

Positionierung von Marko Rogge zum § 202c StGB „Vorbereiten des Ausspähsens und Abfangens von Daten“

(1) 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.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

So lautet die exakte Formulierung des Bundesministeriums der Justiz, mit der die Strafbarkeit von Schadsoftware etc. erklärt werden soll.

Fachleute und Sicherheitsexperten diskutieren seit Monaten darüber, wie sinnvoll wirklich die Einbringung eines solchen Paragraphen in das Strafgesetzbuch ist bzw. war. Denn gültig ist der § 202c bereits.

Grundlegend sei gesagt, dass der Schutz von Daten ein solches Gesetz rechtfertigen könnte, wenn die Sicherheit von Daten damit erreicht oder erhöht werden kann.

Genau das bezweifelt eine breite Front von Experten, die sich der Sicherheit von Netzwerken, Software, Hardware und Unternehmen verschrieben haben.

Es ist nämlich bislang mehr als schwierig, herauszufinden und nicht eindeutig, was alles genau in den strafrechtlich relevanten Bereich fällt und was nicht. Das Gesetz ist schwammig formuliert.

So gab es bereits Selbstanzeigen von Redakteuren namhafter Zeitungen (Heise Verlag), die sich durch den § 202c in Bedrängnis sahen. In einer Ausgabe einer Fachzeitung wurde den Lesern eine Software CD als Beilage beigelegt, um Netzwerkadministratoren gut ausgewählte Software an die Hand zu geben. Mit dieser wäre es möglich, ein Netzwerk oder eine Software auf Schwachstellen zu analysieren kann, um diese Schwachstellen beseitigen zu können. Da mit der gleichen Software auch ein Angriff vorbereitet werden könnte, könnte die Verteilung der Software im Sinne des § 202c einen Straftatbestand darstellen.

In der heutigen Zeit ist es wichtig, sich gegen kriminelle Machenschaften im Internet zu rüsten, um sich deutlich besser schützen zu können.

Es gilt, Schaden von sich und vom eigenen Unternehmen, den Kunden und den Arbeitnehmern abzuwenden. Unternehmenswerte müssen besonders geschützt werden, und das geht nur, indem man auch die Chancen und Möglichkeiten hat, die Methoden der kriminellen Angreifer (diese werden nicht als Hacker bezeichnet) zu studieren. Sicherheitsexperten und Hackern wird durch die Regelung des § 202c diese Möglichkeit der Studien verwehrt, da Codes, die entwickelt werden, nicht ausgetauscht werden dürfen.

Dies jedoch ist eine der wichtigen Notwendigkeiten, um Kollegen die gleichen Chancen für die Erreichung von Sicherheit anbieten zu können. Dass hier der Gesetzgeber durch die Verabschiedung von Gesetzen maßgeblich Unterstützung leisten kann, darf angezweifelt werden. und wird nicht möglich sein. Es ist wahrscheinlich, dass Sicherheit dadurch nicht erreicht oder erhöht werden kann.

Gerade der Bereich Wirtschaftskriminalität zeigt sich in neuen Dimensionen, was passiert, wenn sich Unternehmen nicht ausreichend schützen können. Denn Schutzmechanismen können auch nur aus Erkenntnissen der destruktiven

Vorgehensweise von Angreifern ermittelt werden. Es ist in diesem Zusammenhang mehr als bedeutend, als Sicherheitsexperte immer auf dem aktuellen Stand zu sein. Verschafft sich derzeit ein Sicherheitsexperte einen Schadcode, um diesen zu analysieren, so würde er sich nach § 202c strafbar machen. Das Bundesministerium der Justiz schreibt auf Anfrage, dass es für Sicherheitsexperten in diesem Fall zu keinen Beeinträchtigungen kommen wird.

Es wäre, um den § 202c anwenden zu können, zwingend notwendig, dass eine Straftat vorbereitet oder durchgeführt würde.

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 Zugänglich machen dieser Software - auf eine Computerstraftat beziehen. Schreiben des BMJ vom Oktober 2006

Zitat aus einem [Schreiben des BMJ vom Oktober 2006](#).

Leider muss man hier feststellen, dass nicht klar definiert ist, was ein Schadprogramm im Sinne des § 202c ist.

Als Beispiel schildere ich hierbei, dass ein Sicherheitsexperte einen Sicherheits-Scanner wie nmap verwenden würde, um erste greifbare Informationen über ein Zielsystem zu erhalten. Das Arbeiten mit der Software nmap wäre somit nicht als strafbar anzusehen. Die Software eignet sich aber auch dazu, eine Straftat vorzubereiten. Ein potentieller Angreifer verfügt ebenso über die Möglichkeit, sich die Software nmap zu beschaffen und damit Informationen über ein Zielsystem einzuholen. Ein Sicherheitsexperte dürfte sich eine Software nicht beschaffen, die für eine Sicherheitsanalyse dienen soll, aber auch für kriminelle Zwecke eingesetzt werden könnte. Hier würde das Verschaffen dieser Software greifen, und der Sicherheitsexpert sich strafbar im Sinne des § 202c machen.

Meiner Meinung nach ist der § 202c sicherlich zur Erhöhung der Sicherheit von Computersystemen angedacht gewesen, schafft aber viel Unsicherheit bei Sicherheitsexperten und in der Konsequenz in den Computersystemen. Würde sich jeder Sicherheitsexperte exakt an die Gegebenheiten des § 202c halten, so würden Unternehmen keine effektive Sicherheit mehr herstellen dürfen und würden sich den Angreifern aussetzen müssen.

Eine Sicherheit für Mensch und Maschine ist nur dann denkbar und machbar, wenn man auch die Methoden und Programme der Angreifer beschaffen und studieren kann. Ich sehe immenses Gefahrenpotential, das durch eine falsche Einstufung und Einschätzung von Sicherheitssoftware hervorgerufen wird, die dann nicht mehr für die Sicherheit eingesetzt werden darf.

Marko Rogge zum § 202c StGB, Januar 2009.

<http://www.marko-rogge.de>