AG KRITIS

Arbeitsgruppe Kritische Infrastrukturen

Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Modernisierung des Computerstrafrechts

Version 1.0 – zuletzt editiert am 11.12.2024

Inhaltsverzeichnis

1) Arbeitsgruppe Kritische Infrastrukturen

Dieses Dokument wurde erstellt von Mitgliedern der unabhängigen Arbeitsgruppe Kritische Infrastrukturen (AG KRITIS).

Wir haben uns im Frühjahr 2018 erstmals zusammengefunden, um Ideen und Anregungen zur Erhöhung der Resilienz und Sicherheit kritischer Dienstleistungen von Betreibern kritischer Infrastrukturen im Sinne des Gemeinwohls zu entwickeln. Unser Ziel ist es, die Versorgungssicherheit der deutschen Bevölkerung zu erhöhen, indem wir die Bewältigungskapazitäten des Staates zur Bewältigung von Großschadenslagen, die durch Cyberangriffe hervorgerufen werden, ergänzen und erweitern wollen. Unsere Arbeitsgruppe ist unabhängig von Staat, Verwaltung oder wirtschaftlichen Interessen.

Die AG KRITIS besteht aus ca. 42 Fachleuten und Experten, die sich mit Kritischen Infrastrukturen (KRITIS) gemäß § 2 (Abs 10) BSI-Gesetz[1] und gemäß § 10 BSIG zugehöriger *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz*[2] (BSI-Kritisverordnung - BSI-KritisV) beruflich beschäftigen, zum Beispiel durch Planung, Aufbau, Betrieb sowie Beratung, Forschung oder Prüfung der beteiligten Systeme und Anlagen. Unser Engagement ist getrieben von der Motivation, unabhängig von wirtschaftlichen Interessen eine nachhaltige Verbesserung der Sicherheit jener Anlagen kooperativ mit allen Beteiligten herbeizuführen und damit im Katastrophenfall die öffentliche Sicherheit zu verbessern. Wir sind kein Wirtschaftsverband oder Unternehmen und haben daher auch und insbesondere keine Sponsoren.

Uns eint, dass wir durch unsere Arbeit unabhängig voneinander zu dem Schluss gekommen sind, dass die Ressourcen der Bundesrepublik Deutschland zur Bewältigung von Großschadenslagen auf Grund von informations- und operationstechnischen Vorfällen im Bereich der kritischen Infrastrukturen nicht ausreichen. In der Folge sind resultierende Krisen oder Katastrophen nicht oder kaum zu bewältigen. Es sollen daher Wege gefunden werden, das Eintreten gravierender Folgen dieser Vorfälle durch schnelles und kompetentes Handeln zu verhindern oder zumindest abzuschwächen und eine Regelversorgung in kürzest möglicher Zeit wieder sicherzustellen.

1 https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html
2 https://www.gesetze-im-internet.de/bsi-kritisv/index.html

2) Einleitung

Mit dieser Stellungnahme möchten wir auf den dringenden Bedarf an Rechtssicherheit für IT-Sicherheitsforschende hinweisen, insbesondere für jene, die sich ehrenamtlich und aus gemeinnützigem Interesse für die IT-Sicherheit in Deutschland engagieren. Während kommerzielle IT-Sicherheitsforschung durch vertragliche Vereinbarungen rechtlich abgesichert ist, fehlt es ehrenamtlich Forschenden oft an einer klaren rechtlichen Grundlage. Diese Unsicherheit führt zu einem besorgniserregenden "Chilling-Effekt": Sicherheitslücken werden aus Angst vor strafrechtlichen Konsequenzen nicht mehr gemeldet, wodurch potenzielle Gefahren für die Allgemeinheit unentdeckt bleiben.

Bedauerlicherweise gibt es in Deutschland bereits mehrere Fälle, in denen IT-Sicherheitsforschende strafrechtlich verfolgt wurden, obwohl sie in gutem Glauben und im Interesse der öffentlichen Sicherheit gehandelt haben. Beispielhaft sei der Fall des IT-Sicherheitsforschers erwähnt, der eine schwerwiegende Sicherheitslücke in der Software des Unternehmens "Modern Solution" entdeckte und dafür strafrechtlich verfolgt wurde. Das Landgericht Aachen bestätigte das Urteil gegen ihn, da das Gericht sein Handeln als unbefugten Zugriff nach dem sogenannten Hackerparagraphen (§ 202a StGB) wertete. Ebenso zeigt der Fall der Sicherheitsforscherin Lilith Wittmann, die durch die Entdeckung einer Sicherheitslücke in der CDU-Wahlkampf-App für Aufsehen sorgte und zeitweise rechtliche Konsequenzen fürchten musste, den dringenden Reformbedarf in diesem Bereich auf. Solche Verfahren wirken abschreckend und verhindern, dass Sicherheitsrisiken gesucht, gemeldet und behoben werden können.

Wir begrüßen ausdrücklich die Bemühungen des Bundesministeriums der Justiz (BMJ), den Dialog mit der Zivilgesellschaft durch die Symposien zu suchen. Diese Symposien stellen das beste Beispiel für zivilgesellschaftliche Einbindung dar, das die Bundesregierungen der letzten Jahrzehnte erreicht haben und können als Vorbild für gute Praxis in anderen Ministerien und für andere Beteiligungsverfahren dienen.

Gleichzeitig möchten wir betonen, dass die Fokussierung auf strafrechtliche Reformen allein nicht ausreicht. Auch im Zivilrecht besteht Reformbedarf, z.B. im Urheberrechtsgesetz in Bezug auf das Verbot der Dekompilation oder die fehlende Ausnahme im Geschäftsgeheimnisgesetz (GeschGehG) für die Meldung von Sicherheitslücken. Hier bedarf es klarer rechtlicher Regelungen, die Forschenden Rechtssicherheit bieten, ohne sie unverhältnismäßigen Risiken auszusetzen.

Ein weiterer Bereich, der dringend einer Reform bedarf, betrifft Funkschnittstellen. Das derzeitige Abhörverbot steht einer rechtmäßigen Meldung von Sicherheitslücken im Wege. Hier müssen gesetzliche Ausnahmen geschaffen werden, um Sicherheitsforschenden die verantwortungsvolle Meldung gefundener Schwachstellen wie z.B. unauthentifizierten und

unverschlüsselten Steuerbefehlen für Energieerzeugungsanlagen, Justizvollzugsanstalten oder Verkehrssteueranlagen zu ermöglichen. Auch im Bereich der besonders sensitiven Gesundheitsdaten gibt es immer wieder Vorfälle, in denen beispielsweise Rettungsleitstellen sensible Personendaten in Verbindung mit Gesundheitsdaten und Diagnosen per Funkschnittstelle aussenden.

Wir hoffen, dass unsere Anregungen in die Reform des BMJ einfließen und danken für die Möglichkeit, an dieser Anhörung teilzunehmen.

3) Stellungnahme zum Gesetzesentwurf

Vorsatzlösung für § 202a und § 202b StGB

Die beiden Möglichkeiten, Rechtssicherheit für IT-Sicherheitsforschende zu schaffen, die diskutiert werden, sind:

1. Computerstraftaten ein weiteres Tatbestandsmerkmal hinzuzufügen. Neben der Überwindung einer Zugangssicherung und den anderen Tatbestandsvoraussetzungen wäre es wichtig, auch den Vorsatz einer materiellen Schädigung des Opfers als Tatbestandsmerkmal aufzunehmen. Das würde bedeuten, dass ein ermittelnder Staatsanwalt zumindest prüfen muss, ob Indikationen für einen Vorsatz der Schädigung des Dritten vorliegen.
2. Eine Ausnahme definieren, die unter bestimmten Umständen das Überwinden von Zugangshindernissen in fremde Computern straffrei definiert. Diese Umstände könnte dann ein Beschuldiger im Ermittlungsverfahren geltend machen, so dass dann die Strafverfolgung eingestellt wird.

Durch die vorgenommene Wahl des zweiten Ansatzes wird die Justiz entlastet – jedoch zum Nachteil der IT-Sicherheitsforschenden, die im Zweifel von Vernehmung bis Hausdurchsuchung und mit Monate- oder jahrelanger Beschlagnahmung von Computerhardware rechnen müssen, bevor es zur Einstellung des Verfahrens kommt.

Aus Sicht der IT-Sicherheitsforschenden wäre es deutlich besser, eine Schädigungsabsicht in den Tatbestand aufzunehmen. Dies würde bedeuten, dass es neben den anderen Tatbestandsvoraussetzungen auch noch das Tatbestandsmerkmal des Vorsatzes einer Schädigung des Opfers geben müsste (vgl. § 263 StGB). Dabei sollte zusätzlich klargestellt werden, dass diese Schädigung nicht alleine eine Schädigung des Ansehens des Softwareherstellers sein kann, sondern sich auf konkretere Weise materialisieren muss, z.B. durch Tateinheit mit Taten nach §§ 303a/303b StGB oder durch unbefugtes verbreiten von Zugangsgeheimnissen.

Klarstellung des § 202c StGB

Obwohl uns keine Gerichtsurteile zum Nachteil von IT-Sicherheitsforschenden bekannt sind, bei denen ein Verstoß nach § 202c StGB Teil der Anklage oder des Urteils war, sind wir trotzdem der Meinung, dass der § 202c StGB zumindest neu formuliert gehört. Ohne Fachkenntnis mehrerer Justizentscheidungen, u.A. die Entscheidung der Staatsanwaltschaft Hannover (Az. 1111 Js 181/09) oder die Entscheidung des BVerfG - (2 BVR 2233/07 - 2 BVR 1151/08 - 2 BVR 1524/08) ist es für eine IT-Sicherheitsforschende Person nicht möglich, die Strafbarkeit der verwendeten oder entwickelten IT-Sicherheitswerkzeuge zu verstehen.

Die Lesart des § 202c StGB in der Community der IT-Sicherheitsforschenden weicht grundlegend von der Klarstellung des BVerfG ab. Die Überzeugung, dass schon Netzwerkanalysewerkzeuge wie z.B. nmap oder Live-Systeme wie Kali in Deutschland verboten seien, ist weit verbreitet. Insbesondere Abs. 1 Nr. 2 ist hier missverständlich. Zwar stellt das BVerfG klar, dass der alleinige „Zweck der Begehung einer solchen Tat“ strafbar ist – der daraus folgende Umkehrschluss, dass Computerprogramme deren Zweck nicht alleinig die Begehung von Computerstraftaten im Sinne des § 202c StGB ist, legal sein müssten, ist jedoch nur für Juristen die sich nicht nur mit dem Gesetzestext sondern auch den Entscheidungen befasst haben, erkennbar.

Schon die GGO § 42 (5) sagt: „Gesetzentwürfe müssen sprachlich richtig und möglichst für jedermann verständlich gefasst sein“. Da regelmäßig davon ausgegangen werden muss, das „jedermann“ nicht jede Entscheidung des BVerfG studiert hat, folgt daraus ein Klarstellungsbedarf für den § 202c StGB.

Auch das Gebot der Normenklarheit löst die Verpflichtung des mit öffentlicher Rechtsetzungsmacht ausgestatteten Normgebers aus, seine Rechtsvorschriften so zu formulieren und zu gestalten, dass der Einzelne, ob von der jeweiligen Rechtsvorschrift begünstigt oder belastet, die aus seiner Normunterworfenheit sich ergebende Rechtslage so konkret erkennen kann, dass er sein Verhalten daran auszurichten vermag (BVerfG 29.11. 2023 - 2 BvF 1/21 - Rn. 81). Es ist – als Geltungsvoraussetzung für Rechtsnormen – begründet im Fundamentalprinzip der Rechtsstaatlichkeit (Art. 20 Abs. 3 GG) und dem daraus abgeleiteten Grundsatz der Rechtssicherheit.[3]

Meldestellen

In der Liste der Meldestellen in § 202a (3) Nr 1. StGB-E sollten mindestens die Bundes- und 16 Landesdatenschutzbeauftragten, sowie die auf Landesebene eingerichteten Zentralen Ansprechstellen Cybercrime (ZAC) als mögliche Meldeempfänger aufgenommen werden. Eine entdeckte IT-Sicherheitslücke ist regelmäßig auch ein starkes Indiz eines Datenabflusses durch Dritte. Der Fund der Lücke beweist, dass andere diese auch hätten nutzen können. Es ist daher

3 https://de.wikipedia.org/wiki/Normenklarheit

möglich, dass IT-Sicherheitsforschende nicht die Ursache (die IT-Sicherheitslücke), sondern den resultierenden möglichen Datenabfluss melden und so auch ihr gutwilliges und gemeinnütziges Verhalten dokumentieren.
Ebenfalls sollten die zentralen Ansprechstellen Cybercrime der Länder (ZAC), aufgrund der inhaltlichen Nähe, als Meldestellen in den Katalog aufgenommen werden.

Änderungen an der Begründung

Aus unserer Sicht sollte in der Begründung ergänzt werden, dass eine Meldung nicht vollständig sein muss, um sich als solche zu qualifizieren. Meldungen die eine Sicherheitslücke beschreiben, sollten weder alle Auswirkungen noch alle Ursachen benennen müssen. Die Feststellung einer Sicherheitslücke oder eines Datenabflusses muss ausreichen.

4) Weitere Fehlstellen außerhalb des StGB

Obwohl die vorgeschlagene Reform des Strafrechts die größte Rechtsunsicherheiten für IT-Sicherheitsforschende behebt, ist es nicht ausreichend nur das Strafgesetzbuch zu ändern, wenn das Ziel „Rechtssicherheit für IT-Sicherheitsforschende“ lautet. Weitere Gesetzesänderungen wären notwendig, um alle Arten von Schwachstellen rechtssicher und ohne persönliche Risiken für die IT-Sicherheitsforschenden, melden zu können.

TDDDG § 5

IT-Sicherheitsforschung erfolgt auch im Bereich von Funkübertragungen. Hier steht der § 5 des Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (TDDDG) sogar schon der Meldung an eine zuständige Behörde im Weg. Das Abhörverbot stammt aus einer Zeit, als wirksame Verschlüsselungsgeräte im Bereich von Funkübertragungen unglaublich klobige Geräte waren, die mit Mobilität nichts gemein hatten und eigentlich nur in Gebäuden, Schiffen oder Flugzeugen montiert werden konnten.

Der Stand der Technik hat sich hier erheblich weiterentwickelt. Bei Funkkommunikation in sensitiven Bereichen (beispielsweise KRITIS generell, Staat und Verwaltung, unverschlüsselte personenbezogene Daten) ist verschlüsselte Kommunikation inzwischen die Norm und damit Stand der Technik. Dort wo trotzdem noch unverschlüsselt über Funk kommuniziert wird, ist dies schon seit Jahrzehnten nicht mehr notwendiges Übel, sondern aufgrund der breiten Verfügbarkeit von Verschlüsselungstechnik ein Anlass zur Besorgnis und staatlicher Prüfung. Nach von uns erhaltenen Rückmeldungen von Betreibern unverschlüsselter Funknetze, wird Verschlüsselung – und der damit einhergehende Kompromittierungsschutz und Schutz personenbezogener Daten und Gesundheitsdaten – regelmäßig als „zu teuer“ angesehen. Dies stellt einen Anlass zur Besorgnis und zur Prüfung durch die Aufsichtsbehörden - Bundesnetzagentur und Bundes-/Landesbeauftragte für Datenschutz - dar.

Die Entdeckungen der AG KRITIS rund um die Möglichkeiten Energieerzeugungs- und andere Anlagen über unverschlüsselte und unauthentifizierte Funkkommunikation zu steuern, zeigen das Problem auf, dass der Staat nicht ausreichend in der Lage ist, diese Problematiken zu prüfen. Zwar wird in manchen sensitiven Bereichen der Stand der Technik zumindest für privatwirtschaftliche Betreiber von KRITIS vorgegeben, in staatlichen Einrichtungen gibt es allerdings oft keine Vorgaben für Mindestsicherheitsstandards im Bereich der IT-Sicherheit. In beiden Fällen wird die Umsetzung nicht flächendeckend sondern höchstens stichprobenartig geprüft.

Alleine in der Kalenderwoche 42/2024 sind beim BSI und den LfDIs Schwachstellenmeldungen zu mindestens 6 verschiedenen Funkschnittstellen von 6 Rettungsleitstellen eingegangen, bei denen personenbezogene Daten ungesichert über Funk übertragen wurden. Außerdem gab es mehrere Medienberichte[4] [5] [6] [7] zu missbräuchlich ausgelösten Sirenen zur Warnung der Bevölkerung über deren unverschlüsselte Funkschnittstelle. Die unverschlüsselte Funkkommunikation stellt offensichtlich ein Einfallstor für die Kompromittierung durch technisch interessierte Laien dar.

Der Empfang, die Kenntnisnahme und die fachgerechte Dokumentation solcher unverschlüsselter Kommunikation, mit dem Zweck der Meldung an die zuständige Behörde, muss folglich legalisiert werden. Ein möglicher Ansatz wäre eine Adaption nach dem Wesensgehalt des neuen § 202a (3) StGB-E als neuen § 5 (4) TDDDG.

GeschGehG § 5

Der aktuelle Wortlaut des § 5 Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) erlaubt keine rechtssichere Meldung von Sicherheitslücken an zuständige Stellen, wodurch ein zivilrechtliches Klagerisiko für IT-Sicherheitsforschende entsteht. Dieses Risiko realisiert sich dann, wenn Unternehmen nach der Aufdeckung einer Schwachstelle, zivilrechtliche Schadensersatzansprüche geltend machen. Beispielsweise kann die Dekompilation einer proprietären Applikation als Geschäftsgeheimnisverrats gelten. Das Dekompilieren ist jedoch in vielen Fällen unverzichtbar, etwa um fest programmierte Zugangsdaten im Quellcode zu identifizieren. Zur rechtlichen Absicherung wird die Ergänzung einer neuen Nr 4 im § 5 GeschGehG vorgeschlagen: „zur Feststellung und Meldung einer Sicherheitslücke oder Schwachstelle in einem informationstechnischen System.“

UrhG § 69e

Der Paragraph § 69e des Urheberrechtsgesetzes (UrhG) verbietet das Dekompilieren von Applikationen (Binaries). Diese weit verbreitete Methode in der Sicherheitsforschung ist also derzeit untersagt. Es gibt zwar eine Ausnahme von dieser Norm für die Herstellung von

4 https://bnn.de/pforzheim/pforzheim-stadt/sirenen-fehlalarm-schreckt-menschen-in-pforzheim-auf
5 https://www.radiovest.de/artikel/fehlalarm-sirenen-heulten-in-marl-2054151.html
6 https://www.aachener-zeitung.de/lokales/region-aachen/eschweiler/fehlalarm-sorgt-fuer-aufregung-in-eschweiler/16433152.html
7 https://www.rhein-zeitung.de/lokales/koblenz-region/falscher-alarm-in-ruebenach-sirenen-ausgeloest_arid-2680356.html

Interoperabilität, jedoch nicht für IT-Sicherheitsforschung. Da Software zum Dekompilieren von Applikationen frei verfügbar ist, muss davon ausgegangen werden, dass diese Methode von Cyberkriminellen eingesetzt wird, um Schwachstellen aufzudecken und auszunutzen. Entsprechend ist es notwendig, auch IT-Sicherheitsforschenden dies straffrei zu ermöglichen.
Ein Lösungsansatz könnte sein, dem §69 e einen weiteren Absatz anzufügen, welcher, analog zu § 202a (3) StGB, eine Ausnahme für das Dekompilieren zum Zweck des Aufdeckens von IT-Sicherheitslücken oder Schwachstellen schafft. Hierbei sollte auch festgestellt werden, dass Sicherungsmaßnahmen, die durch Fachkundige umgangen werden können, nicht als Sicherungsmaßnahme gelten dürfen – bei der Bewertung, ob ein Zugangshindernis befugt oder unbefugt umgangen wurde, muss die Tatsache einer erfolgreichen Umgehung zu einer Vermutung nicht ausreichender Sicherung (nicht nach Stand der Technik) auf Seiten des Herstellers oder Betreibers führen.