder sonst Zugänglichmachen - auf eine Computerstraftat beziehen.

Durch die objektive Beschränkung auf Computerprogramme, deren Zweck die Begehung einer Computerstraftat ist, wird bereits auf Tatbestandsebene sichergestellt, dass keine Computerprogramme erfasst werden, die der Überprüfung der Sicherheit dienen. Unter Strafe gestellt werden lediglich solche Programme, denen die illegale Verwendung immanent ist, die also nach Art und Weise des Aufbaus oder ihrer Beschaffenheit auf die Begehung von Computerstraftaten angelegt sind. Hierunter fallen nicht solche Programme, die lediglich zur Begehung von Computerstraftaten missbraucht werden können.

Zudem muss die Tathandlung zur Vorbereitung einer Computerstraftat (§§ 202a, 202b, 303a, 303b StGB) erfolgen. Das ist nicht der Fall, wenn das Computerprogramm – mag es auch den sonstigen Kriterien des § 202c StGB unterfallen – zum Zwecke der Sicherheitsüberprüfung oder zur Entwicklung von Sicherheitssoftware erworben oder einem anderen überlassen wurde. Wenn also in den Fällen des Testens der Sicherheit eines Systems oder des Entwickelns von Sicherheitssoftware auch Schadprogramme erworben werden, dann erfolgt dies nicht zur Vorbereitung einer Computerstraftat. Durch diese Handlung wird gerade nicht eine eigene oder fremde Computerstraftat (also § 202a, 202b, 303a, 303b StGB) ermöglicht, da die Anwendung der Schadprogramme selbst keine Computerstraftat darstellt. Der neue § 202c StGB-E dient also ausschließlich der Sicherheit von Computersystemen.

Mit freundlichen Grüßen

Im Auftrag

Dr. Merz