DIGITAL HUB CYBERSECURITY

The Cyberstartup Know & Do

Rechtssicher zum Markterfolg

Nationale und europäische gesetzliche und regulative Rahmenbedingungen für Cybersecurity-Startups

Dr. Michael Kreutzer, Linda Schreiber und Ute Richter

Hinweis

Die in diesem Beitrag enthaltenen Informationen sind sorgfältig erstellt worden, können eine Rechtsberatung jedoch nicht ersetzen. Eine Haftung oder Garantie dafür, dass die Informationen die Vorgaben der aktuellen Rechtslage erfüllen, wird daher nicht übernommen. Gleiches gilt für die Brauchbarkeit, Vollständigkeit oder Fehlerfreiheit, so dass jede Haftung für Schäden ausgeschlossen wird, die aus der Benutzung dieser Informationen entstehen können. Diese Haftungsbeschränkung gilt nicht in Fällen von Vorsatz.

Inhalt

Einleitung

Nationale sowie europäische gesetzliche und regulative Rahmenbedingungen betreffen grundsätzlich jedes Cybersecurity-Startup, das in Deutschland auf den Markt kommt oder hier seinen Firmensitz hat. Eine Vielzahl an grundlegenden Gesetzen, Verordnungen, Richtlinien sowie sonstigen Regulierungen oder Anforderungen können hier zum Tragen kommen. Angefangen vom Unternehmens- oder Wettbewerbsrecht, Branchen- oder Bereichsgesetzen bis hin zu Gesetzen und Richtlinien zum Thema IT-Sicherheit.

Sich als Cybersecurity-Startup hier einen Überblick zu verschaffen, ist aufwändig. Ganz entscheidend für den Markterfolg von Cybersecurity-Startups ist es, dass ihre Lösungen aktuellen Anforderungen genügen. Mit dieser Publikation geben wir Startups deshalb einen umfassenden Überblick über die grundlegenden Gesetze und Regulierungen, die für Cybersecurity-Startups bzw. ihre Lösungen und Dienstleistungen gelten können[2]. Diese ergänzen wir mit einer gekürzten Übersicht des Regulierungsmappings, das uns bitkom freundlicherweise zur Verfügung gestellt hat.

Zudem erläutert Dr. Michael Kreutzer vom Fraunhofer Institut für Sichere Informationstechnologie SIT im Interview die Implikationen des gesetzlichen und regulativen Frameworks für erfolgreiche Startups.

Da sich der gesetzliche und regulative Rahmen immer wieder ändert, verweisen wir mit Links auf die jeweiligen Regelungen und geben am Schluss auch noch einmal eine Übersicht über Quellen mit denen Startups auf dem Laufenden bleiben. Diese ergänzen wir mit einer Übersicht wichtiger Institutionen und Branchenverbände. Wir planen zudem, diese Publikation immer wieder zu aktualisieren – dazu nehmen wir gerne auch Feedback und Anregungen auf.

Wir wünschen allen eine informative Lektüre!

Das Team vom Digital Hub Cybersecurity

2 In ergänzenden Marktreports werden wir dann auch auf branchenspezifische Anforderungen, Regulierungen und Strukturen eingehen und so Wissen und Know-how für einen erfolgreichen Markteintritt vermitteln.

Ein breites Feld - von der „harten“-Cybersecurity bis hin zu Messengerdiensten

Cybersecurity-Startups oder -lösungen zu definieren, ist nicht so einfach wie es auf den ersten Blick scheint. Manche Lösungen wie Firewalls, Kryptografie oder Privacy zählen ganz eindeutig zu Cybersecurity Lösungen. Andere sind auf dem ersten Blick nicht dem Cybersicherheitsmarkt zugeordnet, sondern anderen Technologiebereichen, beispielsweise Software-, Cloud-, IoT- oder Netzwerktechnologie – dort oftmals als Schlüsselkomponente. Ebenso können sie in eine bestimmte Produktkategorie fallen, wie beispielsweise ein Messengerdienst, der durch den USP einer zentralen Verschlüsselung zu den Cybersicherheitslösungen gezählt werden kann. Wieder andere werden Branchen zugeordnet, wie z. B. Banken, Mobilität oder Logistik.

1. **Cybersicherheit im engeren Sinn**
   Hier es geht es um die Entwicklung von Cybersicherheitslösungen, die im Kern weitgehend unabhängig von bestimmten Technologien oder Anwendungsbereichen sind. Das bedeutet, sie können technologie- und anwendungsübergreifend eingesetzt werden. Beispiele hierfür sind Kryptoverfahren, Kryptobibliotheken, Firewalls, Datenschutzlösungen oder Methoden des Secure Engineerings.

2. **Sichere Technologien**
   Mit sicheren Technologien sind Lösungen gemeint, die spezifisch für bestimmte Informationstechnologien sind. Beispiele sind die Cloud-Technologie, Technologien für Mobilsysteme oder für das Internet der Dinge (IoT). Die Cybersicherheitslösung ist in den Kern der jeweiligen Technologie integriert bzw. ein essentieller Bestandteil der Technologie.

3. **Sichere Branchenlösungen**
   Bei dieser Marktausrichtung geht es um spezifische Absicherungen für bestimmte Anwendungsbereiche aus Branchensicht. Beispiele für die anwendungszentrierte Ausrichtung sind die Finanzbranche, mit ihren für diese Wirtschaftsbranche zugeschnittenen Banking-Anwendungen, die Energiebranche, mit Anwendungen wie Smart Grids oder die Hersteller von Produktionsanlagen mit innovativen Funktionen zur effizienten, flexiblen und dynamisch anpassbaren Produktion, wie sie unter dem Schlagwort Industrie 4.0 diskutiert wird. In der anwendungszentrierten Ausrichtung wird von Informationstechnologien ausgegangen, die sicher aus der spezifischen Sicht der Branchen sind und auch auf Cybersicherheitslösungen im engeren Sinn beruhen.

4. **Produkte mit starkem Cybersecurity-Fokus**
   Cybersicherheit ist entscheidend für die Digitalisierung und kann ein USP für bestimmte Produkte sein. Deshalb werden heute auch Lösungen bzw. Produkte zur Cybersicherheit gezählt, deren USP komplett darauf abzielt. Ein Beispiel dafür sind Messengerdienste, aber auch Cloud-Lösungen, die Sicherheit in den Vordergrund stellen.

Es gibt also weder „das" typische Cybersecurity-Startup noch „die" typische Cybersecurity-Lösung. Cybersicherheit ist ein Querschnittsthema mit unterschiedlichen Marktstrukturen. Je nach Lösung kommen unterschiedliche Anforderungen zum Tragen: beim Messengerdienst gilt es neben den „generellen" Anforderungen an IT-Sicherheit auch noch das Telekommunikationsgesetz zu beachten, bei den Branchenlösungen spezifische Branchengesetzgebung oder –richtlinien.

Cybersecurity-Unternehmen bewegen sich so in einem heterogenen rechtlichen und regulatorischen Rahmen. Ohne dessen Kenntnis ist es schwer, neue Angebote auf den Markt zu bringen. Das ist gerade für junge, in rechtlichen Dingen unerfahrene Gründer – insbesondere aus dem akademischen Umfeld - eine Herausforderung. Denn bei der Behandlung von rein technischen Forschungs- und Entwicklungsfragen werden diese Aspekte oftmals wegabstrahiert beziehungsweise vernachlässigt. Bei der Entwicklung von marktfähigen Angeboten wird jedoch eine Fülle von Gesetzen relevant.

Im Folgenden stellen wir deshalb – ohne Anspruch auf Vollständigkeit – die grundlegenden nationalen und europäischen Gesetze, Verordnungen und Richtlinien vor, die für Cybersecurity-Angebote zum Tragen kommen können. Startups sollten diese bei der Entwicklung ihrer Lösung systematisch überprüfen und sich sachkundig machen, ob weitere – hier nicht dargestellte Gesetze oder Richtlinien – bei ihrer Lösung oder im Hinblick auf ihre Zielmärkte zum Tragen kommen, beispielsweise beim Fokus auf Branchen wie Energie (das Gesetz über die Elektrizitäts- und Gasversorgung (EnWG)) etc. Im Zweifel macht es Sinn hier weitere Beratung in Anspruch zu nehmen oder spezialisierte Fachanwälte hinzuziehen.

Nationale und europäische Gesetzgebung und Regulierung

– eine kurze Begriffsklärung

Bevor wir die Übersicht über die relevanten Gesetze und Richtlinien geben, erläutern wir im Folgenden noch einmal die Begriffe und ihre rechtliche Verbindlichkeit. Das ist nötig, weil diese in der nicht-juristischen Literatur nicht immer ganz trennscharf verwendet werden.

Gesetze oder gesetzliche Regelungen sind sogenannte **Rechtsnormen**. Bestimmten Sachverhalten werden damit Rechtsfolgen zugeordnet und Sanktionen, wenn diese nicht beachtet werden. Eine Rechtsnorm kann entweder ein Verbot oder ein Gebot sein.

Verordnungen sind Rechtsnormen, die von Regierungs- oder Verwaltungsorganen erlassen werden können und in der Normenhierarchie unterhalb von Gesetzen stehen. Verordnungen der Europäischen Union haben nach der Verabschiedung

unmittelbar in allen Mitgliedsstaaten Geltung und müssen nicht erst in nationales Recht umgesetzt werden.

(EU-)Richtlinien sind keine unmittelbar anwendbaren Rechtsnormen. Dazu müssen sie in das nationale Recht der jeweiligen Mitgliedstaaten umgesetzt werden. Allerdings könnten sie bei fehlerhafter oder verspäteter Umsetzung unmittelbar angewendet werden.

Technische Normen werden von den nationalen, europäischen oder internationalen Norm-Ausschüssen einer Norm-Organisation erarbeitet. Die Ausschüsse arbeiten in der Regel ehrenamtlich. Zur Entwicklung der Norm gibt es festgelegte Grundsätze, Verfahren- und Gestaltungsregeln. In den Normausschüssen sitzen idealerweise alle Kreise, die von der Norm betroffen sein werden, und einigen sich im Konsens auf die Norm. Das soll eine hohe Akzeptanz sicherstellen. Bei der Festlegung der Norm berücksichtigen die Ausschussmitglieder u. a. den Stand der Technik sowie die Interessen der Beteiligten.

Technische Standards werden im Gegensatz zur Norm von einem kleineren, für den Standard temporär zusammengesetzten Expertenkreis definiert. Sie sind ein Mittel, um einen innovative Lösung schnell auf den Markt zu bringen. Insofern sind sie manchmal eher als Marketinginstrument einzuordnen. Ein Standard kann die Basis für die Erarbeitung einer Norm sein.

Übersicht der relevanten rechtlichen Rahmenbedingungen

Die von uns dargestellten Gesetze, Regeln oder Normen der IT-Sicherheit haben wir ausgewählt, weil sie für Startups im Hinblick auf die Entwicklung ihrer Lösung von Interesse sind oder weil sie Anforderungen sind, die Unternehmen an Lösungen stellen. Wir gehen nicht ein auf Gesetze, Verordnungen oder Richtlinien, die sich aus dem Unternehmens-, Vertrags- oder Wettbewerbsrecht ergeben. Auch alle branchenspezifischen Regelungen oder Richtlinien können wir im Rahmen der Übersicht nicht abdecken und konzentrieren uns bei den Bereichsgesetzen auf einige wenige. Die von uns dargestellten Regeln oder Gesetze haben wir wie folgt gegliedert:

1. IT-Sicherheit
2. Datenschutz
3. Branchengesetz
4. Strafrecht und Cyberkriminalität
5. Außenwirtschaft
6. Geistige Eigentumsrechte inkl. Geschäftsgeheimnisse
7. Sonstiges
8. Technische Regelwerke

IT-Sicherheit

Vorwegzunehmen ist, dass es nicht das eine, allgemeingültige IT-Sicherheitsgesetz gibt, welches eine allgemeine Verpflichtung aller Unternehmen enthält, für eine angemessene IT-Sicherheit zu sorgen. Stattdessen gibt es eine Reihe bereichsspezifischer Regelungen wie zum Beispiel

im Telekommunikationsgesetz (TKG) oder im Energiewirtschaftsgesetz (EnWG). Darüber hinaus gibt es unmittelbare gesetzliche Vorgaben für Betreiber digitaler Dienste und kritischer Infrastrukturen.

Viele dieser Regelungen stammen aus dem IT-Sicherheitsgesetz, welches im Juli 2015 in Kraft getreten ist. Das IT-Sicherheitsgesetz ist ein Artikelgesetz. Das bedeutet es ist kein einheitliches Gesetz, sondern eine Sammlung an Änderungen und Ergänzungen in anderen, bereichsspezifischen Gesetzen. Dies betrifft beispielsweise Gesetze wie das Telekommunikations- und das Telemediengesetz, das BSIG, das Strafgesetz sowie die Strafprozessordnung.

Das IT-Sicherheitsgesetz zielt darauf ab, die Sicherheit der IT-Systeme und digitalen Infrastrukturen in Deutschland zu erhöhen, insbesondere im Bereich der Kritischen Infrastrukturen (KRITIS) wie etwa Energie, Informationstechnik- und Telekommunikation sowie Wasser und Ernährung. Weitere betroffene Sektoren sind Finanzen, Transport und Verkehr sowie Versicherung. Dort hätte ein Ausfall oder eine Beeinträchtigung der Versorgungsdienstleistungen dramatische Folgen für Wirtschaft, Staat und Gesellschaft in Deutschland.

Andere gesetzliche Maßnahmen sind die Umsetzung der EU-Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie). Die Richtlinie ist im August 2016 in Kraft getreten und soll ein hohes gemeinsames Sicherheitsniveau in allen EU-Staaten gewährleisten.

Zum einen geht es um generelle Rechtsnormen und Richtlinien, die Unternehmen verpflichten, Maßnahmen für die IT-Sicherheit zu ergreifen. Diese Regelugungen müssen Cybersecurity-Startups zwar auch selber erfüllen. Sie stecken aber oftmals auch den Rahmen für die von den Cybersecurity-Startups entwickelten Lösungen ab.

Mehr zum IT-Sicherheitsgesetz:
https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf

Mehr zur NIS-Richtlinie unter
https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016L1148

Mehr zum Umsetzungsgesetz der NIS-Richtlinie unter
https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s1885.pdf

BSI Gesetz (BSIG)

Das dem Bundesinnenministerium unterstellte Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die zentrale Behörde für die IT-Sicherheit. Ihre Aufgaben, Rechte und Pflichten werden im BSI Gesetz (kurz BSIG) definiert. Dazu zählt u. a. auch der Schutz Kritischer Infrastrukturen, beispielsweise über die entsprechenden Verordnungen (BSI-KritisV), erweiterte Aufgaben und Befugnisse im Rahmen der NIS-Richtlinie, die Herausgabe technischer Richtlinien, Mindeststandards für die Infrastruktur des Bundes sowie sonstiger Standards.

Aus dem BSIG ergeben sich zudem direkte Pflichten für Betreiber Kritischer Infrastrukturen. Gemäß § 8a Abs. 1, S.1 des BSIG müssen Betreiber angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Sicherheit vornehmen. Die vier Säulen der IT-Sicherheit sind dabei die Verfügbarkeit, Integrität, Authentizität sowie die Vertraulichkeit.

Zu den Pflichten der Betreiber KRITIS zählen gemäß BSIG weiterhin zweijährlich die Nachweispflicht über IT-Sicherheitsmaßnahmen, die Pflicht zur Einführung eines Risikomanagements sowie eine Meldepflicht bei Störungen.

Kritische Infrastrukturen sind Einrichtungen, Anlagen oder Teile davon, die bestimmten Sektoren angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind (§ 2 Abs. 10 Nr. 1 und 2 BSIG). Dazu zählen die Bereiche Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation, Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr.

Welche Dienstleistungen davon genau erfasst sind und ab welchen Schwellenwerten eine Anlage jeweils als kritisch eingestuft wird, bestimmt sich nach der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV).

Darüber hinaus definiert das BSIG Anforderungen für Anbieter digitaler Dienste, also für Online-Marktplätze, Suchmaschinen und Cloud-Computing-Dienste durch § 8c BSIG.

Betreiber Kritischer Infrastrukturen und digitaler Dienste müssen IT-Sicherheit nach dem „Stand der Technik" umsetzen und deren Einhaltung regelmäßig nachweisen. Sofern Sicherheitsmängel aufgedeckt werden, kann deren Beseitigung angeordnet werden.

Stand der Technik bedeutet, dass „fortschrittliche Verfahren eingesetzt werden, die die praktische Eignung einer Maßnahme zur Erreichung eines allgemein hohen Schutzniveaus als gesichert erscheinen lassen"[2]. Wichtig ist, dass es sich um die besten verfügbaren Techniken handelt – in der Regel hinken diese hinter dem Stand der Forschung hinterher. Der Stand der Technik wird oft in DIN-Normen oder technischen Richtlinien des BSI definiert[3].

Mehr zum BSI unter https://www.bsi.bund.de

Mehr zum BSIG unter
https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html/.

Mehr zur BSI-KritisV unter
https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html/

Ausblick - IT-Sicherheitsgesetz 2.0
Das IT-Sicherheitsgesetz sollte noch 2019 nivelliert werden. Ein entsprechender Referenten-Entwurf ist seit dem Sommer 2019 im Internet verfügbar und kann dort auch kommentiert werden. Zu den wichtigsten Änderungen (Stand: Juni 2019) zählen: die Ausweitung der Befugnisse der Bundesbehörden zum Schutz der Regierungsnetze, die Meldepflichten

2 Vgl. Begründung des IT-Sicherheitsgesetzes
3 S. auch Handreichungen zum „Stand der Technik" technischer und organisatorischer Maßnahmen des TeleTrust, Bundesverbandes IT-Sicherheit e.V.

bei Cybersecurity-Vorfällen sowie die Ausweitung der verpflichtenden Einhaltung von IT-Mindeststandards auf Teile der Wirtschaft, die Einführung eines IT-Sicherheitskennzeichens sowie ein Fokus auf die Bekämpfung der Cyberkriminalität.

Mehr Informationen unter
https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/#2019-03-27_BMI_Referentenentwurf_IT-Sicherheitsgesetz-2

eIDAS
Das alte Signaturgesetz (SigS) wurde 2017 ersetzt durch das Gesetz zur Durchführung der Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Durchführungsgesetz). Ergänzt wird diese durch das Vertrauensdienstegesetz (VDG) sowie die Vertrauensdiensterichtlinie (VDI).

Mehr unter
https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/eIDAS_node.html

Datenschutz

Beinhaltet ein Angebot die Sammlung oder Verarbeitung personenbezogener Daten, werden Datenschutzgesetze relevant. Hier ist beispielsweise die europäische Datenschutzgrundverordnung zu nennen. Datenschutzregelungen haben Auswirkungen auf Gestaltung, Entwurf und Entwicklung von Informationstechnologie.

Datenschutz-Grundverordnung (DSGVO)
Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union. Sie vereinheitlicht die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit.

Zusammen mit der so genannten JI-Richtlinie für den Datenschutz in den Bereichen Polizei und Justiz bildet die DSGVO seit dem 25. Mai 2018 den gemeinsamen Datenschutzrahmen in der Europäischen Union.

Mehr unter https://eur-lex.europa.eu/eli/reg/2016/679/oj sowie in unserer separaten Publikation zum Thema DSGVO (herunterladbar unter https://www.digital-hub-cyberseurity.com)

1. und 2. DSAnpUG-EU
Das Inkrafttreten der DSGVO macht Anpassungen in nationalen Gesetzen notwendig. Diese werden im sogenannten Datenschutz-Anpassungs- und Umsetzungsgesetzes EU (DSAnpUG-EU) geregelt. Das zweite Gesetz hierzu trat Ende November 2019 in Kraft.

Mehr unter http://dipbt.bundestag.de/extrakt/ba/WP19/2390/239070.html

Bundesdatenschutzgesetz (BDSG)
2018 trat die neue Fassung des deutschen Bundesdatenschutzgesetzes (BDSG) in Kraft. Es regelt den Umgang mit personenbezogenen Daten, die digital oder manuell verarbeitet werden. Neben dem BDSG können auch Datenschutzgesetze der Länder und anderen bereichsspezifischen Regelungen zutreffen.

Mehr unter: https://www.gesetze-im-internet.de/bdsg_2018/

Free Flow of Data
Die Free Flow of Data Verordnung der EU regelt und erleichtert die Verarbeitung und Übertragung nicht personenbezogener Daten über nationale Grenzen hinweg in der EU. Sie macht dabei klare Datenlokalisierungsvorgaben.

Mehr unter
https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data

ePrivacy Richtlinie
Die Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy) wurde 2002 erlassen und 2009 durch die sogenannte Cookie-Richtlinie ergänzt. Die Richtlinie wurde in Deutschland durch Regelungen im TKG und TMG umgesetzt.

Mitunter die wichtigste Regelung ergibt sich aus Art. 5 Abs. 3 der Richtlinie. Die Vorschrift verpflichtet Betreiber, den Nutzer klar und umfassend über die Nutzung von Cookies und das Recht die Nutzung zu verweigern zu informieren.

Ein Gesetzesvorhaben der EU zur Reform der Richtlinie durch eine direkt anwendbare Verordnung scheiterte Ende 2019. In diesem Zusammenhang wurden unter anderem verschärfte Vorschriften zur Einwilligung von Nutzern in die Verwendung von Cookies diskutiert. Die EU-Kommission arbeitet derzeit an einem neuen Vorschlag.

Mehr unter
https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32002L0058/

Branchengesetze/Bereichsspezifisches Recht

Mehrere Branchengesetze greifen IT-Sicherheitsaspekte auf – wir haben hier zwei Gesetze dargestellt, die wiederum bereichsspezifisch auch branchenübergreifend Anwendung finden.

Telekommunikationsgesetz (TKG)
Das Telekommunikationsgesetz (TKG) ist historisch entstanden, um die flächendeckende Versorgung von Bürgern mit Telekommunikationsdiensten sicherzustellen, sowie die Nutzung von Telekommunikationsnetzen und Zuteilung von Frequenzen für Anbieter zu regeln. Neben diesen Bereichen dient das TKG heute dem Verbraucherschutz und dem Wettbewerbsschutz im Bereich der Telekommunikation.

Betreiber von öffentlichen Telekommunikationsnetzen und Anbieter von Telekommunikationsdiensten unterliegen einer Reihe besonderer Verpflichtungen. Dazu gehört neben Meldepflichten von sicherheitsrelevanten Vorfällen auch die Benennung eines Sicherheitsbeauftragten und die Erstellung eines Sicherheitskonzepts (§ 109 Abs. 4 TKG). Die Bundesnetzagentur stellt eine Grundlage für ein solches Sicherheitskonzept zur Verfügung.

Mehr unter https://www.gesetze-im-internet.de/tkg_2004/

Telemediengesetz (TMG)
Das Telemediengesetz (TMG) gilt für Anbieter von elektronischen Informations- und Kommunikationsdiensten, wovon beispielsweise alle Arten von Webseiten erfasst sind. Das Gesetz regelt unter anderem die Impressumspflicht (§ 5 TMG), die Webseiten- und App-Anbieter verpflichtet, in leicht erkennbarer und erreichbarer Weise bestimmte Informationen bereitzustellen.

Des Weiteren ergeben sich aus dem Gesetz Haftungsregelungen für die Anbieter von Diensten, zum Beispiel für gesetzeswidrig von Nutzern verbreitete Inhalte, sowie spezielle Datenschutzvorschriften.

Anbieter von Telemedien haben zudem, soweit technisch möglich und wirtschaftlich zumutbar, technische und organisatorische Maßnahmen zu treffen, die ihre technischen Einrichtungen gegen unerlaubten Zugriff sichern.

Mehr unter https://www.gesetze-im-internet.de/tmg/

Strafrecht

Das Strafgesetzbuch (StGB) definiert an mehreren Stellen Straftatbestände im Bereich der IT. Zu den relevantesten gehören der sogenannte Hackerparagraph §202 sowie der Paragraph §303.

Hackerparagraph (StGB §202c)
Der sogenannte Hackerparagraph wurde im Jahr 2007 ins Strafgesetzbuch aufgenommen. Nach diesem macht sich eine Person beispielsweise strafbar, wenn sie Computerprogramme herstellt, die den Zugriff auf Sicherungscodes ermöglichen.

Es war zunächst unklar, ob ethisches Hacking, z. B. um Sicherheitslücken aufzudecken und diese zu schließen, ebenfalls unter den §202c fällt. Zwar wird momentan davon ausgegangen, dass gutartige Tätigkeiten (im Dienste der IT-Sicherheit) bei verfassungskonformer Auslegung sowie ausführlicher Dokumentation nach diesem Paragraphen nicht strafbar sind, dies sollte aber auf alle Fälle noch einmal rechtlich geprüft werden.

Mehr unter https://www.gesetze-im-internet.de/stgb/__202c.html

Sachbeschädigung (StGB §303)
Der §303a des StGB regelt den Straftatbestand der Datenveränderungen (löschen, unterdrücken, unbrauchbar machen oder verändern). Paragraph 303b definiert und regelt den Straftatbestand der Computersabotage.

Mehr unter https://www.gesetze-im-internet.de/stgb/__303a.html ff.

Exkurs Responsible Disclosure
Wer durch Cybersicherheitsforschung oder ethisches Hacking Sicherheitslücken in der Hard- oder Software anderer Unternehmen entdeckt, steht vor dem Problem wann und wie mit dieser Information an das jeweilige Unternehmen und die Öffentlichkeit getreten werden sollte.
Zum einen kann die Öffentlichkeit ein berechtigtes Interesse daran haben, über die Sicherheitsrisiken bei der Verwendung eines Produktes informiert zu werden. Auf der anderen Seite kann die Verbreitung dieser Information

die Gefahr erhöhen, dass diese Sicherheitslücke ausgenutzt wird bevor der Hersteller die Gelegenheit hatte sie zu beheben.
Verschiedene Initiativen und größere Unternehmen haben Policies und Guidelines, die Anleitung geben für einen verantwortungsvollen Umgang mit Sicherheitslücken, sowohl für die Entdecker als auch für das jeweilige Unternehmen.
Anleitung des Niederländischen Nationalen Cyber Security Centres für einen Coordinated Vulnerability Disclosure Prozess: https://www.enisa.europa.eu/news/member-states/WEB_115207_BrochureNCSC_EN_A4.pdf

Richtlinie 2013/40/EU
Diese Richtlinie über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates vereinheitlicht den Umgang mit Angriffen auf Informationssystemen innerhalb der EU.

Mehr unter https://eur-lex.europa.eu/eli/dir/2013/40/oj

E-Evidence
Die EU-Kommission hat einen Vorschlag für eine Verordnung bzw. Richtlinie für den Bereich e-Evidence entwickelt. Hier sollen beispielsweise Datenherausgabe/Datensicherung geregelt werden, Rechte der EU-ausländischen Strafverfolgungsbehörden, Prüfungspflichten durch den Provider etc. Das Inkrafttreten dieses Vorschlags ist aktuell offen.

Mehr unter https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en

Außenwirtschaftsrecht

Manche Sicherheitslösungen könnten unter Bestimmungen des nationalen und europäischen Außenwirtschaftsrechts fallen. Eine gute Einführung über das Außenwirtschaftsrecht samt Hintergrund und Verflechtungen mit den europäischen Bestimmungen bietet das BMWi auf seinen Seiten.

Mehr unter Link: https://www.bmwi.de/Redaktion/DE/Artikel/Aussenwirtschaft/aussenwirtschaftsrecht.html.

Die zuständige Behörde für Ausfuhrgenehmigungen in der Bundesrepublik Deutschland ist das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA). Dieses erteilt auch Auskünfte zur Güterliste und Nullbescheide.

Eine gute Quelle sind ebenfalls die Seiten des Zolls (Mehr unter: https://www.bafa.de/DE/Home/home_node.html).

Außenwirtschaftsgesetz (AWG) und Außenwirtschaftsverordnung (AWV)
Eine Reihe von Cybersicherheitsprodukten unterliegen besonderen Exportbeschränkungen. Sie dürfen beispielsweise nicht oder nur mit einer ausdrücklichen Genehmigung des Bundesamtes für Wirtschaft und Ausfuhrkontrolle exportiert werden. Die Beschränkung kann genereller Natur sein oder nur für bestimmte Länder gelten. Bei Verstößen drohen Unternehmen bzw. den verantwortlichen Personen Strafen. Wichtig: Dieses Verbot kann nicht nur eine Lösung, sondern

bereits eine Publikation, einen Vortrag oder das Mitführen von bestimmten Daten, beispielsweise aus Notebooks oder USB-Sticks, betreffen.

Inwiefern ein Produkt, eine Lösung oder eine Publikation unter diese Einschränkungen fällt, kann anhand der Güterliste geprüft werden – sie ist eine Anlage der Außenwirtschaftsverordnung (AWV). In diesen Güterlisten werden genehmigungspflichtige Güter definiert. Für IT-Produkte werden diese in Kategorie 5, Teil 2 definiert. Für die konkrete Exportkontrolle ist dann das Bundesamt für Wirtschaft und Ausfuhrkontrolle zuständig.

Mehr unter http://www.gesetze-im-internet.de/awg_2013/ sowie http://www.gesetze-im-internet.de/awv_2013/

EG-Dual-Use-Verordnung – (EG Nr. 428/2009)
Neben den bereits dargestellten AWG und AWV greift bei Exporten auch die EG-Dual-Use-Verordnung. Die EG-Dual-Use-VO legt für alle EU-Mitgliedstaaten gemeinsame Genehmigungspflichten und Verfahrensweisen bei der Ausfuhr von Gütern mit doppeltem Verwendungszweck fest. Mit doppeltem Verwendungszweck ist gemeint, dass die Güter sowohl zivil als auch militärisch nutzbar sind (z. B. bestimmte Chemikalien, Maschinen, Technologien und Werkstoffe, aber insbesondere auch Software oder Technologien).

Link: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:de:PDF

Good Practice Beispiel Exportkontrolle
Wenn es einen Bezug zum Ausland gibt (Verkauf, Vortrag, Präsentation etc.), sollten Startups prüfen, ob sie unter das AWG fallen und eine Genehmigung für den Export benötigen. Export bezieht sich dabei auf Software, Güter, Know-how etc.

Die Genehmigungspflicht ergibt sich aus der deutschen Ausfuhrliste Teil a und b sowie auf der EU-Ebene auf der EG-Dual-Use-Verordnung. Dort deckt die Kategorie 5 Teil 2 speziell den Bereich Informationssicherheit ab. In dieser Kategorie werden verschiedene Güter mit verschiedenen Nummern aufgelistet, die dann geprüft werden.

Ein Beispiel: Software, die Kryptografie beinhaltet. Krypto ist als ein Nummerpunkt in der Kategorie 5 Teil 2 aufgeführt. Ein Startup sollte nun prüfen, ob ein neues Kryptoverfahren Bestandteil des Gutes ist. Wenn das zutrifft, muss eine Checkliste mit weiteren Fragen (Produktinformationen etc.) abgearbeitet werden. Diese dient dem Bundesamt für Ausfuhrkontrolle

als Grundlage zur Prüfung, ob der Export genehmigungspflichtig ist und ein entsprechender Antrag gestellt werden muss.

Prüfung der Genehmigungspflicht – Antragsstellung bei der BAFA
Ein vereinfachtes Verfahren beim BAFA (ELAN K2 Ausfuhr) für die Freigabe von Gütern kann sowohl für Publikationen, Wissen, Know-how, etc. und auch für das Produkt selbst angewendet werden.

Wer ganz sicher sein will, sollte eine Risikoeinschätzung von einem auf dieses Gebiet spezialisierten Juristen vornehmen lassen. Gleichermaßen sollten Startups aber immer nachweisen können, dass sie für diesen Bereich ein funktionierendes Risikomanagement haben – zum Beispiel über eine Checkliste, Organisationsanweisung oder Organisationsverfahren. Startups sollten ein Verfahren haben, wie sie die Produkte und Lösungen absichern. Startups, die sich mit dem Thema intensiver beschäftigen, können sich umfassender auf den Tagungen der BAFA informieren.

Sektorspezifische Investitionsprüfungen
Neben den o.g. Ausfuhrbeschränkungen sollten Startups, die ausländische Investoren an Board nehmen oder das Unternehmen an diese verkaufen wollen, aber auch daran denken, dass sie möglicherweise sogenannten sektorspezifischen Investitionsprüfungen unterliegen. Das trifft beispielsweise für IT-Sicherheitsunternehmen zu, deren Lösungen für staatliche Verschlusssachen eingesetzt werden. Ziel dieser sektorspezifischen Investitionsprüfungen ist es, Sicherheitsgefährdungen zu vermeiden. Der Rahmen dafür wird im AWG bzw. in der AWV beschrieben (sogenannte sektorspezifische Investitionsprüfung, §§ 4 Abs. 1 Nr. 1, 5 Abs. 3 AWG, §§ 60 bis 62 AWV).

Link: https://www.bmwi.de/Redaktion/DE/Artikel/Aussenwirtschaft/investitionspruefung.html

Geistige Eigentumsrechte

Bei dem Vertrieb von IT-Diensten und Lösungen sind eine Reihe von Gesetzen aus dem Bereich des Geistigen Eigentumsrechts zu beachten. Dieses betrifft nicht nur Lösungen der Cybersicherheit.

Urheberrecht
Software ist urheberrechtlich geschützt. Dadurch hat der Urheber bzw. das jeweilige Unternehmen bei dem dieser angestellt ist eine Reihe exklusiver Rechte an dem Werk. Sowohl beim Vertrieb von Software als auch bei der Verwendung von lizensierten Programmen ist es daher wichtig, die genauen Nutzungsrechte vertraglich zu vereinbaren. Dabei zu berücksichtigende Aspekte sind etwa die örtliche Begrenzung der Nutzung, die sachliche Einschränkung von Nutzungsformen und die zeitliche Begrenzung der Lizensierung.

Viele Schwachstellen in IT-Produkten basieren auf Fehlern, die beim Entwurf und bei der Programmierung von Software entstanden sind. Möchten Cybersicherheitsexperten jedoch die Lücke in der Software schließen, kann es sein, dass ihnen hierzu die notwendigen Bearbeitungsrechte am Programm fehlen. Deshalb

braucht es hierfür entsprechendes rechtliches Hintergrundwissen, unter welchen Bedingungen dies möglich ist.

Mehr unter https://www.gesetze-im-internet.de/urhg/

Lizenzbestimmungen Open Source

Software wird oftmals mit bestimmten Open-Source-Lizenzbestimmungen zur Verwendung oder Weiterentwicklung zur Verfügung gestellt. Auch wenn diese Form der Software kostenlos und frei im Internet verfügbar ist, bedeutet es nicht, dass sie „frei" ist wie in „free beer"[4].

Bei der Verwendung und Bearbeitung von Open-Source-Komponenten müssen die Bedingungen der jeweiligen Open-Source-Lizenz beachtet werden. In vielen Fällen ist dies das Anbringen eines Hinweises auf die entsprechende Lizenz, die Aufnahme von Copyright-Hinweisen oder das Zurverfügungstellen der jeweiligen Komponente im Source Code. Bei stärkeren Lizenzen kann es unter Umständen erforderlich sein, dass das eigene Programm, das Open-Source-Komponenten verwendet, auch im Source Code zur Verfügung gestellt werden muss.

Besondere Herausforderungen entstehen häufig dann, wenn Open-Source-Software in eigener Software, die nicht als Open-Source-Software entwickelt wurde, integriert werden soll. Damit keine Rechtsprobleme entstehen, ist es notwendig, die Möglichkeiten und Beschränkungen der Lizenzmodelle entsprechend gut zu kennen.

Es empfiehlt sich eine genaue Dokumentation der in einem Programm verwendeten Open-Source-Komponenten in ihrer jeweiligen Version. Viele größere Unternehmen bestehen mittlerweile beim Einkauf auf die Lieferung einer vollständigen Liste verwendeter Komponenten, was ein Knock-Out-Kriterium im Vertrieb sein kann.

Auch aus IT-Sicherheitssicht ist eine genaue Dokumentation der verwendeten Komponenten wichtig. Vulnerabilities in Open-Source-Komponenten sind über CVE IDs identifizierbar und entsprechende Patches können hierüber implementiert werden.

Mehr beispielsweise unter https://www.urheberrecht.de/open-source/

Marken und Patente

Schutzrechte wie Patente oder Marken sichern Innovationen bzw. das Agieren von Unternehmen im Wettbewerb ab. Neben den Möglichkeiten für Unternehmen, das eigene Handeln am Markt abzusichern, können Schutzrechte jedoch auch von anderen eingesetzt werden und das eigene Handeln am Markt verhindern und Wettbewerber in eine bessere Position am Markt bringen.

Wer ein Unternehmen startet, sollte sich früh Gedanken über den Schutz von Produkt- und Firmennamen machen. Wörter, Bilder, Wort/Bild-Kombinationen aber auch Farben und dreidimensionale Gestaltungen können als Marken geschützt werden. Bevor man anfängt ein Produkt oder Unternehmen im geschäftlichen Verkehr zu bewerben, sollte man auf der Datenbank des Deutschen Patent und Markenamts recherchieren, ob eben diese Marke bereits von jemand anderem eingetragen ist. Nutzt man eine Bezeichnung für die gleichen Waren und

4 https://www.gnu.org/philosophy/free-sw.en.htmlRichard Stallmann Zitat einfügen?

Dienstleistungen riskiert man eine Unterlassungsklage und kann schon im frühen Stadium des Unternehmens zu einer Namensänderung gezwungen sein.

Ist die Marke noch frei, sollte man sich das Schutzrecht möglichst schnell durch Registrierung schützen lassen. Je nach geplantem Vertriebsbereich kann bei der Anmeldung direkt der Schutz auf die EU und andere Länder ausgeweitet werden.

Patente schützen Erfindungen auf allen Gebieten der Technik und müssen ebenfalls beim Patentamt angemeldet werden. Wer ein Patent anmelden möchte muss darauf achten, dass die Erfindung bei Anmeldung neu ist – anders als bei der Marke. Neu bedeutet, dass die Erfindung noch nicht öffentlich zugänglich war, also beispielsweise auf einer Messe präsentiert wurde. Die Formulierung eines Patentanspruchs und die Patentanmeldung selbst sind komplex, weshalb sich die Hinzuziehung eines spezialisierten Anwalts empfiehlt.

Datenbanken zur Recherche von Marken und Patenten beim Deutschen Patent und Markenamt: https://www.dpma.de/

Mehr zum Markengesetz unter https://www.gesetze-im-internet.de/markeng/
Mehr zum Patentgesetz unter https://www.gesetze-im-internet.de/patg/

Geschäftsgeheimnisse
Bei Geschäftsgeheimnissen handelt es sich ebenfalls um gewerbliche Schutzrechte, die seit 2019 durch ein eigenständiges Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) geschützt werden. Gegenstand des Schutzes können alle Arten von technischen und kaufmännischen Informationen sein, die im Zusammenhang mit einem Unternehmen stehen. Das Gesetz schützt so beispielsweise vor Reverse Engineering und Betriebsspionage.

Um als Geschäftsgeheimnis geschützt zu werden, bedarf es keiner Neuheit oder Anmeldung. Voraussetzung für den Schutz ist, dass die Information nicht offenkundig ist und daher von wirtschaftlichem Wert ist, dass sie Gegenstand angemessener Geheimhaltungsmaßnahmen ist und ein berechtigtes Interesse an der Geheimhaltung besteht. An die Voraussetzung der Geheimhaltungsmaßnahmen ist kein zu hoher Anspruch zu stellen, einfache betriebsorganisatorische Maßnahmen wie Vertraulichkeitsvermerke und –vereinbarungen oder das Need-to-know-Prinzip können bereits ausreichen.

Mehr unter http://www.gesetze-im-internet.de/geschgehg/BJNR046610019.html

Sonstiges

Haftung, insbesondere IT-bezogene Haftung für Sicherheitsprodukte:
Die Haftung bei IT-Sicherheitsprodukten ist ein Thema des aktuellen Diskurses. Wenn Produkte Sicherheit versprechen und nicht das zugesagte Sicherheitsniveau bieten, sodass der Anwender zu Schaden kommt, so stellt sich die Frage der Haftung.

Technische Regelwerke: Zertifizierung & Normen

Bei der Überprüfung der rechtskonformen Umsetzung von IT-Sicherheitspflichten werden technische Regelwerke genutzt. Die relevantesten stellen wir nachfolgende kurz vor.

BSI Grundschutzkatalog

Der BSI Grundschutzkatalog ist ein vom BSI seit 1994 veröffentlichter Standard, der detailliert Standard-Sicherheitsmaßnahmen beschreibt, die mit normalem Schutzbedarf kompatibel sind. Er gibt sehr differenzierte Empfehlungen zu Methoden, Prozessen und Verfahren. Die aktuelle 2017 veröffentliche Version besteht aus drei Standards, die einzeln oder zusammen genutzt werden können.

- BSI-Standard 200-1- Anforderungen an ein Informations-Managementsystem; kompatibel mit ISO 27001-Standard
- BSI Standard 200-2 – drei Vorgehensweisen zur Umsetzung eines Informationssicherheits-Managementsystems (Basis, Standard, Kern)
- BSI Standard 200-3 - Risikoanalyse

Mehr unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Standards/ITGrundschutzStandards_node.html

ISO/IEC 27001 und die 2700x-Familie

ISO oder IEC[5] Normen sind internationale Regelwerke. Die ISO/IEC 27001 Norm ist eine Möglichkeit, das Management der Informationssicherheit an eine international anerkannte ISO-Norm auszurichten. Das BSI erkennt diese im Rahmen des IT-Grundschutzes an. Die Norm beschreibt grundlegende Anforderungen an ein IT-Sicherheits-Managementsystem. Eine Zertifizierung nach dieser Norm wird auch von größeren Unternehmen oftmals explizit als Voraussetzung an potenzielle Geschäftspartner genannt, um eine Geschäftsbeziehung einzugehen.

In manchen Bereichen ist die Zertifizierung nach ISO 27001 verpflichtend, beispielsweise Strom- und Gasnetzbetreiber, oder wird ausdrücklich referenziert. Das BSI erkennt die ISO/IEC als rechtskonform an und ermöglicht die Zertifizierung auf der Basis der BSI-Grundschutz-Vorgehensweise. Die ISO/IEC-Zertifizierung erfolgt durch einen externen Prüfer.

Neben der ISO 27001 wird oft auch die ISO 27002 referenziert. Die ISO 2700x-Familie fasst diverse Standards zur Information Technology – Security Techniques zusammen und soll künftig weiter ausgebaut werden.

Mehr unter https://www.iso.org/isoiec-27001-information-security.html

IT Infrastructure Library (ITIL)

ITIL ist ein Rahmen bzw. eine Sammlung von Best Practices. Sie beschreibt die typischen Prozesse, Funktionen und Rollen in der IT-Infrastruktur von Unternehmen und wurde ursprünglich für die britische Regierung entwickelt. Aktuell ist die Version ITIL 4, die 2019 veröffentlicht wurde und einige neue Elemente enthält. ITIL ist kein frei verfügbarer Standard, sondern wird kommerziell von AXELOS herausgegeben.

Mehr Informationen unter https://www.tsoshop.co.uk/Business-and-Management/AXELOS-Global-Best-Practice/ITIL-4/?DI=650015

5 ISO Normen werden von der International Organization for Standards veröffentlicht – IEC Normen von der International Electrotechnical Commission veröffentlicht.

Common Criteria (CC) und Information Technology Security Evaluation Criteria (ITSEC)

Um zu verhindern, dass Unternehmen Produkte oder Lösungen in internationalen (nicht-europäischen) Märkten neu zertifizieren werden müssen, gibt es internationale und von den entsprechenden Staaten unterzeichnete Abkommen. Um die Mehrfach-Zertifizierung des gleichen Produktes in verschiedenen Staaten zu vermeiden, müssen die IT-Sicherheitszertifikate auf ITSEC oder CC beruhen.

WICHTIG: Es gibt Einschränkungen bei der Anerkennung von Zertifikaten, wenn diese nationalen, internationalen oder EU-Gesetzen und -Verordnungen entgegenstehen. Dies gilt insbesondere in Anwendungsbereichen der nationalen Sicherheit. So ist die Anerkennung nach CC oder ITSEC eingeschränkt in Bezug auf:

- Auswahl kryptographischer Algorithmen und Funktionen und
- Prüfergebnisse zur Implementierung und zur Stärke von kryptographischen Algorithmen und Funktionen

Hier haben nationale Regelungen und Vorschriften Vorrang.

Mehr dazu hier https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/InternatAnerkennung/interanerkennung.html

sowie auf den Seiten von CC (https://www.commoncriteriaportal.org) sowie ITSEC

EU Cybersecurity Act (CSA)

Am 27. Juni 2019 ist mit dem EU Cyberact ein EU-weiter Rahmen zur Zertifizierung von IT-Sicherheit geschaffen worden. Es handelt sich um ein ständiges Mandat für die europäische Cybersicherheitsbehörde ENISA (European Union Agency for Cybersecurity). Hersteller können so ihre IT-Produkte, Dienstleistungen und Prozesse freiwillig zertifizieren lassen, um deren IT-Sicherheit transparent zu machen.

Mehr unter: https://www.enisa.europa.eu/news/enisa-news/the-european-union-agency-for-cybersecurity-a-new-chapter-for-enisa

Sonstiges

Neben den oben dargestellten allgemeinen Richtlinien erwarten Unternehmen in bestimmten vertikalen Branchen wie der Automobilindustrie in den letzten Jahren zudem oft, dass Zulieferer oder IT-, Software- oder Security-Anbieter zusätzlich branchenspezifische Compliance-Anforderungen erfüllen. Wer also vorhat, seine Lösung in bestimmten Branchen zu verkaufen, sollte sich hier frühzeitig informieren.

Große Unternehmen setzen zudem voraus, dass Anbieter compliant sind mit Vorgaben wie Sarbannes-Oxley, die sich beispielsweise aus dem Börsenrecht ergeben. Wer als Cybersecurity-Startup plant, mit diesen Unternehmen ins Geschäft zu kommen, sollte dies unbedingt recherchieren und berücksichtigen.

Kurzübersicht Regulierungsmapping IT-Sicherheit

Der Arbeitskreis IT-Sicherheitspolitik des Branchenverbands Informationswirtschaft, Telekommunikation und neue Medien e.v. (bitkom e.V.) hat im August 2019 erstmals ein Regulierungsmapping IT-Sicherheit veröffentlicht. Darin werden gesetzliche Anforderungen auf nationaler und europäischer Ebene dargestellt u.a. auch einige, die wir in unserer Übersicht nicht aufgenommen haben. Die folgende Tabelle ist eine gekürzte Version, die wir mit Genehmigung der bitkom veröffentlichen – die vollständige Version findet sich hier https://www.bitkom.org/Bitkom/Publikationen/Regulierungsmapping-IT-Sicherheit.

Bitkom Regulierungsmapping - gekürzt

Regulierung	VO oder RL	National oder EU	Inkrafttreten	Adressaten	Verpflichtend/ freiwillig (V oder F)
Telekommunikationsgesetz (TKG)	z. T. Umsetzung europäischer Vorgaben	National	22.06.2004, zahlreiche Novellen seitdem	Betreiber von öffentlichen Telekommunikationsnetzen und die Anbieter von öffentlich zugänglichen Telekommunikationsdiensten	V
Telemediengesetz (TMG)	z. T. Umsetzung europäischer Vorgaben, z. B. ePrivacy RL	National	26.02.2007, zahlreiche Novellen seitdem	Anbieter von Telemedien nach § 1 TMG	V
NIS RL	Richtlinie	EU	29.6.2016	MS	V
IT Sicherheitsgesetz (Artikelgesetz, Auswirkung auf: TKG, TMG, StGB, StPO, BSI-Gesetz)		Deutsche Umsetzung der NIS RL	30.06.2017, seit 10.05.2018 für Anbieter digitaler Dienste	Betreiber folgender wesentlicher Dienste: Finanzen und Versicherungen, Gesundheit, Transport und Verkehr, Energie, IT und Telekom munikation, Wasser, Lebensmittel	V
IT Sicherheitsgesetz 2.0		National (D)			V (KRITIS Erweiterung) und F (Zertifizierung & Gütesiegel)
EU Cybersecurity Act	VO	EU	27.6.2019	MS / Unternehmen die auf dem Europäischen Markt verkaufen möchten	F
E-Evidence	VO und RL	EU	derzeit offen, EP-Befassung und Trilog stehen noch bevor	MS	V
Datenschutzgrundverordnung (DSGVO)	VO (+ parallel Richtlinie für Polizei und Justiz)	EU	43245	MS	V
1. und 2. DSAnpUG	Nationale Umsetzung DSGVO	National	1.DSAnpUG: 25.05.2018	»Verantwortliche« im Sinne des DS-Rechts	V
	RL	EU	16.7.2019	MS	V
Free Flow of Data	VO	EU	Verbindliche Anwendung EU weit seit 28.05.2019	MS	V
eIDAS Verordnung	VO	EU	1.7.2016	MS	V
Vertrauensdienstegesetz (VDG)	Nationales Gesetz	National	29.7.2017	Vertrauensdiensteanbieter in Deutschland	V
Vertrauensdiensteverordnung (VDV)	Nationales Gesetz	National	28.2.2019	Vertrauensdiensteanbieter in Deutschland	V

Große Bedeutung der IT-Regulatorik für Technologie von Cyber-Startups

Dr. Michael Kreutzer ist am Fraunhofer-Institut für Sichere Informationstechnologie SIT zuständig für Internationalisierung und strategische Industriebeziehungen. Zudem berät er Cyber-Startups in technischer Marktexpertise im Rahmen des Darmstädter Gründungsinkubators StartUpSecure, der vom Bundesministerium für Bildung und Forschung gefördert wird. Seine aktuellen Forschungsschwerpunkte spiegeln Kernthemen der modernen IT-Sicherheitsforschung wider: Sie liegen in der Aufdeckung und Bekämpfung von Desinformation, in Technologien der Dezentralität wie Blockchain, in der Kryptoagilität, in der Netzwerksicherheit, im Quantencomputing, im Quantenschlüsselaustausch sowie in der Post-Quantum Kryptographie.

„Datenschutz ist zentral für IT-Sicherheits-Startups“

F: Herr Kreutzer, wir stellen in dieser Publikation eine Vielzahl an regulativen und gesetzlichen Anforderungen vor. Gibt es gesetzliche Anforderungen, die von Startups immer beachtet werden sollten?

A: Es gibt Regularien wie die DSGVO oder die NIS-Richtlinie, die über den gesamten EU-Wirtschaftsraum hinweg gelten. Die DSGVO zu kennen, ist unabdingbar. Bezüglich der NIS-Richtlinie sollten Startups zumindest wissen, ob sie einschlägige Regularien bereits bei der Gründung berücksichtigen müssen oder ihre Umsetzung bei starkem Wachstum vorausdenken müssen. In Deutschland müssen Star-tups, die in Richtung Reverse Engineering oder Pentesting gehen, die einschlägigen Gesetze des Strafgesetzbuchs und des Urheberrechts kennen.

F: Sie sehen viele Konzepte und Entwürfe für Startups. Was sind aus Ihrer Sicht – in Bezug auf die Berücksichtigung der gesetzlichen und regulativen Anforderungen – die typischen Fehler, die potenzielle Gründer machen?

A: Ein typischer Fehler ist die Nichtbeachtung des Datenschutzes. Vielen Gründenden ist nicht bewusst, dass sie sich einem sehr regulierten Rahmen bewegen, wenn sie personenbeziehbare Daten erheben und erfassen. Sie kennen die gesetzlichen Auflagen oftmals nicht oder sie wissen nicht, wie sie diese umsetzen müssen.

F: Haben Sie hier ein Beispiel?

A: Ja, der Arbeitnehmerdatenschutz. In Deutschland muss vielfach die Arbeitnehmervertretung eingeschaltet werden und ihre Zustimmung geben, wenn Lösungen beispielsweise Arbeitszeiten erfassen oder eine Leistungskontrolle ermöglichen könnten. Das ist vielen Gründerteams gar nicht bewusst.

F: Die Arbeitnehmervertretung mit den von Ihnen geschilderten Rechten ist allerdings ein sehr deutsches Thema: Ist das ein Beispiel dafür, dass es in Deutschland schwieriger ist, IT-Sicherheit zu verkaufen?

A: Es ist in Deutschland nicht schwieriger: In anderen Ländern gibt es ebenfalls Auflagen. Jedes Land hat eine eigene Kultur und Geschichte und damit einhergehend einen etwas anderen Blick auf den Datenschutz. Im US-amerikanischen Verständnis kann – vereinfacht gesagt – im Betrieb grundsätzlich mehr über Mitarbeitende erfasst werden als in Europa. Gleichwohl gibt es dort eigene Privacy-Gesetze für einzelne Branchen wie beispielsweise für den Finanzsektor und das Gesundheitswesen und die Strafen bei Übertretung können durchaus höher sein als bei der DSGVO. Die jeweils einschlägigen Regularien des Datenschutzes sollten Gründende kennen, wenn sie beispielsweise internationale Märkte adressieren wollen.

„Anforderungen antizipieren und modular umsetzen“

F: Künftige Märkte und Anforderungen zu antizipieren ist für Gründende im IT-Sicherheitsmarkt nicht einfach. Was sind Ihre Tipps für eine gute Umsetzung?

A: Gründende müssen heutige und künftige Bedarfe und mögliche technische Anforderungen von Anfang an adressieren und Datenschutz und IT-Sicherheit von Beginn an und über den gesamten Lebenszyklus vorausdenken. Außerdem sollten sie ihre Lösungen modular entwickeln, sodass Funktionen, die spezifische Regularien erfüllen, zuschaltbar, abschaltbar und einfach konfigurierbar sind. Wichtig ist auch, dass Features klar getrennt und nicht vermischt werden. Ich empfehle ein Design zu realisieren, das darauf ausgelegt ist, Compliance mit unterschiedlichen Anforderungen zu ermöglichen.

F: Und wie setzt man diese Modularität um?

A: Da gibt es technisch viele Möglichkeiten. Eine Beispielumsetzung besteht darin, Regeln in einer eigenen Engine oder einem Repository zu realisieren – dies ist für viele IT-Produkte und -Dienste möglich.

F: Gibt es ein konkretes Beispiel für ein Unternehmen, das diesen modularen Ansatz erfolgreich umsetzt?

A: SAP ist ein Beispiel dafür. Deren Produkte und Lösungen können weltweit an Regularien von verschiedenen Ländern angepasst werden. Allerdings geht mit der hohen Konfigurierbarkeit oft auch ein hoher Erklärungsbedarf eines Produktes einher.

F: Ein Startup hat allerdings nicht SAPs Ressourcen und kann möglicherweise auch nicht alle Märkte antizipieren. Manche Marktexpansion ist ja nicht oder nicht zu diesem Zeitpunkt geplant.

A: Ja, das stimmt, gleichzeitig gilt: Das Cybersicherheits-Startup kann sein Produkt von Anfang an im Design so modular wie möglich aufbauen und dann flexibel weiterentwickeln und anpassen. So bleibt es zukunftssicher, selbst wenn es am Anfang eine Entwicklung nicht vorhergesehen hat. Später kann es dann gezielt beispielsweise Verschlüsselungs-, Pseudonymisierungs- oder Anonymisierungskomponenten einbauen oder Daten anders aggregieren. Durch eine hinreichend modulare und objektorientierte Programmierung können Anforderungen problemlos neu implementiert werden. Schwierig ist es, wenn die Dinge vermischt und hard coded sind.

„Infrastruktur und Internet sind Märkte, in die Startups nur schwer reinkommen“

F: IT-Sicherheit erfordert oft Infrastrukturlösungen. Welche Auswirkungen hat das auf Startups?

A: Es ist für Startups sehr schwer, Infrastrukturlösungen anzubieten, denn dafür braucht man eine gewisse Marktmacht. Wenn man eine durchgehende Verschlüsselungslösung ohne einen ausreichend großen Nutzerkreis anbietet, wird das schwierig in der Umsetzung. Dasselbe gilt für Produkte, die auf das Dezentralitätsparadigma setzen und für ihr Geschäftsmodell viele Marktakteure brauchen, wie permissionless, public Blockchains. Die dafür notwendige Marktmacht haben zurzeit nur wenige, große Konzerne. Für Cybersicherheits-Startups gilt: Egal wie cool die Infrastrukturlösung ist – sie wird sich sehr wahrscheinlich am Markt nicht durchsetzen.

F: Wie steht es mit Lösungen für das Internet?

A: Für das Internet als Infrastruktur gäbe es theoretisch einen riesigen Markt für Cybersecurity. Leider hat Sicherheit beim Entwurf des Internets nur eine untergeordnete Rolle gespielt: Es gibt dort viele unsichere Mechanismen und Protokolle. Vielfach sind Umsetzungen fehlerhaft programmiert oder konfiguriert, oder es handelt sich um Dienste, die veraltete, unsichere Protokolle einsetzen oder unterstützen. Allerdings bieten die wirtschaftlichen Zusammenhänge kaum Anreize für Sicherheit. Der First Mover hat in der Regel nur Nachteile. Es kann sein, dass das Produkt zwar sicher aber inkompatibel ist. Oft ist es auch so, dass diejenigen, die Sicherheitsmechanismen implementieren, das für ihre Kunden tun, aber selbst nichts davon haben. Das sind vertrackte Abhängigkeiten und Verantwortlichkeiten, die letztlich die Umsetzung von IT-Sicherheit im Internet stark behindern.

F: Müsste man als Startup in solchen Märkten eine Second Mover Strategie fahren?

A: Auch hier dürfen die Hindernisse nicht unterschätzt werden. Letztlich kann man hier nicht allein agieren, Unternehmen mit diesem Interesse könnten sich vernetzen und mittels Verbänden und Standardisierung Einfluss nehmen sowie Regierungen als Mitstreiter für das Projekt gewinnen. Das Internet ist global und es gibt kaum Anzeichen, dass die EU da im Alleingang substanziell neue Wege gehen wird. Das ist ein Dilemma, denn es gibt gerade in diesem Bereich wirklich sehr gute Lösungen, die die Welt sicherer machen würden, beispielsweise von Frau Dr. Haya Shulman vom Fraunhofer SIT. Aber Stand heute werden sie so bald nicht zum Einsatz kommen.

„KRITIS stellt Startups vor Herausforderungen“

F: Gibt es weitere Märkte, die durch die Regulierungen besonders schwierig für Startups sind?

A: Ja, zum Beispiel die kritischen Infrastrukturen (KRITIS). Ein Markteintritt ist hier für ein Startup sehr schwierig, weil es – unabhängig von den Auflagen, die ja für alle gleichermaßen gelten - vielfach Anforderungen an seinen langjährigen Bestand und sein garantiertes, langjähriges Überleben etc. nicht erfüllen kann.

F: Das IT-Sicherheitsgesetz spricht von der Berücksichtigung des Standes der Technik, der wiederum oft in Spezifikationen der Zertifizierungen etc. beschrieben wird. Das bedeutet doch, dass Startups kontinuierlich Ressourcen in Forschung und Entwicklung stecken müssen.

A: Ja, das stimmt. Es gibt da aber keinen Unterschied zwischen Cybersicherheits-Startups und etablierten Unternehmen. Startups haben zumindest am Anfang oft einen Vorteil durch ihre innovative Lösung, die sich oft direkt aus einem Forschungsvorhaben heraus entwickelt hat. Für den Stand der Technik wiederum gibt es meist branchenspezifisch schon Regularien. Das macht die Umsetzung relativ einfach.

F: Der Stand der Technik wird ja insbesondere bei den Kritischen Infrastrukturen gefordert. Im IT-Sicherheitsgesetz 2.0 sollen diese auf weitere Branchen, zum Beispiel Banken ausgeweitet werden. Was müssen Startups dabei beachten?

A: Der Finanzmarkt ist ohnehin schon eine sehr regulierte Branche. Gründer in diesem Bereich kommen häufig aus der Branche oder sie kennen sich zumindest damit aus. Das ist auch notwendig, da sie sonst sehr schnell Gefahr laufen, Lösungen zu entwickeln, die nicht compliant sind. Ein Beispiel: Authentifizierungslösungen können unter bestimmten Umständen dem Geldwäschegesetz unterliegen. Das muss man direkt von Anfang an berücksichtigen.

„Good Practice ist Marktverständnis und Austausch mit Experten“

F: Welche Good Practice Maßnahmen sollte ein Cybersecurity-Startup im Blick haben, um sicherzustellen, die regulativen Anforderungen richtig umzusetzen?

A: Good Practice beinhaltet, wirtschaftliche Zusammenhänge, Märkte und Regularien im Blick zu haben. Dazu gehört es, die spezifischen rechtlichen Rahmenbedingungen und die Compliance Regeln sehr gut zu kennen.

F: Was bedeutet Good Practice für die technische Umsetzung einer Cybersicherheitsinnovation?

A: Good Practice bedeutet auch hier, sich umfangreich zu informieren und sich mit Expertinnen und Experten auszutauschen. Viele Gründerteams im Bereich Cybersicherheit sind von ihrer Lösung so überzeugt, dass sie nicht nach rechts oder links schauen. So merken sie nicht, dass die Lösung schon existiert, beispielsweise als Add-on eines Produktes. Oft beachten die Teams auch nicht, dass es für ihre Lösung bereits eine technische Richtlinie gibt. Solche Richtlinien können alles enorm vereinfachen und unterstützen, zugleich geben sie auch den Rahmen für die Lösung vor. Das ist vielen Startups einfach nicht bewusst. Werden von extern vorgegebene Rahmen ignoriert, laufen die Gründungsteams Gefahr, dass sie ihre Entwicklung später in die Tonne kicken müssen.

F: Aber eine Marktrecherche durchzuführen, bevor eine Idee vorangetrieben wird, ist doch Good Practice, oder?

A: Das ist Good Practice und im Prinzip machen das die meisten, viele haben hierbei aber eine ungeschickte Vorgehensweise. Das hängt damit zusammen, dass Cybersecurity wirklich sehr komplex und breit ist. Selbst langjährig in der Branche Tätige kennen jeweils nur ihren Ausschnitt wirklich gut. Ich empfehle Gründerteams deshalb mit Fachexpertinnen und -experten zu sprechen, die

in dem technischen Feld, in dem die Gründung erfolgen soll, wirklich tief drin sind.

Hierfür ein Beispiel: Gründende recherchieren oftmals nach Stand-Alone-Lösungen. Manchmal ist die Sicherheitsfunktionalität aber als Add-on eines bestehenden Produktes erhältlich. Entwickelt ein Startup dann eine Einzellösung wird es sehr schwer, am Markt erfolgreich zu sein.

„Deutscher Markt kann Hunger nach internationaler Expansion hemmen“

F: Ist es ein Vorteil für deutsche Startups, dass sie sich in einem sehr regulierten Markt bewegen?

A: Frei nach Frank Sinatra sage ich: If you can make it here, you can make it anywhere. Wenn sie es woanders nicht schaffen, dann liegt das wohl an ihrer selbst gewählten Genügsamkeit. Deutsche IT-Sicherheitsunternehmen können einen Markt mit 80 Mio. Personen direkt adressieren, im deutschsprachigen Raum noch wesentlich mehr. Sie profitieren von der Wirtschaftskraft des stärksten EU-Landes. Startups, die genügsam sind, können sich in einer Nische einrichten und moderat wachsen. In Israel ist das beispielsweise ganz anders. Dort sind Startups von vorneherein immer auf Wachstum und internationale Expansion ausgelegt, da sie anders gar nicht überleben können. Das ist eine ganz andere Mentalität und Kultur als bei uns.

„IP von Anfang an schützen“

F: Sie haben selbst mal eine Entwicklung gemacht und diese nicht patentieren lassen. Ist das ein typischer Fehler? Schützen Gründer ihre IP nicht richtig?

A: Damals – vor ca. 20 Jahren – wurde das Patentieren von Universitäten noch nicht so unterstützt wie heute. Wir haben dann kurzerhand ein Paper publiziert, um zumindest unsere Namen mit der Innovation dauerhaft zu verknüpfen. Heute ist das anders: Die EU verpflichtet Unis dazu, Innovationen der Verwertung zuzuführen, beispielsweise durch Patentierung. Trotzdem kann es natürlich sein, dass Gründerteams wegen ihrer Unerfahrenheit zu sorglos und naiv mit Ideen umgehen und sie nicht ausreichend schützen.

„Open Source oder Closed Source hängt vom Anwendungsszenario ab“

F: Wie ratsam ist es, eine Cybersicherheitslösung auf Basis von Open Source zu entwickeln?

A: Bei Open Source gibt es mehrere Aspekte. Fast alle Unternehmen, also auch die Konzerne, verwenden Open-Source-Komponenten in der Programmierung und in der Hardware. Das beinhaltet zugleich Risiken: was tun, wenn das Open-Source-Projekt nicht weitergeführt wird? Wie gehe ich als Unternehmen dann mit Service Level Agreements um? Wie mit Patches? Kann ich mich darauf verlassen, dass die Community Fehler behebt und Sicherheitslücken schließt, wenn ich sie melde? Wie schnell geschieht das? Muss ich Sicherheitslücken eventuell selbst schließen? Alle diese Punkte führen zu einer hohen Abhängigkeit von anderen, die vielfach in keiner vertraglichen Beziehung stehen. Das ist gerade bei Dingen, die eine dauerhafte Gewähr und ein hohes Sicherheitsniveau haben sollten, schwierig. Open Source kann insofern ein Risiko sein.

F: Trotzdem wird Open Source, auch im Cybersicherheitsbereich, eingesetzt.

A: Heutige Cybersicherheitsprodukte sind so groß, dass nicht alle Komponenten komplett selbst programmiert werden können, Open-Source-Produkte sind meist qualitativ hochwertig und natürlich erstmal kostengünstig. Manche Gründerteams gründen ihre Produkte auch auf selbst geschriebener Open Source, als gezielte Distributionsstrategie. Das sieht dann so aus: Die Kernkomponenten werden als Open Source entwickelt. Die Veredelung, beispielsweise das User Interface, die spezielle Geschäftslogik oder weitere Anpassungen mache ich mit den Kundenunternehmen und verdiene damit mein Geld.

F: Trage ich mir mit Open Source Lücken ins Unternehmen?

A: Diese Diskussion wird vielfach emotional geführt. Manche sagen: Da ich in den Code schauen kann, finde ich ggf. auf die Unsicherheiten. Es gibt aber beispielsweise auch Lücken bei sehr weit verbreiteter Open-Source-Software die nicht schnell bemerkt werden: Im Falle von Heartbleed hat es mehr als zwei Jahre gedauert. Umgekehrt heißt das aber nicht, dass es bei eigenen Entwicklungen keine Sicherheitslücken gibt. Hier gilt wiederum: Wenn weniger Leute drauf schauen, dann können durchaus im Verhältnis mehr Sicherheitslücken drin sein als bei Open Source. Was sicherer ist oder nicht, ist die falsche Frage.

F: Was ist die richtige Frage?

A: Für welche Anwendung will ich Open Source benutzen? Es gibt beispielsweise den Standpunkt, dass besonders Privacy-kritische Teile oder Anwendungen in Open Source programmiert sein sollten. Die Volksverschlüsslung ist beispielsweise eine Anwendung, die quelloffen zur Verfügung gestellt wird. So kann nachgeprüft werden, wie die Daten verarbeitet werden und es lässt sich nachvollziehen, dass es eine echte Ende-zu-Ende-Verschlüsselung ist. Da macht Open Source als Qualitätsmerkmal absolut Sinn.

F: Können sich Cybersicherheits-Startups denn überhaupt etwas Anderes leisten, als in Open Source zu programmieren?

A: Warum nicht? Viele werden aus guten Gründen nicht auf Open Source setzen, sondern auf einen geschlossenen Quellcode. Dies würde ich insbesondere dann machen, wenn ich mein geistiges Eigentum schützen möchte und eine vom Programmierumfang kleine Lösung habe.

F: Aber für Closed Source braucht man doch mehr Arbeitskraft etc.

A: Open Source kann sich als sehr kosten- und personalintensiv entpuppen. Wenn beispielsweise eine Bibliothek verwendet wird, die plötzlich nicht mehr weiter unterstützt wird und Gründungsteams diese dann weiterpflegen müssen, weil sie in ihrer Lösung eingesetzt ist, dann kann das sehr ressourcenintensiv werden. Es ist wirklich wichtig, dass am Anfang mal richtig zu überdenken und die wirtschaftlichen Implikationen beider Optionen durchzuspielen.

F: Können Cybersicherheits-Gründungsteams denn kommerzielle Lösungen einfach so als Open Source entwickeln?

A: Das ist eine Frage, die eigentlich die ganze IT-Branche betrifft. Die Antwort lautet in aller Kürze: Es hängt von der Lizenz ab und da gibt es auch bei Open Source große Unterschiede, Open Source ist nicht gleich Open Source. Es kann sein, dass ich aus einer bestimmten Open-Source-Software gar kein kommerzielles Produkt machen darf, oder dafür Lizenzgebühren zahlen muss.

Open Source kann auch die Frage der Schutzrechte verkomplizieren: Stellen Sie sich mal vor, dass drei Leute ein Open-Source-Projekt vorantreiben. Zwei davon gründen darauf basierend eine Firma, aber die dritte Person im Bunde hat auch Rechte aus der Vergangenheit, weil die Urheberschaft auch auf ihrem intellektuellen Eigentum basiert. Diese Konstellation kann schwierig werden. Wenn ich mir von vornherein rechtliche Probleme ersparen will und die Dinge unter meiner Kontrolle haben möchte, dann könnte Closed Source die bessere Variante sein.

„Kunden statt Produkte diversifizieren“

F: Angenommen ich stelle fest, dass ich meine Cybersicherheitslösung auf Kundenwünschen basierend weiterentwickelt habe, aber dabei beispielsweise die Modularität aus dem Blick verloren habe. Was raten Sie dann?

A: Das hängt natürlich auch davon ab, wie umfangreich das Produkt ist. Meiner Erfahrung nach machen gerade in der erklärungsbedürftigen Cybersicherheitsbranche viele Gründungsteam folgenden Fehler: Sie konzentrieren sich auf die ersten wenigen Kunden und gehen auf deren Feature-Wünsche ausführlich ein. Damit überlasten sie sich. Es wäre oft besser, die Kundenbasis zunächst zu verbreitern und nicht das Produkt auf wenige Kunden zuzuschneiden. Dann haben Cybersicherheits-Startups meist eine höhere Überlebenschance.

F: Vielen Dank für das Gespräch!

Autoren

Dr. Michael Kreutzer ist am Fraunhofer-Institut für Sichere Informationstechnologie SIT zuständig für Internationalisierung und strategische Industriebeziehungen. Zudem berät er Cyber-Startups in technischer Marktexpertise im Rahmen des Darmstädter Gründungsinkubators StartUpSecure, der vom Bundesministerium für Bildung und Forschung gefördert wird. Seine aktuellen Forschungsschwerpunkte spiegeln Kernthemen der modernen IT-Sicherheitsforschung wider: Sie liegen in der Aufdeckung und Bekämpfung von Desinformation, in Technologien der Dezentralität wie Blockchain, in der Kryptoagilität, in der Netzwerksicherheit, im Quantencomputing, im Quantenschlüsselaustausch sowie in der Post-Quantum-Kryptographie.

Ute Richter leitet den Digital Hub Cybersecurity und hat ihn gemeinsam mit dem Team zur führenden Innovationscommunity für Cybersecurity-Startups ausgebaut. Sie hat über 25 Jahre Erfahrung darin, erfolgreiche und effektive Kampagnen für Technologieunternehmen sowohl aus dem B2C- als auch aus dem B2B-Bereich zu entwickeln und umzusetzen. Utes Schwerpunkt ist aktuell Erfolgsfaktoren für Cyber-Startups zu erforschen und diese pragmatisch, messbar und agil umzusetzen. Sie hat einen Magister Artium in Germanistik und einen Master-Abschluss in Beratung, Coaching und Supervision in der Arbeitswelt.

Linda Schreiber ist wissenschaftliche Referentin in der Geschäftsstelle des Nationalen Forschungszentrums für angewandte Cybersicherheit am Fraunhofer SIT. Sie hat Informationsrecht (LL.B.) und Internationales Lizenzrecht (LL.M.) an der Hochschule Darmstadt, sowie Innovation, Technology and the Law an der University of Edinburgh studiert. Sie verfügt über Erfahrungen im Bereich IT-Vertragsgestaltung und Open Source Compliance.

Interessante Links und Quellen

Das Bundesgesetzblatt (Bürgerzugang): Offizielles Verkündungsblatt der Bundesrepublik Deutschland. Mehr unter https://www.bgbl.de.

Parlamentarische Drucksachen inklusive eines Gesetzgebungskalenders

https://www.gesetze-im-internet.de – vom Ministerium für Justiz und Verbraucherschutz und vom Bundesamt für Justiz betreutes Portal, dass fast das ganze Bundesrecht abdruckt inkl. einer Möglichkeit auch Verwaltungsvorschriften zu recherchieren.

https://n-lex.europa.eu/- Portal, das den Zugang zu den Quellen des nationalen Rechts der EU Staaten bietet.

Links zu primär und sekundär Recht auf der offiziellen Seite der EU - https://europa.eu/european-union/law_de -

Zusammenfassung der EU Gesetzgebung unter https://eur-lex.europa.eu/browse/summaries.html?locale=de

Relevante Institutionen und Verbände

- Bundesamt für Wirtschaft du Ausfuhrkontrolle (BAFA). Mehr unter https://www.bafa.de/.
- Bundesnetzagentur. Mehr unter https://www.bundesnetzagentur.de/.
- Bundesamt für Sicherheit in der Informationstechnik (BSI). Mehr unter https://www.bsi.bund.de/.
- Zoll. Mehr unter https://www.zoll.de/.
- European Union Agency for Cybersecurity. Mehr unter https://www.enisa.europa.eu/.
- Forum of European Supervisory Authorities for Electronic Signatures (FESA) http://www.fesa.eu/
- Bitkom https://www.bitkom.org/
- Teletrust https://www.teletrust.de/

Literaturtip

Voigt, P. (2018). IT-Sicherheitsrecht - Pflichten und Haftung in Unternehmen. Köln: Verlag Dr. Otto Schmidt

Digital Hub Cybersecurity

Der Digital Hub Cybersecurity ist die führende Innovations Community für Cybersecurity in Deutschland. Er vernetzt Akteure aus Unternehmen, Forschung und Gründerszene und schafft Aufmerksamkeit bei Influencern, Investoren und Stakeholdern. Der Digital Hub Cybersecurity ist Teil der Digital Hub Initiative des Bundesministeriums für Wirtschaft und Energie und Teil von Athene, dem Nationalen Forschungszentrum für Angewandte Cybersicherheit. Er hat seinen Sitz in Darmstadt und wird vom Fraunhofer SIT, der TU Darmstadt, der IHK Darmstadt sowie der Stadt Darmstadt unterstützt. www.digitalhub-cybersecurity.com

Unser Netzwerk

Das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE ist ein Forschungszentrum der Fraunhofer-Gesellschaft für ihre beiden Darmstädter Institute SIT und IGD unter Beteiligung der Technischen Universität Darmstadt und der Hochschule Darmstadt. Dieses einzigartige und innovative Kooperationsmodell der universitären und außeruniversitären Forschung kombiniert die Kompetenzen und Stärken der Fraunhofer-Institute mit den Kompetenzen und Stärken der Universitäten und ermöglicht Spitzenforschung zum Wohle von Gesellschaft, Wirtschaft und Staat. ATHENE ist das größte Forschungszentrum für angewandte Cybersicherheit und Privatsphärenschutz in Europa. www.athene-center.de

Die Digital Hub Initiative trägt zur Transformation Deutschlands als weltweit führenden Digitalstandort bei. Hierfür fördert die Initiative den Aufbau und die Vernetzung zwölf Digitaler Hubs mit spezifischen Themenschwerpunkten. Unter der gemeinsamen Dachmarke de:hub entsteht durch die enge Kooperation zwischen Startups, etablierter Wirtschaft, Forschungseinrichtungen und Experten ein einzigartiges, innovatives Netzwerk. Um Gründer und Investoren aus dem Ausland für den Digitalstandort Deutschland zu gewinnen, werden in den zwölf Hubs konkrete Programme für die Herausforderungen der Digitalisierung entwickelt.

Zu den Digital Hubs zählen Berlin (IoT & FinTech), Dortmund (Logistics), Dresden/Leipzig (Smart Systems & Smart Infrastructure), Frankfurt/Darmstadt (FinTech & Cybersecurity), Hamburg (Logistics), Karlsruhe (Artificial Intelligence), Köln (InsurTech), Mannheim/Ludwigshafen (Digital Chemistry & Digital Health), München (Mobility & InsurTech), Nürnberg/Erlangen (Digital Health), Potsdam (MediaTech) und Stuttgart (Future Industries). Träger der Digital Hub Initiative ist das Bundesministerium für Wirtschaft und Energie. Teil der Digital Hub Initiative sind die Digital Hubs Berlin, Dortmund, Frankfurt a. M. und Darmstadt, Hamburg, Karlsruhe, Köln, Leipzig und Dresden, Ludwigshafen und Mannheim, München, Nürnberg und Erlangen, Potsdam sowie Stuttgart. www.de-hub.de

Kontakt

Digital Hub Cybersecurity
Rheinstr. 75
64295 Darmstadt
Tel. 06151-869-521

Mail: info[at]digitalhub-cybersecurity.com
https://www.digitalhub-cybersecurity.com

Autor*innen
Dr. Michael Kreutzer, Linda Schreiber und Ute Richter
Aktualisiert: November 2019

Grafikdesign: enver@simsek.design

Bildrechte: Umschlag, istock/ A-Basler

Der Digital Hub Cybersecurity wird gefördert
aus Mitteln des Landes Hessen.