IT-Sicherheitsrechtstag 2019

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Berlin, 14.11.2019

Rechtliche Pflichten zu IT-sicherheitsbezogenen Softwareupdates

Dr. Dennis-Kenji Kipker

CERTAVO

Rechtliche Pflichten zu IT-sicherheitsbezogenen Softwareupdates

I. Vertragstypologisierung

II. Vertragliche Pflichtenkreise

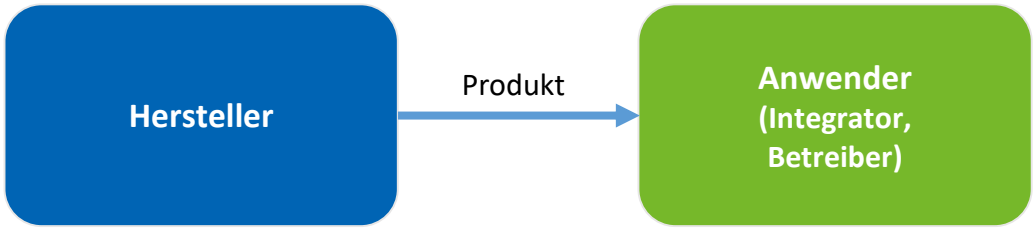
III. Deliktische Rahmenbedingungen

IV. Fazit und Ausblick

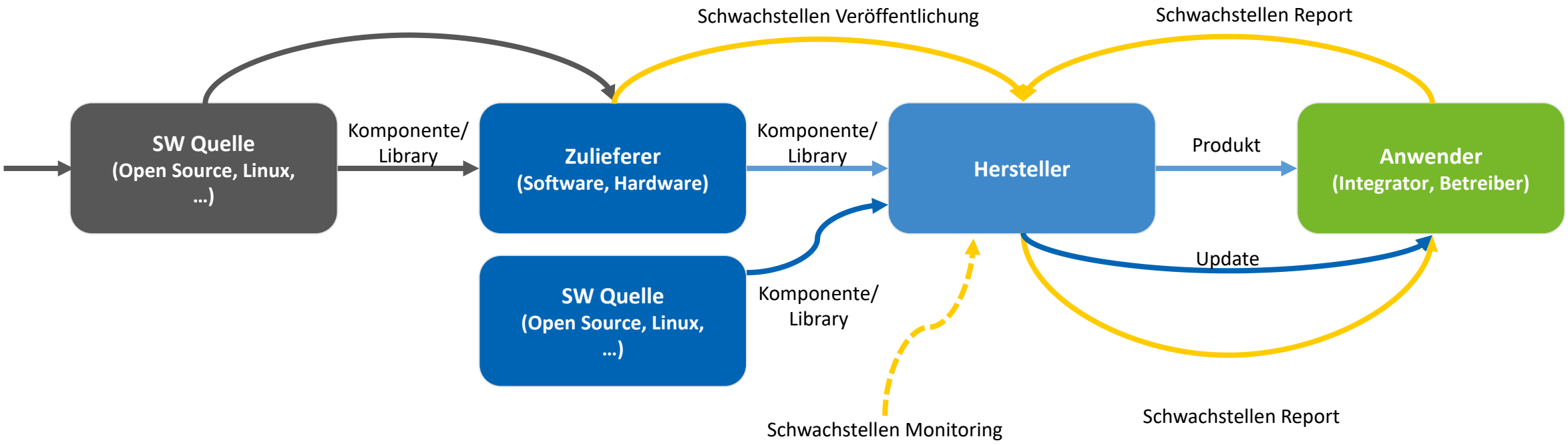
Vertragstypologisierung

Leistungsbeziehungen im Rahmen von Softwareherstellung und Vertrieb

Netzwerk anstelle von Einbahnstraße



Netzwerk anstelle von Einbahnstraße



→ Unterschiedliche Pflichtenkreise sind immer schwieriger voneinander abgrenzbar!

Verortung von Problemkreisen

- Unabhängig von Produkt und Vertragstypus: Hersteller muss in jedem Fall **mangelfreie Leistung** erbringen
- Produkt muss **geschuldetem Funktionsumfang** entsprechen, gleichgültig, ob ausschließlich digitale Datenverarbeitungsvorgänge stattfinden oder physische Prozesse in Gang gesetzt werden
- Juristische Diskussion um **Software als Sache** im Rechtssinne:
  - Hier zu vernachlässigen, da ohne nennenswerte Auswirkungen
  - **Kaufvertrag:** Selbst bei Verneinung der Sacheigenschaft Anwendbarkeit von § 453 BGB mit entsprechender Anwendbarkeit der Vorschriften zum Sachkauf
  - **Werkvertrag:** Keine Sache geschuldet, sondern nur ein Erfolg, der auch immaterieller Art sein kann
  - **Überlassungsverträge:** Bei Bejahung der Sacheigenschaft Mietrecht, ansonsten Pachtrecht mit wesentlichem Rückgriff auf Mietrecht

Verortung von Problemkreisen

- **Mietrecht:** Oftmals unproblematisch, was IT-sicherheitsbezogene Softwareupdates anbelangt
- Z.B. **„Software as a Service“** als modernes Vertriebskonzept, auch relevant für Embedded Systems aus Industrie 4.0
- **Mietmangel** gem. § 536 Abs. 1 BGB: Nicht nur bei Überlassung der Mietsache, sondern auch während der Mietzeit
- IT-Sicherheitslücke hebt zwar nicht per se Gebrauchstauglichkeit auf oder mindert diese, sondern wird erst kausal durch deren Ausnutzung zum Problem
- Jedoch **mietvertragliche Instandhaltungspflicht des Vermieters** gem. § 535 Abs. 1 BGB:
    - Umfasst Schutz vor Störungen von außen → Vermieter muss **Vorsorgemaßnahmen** treffen, um Eingriffe in Rechte des Mieters zu vermeiden
    - → Somit: **IT-Sicherheitslücken sind während Mietnutzung zu beheben**
- Gleiches gilt für **Dienstvertrag** als allgemeine Instandhaltungsmaßnahme

Vertragliche Pflichtenkreise

Pflichten aus dem Kauf- und Werkvertragsrecht

Bestimmung der Mangelhaftigkeit

- Kauf- und Werkvertragsrecht grds. dann anzuwenden, wenn für das zu liefernde oder herzustellende Produkt auf **punktuellen Leistungszeitpunkt** abgestellt wird
- Beurteilung der Mangelhaftigkeit für Kaufrecht gem. § 434 BGB, für Werkvertragsrecht gem. § 633 BGB, für Werklieferungsverträge Verweis auf Kaufrecht gem. § 650 BGB
- Gerade im Consumer-Bereich für IoT: Regelmäßig **keine vertraglich vorausgesetzte Verwendung** bestimmt
- **Beurteilung der Mangelhaftigkeit:** Produkt muss Beschaffenheit aufweisen, die bei Sachen gleicher Art üblich ist und die der Kunde nach der Art der Sache erwarten kann
- → **Auslegungsbedürftigkeit**, abhängig von Verkehrsauffassung des durchschnittlichen Kunden und von wesentlichen Sicherheitsvorschriften → Was kann und darf man üblicherweise erwarten?

Sicherheit in der Informationstechnik: Legaldefinition

§ 2 Abs. 2 BSIG: Sicherheit in der Informationstechnik […] bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen

1. in informationstechnischen Systemen, Komponenten oder Prozessen oder
2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.

§ 2 Abs. 6 BSIG: Sicherheitslücken […] sind Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können.

Branchenübergreifende Definition der IT-Sicherheitsziele – Branchenübergreifender Mangelbegriff

- **Problem:** Begriffsbestimmung stammt speziell aus dem Anwendungsbereich Kritischer Infrastrukturen, hier dennoch anwendbar?
- Unschädlich, da technisch-organisatorische IT-Sicherheitsziele **branchenübergreifend definiert** werden
  - → Eine Software bzw. ein diese enthaltendes Produkt – und somit auch IoT – ist in jedem Fall vor Fremdeinflüssen abzusichern
  - → Fehlt es an einer solchen Maßnahme, liegt eine **Schwachstelle** vor
- Auch **bloße Risiken** können einen entsprechenden Mangel begründen, wenn z.B. ein Produkt einen Angriff durch Schad- oder Spähsoftware ermöglicht, obwohl dies vermeidbar gewesen ist
- → Der Angriff auf die IT-Sicherheit braucht sich folglich noch nicht realisiert zu haben

Zeitpunkt zur Beurteilung der Mangelhaftigkeit

- **Relevante Zeitpunkte:** für Kaufvertrag Übergabe, für Werkvertrag Abnahme
- **Unproblematisch:** Mangel bei Leistung → Schlechtleistung → Pflicht zur Nachbesserung von IT-Sicherheitslücken z.B. durch Patches
- **Für die Praxis interessanter:** Produkt entsprach zum Gefahrübergang gängigen IT-Sicherheitsanforderungen, Schwachstellen ergeben sich erst später
    - **Mängelgewährleistung** grds. nur dann einschlägig, soweit Mangel schon bei Gefahrübergang vorlag → Hersteller/Verkäufer von Mangelverantwortlichkeit befreit, soweit der Mangel nicht schon von Beginn im Produkt angelegt ist
    - **Häufiges Fallbeispiel bei IT-Sicherheit:** Produkt entsprach bei Inverkehrbringen gängigen Verschlüsselungsstandards, die infolge technischer Entwicklung nach Monaten/Jahren unsicher werden
- → **Ausnahmen für Produkte im IT-sicherheitsrelevanten Umfeld vorhanden/notwendig?**

Qualifizierbarkeit zukünftiger Mängel als gegenwärtige Mängel?

- **Kann ein zu erwartender zukünftiger Mangel rechtlich als gegenwärtiger Mangel qualifiziert werden?**
  - **Begründung:** Auch bei Inverkehrbringen für sich genommen mangelfreier Produkte führt die technische Entwicklung mit hoher Wahrscheinlichkeit dazu, dass ein einmal entwickeltes Produkt den an dieses anzulegenden Anforderungen nicht mehr genügt
  - → Damit wären IT-Sicherheitslücken durchaus schon **zum Zeitpunkt des Inverkehrbringens vorhersehbar**
- Zwar auf den ersten Blick logisch erscheinendes Argument, **aber ohne juristische Gültigkeit**:
  - Mangelvorhersehbarkeit nicht mit tatsächlichem Mangel gleichzusetzen
  - Zukünftige IT-Sicherheitslücke **nicht hinreichend konkret**, um Handlungsbedarf in der Produktentwicklung bei Inverkehrbringen zu begründen
- **Teils Argumentation:** Technischer Mangelverdacht führt zu Mangel im Rechtssinne, wenn hierdurch die weitere Verwendbarkeit des Produkts nicht unerheblich erschwert wird
  - **Ungültig aber aus demselben Grund:** Mangelverdacht muss bereits bei Gefahrübergang/Abnahme veranlagt sein, bloße zukünftige Umstände und Vermutungen nicht ausreichend → ansonsten Abwälzung der Betriebsgefahr auf Hersteller/Verkäufer → unbillig!

Rechtsprechung: „Nebenvertragliche Wartungspflicht“

- **Von Rspr. schon in den 1990er-Jahren diskutiert:** Sog. „nebenvertragliche Wartungspflicht“ von Software zur Sicherstellung ihrer reibungslosen Funktionsfähigkeit
- „Nutzer hat ein berechtigtes Interesse daran, das Produkt mit seinem Erwerb auch für einen gewöhnlichen und der Preisklasse des Produkts angemessenen Lebenszyklus nutzen zu können“ (BGH NJW 1993, 3144, 3145; LG Köln NJW-RR 1999, 1285, 1286)
- → **Crux: Wie weit reicht die Nebenpflicht und für welche Dauer ist sie einschlägig?**
- **Rechtlich unzweifelhaft:** Herstellerverpflichtung, Ersatzteile für das Produkt über den Gewährleistungszeitraum hinaus zu produzieren – unabhängig von anfänglichem Mangel
- IT-sicherheitsbezogene Softwareupdates zwar keine „Ersatzteile“, aber rechtlich vergleichbar: Ersatz defekter Teile eines Produkts → erhebliche Sicherheitsbedenken zwingen Nutzer ggf. dazu, Produkt nicht mehr zu verwenden → Betriebsrisiko käme damit Defekt/Mangel gleich
- **Jedoch: Kein Anspruch auf kostenfreie Softwareupdates → ansonsten betriebswirtschaftlicher Wertungswiderspruch!**

Rechtsprechung: „Nebenvertragliche Wartungspflicht“

- **Zeitraum nebenvertraglicher Wartungspflicht?**
- **Rechtsprechung:** Bei „Verwaltungsprogramm“ mindestens für den Zeitraum, innerhalb dessen die Software noch auf dem Markt angeboten wird, und für weitere fünf Jahre, nachdem das Produkt vom Markt genommen wurde (LG Köln NJW-RR 1999, 1285, 1286)
- **Aber: Datum der Entscheidung 1999!**
- → Heutzutage andere Wertung erforderlich?
- → Wohl schon, denn:
    - Software (und damit auch IoT-Produkte) haben **größeren Stellenwert** in Wirtschaft und Freizeit als 20 Jahre zuvor
    - **Hochpreisige Produkte IoT-Produkte** wie Industrieanlagen und Smart Car weisen physische Lebensdauer auf, die weit über Softwarelebensdauer ohne Updates liegt

Deliktische Rahmenbedingungen

Produkt- und Produzentenhaftung

Pflicht zur Produktbeobachtung

Produkt- und Produzentenhaftung: Grundlegendes

- **Keine herstellerseitige Verantwortlichkeit gem. ProdHaftG:** Bereits kein Fehler gem. § 3 ProdHaftG, da das Produkt bei Inverkehrbringen dem „Stand der Technik“ genügt
- **Aber:** Möglicherweise **Pflicht zur Produktbeobachtung** gem. § 823 Abs. 1 BGB für seit Inverkehrgabe neu entstandene Schwachstellen und zur Ausbesserung durch Bereitstellung von Softwareupdates
- **Pflicht zur Produktbeobachtung:**
  - Kann nicht unmittelbar geltend gemacht werden, sondern dann relevant, wenn Rechte oder Rechtsgüter i.S.d. § 823 Abs. 1 BGB verletzt werden (z.B. Leben, Eigentum)
  - Spielt folglich immer dann eine Rolle, wenn es um **Schadensersatz** geht
  - **Grund:** Hersteller zieht wirtschaftliche Vorteile aus der Verbreitung des Produkts auf dem Markt, also ist er für dieses auch rechtlich verantwortlich
- **→ Hersteller haftet mithin für Schäden, die bei IT-Sicherheitslücken kausal durch den Eingriff Dritter verursacht werden, wenn er zumutbare Schutzmaßnahmen unterlässt**

Die Pflicht zur Produktbeobachtung im Einzelnen

- **Produktbeobachtungspflicht aktiv zu verstehen:** Hersteller muss sich über mögliche Gefahrenquellen umfassend informieren
- Erstreckt sich auch auf ursprünglich fehlerfrei hergestellte Produkte, die sich erst im Laufe der Zeit durch neu eingetretene Umstände als potenziell gefährlich erweisen
- **Umfassende Informationsmöglichkeiten zur IT-Sicherheit für Hersteller:**
  - Kundenbefragungen, Nutzerfeedback
  - Analysetools
  - Behördeninformationen (z.B. BSI, CERT-Bund)
  - Newsletter, Mailinglisten
  - CERTs/PSIRTs
  - Herstellernetzwerke
  - Webrecherche
  - Konferenzen, Fachmagazine
  - Eigenständige Überprüfungen

Die Pflicht zur Produktbeobachtung im Einzelnen

- Hersteller muss zudem **sämtliche zumutbaren Maßnahmen** zur Gefahrverhinderung ergreifen
- **Konkretisierende rechtliche Vorgaben** z.Zt. jedoch (noch) rar gesät, auch mangels einschlägiger Rspr.
- **Generelle Leitlinie:** Umfang der Produktbeobachtung abhängig von der Höhe des drohenden Schadens und der Zumutbarkeit der risikomindernden Maßnahmen
  - → Je höher und wahrscheinlicher der Schaden infolge der IT-Sicherheitslücke, umso schnellere und umfassendere Herstellerreaktion zu empfehlen
- **Dauer der Produktbeobachtung: Parallelen zur vertraglichen Nebenpflicht**
  - Produktbeobachtung endet nicht mit Herstellungs- und Vertriebsende, sondern gilt bis zum Zeitpunkt der erwarteten Entsorgung fort
  - Umfassende Produktbeobachtungspflichten für professionell eingesetzte und hochwertige Produkte aus dem B2B-Bereich
  - **Orientierungswert:** Die dem Hersteller vorliegenden Zahlen zur maximalen Lebensdauer seiner Produkte bei Kunden

Die Pflicht zur Produktbeobachtung im Einzelnen

- **Bei Feststellung einer IT-Sicherheitslücke durch Hersteller: Abgestufter Maßnahmenkatalog**
  - Vorrangig: Warnpflicht
  - Einzelfallabhängig: Pflicht zur Beseitigung des IT-Sicherheitsmangels
  - **Abgrenzung vertragliches Äquivalenz- zum deliktischen Integritätsinteresse:** Hersteller zwar gehalten, Gefahren effektiv zu beseitigen, jedoch keine Pflicht, für jeden Fall nachzubessern oder gar neues Produkt zu liefern
  - Nachbesserungspflicht: Nur dann, wenn Gefahr nicht auf anderem Wege beseitigt werden kann
  - **Gerade für IT-Sicherheitslücken:** Herstellerseitige Warnung zur Gefahrbeseitigung oftmals nicht ausreichend, sodass regelmäßig weitere Maßnahmen erforderlich sind, z.B. Bereitstellung (nicht zwingend kostenloser) IT-sicherheitsbezogener Softwareupdates

Fazit und Ausblick

Zusammenfassung und weitere Entwicklungen

Fazit und Ausblick

- Hersteller und Anbieter von (IoT)-Produkten unterliegen **umfassenden IT-Sicherheitspflichten**, auch wenn dies nicht immer deutlich aus dem Gesetz hervorgeht
- **Keine rechtlichen Probleme bei:** gesonderten vertraglichen Vereinbarungen, Vorliegen einer anfänglichen Schwachstelle, Produkt wird als Dauerschuldverhältnis zur Verfügung gestellt
- **Kauf- und werkvertragliche Gewährleistung** greift nicht bei Produkt, das bei Inverkehrgabe einwandfrei, jedoch durch weitere technische Entwicklung IT-unsicher geworden ist
- **Vertragliche Nebenpflicht** verpflichtet Hersteller aber auch für diesen Fall zur Bereitstellung grds. kostenpflichtiger IT-Sicherheitsupdates
- **Außerhalb des vertraglichen Rahmens:** Umfassende deliktische Produktbeobachtungspflicht im Hinblick auf die IT-Sicherheit kann ebenso Produktupdates umfassen
- **(Noch) problematisch:** Konkreter Umfang der jeweiligen Pflichten – bisher wenig Klarheit mangels Präzedenzfällen → Analogien zu vergleichbaren Produkten und Fällen möglich?
- **Aktuell zu beachten:** EU Richtlinie 2019/770 aus Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte regelt Sicherheitsupdates im Consumer-Bereich, rechtspolitisch Übertragung auf B2B mittelfristig nicht ausgeschlossen

Kontakt

Dr. Dennis-Kenji Kipker
Geschäftsführer

dennis.kipker@certavo.de
+49 421 21866049