VDA | Verband der Automobilindustrie

Positionspapier

Cybersecurity-Tests

Anpassung des Strafrechts bezüglich der Durchführung von Cybersecurity-Tests

Berlin, den 12. August 2024

Zusammenfassung

Fahrzeughersteller sind heute verpflichtet, durch Penetrationstests Sicherheitslücken ihrer Produkte zu identifizieren und zu beseitigen. Sowohl für mit der Durchführung solcher Tests beauftragte Spezialisten als auch für unabhängig agierende, ethische Sicherheitsforscher besteht dabei nach heutiger Gesetzeslage jedoch die Gefahr, sich strafbar zu machen.

Der VDA empfiehlt, im Rahmen der seitens des BMJ angekündigten Strafrechtsnovelle in den relevanten Gesetzen als Kriterium der Strafbarkeit nicht mehr nur die Zustimmung zur Testdurchführung durch den Verfügungsberechtigten allein, sondern gleichberechtigt auch die - positive oder negative - Intention des Testers einzusetzen.

Eine positive Intention kann nach Auffassung des VDA primär an folgenden Indizien festgemacht werden:

- verantwortungsvoller Umgang mit identifizierten Sicherheitslücken (z.B im Rahmen einer Coordinated Vulnerability Disclosure)
- erkennbarer Beitrag zur Bestätigung oder Stärkung der Cybersicherheit des getesteten Systems
- erkennbarer Beitrag zum Schutz des Systemherstellers
- erkennbarer Beitrag zum Schutz von Nutzern

Eine negative Intention kann im Gegensatz dazu an der Erlangung insbesondere monetärer (über eine Bug Bounty hinausgehenden) Vorteile für sich oder Dritte festgemacht werden.

Zielsetzung

Dieses Positionspapier soll die aktuelle rechtliche und politische Situation der Automobilindustrie bei der Durchführung von Penetrationstests zur Detektion von Cybersecurity-Lücken aufzeigen und daraus abgeleitet eine Empfehlung zur Anpassung der in Form des § 202 a ff StGB[1] (sog. „Hackerparagraph“) und weiterer Rechtsnormen geltenden strafrechtlichen Rahmenbedingungen geben.

Im Fokus dieser VDA-Position stehen Sicherheitstests an Fahrzeugen, nicht aber an Extended Vehicle (Backend), Apps, Infrastruktur (z.B. Ladestationen) oder anderen IT-Systemen.

[1] *§ 202a StGB - Einzelnorm (gesetze-im-internet.de)*

1. Ausgangssituation

1.1 Ausgangslage

Der europäische und deutsche Gesetzgeber verlangt in verschiedenen Regulierungen berechtigterweise von Herstellern, dass bei der Entwicklung von Produkten deren Cybersecurity im ausreichenden Maße berücksichtigt wird. Dies schließt insbesondere auch das Testen der Produkte in angemessenem Maße mit ein. So fordert auch die Branchenregulierung UNECE R 155[2] i.V.m. VO (EU) 2019/2144[3] von Automobilherstellern im Rahmen zu implementierender Cybersecurity-Managementsysteme die Durchführung von Cybersecurity-Tests, um die Effektivität implementierter Cybersecurity-Maßnahmen zu überprüfen. Nach dem heutigen Stand von Wissenschaft und Technik sind dazu insbesondere auch invasive Testverfahren notwendig, u.a. auch die Durchführung von Penetrationstests zur Aufdeckung von Cybersicherheitslücken. Auswirkungen von Cyberangriffen können gemäß UNECE R155 sein:

- unsicherer Betrieb der betroffenen Fahrzeuge
- Einschränkung von Fahrzeugfunktionen
- Verletzung der Datenintegrität etc.

Personengruppen, die im Sinne des Herstellers / Systementwicklers mit guter Intention Tests zur Detektion von Sicherheitslücken durchführen sind:

1. interne Tester des Herstellers / Systementwicklers oder von diesem beauftragte externe Tester / Fachfirmen (Standardfall)

2. vom Hersteller / Systementwickler nicht direkt beauftragte, eigenmotivierte und ggf. über Auslobung einer sog. „Bug Bounty“ incentivierte externe, unabhängige Sicherheitsforscher (sog. „White Hat Hacker“ oder „ethische Hacker“).
   Mit Bug Bounty wird dabei der breite Aufruf eines Systementwicklers an die Sicherheitsforscher-Community bezeichnet, sein System anzugreifen, verbunden mit der Zusage einer Prämie für dabei gefundene und zurückgemeldete Schwachstellen.
   Als Beleg ihrer guten Intention verpflichten sich White Hat Hacker häufig einem entsprechenden Code of Conduct.

Darüber hinaus gibt es auch Personengruppen, die mit negativer Intention (Schädigungsabsicht, über Bug-Bounty hinausgehende Gewinnerzielungsabsicht, Geltungssucht …) Sicherheitslücken ausspähen und ggf. nutzen (sog. „Black Hat Hacker“).

---

[2] *R155e (2).pdf (unece.org)*

[3] *Verordnung - 2019/2144 - EN - EUR-Lex (europa.eu)*

1.2 Rechtliche Situation

Für Hersteller ergibt sich mit Blick auf die regulatorischen Cybersecurity-Anforderungen an ihre Produkte ein schwer lösbarer Zielkonflikt, da insbesondere die Durchführung von Cybersecurity-Tests in Form von Penetrationstests nach den folgenden Rechtsnormen strafrechtliche Risiken birgt:

- § 202a StGB: Unberechtigter Datenzugriff
- § 202b StGB: Unberechtigtes Abfangen von Daten
- § 202c StGB: Vorbereitung einer unerlaubten Handlung nach § 202a oder § 202b StGB
- § 303a ff. StGB[4]: Unberechtigte Datenveränderung
- § 23 GeschGehG[5]: Verletzung von Geschäftsgeheimnissen
- §§ 106 - 108b UrhG[6]: Unberechtigte Vervielfältigung und Verwertung

Im Mittelpunkt des strafrechtlichen Risikofeldes steht dabei § 202a StGB. Nach § 202a Abs. 1 StGB macht sich strafbar, wer unter Überwindung einer Zugangssicherung unbefugt in Computersysteme eindringt und dadurch Zugang zu Daten erlangt, die nicht für ihn bestimmt sind. Die tatbestandlich vorausgesetzte Zugangssicherung ist eine niedrige Hürde und regelmäßig bereits bei Vorliegen eines einfachen Passwortschutzes gegeben. Nicht für den Tester bestimmt sind die Daten dann, wenn dieser die Daten nicht gespeichert und gesichert hat. „Unbefugt“ im Sinne der Norm handelt der Tester zudem, wenn er ohne ausdrückliche Zustimmung der berechtigten Person – also der Person, die die Daten gespeichert und gesichert hat – auf das für ihn fremde System zugreift. Der Tester muss vor Durchführung eines Penetrationstests deshalb regelmäßig sicherstellen, die ausdrückliche Zustimmung der berechtigten Person einzuholen.

Für interne, insbesondere aber auch für beauftragte externe Tester ergibt sich damit die praktische Schwierigkeit, die berechtigten Personen entlang der – mitunter vielschichtigen – Lieferkette zunächst zu identifizieren und in einem zweiten Schritt von diesen eine ausdrückliche und damit rechtssichere Zustimmung einholen zu müssen. Enthält die zu testende Software zudem auch – wie üblich – Komponenten eines Drittunternehmens, kann diese Einholung der Zustimmung zur Testung ein zeitintensives, teures und insgesamt schwer umsetzbares Unterfangen sein. Erteilt eine berechtigte Person bzw. ein berechtigtes Unternehmen keine Zustimmung zur Testung und kommt keine anderweitige rechtliche Legitimation des Tests in Betracht, muss von einer Testung abgesehen werden, wodurch der Hersteller dann weder vollumfänglich seinen regulatorischen Pflichten nachkommen noch die Cybersecurity seiner Produkte lückenlos sicherstellen kann.

Für externe, nicht direkt beauftragte Sicherheitsforscher ist es in der Regel sogar unmöglich, eine Zustimmung der berechtigten Personen zur Durchführung von Penetrationstests einzuholen. Handelt ein solcher Sicherheitsforscher ohne Zustimmung und entdeckt im Rahmen seiner Testaktivitäten Sicherheitslücken, wird er diese nur unter dem erheblichen Risiko einer Strafverfolgung gegenüber dem Hersteller offenlegen können. Aus (berechtigter) Sorge vor Strafverfolgung legen nicht-beauftragte Sicherheitsforscher ihre Erkenntnisse deshalb häufig nicht gegenüber den Herstellern offen. Darunter leidet zuvorderst die Cybersecurity der betroffenen Produkte, da der Hersteller nur bei Kenntnis der Sicherheitslücke die Möglichkeit zu deren Behebung hat.

---

[4] *§ 303a StGB - Einzelnorm (gesetze-im-internet.de)*

[5] *§ 23 GeschGehG - Einzelnorm (gesetze-im-internet.de)*

[6] *§ 106 UrhG - Einzelnorm (gesetze-im-internet.de)*

Die derzeitige Rechtslage bevorteilt damit allein solche Personen, die Sicherheitslücken mit Schädigungsabsicht ausspähen: Während Hersteller und Sicherheitsforscher aus (berechtigter) Sorge vor Strafverfolgung von Penetrationstests absehen müssen und Sicherheitslücken deshalb unentdeckt und unbehandelt bleiben, haben Black Hat Hacker bei der Entdeckung und schädigenden Nutzung von Sicherheitslücken umso leichteres Spiel.

Die deutsche Automobilindustrie ist deshalb der Auffassung, dass eine Anpassung der einschlägigen Regulierungen zur Sicherstellung der Produkt-Cybersecurity erforderlich ist. Beauftragte interne und externe Tester wie auch nicht-beauftragte externe Sicherheitsforscher müssen ohne strafrechtliches Risiko Penetrationstestungen bei gleichzeitiger Pflicht zur verantwortungsvollen, vertraulichen Offenlegung (sog. „Coordinated Vulnerability Disclosure“) ihrer Erkenntnisse über Sicherheitslücken gegenüber den betroffenen Unternehmen durchführen können.

1.3 Aktuelle politische Situation

Die Bundesregierung hat diesen Interessenskonflikt erkannt und im aktuellen Koalitionsvertrag vereinbart, dass „Identifizieren, Melden und Schließen von Sicherheitslücken … legal durchführbar“ sein soll. Darüber hinaus hat das BMJ im Herbst 2023 eine Novelle des Strafrechts angekündigt, die Anpassungen der §§ 202a ff. StGB beinhalten soll. Ein Eckpunktepapier für einen entsprechenden Gesetzentwurf sollte bis Ende Q2 2024 veröffentlicht werden.

Im Sinne der Rechtssicherheit für die Hersteller von Cybersecurity-relevanten Produkten sowie deren Angestellte und Partner befürwortet die deutsche Automobilindustrie diese Initiative der Bundesregierung ausdrücklich. Aufgrund der wachsenden Anzahl von insbesondere europäischen Cybersecurity-Regelungen und der zuvor erläuterten Notwendigkeit zur Durchführung invasiver Cybersecurity-Testverfahren ist es notwendig, die angekündigte Strafrechts-Novelle auf die unter 1.2 genannten strafrechtlichen Regelungen auszudehnen und ihre Umsetzung zu beschleunigen.

2 Aktuelle Problematik / Auswirkungen auf die Automobilindustrie

Die Durchführung von Penetrationstest ist unter Zugrundelegung der normativen Rahmenbedingungen für die Cybersecurity-Typzulassung gem. UNECE R 155 i.V.m. der VO (EU) 2019/2144 in der konsolidierten Fassung vom 05.09.2022 ein maßgebliches Kernelement der Risikobewertung von Fahrzeug(teil-)systemen (vgl. hierzu auch Kapitel 1.1). Mittels Penetrationstest werden potenzielle Schwachstellen in Hard- und Software über die gesamte Wertschöpfungskette der Fahrzeughersteller identifiziert und sodann dem Regelkreislauf des Automotive Cybersecurity-Risikomanagements zugeführt. Die Nichtdurchführung derartiger Tests verstößt insoweit nicht nur gegen die branchenübliche Praxis, sondern könnte auch zur Versagung einer Typgenehmigung führen.

Dem Bestreben aller Akteure in der automobilen Wertschöpfungskette, potenzielle Schwachstellen mittels Penetrationstests zu identifizieren, steht jedoch die derzeitige Rechtslage in Deutschland zur strafrechtlichen Sanktionierung von Penetrationstests diametral gegenüber. Hierbei treffen die genannten sanktionsrechtlichen Folgen primär den im Angestelltenverhältnis beschäftigten Penetrationstestenden (beispielsweise in Ausführung seiner arbeitsrechtlich geschuldeten Tätigkeit als Teil eines sog. „Red Teams“), aber auch den unabhängigen Sicherheitsforscher, der im Rahmen eines Verfahrens zur Coordinated Vulnerability Disclosure Schwachstellen an Fahrzeugen und deren Teilsystemen identifiziert und dem OEM bzw. dem Komponentenzulieferer zurückmeldet.

Wenngleich, wie schon unter Kapitel 1.2.dargestellt, die strafrechtliche Sanktionierung von Penetrationstests maßgeblich davon abhängt, ob das tatbestandsmäßige Verhalten des Penetrationstestenden unbefugt erfolgte, ist dieser Aspekt für die weitere Betrachtung des Konfliktverhältnisses von Sanktionsnorm auf der einen und Automotive Cybersecurity-Regulierung auf der anderen Seite von geringer Bedeutung: Zwar können die Akteure in der automobilen Wertschöpfungskette durch vertragliche Vereinbarungen den Nutzungsumfang von Leistungsschutzrechten dezidiert regeln und sich insoweit auch mit der Durchführung von Penetrationstests einverstanden erklären. Andererseits bedingt die Komplexität von automobilen Komponenten und Funktionen sowie die Tiefe der Wertschöpfungskette in der Automobilindustrie ein nicht zu vernachlässigendes Risiko der Unvollständigkeit von bestimmten Assetverzeichnissen wie bspw. einer Software Bill of Materials (SBOM). In derartigen Fallgestaltungen müsste der einzelne angestellte Penetrationstestende das Risiko einer unzureichenden Einverständniserklärung eines potenziellen Rechteinhabers gegenüber seinem Arbeitgeber tragen. Unabhängige Sicherheitsforscher würden von derartigen Einverständniserklärungen dagegen gar nicht erfasst und könnten entsprechende Erklärungen unmöglich selbst einholen.

In der Konsequenz führt die Sanktionsandrohung für den Fall der Durchführung von Penetrationstests in der automobilen Wertschöpfungskette dazu, dass allein schon aus der arbeitsrechtlichen Fürsorgepflicht des Arbeitsgebers heraus eine derartige Tätigkeit durch angestellte Mitarbeiterinnen und Mitarbeiter zu unterbinden wäre.

Werden deshalb Penetrationstests nicht durchgeführt, führt der fehlende Erkenntnisgewinn zu einer generellen Schwächung der Cybersicherheit des Fahrzeugs. In der Folge gehen von diesem Fahrzeug dann deutlich mehr Risiken aus, welche den Fahrzeugnutzer treffen. Diese Entwicklung wird durch die kontinuierliche Erweiterung des Dunkelfelds potenzieller Schwachstellen im Fahrzeug noch verstärkt. Black Hat Hacker werden unabhängig von der Sanktionsdrohung nach deutschem Recht weltweit weiterhin aktiv an der Ausnutzung dieser Schwachstellen arbeiten. Somit gewinnen Black Hat Hacker einen immer größer werdenden Wissensvorsprung vor den Herstellern.

Letztlich ist aufgrund der Sanktionsandrohung auch mit einem Brain-Drain am Wirtschaftsstandort Deutschland zu rechnen. Dringend benötigte Fachkräfte würden ihre Tätigkeiten in das europäische Ausland verlagern, wo deren Tätigkeit nicht kriminalisiert wird.

3. Vorschläge der Automobilindustrie zur Anpassung der aktuellen Gesetzeslage

3.1 Ziel der Automobilindustrie

Wie in den vorangehenden Kapiteln ausgeführt, sind in der Automobilindustrie heute zusätzlich zu den im Rahmen der Systementwicklung durchgeführten Tests invasive Sicherheitstests zur Detektion von Sicherheitslücken vorgeschrieben, um die Cybersecurity der Fahrzeuge weiter zu steigern. Neben den internen oder beauftragten externen Testern beim Hersteller / Systementwickler führen vor allem auch externe, nicht direkt beauftragte Sicherheitsforscher (White Hat Hacker, vergl. Kapitel 1.1) diese Tests durch.

White Hat Hacking bezeichnet das erwünschte, ethisch motivierte Eindringen in Computersysteme und Netzwerke mit dem Ziel, Sicherheitslücken zu identifizieren und zu beheben, bevor sie von böswilligen Black Hat Hackern ausgenutzt werden können. White Hat Hacker sind in der Regel eigenmotivierte Spezialisten, die mit ihren fachlichen Fähigkeiten einen gesellschaftlichen Beitrag zur Stärkung der Informationssicherheit und Cybersecurity leisten möchten.

Sowohl den beauftragten als auch den nicht beauftragten Testern drohen aus den in Kapitel 1.2 genannten Rechtsnormen ggf. strafrechtliche Konsequenzen infolge ihres Handelns. Die Automobilindustrie fordert deshalb, diese Rechtsnormen so anzupassen, dass für beide Personengruppen Rechtssicherheit vor Strafverfolgung geschaffen wird.

Für eine Anpassung gelten dabei aus Sicht der Automobilindustrie die folgenden Prämissen:

- Ziel ist eine widerspruchsfreie Regelungslandschaft.
- Rechtssicherheit soll auch für das Testen von vom Beauftragenden nicht verantworteten Systemen/Komponenten gelten.
- Tests sollen von beiden genannten Personengruppen weiterhin mit möglichst wenig Restriktionen durchgeführt werden können. Gleichzeitig sollte aber ein rechtlicher Rahmen für den Umgang mit den beim Testen generierten Erkenntnissen geschaffen werden, an den sich auch Tester mit positiver Intention halten müssen („so frei wie möglich, so reguliert wie nötig“).
- Eine Akkreditierung oder Zertifizierung unabhängiger Sicherheitsforscher stellt aus Sicht des VDA keine gangbare Lösung dar. Sie widerspricht den Gepflogenheiten und Werten der Community und würde kaum Akzeptanz erfahren. Gleichzeitig besteht die Gefahr, dass Black Hat Hacker sich Akkreditierung verschaffen werden, um unbemerkt an Daten zu gelangen oder Systeme böswillig zu manipulieren.

3.2 Intention als Kriterium der Strafbarkeit

Ausschlaggebend für die Strafbarkeit eines Tests bzw. Angriffs sollte aus Sicht des VDA nicht die Zustimmung zum Test, sondern die – positive oder negative – Intention des Testers sein. Für beauftragte Tester ist eine positive Intention für Handlungen im Rahmen seines Auftrags in der Regel per se gegeben, selbst wenn er bei der Testdurchführung auf Daten und Systeme stößt, für die der Beauftragende nicht verfügungsberechtigt ist. Gleichwohl können beauftragte Tester aber auch mit negativer Intention agieren, etwa durch unverantwortlichen Umgang mit den von Ihnen gefunden Erkenntnissen.

Beim nicht beauftragten White Hat Hacker zeigt sich die Intention dagegen erst im konkreten Umgang mit einer gefundenen Sicherheitslücke. Somit sollte auch die Vorbereitung von Tests gemäß § 202c StGB nicht strafbar sein. Hierbei wäre eine Klarstellung des Gesetzgebers zu begrüßen, was als Überwindung einer Zugangssicherung im Sinne des § 202a StGB gilt. Dies gilt insbesondere vor dem Hintergrund der jüngsten Rechtsprechung des Landgerichts Aachen v. 27.7.23, 60 Qs 16/23.

Der VDA sieht den Anpassungsbedarf auf der Tatbestandsebene. Die positive Intention einer Testung rein als Rechtfertigungsgrund bei gegebener Strafbarkeit zu bewerten ist aus unserer Sicht nicht ausreichend. Kriterien zur objektiven Beurteilung der Intention könnten z.B. sein:

- **Indizien einer positiven Intention, z.B.**
  - verantwortungsvoller Umgang mit identifizierten Sicherheitslücken z.B. im Rahmen einer Coordinated Vulnerability Disclosure,
  - erkennbarer Beitrag zur Bestätigung oder Stärkung der Cybersicherheit des getesteten Systems,
  - erkennbarer Beitrag zum Schutz des Systemherstellers oder
  - erkennbarer Beitrag zum Schutz von Nutzern.

- **Indizien einer nicht-positiven Intention, z.B.**
  - Erlangung insbesondere monetärer (über eine Bug Bounty hinausgehenden) Vorteile für sich oder Dritte,
  - Bloßstellung des Systemherstellers (Shaming) und andere Elemente eines nicht-verantwortungsvollen Umgangs mit gefundenen Erkenntnissen oder
  - Veröffentlichung von Daten, auf die im Rahmen von Tests Zugriff erlangt wurde, außerhalb eines verantwortungsvollen Umgangs mit diesen Daten.

Ansprechpartner

Dr. Marcus Bollig
Geschäftsführer

marcus.bollig@vda.de

Martin Lorenz
Abteilungsleiter Security, Daten & Digitalisierung

martin.lorenz@vda.de

Dr. Julian Weber
Referent Daten, Digitalisierung & Künstliche Intelligenz

julian.weber@vda.de

Der Verband der Automobilindustrie (VDA) vereint rund 620 Hersteller und Zulieferer unter einem Dach. Die Mitglieder entwickeln und produzieren Pkw und Lkw, Software, Anhänger, Aufbauten, Busse, Teile und Zubehör sowie immer neue Mobilitätsangebote.

Wir sind die Interessenvertretung der Automobilindustrie und stehen für eine moderne, zukunftsorientierte multimodale Mobilität auf dem Weg zur Klimaneutralität. Der VDA vertritt die Interessen seiner Mitglieder gegenüber Politik, Medien und gesellschaftlichen Gruppen.

Wir arbeiten für Elektromobilität, klimaneutrale Antriebe, die Umsetzung der Klimaziele, Rohstoffsicherung, Digitalisierung und Vernetzung sowie German Engineering. Wir setzen uns dabei für einen wettbewerbsfähigen Wirschafts- und Innovationsstandort ein. Unsere Industrie sichert Wohlstand in Deutschland: Mehr als 780.000 Menschen sind direkt in der deutschen Automobilindustrie beschäftigt.

Der VDA ist Veranstalter der größten internationalen Mobilitätsplattform IAA MOBILITY und der IAA TRANSPORTATION, der weltweit wichtigsten Plattform für die Zukunft der Nutzfahrzeugindustrie.

Herausgeber	Verband der Automobilindustrie e. V.(VDA) Behrenstraße 35,10117 Berlin www.vda.de
	Deutscher Bundestag Lobbyregister-Nr.: R001243 EU-Transparenz-Register-Nr.: 9557 4664 768-90

Version	v1.0 | August 2024