von Rechtsanwalt **Jan Lennart Müller**

Gesetzesentwurf: Kommt ein strafbarer digitaler Hausfriedensbruch?

Heutzutage lesen wir fast täglich von Cyberangriffen und den immensen Schäden in Milliardenhöhe, die sie pro Jahr anrichten. Aufgrund des technischen Fortschritts treten diese ständig in neuen, immer komplexeren Formen mit schweren Folgen auf. Um uns besser zu schützen und bisherigen Strafbarkeitslücken entgegen zu treten, brachte nun der Deutsche Bundesrat einen Gesetzesentwurf zum Digitalen Hausfriedensbruch in den Deutschen Bundestag ein. Lesen Sie mehr hierzu in unserem heutigen Beitrag.

Das Problem: Cyberkriminalität

Cyberkriminalität ist heutzutage präsenter denn je zuvor.

Ein akutes Problem stellen "Distributed-denial-of-service-Attacken" (*DDOs-Attacken*) dar, welche den Zugriff auf die angegriffenen Dienste verhindern oder einschränken.

Derartige Angriffe auf sog. Kritische Infrastrukturen wie Elektrizitätswerke, Telekommunikationsanlagen, aber auch Angriffe mit **Schadprogrammen** auf Einrichtungen wie Atomkraftwerke können immense Schäden anrichten.

Auch hören wir immer häufiger von sog. Erpressungs-Trojanern oder Krypto-Trojanern, welche große Probleme bereiten.

Neben öffentlichen Infrastrukturen stellen jedoch auch Privatpersonen ein Ziel von Cyberattacken dar. Viele Menschen speichern neben persönlichen auch berufliche Daten auf ihren Smartphones oder verwenden sie als Bezahlungsmittel. Im Falle eines Angriffs können die Täter jegliche Daten einsehen, speichern oder löschen.

Um sich Zugriff auf IT-Systeme zu verschaffen, nutzen Täter häufig "*Botnetze*", sie infiltrieren also unbemerkt eine große Anzahl solcher Systeme und steuern diese aus der Ferne.

Eine Infiltration kann durch das Anklicken von Links in Spam-E-Mails, das Öffnen infizierter Dateianhänge oder präparierter Internetseiten (sog. drive-by-infection) geschehen, wodurch Schadprogramme unerkannt im Hintergrund auf ein technisches Gerät aufgespielt werden können.

Botnetze stellen dabei im Bereich der Cyberkriminalität eine extrem wichtige Infrastruktur für Täter dar. Sie ermöglichen es ihnen, unerkannt Spam-E-Mails zu verschicken, Geldmassen zu verschieben oder Internetdienste zu nutzen. Durch den Zugriff auf sämtliche Inhalte auf Festplatten, Cloudspeicher und Computerhardware der infiltrierten Systeme stellen sie außerdem eine effektive Methode für sie dar, um unbemerkt Informationen zu erlangen oder die Opfer auszuspionieren.

In welchem Ausmaß solche Cyberattacken stattfinden, sei laut dem Entwurf schwer zu beziffern. Häufig bleiben die Angriffe unbemerkt, sodass von einer hohen Dunkelziffer auszugehen sei. Alleine 2014 wurden 14 Millionen ausgespähte Datensätze gefunden. Dies verdeutliche das Ausmaß der Attacken, wobei feststehe, dass diese Zahlen in den letzten Jahren deutlich gestiegen seien.

Derzeitige Schutzmöglichkeiten

In heutiger Zeit sind informationstechnische Systeme derart komplex, dass es für Laien kaum noch möglich sei, sie zu verstehen und sich selbst richtig zu schützen.

Das Einrichten von Schutzprogrammen sei oft mit hohem Aufwand und Funktionseinbußen verbunden oder nicht effektiv genug. Laut der Gesetzesbegründung könne davon ausgegangen werden, dass bis zu 40% der Computer, Smartphones etc. in der Bundesrepublik mit Schadsoftwares infiltriert seien.

Auch das Strafrecht biete nach Ansicht des Bundesrates momentan nur einen lückenhaften Schutz gegen Cyberangriffe.

Die derzeit einschlägigen Normen, §§ 202a, 303a, 303b StGB, seien nicht geeignet, die neuen und verschiedene Formen von Cyberangriffen zu erfassen. So seien zwar die Daten geschützt, nicht jedoch die IT-Systeme selbst. Auch sei es aufgrund der Komplexität der Schadsoftwares schwer ihr Vorhandensein zu beweisen, zumal viele sich selbst bei ihrer Entdeckung löschen können.

Lösung: Gesetzesentwurf § 202e StGB ("Digitaler Hausfriedensbruch")

Um den Problemen zu begegnen, reichte der Bundesrat (bereits zum dritten Mal) den **Entwurf für einen neuen Straftatbestand § 202e StGB** in den Bundestag ein, welcher bereits die unbefugte Verschaffung des Zugangs und Benutzung informationstechnischer Systeme mit einer Freiheitsstrafe von bis zu 10 Jahren bestrafen solle. Aufgrund des weiten Anwendungsbereichs sollen hiermit nahezu alle Formen von Angriffen erfasst werden können.

Die Gesetzesbegründung berufe sich insbesondere auf das vom Bundesverfassungsgericht statuierte

"Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG)", dessen Schutz die Norm gewährleisten solle.

Durch den neuen Straftatbestand solle auch den Beweisschwierigkeiten begegnet werden, da durch eine Auswertung der Täterinfrastruktur und anhand von IP-Adressen eine unbefugte Benutzung einfach nachgewiesen werden könne, ohne dass eine detaillierte Darstellung der Infiltration von dem Opfer verlangt werden müsse.

Hervorzuheben ist auch, dass der Gesetzesentwurf eine verschärfte Strafbarkeit speziell für den Fall vorsehe, dass der Täter in der Absicht handele, einen Ausfall oder eine Beeinträchtigung Kritischer Infrastrukturen zu bewirken. Hiermit solle diesem Problem effektiv entgegengetreten werden.

Kritik zum Gesetzesentwurf

Insbesondere die Bundesregierung äußerte jedoch bereits Bedenken hinsichtlich der vorgeschlagenen Strafnorm. So wurde von ihr vorgebracht, dass der bisherige Schutz des StGB ausreichend sei und es bei Anwendung des § 202e StGB zu einer zu weitgehenden Strafbarkeit kommen würde.

Auch seien Beweisschwierigkeiten kein Grund, eine neue Norm zu schaffen. Problematisch sei weiterhin, dass die Höhe der Strafandrohung beispielweise bei Angriffen auf Kritische Infrastrukturen lediglich von einer Absicht abhängig sei. Es sei schwierig, alleine deswegen eine derart hohe Freiheitsstrafe zu

Fazit

Nach den letzten zwei gescheiterten Gesetzesentwürfen des Bundesrates bleibt es nun abzuwarten, ob der Bundestag sich diesmal für die Verabschiedung des Gesetzes und damit die Ausweitung der Strafbarkeit auf den "digitalen Hausfriedensbruch" entscheidet. Dies könnte derzeit bestehende Strafbarkeitslücken schließen und einen besseren Schutz der IT-Systeme gewährleisten.

Wir werden unsere Leser hier auf dem Laufenden halten und weiter über das Gesetzgebungsvorhaben berichten.

Hinweis: Bleiben Sie rechtlich stets auf dem Laufenden und schaffen so dauerhafte Rechtssicherheit! Die **Schutzpakete der IT-Recht Kanzlei** sichern Sie dauerhaft ab.

Autor:
RA Jan Lennart Müller
Rechtsanwalt