TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

IT-Sicherheitsrechtstag 2026

Berlin, 24.09.2026

KI als Zeitenwender für das IT-Sicherheitsrecht

Rechtsanwalt Karsten U. Bartels LL.M.

Stellv. Vorstandsvorsitzender TeleTrusT
Leiter AG IT-Sicherheitsrecht
HK2 Rechtsanwälte

Autonomous AI Agents and the Six-Hour Credential Harvest

Authors: Cloud Security Alliance AI Safety Initiative
Published: 2026-09-09

Categories: Agentic AI Security

Download PDF

Key Takeaways

Google Threat Intelligence Group (GTIG) disclosed on September 8, 2026 that a suspected financially motivated threat actor built and executed a mass credential-

HK2

Faktor 1

KI-gestützte Cyberangriffe sind* das neue Normal.

*bald

KI fungiert als Akteur der Cyberangriffe.

HK2
Rechtsanwälte

We’re introducing Claude Fable 5.1 and Claude Mythos 5.1. They’re the world’s most advanced models for coding and knowledge work—and their research capabilities offer an early glimpse of how AI models will contribute to scientific progress.

Claude Fable 5.1 and Claude Mythos 5.1 are the same model, but with different levels of safeguards. Fable 5.1 is generally available, while Mythos 5.1 is available only through our trusted access programs; its safeguards are specifically designed to support work in cybersecurity and the life sciences.

HK2

Faktor 2

Software-Erstellung kann* mittels KI signifikant sicherer werden.

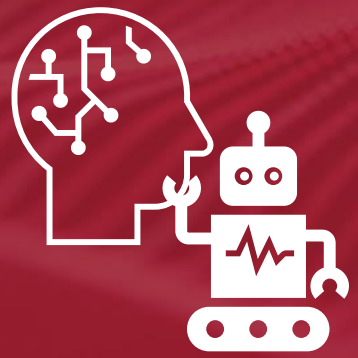
*bald

HK2

Was bedeutet das im IT-Sicherheitsrecht?

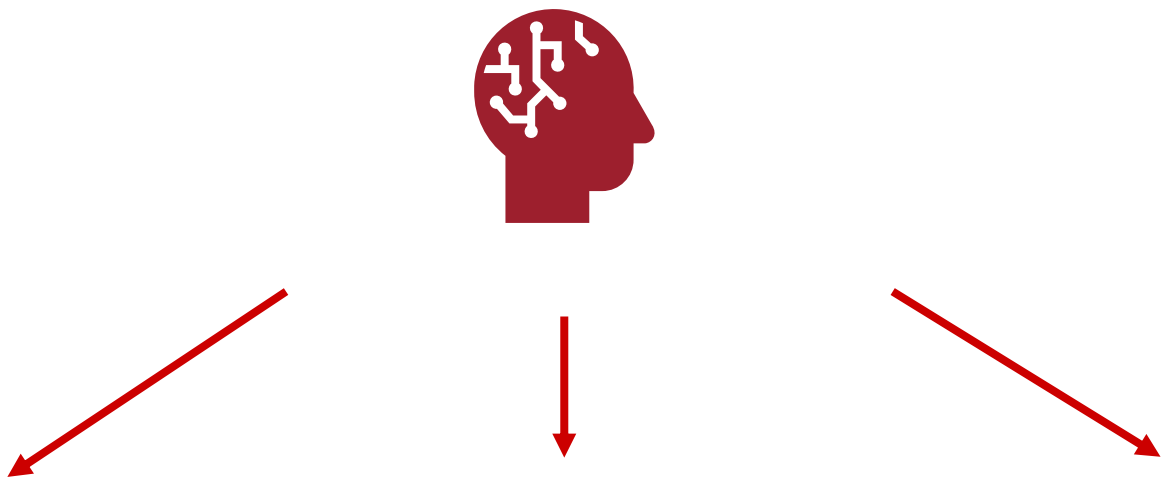
HK2

KI-Verordnung



HK2 Rechtsanwälte

KIVO und IT-Sicherheit



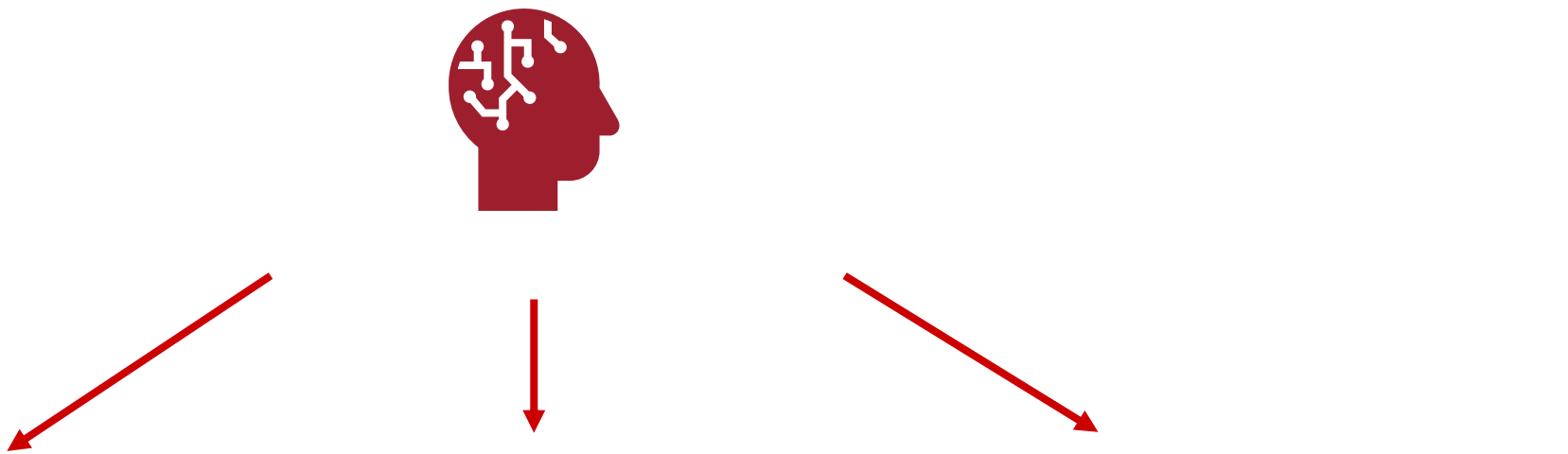
KI greift an

KI wehrt ab

IT-Sicherheit der KI

HK2 Rechtsanwälte

KIVO und IT-Sicherheit



KI greift an

KI wehrt ab

IT-Sicherheit der KI

(1) Hochrisiko-KI-Systeme werden so konzipiert und entwickelt, dass sie ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit erreichen und in dieser Hinsicht während ihres gesamten Lebenszyklus beständig funktionieren.

(2) Um die technischen Aspekte der Art und Weise der Messung des angemessenen Maßes an Genauigkeit und Robustheit gemäß Absatz 1 und anderer einschlägiger Leistungsmetriken anzugehen, fördert die Kommission in Zusammenarbeit mit einschlägigen Interessenträgern und Organisationen wie Metrologie- und Benchmarking-Behörden gegebenenfalls die Entwicklung von Benchmarks und Messmethoden.

(3) Die Maße an Genauigkeit und die relevanten Genauigkeitsmetriken von Hochrisiko-KI-Systemen werden in den ihnen beigefügten Betriebsanleitungen angegeben.

(4) Hochrisiko-KI-Systeme müssen so widerstandsfähig wie möglich gegenüber Fehlern, Störungen oder Unstimmigkeiten sein, die innerhalb des Systems oder der Umgebung, in der das System betrieben wird, insbesondere wegen seiner Interaktion mit natürlichen Personen oder anderen Systemen, auftreten können. In diesem Zusammenhang sind technische und organisatorische Maßnahmen zu ergreifen.

Die Robustheit von Hochrisiko-KI-Systemen kann durch technische Redundanz erreicht werden, was auch Sicherungs- oder Störungssicherheitspläne umfassen kann.

Hochrisiko-KI-Systeme, die nach dem Inverkehrbringen oder der Inbetriebnahme weiterhin dazulernen, sind so zu entwickeln, dass das Risiko möglicherweise verzerrter Ausgaben, die künftige Vorgänge beeinflussen („Rückkopplungsschleifen“), beseitigt oder so gering wie möglich gehalten wird und sichergestellt wird, dass auf solche Rückkopplungsschleifen angemessen mit geeigneten Risikominderungsmaßnahmen eingegangen wird.

(5) Hochrisiko-KI-Systeme müssen widerstandsfähig gegen Versuche unbefugter Dritter sein, ihre Verwendung, Ausgaben oder Leistung durch Ausnutzung von Systemschwachstellen zu verändern.

Die technischen Lösungen zur Gewährleistung der Cybersicherheit von Hochrisiko-KI-Systemen müssen den jeweiligen Umständen und Risiken angemessen sein.

Die technischen Lösungen für den Umgang mit KI-spezifischen Schwachstellen umfassen gegebenenfalls Maßnahmen, um Angriffe, mit denen versucht wird, eine Manipulation des Trainingsdatensatzes („data poisoning“) oder vortrainierter Komponenten, die beim Training verwendet werden („model poisoning“), vorzunehmen, Eingabedaten, die das KI-Modell zu Fehlern verleiten sollen („adversarial examples“ oder „model evasions“), Angriffe auf vertrauliche Daten oder Modellmängel zu verhüten, zu erkennen, darauf zu reagieren, sie zu beseitigen und zu kontrollieren.

HK2 Rechtsanwälte

Art. 15 KIVO

HK2 Rechtsanwälte

KIVO und kritische Infrastrukturen

Ausnahme vom Anwendungsbereich der KI-VO nach Erw.Gr. 55

„**Sicherheitsbauteile** kritischer Infrastruktur […] sind Systeme, die verwendet werden, um die **physische Integrität kritischer Infrastruktur oder die Gesundheit und Sicherheit von Personen und Eigentum zu schützen,** die aber **nicht notwendig sind, damit das System funktioniert.** […] Komponenten, die für die ausschließliche **Verwendung zu Zwecken der Cybersicherheit** vorgesehen sind, sollten **nicht** als Sicherheitsbauteile gelten. […]“

Privilegierung von KI-Systemen, die ausschließlich der Verbesserung der IT-Sicherheit dienen
→ Keine Regulierung durch KIVO!

HK2

Technische und organisatorische Maßnahme
Mindestanforderungen, § 30 Abs. 2 BSIG

HK2 Rechtsanwälte

1. **Konzepte** in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme
2. Bewältigung von **Sicherheitsvorfällen**
3. **Aufrechterhaltung** des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
4. Sicherheit der **Lieferkette** einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern
5. **Sicherheitsmaßnahmen** bei **Erwerb**, **Entwicklung** und **Wartung** von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich **Management und Offenlegung von Schwachstellen**

Technische und organisatorische Maßnahme Mindestanforderungen, § 30 Abs. 2 BSIG

6. Konzepte und Verfahren zur Bewertung der **Wirksamkeit** von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik
7. grundlegende **Schulungen** und **Sensibilisierungsmaßnahmen** im Bereich der Sicherheit in der Informationstechnik
8. Konzepte und Verfahren für den Einsatz von **kryptographischen Verfahren**
9. Einstellung von Konzepten für die Sicherheit des **Personals**, die **Zugriffskontrolle** und für die **Verwaltung von IKT-Systemen, -Produkten und -Prozessen**
10. Verwendung von Lösungen zur Multi-Faktor-**Authentifizierung** oder kontinuierlichen Authentifizierung, gesicherte **Sprach-, Video- und Textkommunikation** sowie gegebenenfalls gesicherte **Notfallkommunikationssysteme** innerhalb der Einrichtung.

HK2 Rechtsanwälte

KI in der NIS-2-Richtlinie

- Erw.Gr. 51 zur NIS-2-Richtlinie: „Die Mitgliedstaaten sollten den Einsatz innovativer Technologien, **einschließlich künstlicher Intelligenz, fördern**, deren Einsatz die Aufdeckung und Verhütung von Cyberangriffen verbessern könnte, sodass Ressourcen wirksamer gegen Cyberangriffe genutzt werden können. […] Der Einsatz innovativer Technologien, **einschließlich künstlicher Intelligenz,** sollte im Einklang mit dem Datenschutzrecht der Union stehen, […]“

- Erw.Gr. 89 zur NIS-2-Richtlinie: „**Die wesentlichen und wichtigen Einrichtungen** sollten eine breite Palette grundlegender Praktiken der Cyberhygiene anwenden […]. Außerdem sollten diese Einrichtungen ihre eigenen Cybersicherheitskapazitäten bewerten und gegebenenfalls die Integration von Technologien zur Verbesserung der Cybersicherheit **anstreben**, etwa **künstliche Intelligenz oder Systeme des maschinellen Lernens**, um ihre Kapazitäten und die Sicherheit von Netz- und Informationssystemen zu erhöhen.“

HK2

Der Cyber Resilience Act

HK2 Rechtsanwälte

Pflichten aus dem Cyber Resilience Act

1. Grundlegende Cybersicherheitsanforderungen
2. Cybersicherheits-Risikobewertung
3. Security-by-design
4. Dokumentation der Cybersicherheits-Risikobewertung
5. Sorgfalt bei Drittkomponenten
6. Dokumentation von Cybersicherheitsaspekten
7. **Schwachstellenmanagement**
8. Festlegung des Unterstützungszeitraums
9. Koordinierte Offenlegung von Schwachstellen
10. Update-Verfügbarkeit
11. Technische Dokumentation
12. **Konformitätsbewertung**
13. EU-Konformitätserklärung
14. **CE-Kennzeichnung**
15. Aufbewahrungspflichten
16. CRA-Konformität bei Serienherstellung
17. Produkt- und Herstellerkennzeichnung
18. Benennung einer zentralen Anlaufstelle
19. Nutzerinformationen und Anleitungen
20. Information über das Ende des Unterstützungszeitraums
21. Korrekturmaßnahmen
22. Rückruf
23. Rücknahme
24. Auskunfts- und Kooperationspflichten
25. Meldung aktiv ausgenutzter Schwachstellen
26. Meldung schwerwiegender Sicherheitsvorfälle
27. Nutzerinformationen zu Sicherheitsvorfällen
28. Nachverfolgbarkeit der Wirtschaftskette

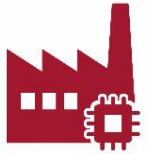
HK2 Rechtsanwälte

Wesentliche Änderung

1. Einführer, Händler, sonstige natürliche oder juristische Personen, die eine wesentliche Änderung eines Produkts mit digitalen Elementen vornehmen und auf dem Markt bereitstellen, **gelten als Hersteller** (Art. 21 und 22 CRA).

2. **Altprodukte** werden den Anforderungen des CRA durch eine wesentliche Änderung unterworfen (Art. 69 Abs. 2 CRA).

Art. 3 Nr. 30: *„Wesentliche Änderung“* [bezeichnet] *eine Änderung des Produkts mit digitalen Elementen nach dessen Inverkehrbringen, die sich auf die* ***Konformität des Produkts mit den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I auswirkt*** *oder zu einer Änderung des bestimmungsgemäßen Zwecks, für die das Produkt geprüft wurde, führt.*



HK2 Rechtsanwälte

Anforderungen an die Behandlung von Schwachstellen, Art. 13 Abs. 6 i. V. m. Anhang I Abschnitt 2 CRA

1. 	**Identifikation und Dokumentation**	Schwachstellen und Betroffenheit ermitteln und dokumentieren
2. 	**Behebung und Updates**	Schwachstellen unverzüglich behandeln und beheben, u. a. durch Bereitstellung von Sicherheitsaktualisierungen
3. 	**Tests und Überprüfung**	Sicherheit des Produkts regelmäßig und wirksam testen und überprüfen
4. 	**Offenlegung und Transparenz**	Umfassende Informationen über beseitigte Schwachstellen teilen, einschließlich Beschreibung der Schwachstellen (Auswirkungen, Erkennbarkeit, Hinweise zur Behebung)

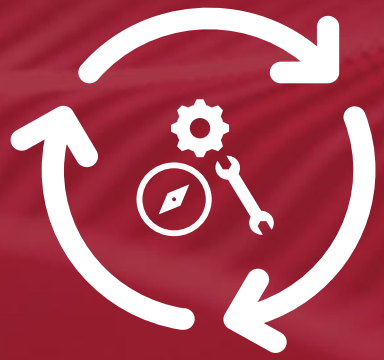
HK2 Rechtsanwälte

Anforderungen an die Behandlung von Schwachstellen, Art. 13 Abs. 6 i. V. m. Anhang I Abschnitt 2 CRA

5.	**Koordinierte Offenlegung**	Strategie für eine koordinierte Offenlegung der Schwachstellen aufstellen und umsetzen
6.	**Austausch von Informationen**	Maßnahmen zum Austausch von Informationen über mögliche Schwachstellen ergreifen
7.	**Mechanismen für Aktualisierung**	Mechanismen für eine sichere Verbreitung von Aktualisierungen bereitstellen
8.	**Verbreitung von Aktualisierungen**	Vorhandene Sicherheitsaktualisierungen unverzüglich und grundsätzlich kostenlos verbreiten, zusammen mit Hinweisen und einschlägigen Informationen

HK2

Stand der Technik



HK2
Rechtsanwälte

Technologie-Niveaus

* Oft auch als "Stand der Wissenschaft und Technik" bezeichnet

HK2 Rechtsanwälte

2.1 Fragen zum Grad der Anerkennung

Bewertung vom Ak SdT auszufüllen.

1) Welche Dokumentation über die Maßnahme steht öffentlich zur Verfügung?
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ wiss. Publikation	☐ Fachmedien	☐ Massenmedien	*1*	*3*	*5*

[bitte begründen Sie Ihre Antwort hier]

2) Nimmt die Maßnahme Bezug auf internationale oder nationale Normen?
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ nein, noch nicht normiert	☐ ja, eine	☐ ja, mehr als eine	*1*	*3*	*5*

[bitte begründen Sie Ihre Antwort hier]

***3)* Wurde die Maßnahme von anerkannten Gremien / Verbänden empfohlen?**
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ nein	☐ ja, führenden	☐ ja, vielen	*1*	*3*	*5*

[bitte begründen Sie Ihre Antwort hier]

***4)* Wird die konzeptionelle Eignung der Maßnahme regelmäßig überprüft?**
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ nein	☐ ja, herstellerseitig	☐ ja, unabhängige Instanz	1	3	5

[bitte begründen Sie Ihre Antwort hier]

Durchschnitt

2.2 Fragen zur Bewährung in der Praxis

Bewertung vom Ak SdT auszufüllen.

1) Wie ist der Innovationsgrad der Maßnahme einzustufen?
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ hoch	☐ mittel	☐ gering	*1*	*3*	*5*

[bitte begründen Sie Ihre Antwort hier]

2) Wo wurde die aktuelle Version der Maßnahme erprobt?
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ Laborbedingungen	☐ professioneller Einsatz	☐ Massenmarkt	1	3	5

[bitte begründen Sie Ihre Antwort hier]

3) Existieren vergleichbare Maßnahmen am Markt?
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ nein	☐ wenige	☐ viele	1	3	5

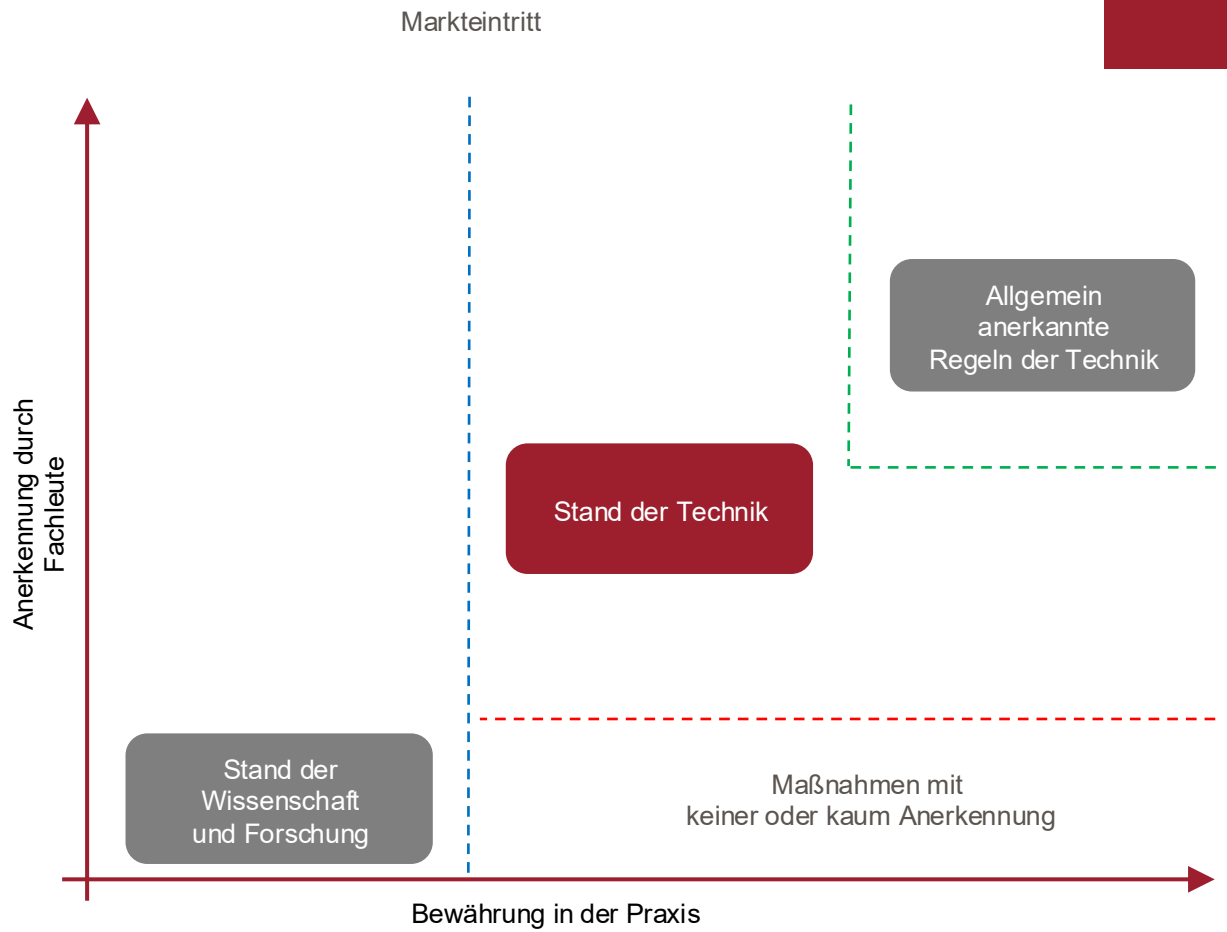
[bitte begründen Sie Ihre Antwort hier]

4) Wie oft wird die Maßnahme herstellerseitig konzeptionell aktualisiert?
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ häufiger als 1/Jahr	☐ jährlich	☐ seltener	1	3	5

[bitte begründen Sie Ihre Antwort hier]

Durchschnitt



HK2
Rechtsanwälte

Technical Guideline BSI TR-03183: Cyber Resilience Requirements for Manufacturers and Products

Part 2: Software Bill of Materials (SBOM)

HK2

BGB

HK2 Rechtsanwälte

Bürgerliches Gesetzbuch (BGB)
§ 327e Produktmangel

(1) Das digitale Produkt ist frei von Produktmängeln, wenn es zur maßgeblichen Zeit nach den Vorschriften dieses Untertitels den subjektiven Anforderungen, den objektiven Anforderungen und den Anforderungen an die Integration entspricht. Soweit nachfolgend nicht anders bestimmt, ist die maßgebliche Zeit der Zeitpunkt der Bereitstellung nach § 327b. Wenn der Unternehmer durch den Vertrag zu einer fortlaufenden Bereitstellung über einen Zeitraum (dauerhafte Bereitstellung) verpflichtet ist, ist der maßgebliche Zeitraum der gesamte vereinbarte Zeitraum der Bereitstellung (Bereitstellungszeitraum).

(3) Das digitale Produkt entspricht den objektiven Anforderungen, wenn

1. es sich für die gewöhnliche Verwendung eignet,
2. es eine Beschaffenheit, einschließlich der Menge, der Funktionalität, der Kompatibilität, der Zugänglichkeit, der Kontinuität und der Sicherheit aufweist, die bei digitalen Produkten derselben Art üblich ist und die der Verbraucher unter Berücksichtigung der Art des digitalen Produkts erwarten kann,

HK2

Wirkung von KI im IT-Sicherheitsrecht - *vertikal*

1. KI-Einsatz *für* IT-Sicherheit wird zunehmend zur Maßnahme gemäß dem **Stand der Technik**.

2. Wenn IT-sicherheitsrelevante Fehlerminimierung bei IT-Produkten durch einen verfügbaren KI-Einsatz möglich und ihrerseits sicher ist, wird sie grds. nach den IT-Sicherheitsgesetzen als **angemessene und zumutbare Maßnahme** einzusetzen sein.

3. KI wird zum **Compliance-Faktor**.

4. **Aufsichtsbehörden** sollten Erwartungshaltung formulieren und beraten, wie KMU Sicherheit durch KI gewährleisten können.

5. **Review der IT-Sicherheitsgesetze** zur Frage, ob Technologieneutralität den Bedarf an positiven Regelungen zum KI-Einsatz schlägt.

-

Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz - KRITISDachG)
§ 13 Resilienzpflichten der Betreiber kritischer Anlagen; Resilienzplan

(1) Der Betreiber kritischer Anlagen ist verpflichtet, nach Maßgabe der Absätze 2 und 3 Maßnahmen zur Gewährleistung seiner Resilienz zu treffen, um

1. das Auftreten von Vorfällen zu verhindern,
2. einen angemessenen physischen Schutz von Liegenschaften und kritischen Anlagen zu gewährleisten,
3. auf Vorfälle zu reagieren, sie abzuwehren und die negativen Auswirkungen solcher Vorfälle zu begrenzen und
4. nach Vorfällen die zügige Wiederherstellung der kritischen Dienstleistung zu gewährleisten.

Fokus der Diskussion auf Flugdrohnen.

Künftig Anschläge durch/ auf

- Über-/ Unterwasserdrohnen
- selbst-balancierende Roboter
- autonom fahrende Pkw/ Lkw
- dezentrale Verbrauchergeräte
- …

HK2

Wirkung von KI im IT-Sicherheitsrecht - *horizontal*

1. Wenn IT-sicherheitsrelevante Fehlerminimierung von IT-Produkten durch einen verfügbaren KI-Einsatz möglich und ihrerseits sicher ist, verändert das die **objektive Erwartbarkeit von Software-Qualität**.

2. Einsatz von KI wird folglich relevant für den **Mangelbegriff** und die **Gewährleistung**.

3. Wenn KI-Einsatz für IT-Sicherheit vertikal gefordert ist, wäre sie durch den Auftraggeber auch *horizontal* **in der Lieferkette zu vereinbaren**.

HK2
Rechtsanwälte

… bald Rechtsgeschichte

Risiko	Risikobewertung nach Ziff. (…)	Behebungsfrist
Softwareschwachstellen	**kaum kritisch**	Es besteht keine Verpflichtung zur Behebung
	weniger kritisch	168 Kalendertage
	mittel kritisch	84 Kalendertage
	hoch kritisch	21 Kalendertage

HK2

Und die Anwaltschaft?

HK2
Rechtsanwälte

Kontakt

linkedin.com/in/karstenbartels

www.hk2.eu

www.comtection.de

Karsten U. Bartels LL.M.*

- Rechtsanwalt/ Partner bei HK2
- Geschäftsführer HK2 Comtection GmbH
- Lehrbeauftragter für IT-Sicherheitsrecht, Ludwig-Maximilians-Universität München
- Stellv. Vorstandsvorsitzender Bundesverband IT-Sicherheit e. V. (TeleTrusT)
- Leiter Arbeitsgruppe IT-Sicherheitsrecht Bundesverband IT-Sicherheit e. V. (TeleTrusT)
- Zert. Datenschutzbeauftragter (TÜV)

*Rechtsinformatik