KURZFASSUNG

Wussten Sie schon…

…dass Sie lange Gefahr liefen, sich bei der Überprüfung von Sicherheitslücken in Ihrer IT strafbar zu machen?

Lange Zeit war der so genannte Hackerparagraf in der Diskussion, der die Verwendung von Software zur Aufspürung von Sicherheitslücken unter Strafe stellt. Dieser lautet:

> *§ 202c Vorbereiten des Ausspähens und Abfangens von Daten*
>
> *Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er*
> *1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen,*
> *oder*
> *2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,*
> *herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.*

Dem Wortlaut nach kann man annehmen, dass auch der rechtschaffene Dienstleister, der die IT-Sicherheit überprüft, eine solche Straftat begehen kann. Dies wurde auch in der Diskussion zu der umstrittenen Vorschrift scharf kritisiert. Das Bundesverfassungsgericht hat jetzt aber klar gestellt, dass dies so nicht der Fall ist und die Kriterien der Vorschrift erklärt.

Timo Schutt
Rechtsanwalt & Fachanwalt für IT Recht
www.schutt-waetke.de

Eine Kommentierung der Entscheidung des Bundesverfassungsgerichts finden Sie hier.

LANGFASSUNG

Das Bundesverfassungsgericht hatte am 18.05.2009 über drei Verfassungsbeschwerden zu entscheiden, die sich jeweils gegen den umstrittenen so genannten „Hackerparagrafen“ § 202c des Strafgesetzbuches wendeten.

Die Beschwerdeführer trugen, die jeweils aus unterschiedlichen beruflichen Gründen mit Sicherheitsanalysetools arbeiten, vor, bei ihrer Arbeit aufgrund dieses Straftatbestandes immer das latente Risiko einer Strafverfolgung einzugehen. Sie rügten unter anderem durch die Vorschrift in ihren Grundrechten, unter anderem dem Grundrecht der Berufsfreiheit (Art. 12 GG), verletzt zu sein.

Das Bundesverfassungsgericht nahm die Beschwerden nicht zur Entscheidung an. Wichtig ist hierbei die Begründung der obersten Richter: Die von den Beschwerdeführern eingesetzten Programme seien schon keine tauglichen Tatobjekte der Strafvorschrift. Bereits nach dem Wortlaut sei es nicht ausreichend, dass ein Programm für die Begehung der genannten Computerstraftaten lediglich geeignet sei. Maßgeblich für die Zweckbestimmung des jeweiligen Programms seien vielmehr die Absichten des Entwicklers. Die Bezeichnung von Software als „Sicherheitsanalysewerkzeug“ deute darauf hin, dass bei diesen Programmen nicht der illegale, sondern der legitime Verwendungszweck im Vordergrund stehe. Außerdem scheide in Fällen der legitimen Nutzung solcher Programme für IT-

Sicherheitstests eine Straftat auch aus, weil das subjektive Merkmal der Vorbereitung einer Computerstraftat fehle. Ein unbefugtes Handeln könne nicht vorliegen, wenn der Nutzer der Software im Auftrag und mit dem Einverständnis des Inhabers des Computersystems handle.

Damit dürfte die heiße Diskussion um diesen Paragrafen beendet sein. Das Bundesverfassungsgericht hat einer anderen Auslegung, als der oben geschilderten eine klare Absage erteilt. Trotzdem wird es im Einzelfall auch in Zukunft zu Problemen kommen, wenn die subjektive Seite nicht klar erkennbar ist und/oder die verwendete Software nicht eindeutig für legale Zwecke entwickelt wurde. Zur Vorsicht muss also trotzdem geraten werden.

(Bundesverfassungsgericht, Beschluss vom 18.05.2009 – 2 BvR 2233/07, 2 BvR 1151/08, 2 BvR 1624/08)

Timo Schutt
Rechtsanwalt & Fachanwalt für IT Recht
www.schutt-waetke.de