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

TeleTrusT-"IT-Sicherheitsrechtstag" 2024

Berlin, 25.09.2024

NIS-2-Umsetzungsgesetz im Vertragsverhältnis: Weitergabe von IT-Sicherheitspflichten

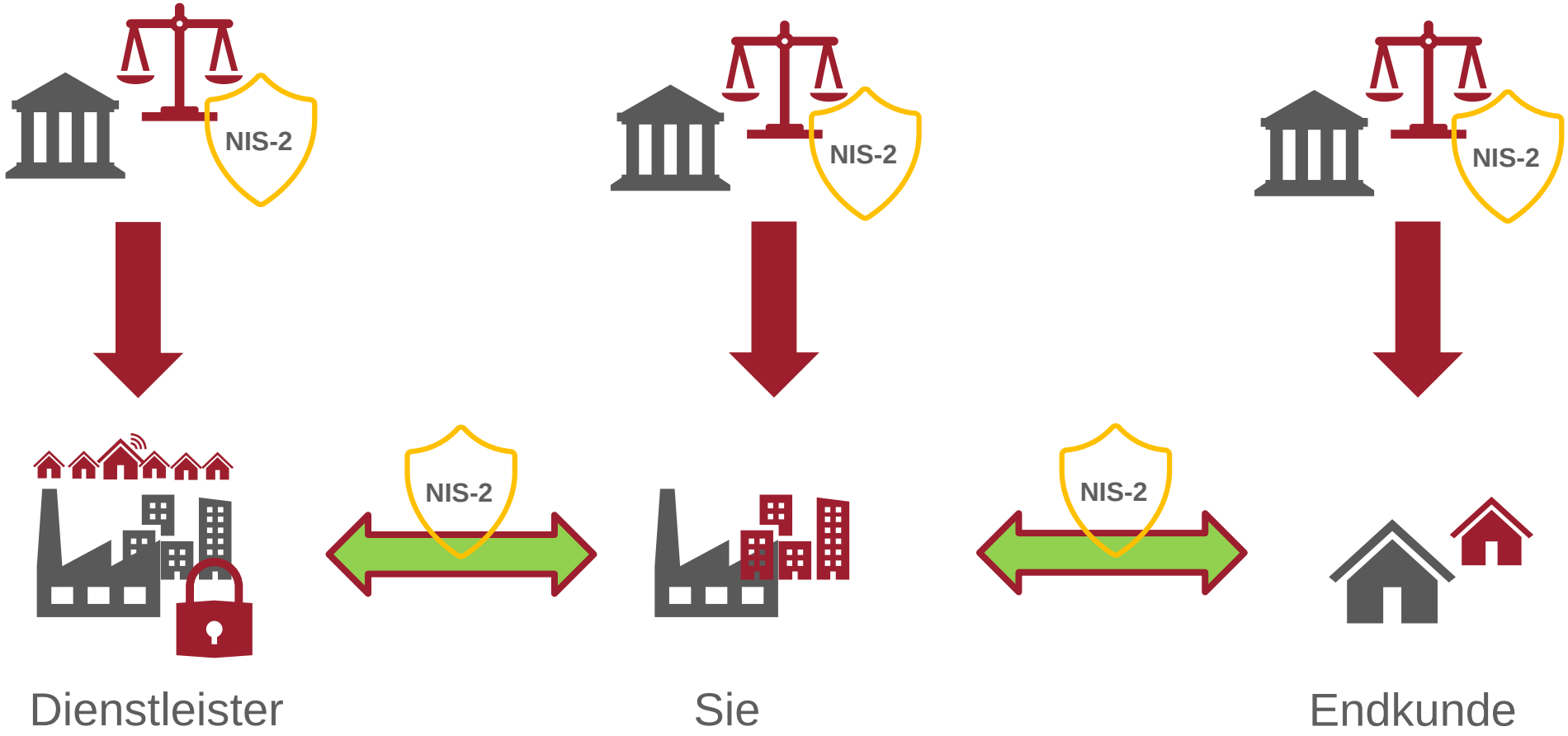
Rechtsanwalt Karsten U. Bartels LL.M.

Stellv. Vorstandsvorsitzender TeleTrusT
Leiter AG IT-Sicherheitsrecht
HK2 Rechtsanwälte


HK2
IT- und Datenrecht
Technik-Recht
IT-Sicherheitsrecht
Datenschutzrecht

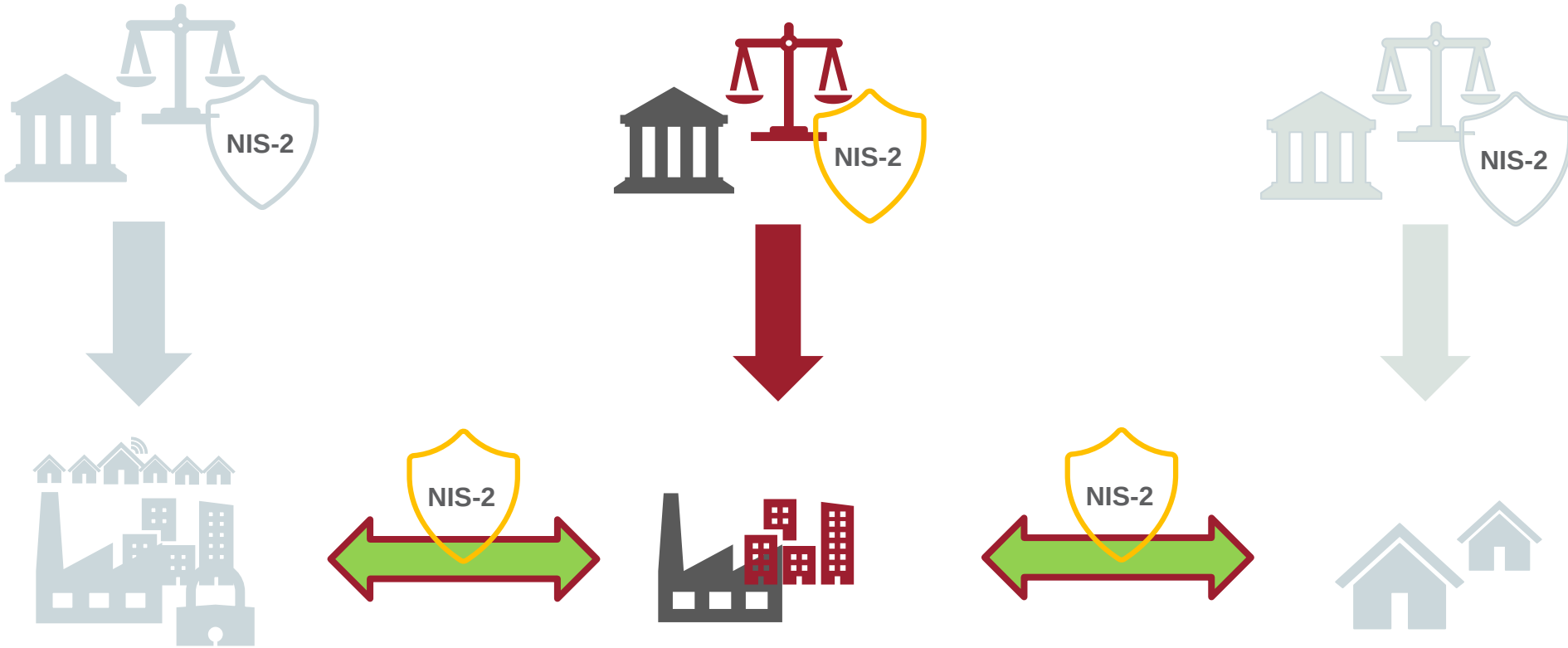
HK2
Rechtsanwälte

Vertikale Pflichten. Horizontale Pflichten.



HK2
Rechtsanwälte

Vertikale Pflichten. Horizontale Pflichten.



HK2
Rechtsanwälte

IT-Compliance durch Technik, Organisation + Recht

Verträge zur IT-Sicherheit

Verträge zur IT-Sicherheit

Dienstleister

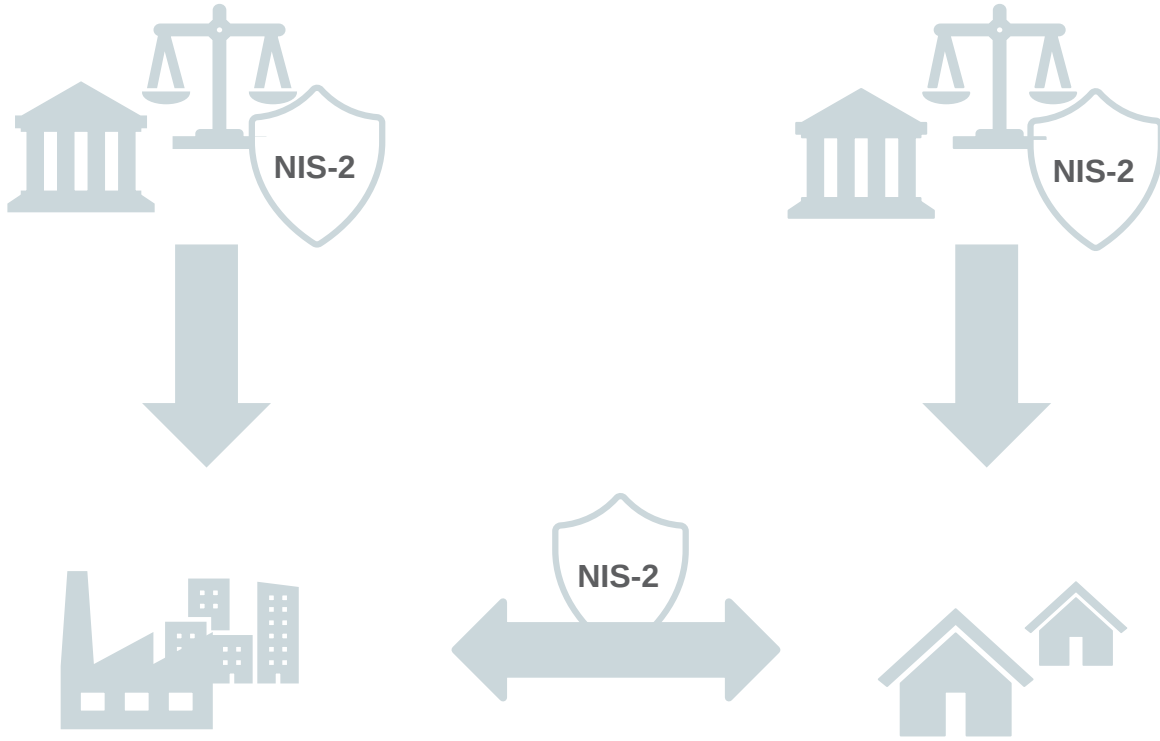
Sie

Endkunde

HK2 Rechtsanwälte

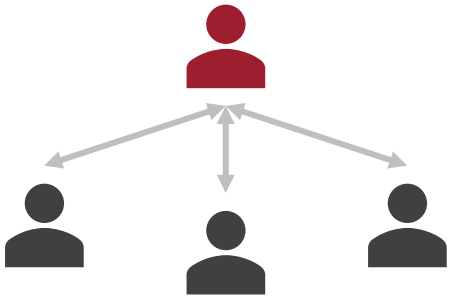
Verträge zur IT-Sicherheit

- Leistungsverträge
- Individuelle Verträge/ AGB
- Service Level Agreements
- AV-Vereinbarungen
- NDA
- Weitere Vereinbarungen über IT-Sicherheitsleistungen
- betrifft ggf. Geschäftsmodell

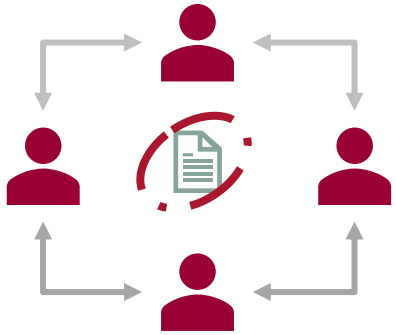


HK2
Rechtsanwälte

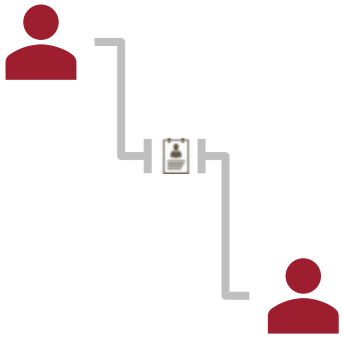
IT-Sicherheitsvereinbarung: Ist ./. Soll



Auftragsverarbeitung



Joint controllers



getrennt Verantwortliche

KRITIS-Kontext

HK2
Rechtsanwälte

Zweck eines Vertrages

- Einwirkung auf Vertragspartner
  - Sicherstellung des Verhaltens (rechtliche Sicht)
  - Schaffung von Vertrauen durch Einigung (psychologische Sicht)
- Rechte begründen/ ändern
  - Schaffung von Ansprüchen
  - Rechtsgrundlage zum Abweichen von gesetzlicher Vorgabe
- Klarstellen
  - Bestimmung der Pflichten/ Leistung: Inhalte
  - Rechtsicherheit
  - Sicherung eigener Rechte
  - Strukturierung der Leistungserbringung
- Organisieren
  - Risikomanagement
  - Widerspruchsfreie Darstellung des Inhalts und Ablaufs des Projekts

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

HK2
Rechtsanwälte

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

Präambel

HK2
Rechtsanwälte

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

Präambel

1. Begriffsbestimmungen

HK2 Rechtsanwälte

Schwachstelle

Art. 6 Ziff. 15 NIS-2-Richtlinie (RL 2022/2555/EU)

„Schwachstelle“ ist eine **Schwäche**, **Anfälligkeit** oder **Fehlfunktion** von IKT-Produkten oder IKT-Diensten, die bei einer Cyberbedrohung ausgenutzt werden kann.

§ 2 Nr. 38 NIS2UmsuCG-E

„Schwachstelle“ [ist] eine **Eigenschaft** von IKT-Produkten oder IKT-Diensten, die von Dritten ausgenutzt werden kann, um sich **gegen den Willen des Berechtigten Zugang** zu den IKT-Produkten oder IKT-Diensten zu verschaffen oder die **Funktion** der IKT-Produkte oder IKT-Dienste zu beeinflussen.

HK2 Rechtsanwälte

IT-Sicherheitsvorfall

Art. 6 Ziff. 6 NIS-2-Richtlinie (RL 2022/2555/EU) bzw. § 2 Nr. 40 NIS2UmsuCG-E

„Sicherheitsvorfall“ ein **Ereignis**, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter **Daten** oder der **Dienste**, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, **beeinträchtigt**.

HK2
Rechtsanwälte

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

Präambel

1. Begriffsbestimmungen
2. Geltungs- und Anwendungsbereich

HK2
Rechtsanwälte

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

Präambel

1. Begriffsbestimmungen
2. Geltungs- und Anwendungsbereich
3. Leistungen

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

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 zwischen den einzelnen Einrichtungen und ihren 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-E

6. Konzepte und Verfahren zur Bewertung der **Wirksamkeit** von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
7. grundlegende Verfahren im Bereich der **Cyberhygiene** und **Schulungen** im Bereich der Cybersicherheit
8. Konzepte und Verfahren für den Einsatz von **Kryptografie** und **Verschlüsselung**
9. Sicherheit des **Personals**, Konzepte für die **Zugriffskontrolle** und **Management von Anlagen**
10. Verwendung von Lösungen zur Multi-Faktor-**Authentifizierung** oder kontinuierlichen Authentifizierung, gesicherte **Sprach-, Video- und Textkommunikation** sowie gegebenenfalls gesicherte **Notfallkommunikationssysteme** innerhalb der Einrichtung.

Rechtliche Prüfung, § 30 Abs. 2 BSIG-E

HK2 Rechtsanwälte

	Risikomanagementmaßnahme	Rechtliche Prüfung betrifft u. a.	Beispiele
1	Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik		
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 zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern	Prüfung der Verträge über IT-Leistungen mit Sicherheitsbezügen: - Beschaffung/ Einkauf von Software (SaaS/ Cloud/ On Premises, …) - SLA/ Wartung/ Pflege - Endkundenvertrag - Datenschutzvereinbarungen	Qualität und Aktualität der Vertragsmuster: - Umgang mit Stand der Technik - Leistungsbeschreibung - Durchsetzbarkeit der Sicherheitsleistungen - Anpassbarkeit - IT-Compliance-Klausel - IT-Sicherheit als Neben-/ Hauptleistung - Umgang mit fremden AGB
5	Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen		
6	Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik		
7	Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik		
8	Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung		
9	Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das Management von Anlagen		
10	Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie ggfs. gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung		

Weitere besondere Pflichten für Betreiber kritischer Anlagen §§ 31, 41 BSIG-E

- Aufwändigere Maßnahmen grds. verhältnismäßig, § 31 Abs. 1 BSIG-E

- Systeme zur Angriffserkennung, § 31 Abs. 2 BSIG-E
  - definiert in § 2 Nr. 41 BSIG-E
  - Identifizierung von Bedrohungen
  - Stand der Technik, aber verhältnismäßiger Aufwand

- Einsatz kritischer Komponenten, § 41 BSIG-E
  - definiert in § 2 Nr. 23 BSIG-E
  - Anzeigepflicht an BSI vor Einsatz der Komponente
  - Untersagung durch BSI innerhalb von 2 Monaten möglich
  - Einsatz nur bei Erklärung über Vertrauenswürdigkeit durch Hersteller der Komponente (Garantieerklärung)

Schwachstellen-Management

HK2 Rechtsanwälte

Schwachstellen

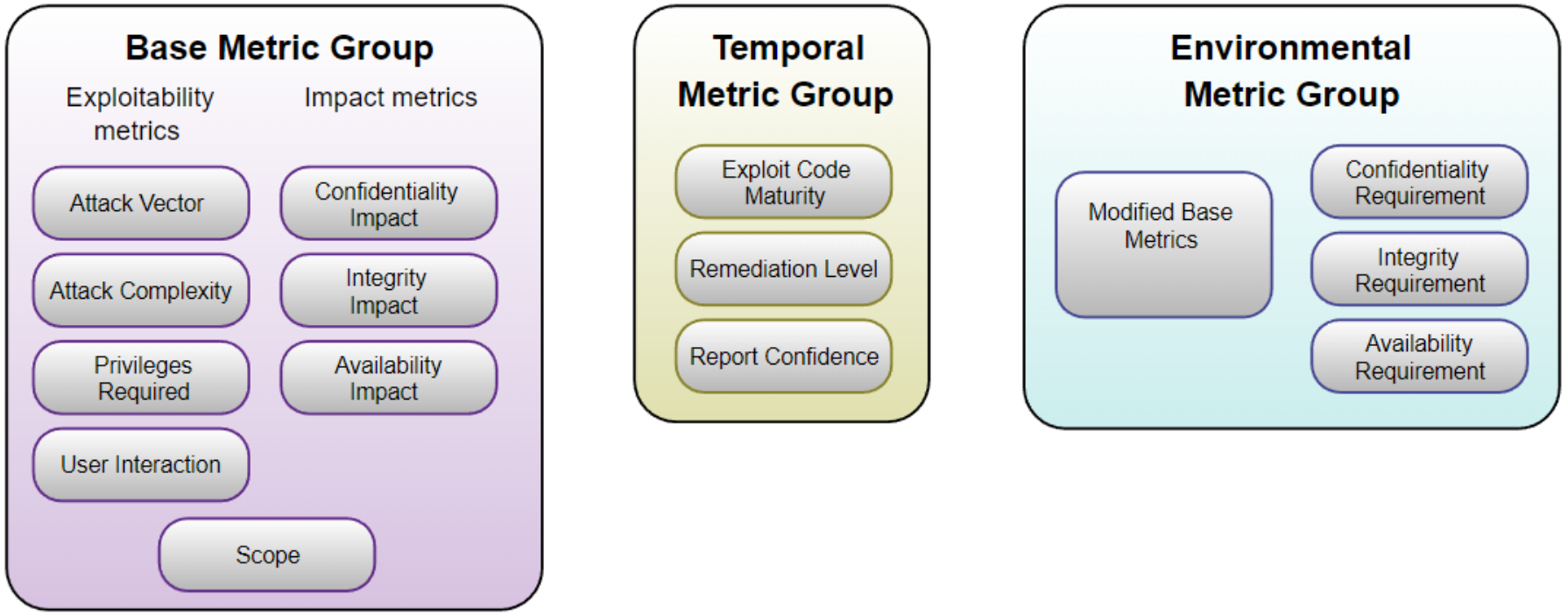
- erkennen
- bewerten + priorisieren
- beheben/ zeitweise abmildern
- reporten

HK2 Rechtsanwälte

Bewertung

- auf Basis von Schutzbedarfsfeststellung + Kritikalität der Schwachstelle
- Schutzbedarf
  - individuell festgelegt
  - nach branchenspezifischem Sicherheitsstandard
  - nach ISO 27xxx oder BSI IT Grundschutz?
- Kritikalität der Schwachstelle
  - z. B. Common Vulnerability Scoring System (CVSS)

Bsp. Methode zur Schwachstellenbewertung
Common Vulnerability Scoring System (CVSS)



https://www.first.org/cvss/v3.1/specification-document

Schwachstellenmanagement gemäß Art. 10 Abs. 6 i. V. m. Anhang I Abschnitt 2 Cyber Resilience Act-E (COM(2022) 454 final)

HK2 Rechtsanwälte

2. ANFORDERUNGEN AN DIE BEHANDLUNG VON SCHWACHSTELLEN

Die Hersteller der Produkte mit digitalen Elementen müssen

(1) Schwachstellen und Komponenten des Produkts ermitteln und dokumentieren, u. a. durch Erstellung einer Software-Stückliste in einem gängigen maschinenlesbaren Format, aus der zumindest die obersten Abhängigkeiten des Produkts hervorgehen;

(2) im Hinblick auf die Risiken im Zusammenhang mit den Produkten mit digitalen Elementen unverzüglich Schwachstellen behandeln und beheben, unter anderem durch Bereitstellung von Sicherheitsaktualisierungen;

(3) die Sicherheit des Produkts mit digitalen Elementen regelmäßig und wirksam testen und überprüfen;

(4) sobald eine Sicherheitsaktualisierung bereitgestellt worden ist, Informationen über beseitigte Schwachstellen veröffentlichen, einschließlich einer Beschreibung der Schwachstellen mit Angaben, anhand deren die Nutzer das betroffene Produkt mit digitalen Elementen, die Auswirkungen der Schwachstellen und ihre Schwere erkennen können, sowie Informationen, die den Nutzern helfen, die Schwachstellen zu beheben;

(5) eine Strategie für die koordinierte Offenlegung von Schwachstellen aufstellen und umsetzen;

(6) Maßnahmen ergreifen, um den Austausch von Informationen über mögliche Schwachstellen in ihrem Produkt mit digitalen Elementen und darin enthaltenen Komponenten Dritter zu erleichtern, und dazu u. a. eine Kontaktadresse für die Meldung der in dem Produkt mit digitalen Elementen entdeckten Schwachstellen angeben;

(7) Mechanismen für die sichere Verbreitung von Aktualisierungen für Produkte mit digitalen Elementen bereitstellen, damit ausnutzbare Schwachstellen rechtzeitig behoben oder eingedämmt werden;

(8) dafür sorgen, dass Sicherheits-Patches oder -Aktualisierungen, die zur Bewältigung festgestellter Sicherheitsprobleme zur Verfügung stehen, unverzüglich und kostenlos verbreitet werden, zusammen mit Hinweisen und einschlägigen Informationen, auch über zu treffende mögliche Maßnahmen.

HK2
Rechtsanwälte

Schwachstellenmanagement sollte auch umfassen:

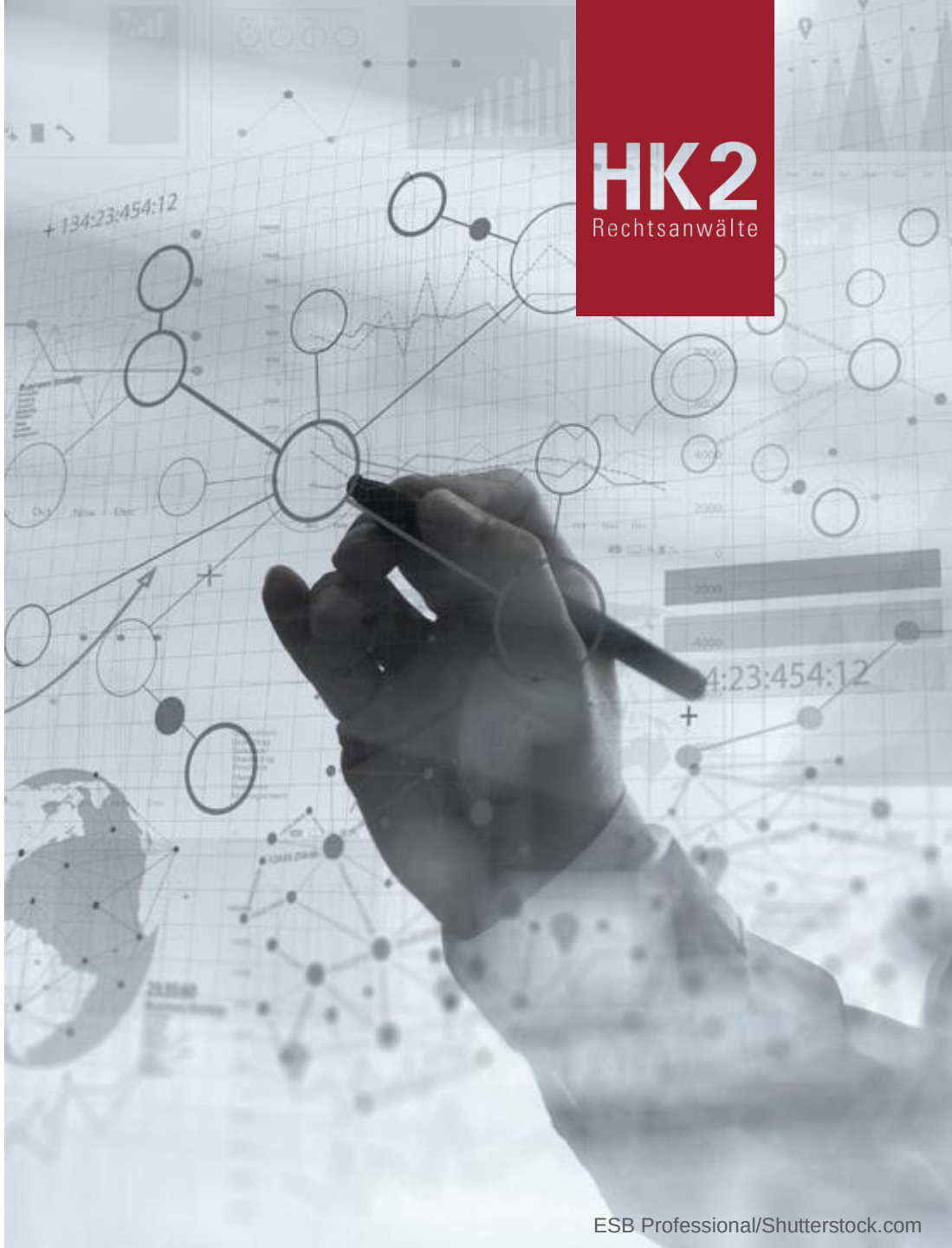
Cyberbedrohungen und deren Entschärfung.

Incident Management

- Routine-Untersuchung
- forensische Maßnahmen
- Beschreibung nach vereinbartem Schema
- Verfügbarkeit/ Unterstützung für/ bei Abhilfe

Beispiele wichtiger TOM

- SBOM (Software Bill of Materials) v. a. gegen die aktuellen Supply-Chain-Attacken
- SIEM (Security Information and Event Management)/ Log Management
- Geo-Redundanzen gem. Standort-Kriterien für RZ nach BSI
- Zero-Trust-Maßnahmen
- Kryptoagilität sicherstellen
- *Dark Web Monitoring*
- …



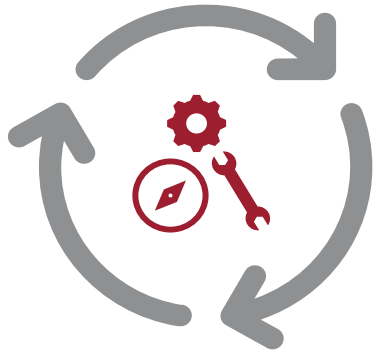
ESB Professional/Shutterstock.com

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

Präambel
1. Begriffsbestimmungen
2. Geltungs- und Anwendungsbereich
3. Leistungen
4. Leistungserbringung nach dem Stand der Technik

Technische und organisatorische Maßnahmen
§ 30 Abs. 2 BSIG-E

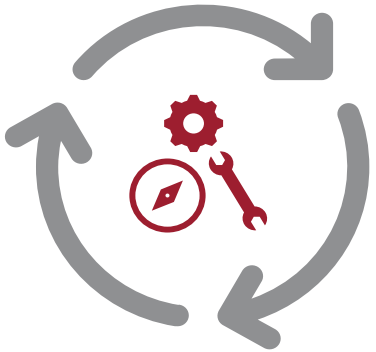
„Maßnahmen nach Absatz 1 ***sollen*** *den* ***Stand der Technik einhalten****, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen: …“*



Stand der Technik

HK2
Rechtsanwälte

Beim Stand der Technik handelt es sich um die im Waren- und Dienstleistungsverkehr **verfügbaren** Verfahren, Einrichtungen oder Betriebsweisen, deren Anwendung die Erreichung der jeweiligen **gesetzlichen Schutzziele** am **wirkungsvollsten gewährleisten** kann.

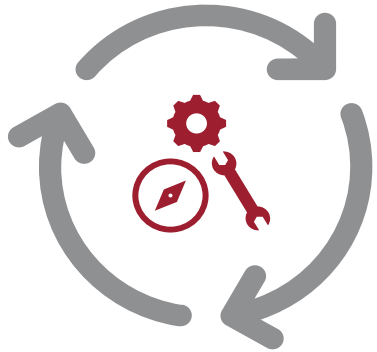


[Bartels/ Backer/ Schramm: Der „Stand der Technik“ im IT-Sicherheitsrecht - Wirkung des Verweisungsbegriffs und Lösungsansätze zur legislativen Verwendung, Tagungsband 15. Deutscher IT-Sicherheitskongress, S. 503]

HK2
Rechtsanwälte

Kurz:

Stand der Technik = die am Markt verfügbare Bestleistung zur Erreichung eines gesetzlichen IT-Sicherheitszieles



HK2
Rechtsanwälte

www.stand-der-technik-security.de/, Stand: 12.09.2024.

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

Präambel
1. Begriffsbestimmungen
2. Geltungs- und Anwendungsbereich
3. Leistungen
4. Leistungserbringung nach dem Stand der Technik

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

Präambel
1. Begriffsbestimmungen
2. Geltungs- und Anwendungsbereich
3. Leistungen
4. Leistungserbringung nach dem Stand der Technik
5. Weitere Anforderungen an Leistungserbringung
6. Compliance- und KRITIS-Zulieferer-Verpflichtungen

Meldepflichten, § 32 BSIG-E

- Betrifft **besonders wichtige und wichtige Einrichtungen**
- Meldepflicht an Meldestelle bei **erheblichen Sicherheitsvorfällen**
  - Sicherheitsvorfall, § 2 Nr. 40 BSIG-E
  - Erheblicher Sicherheitsvorfall, § 2 Nr. 11 BSIG-E
- Mehrstufiges Meldeverfahren in Abs. 1 (s. sogleich)
- Zusätzliche Meldepflicht für KRITIS-Betreiber in Abs. 3

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

Präambel
1. Begriffsbestimmungen
2. Geltungs- und Anwendungsbereich
3. Leistungen
4. Leistungserbringung nach dem Stand der Technik
5. Weitere Anforderungen an Leistungserbringung
6. Compliance- und KRITIS-Zulieferer-Verpflichtungen
7. Dokumentationen

Nachweispflichten für Betreiber kritischer Anlagen, § 39 BSIG-E

- Nachweis der Erfüllung der Anforderungen nach §§ 30 Abs. 1 S. 1 , 31 Abs. 1, Abs. 2 S. 1 BSIG-E für KRITIS-Betreiber
- Frühestens **drei Jahre** nach erstmaliger/ erneuter Geltung als KRITIS, anschließend alle drei Jahre
- Kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen
- Übermittlung an BSI, ggf. Nachweis auch über die Beseitigung aufgetretener Mängel

Achtung: Nachweispflichten (on demand) auch für wichtige und besonders wichtige Einrichtungen

- § 61 Abs. 3, Aufsichts- und Durchsetzungsmaßnahmen für **besonders wichtige Einrichtungen**:
  - BSI kann gegenüber besonders wichtigen Einrichtungen frühestens **drei Jahre** nach Inkrafttreten des Gesetzes die Vorlage von Nachweisen über die Erfüllung bestimmter Pflichten anordnen

- Nach § 62 BSIG-E hat BSI gegenüber **wichtigen Einrichtungen** die Rechte gemäß § 61
  - Voraussetzung: Tatsachen rechtfertigen die Annahme, dass Pflichten aus § 61 nicht oder nicht richtig umgesetzt werden

HK2 Rechtsanwälte

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

Präambel
1. Begriffsbestimmungen
2. Geltungs- und Anwendungsbereich
3. Leistungen
4. Leistungserbringung nach dem Stand der Technik
5. Weitere Anforderungen an Leistungserbringung
6. Compliance- und KRITIS-Zulieferer-Verpflichtungen
7. Dokumentationen
8. Zertifikate, Testate und Audits
9. Unterbeauftragungen
10. Ansprechpartner, Weisungen, Mitarbeiter
11. Geheimhaltung, Datenschutz

Bundesamt
für Sicherheit in der
Informationstechnik

Merkblatt zum sicheren Informationsaustausch mit dem Traffic Light Protocol (TLP), Version 2.0

Das Traffic Light Protocol (TLP) ist eine standardisierte Vereinbarung zum Austausch schutzwürdiger aber nicht formell eingestufter Informationen. Alle Dokumente werden in TLP-Stufen eingeteilt, die die Bedingungen für ihre Weitergabe regeln.

Das TLP regelt nicht den Schutz staatlich geheimzuhaltender Informationen. Dieser ist in der Verschlusssachenanweisung des Bundes[1] geregelt.

Die vom BSI verwendete TLP-Version 2.0 basiert auf der Definition der TLP Version 2.0[2] des „Forum of Incident Response and Security Teams" (FIRST).

Im TLP-Informationsaustausch können folgende Rollen unterschieden werden:

- **Informationsersteller**
- **Verteiler** (z. B. BSI, CERT, SPOC, Verbände)
- **Empfänger** (z. B. Behörden, Betreiber, Unternehmen),
- ggf. **Partner** des Empfängers (i. d. R. vertraglich verbundene Organisationen, entweder als Dienstleister oder als Kunden)

Die Einschränkungen zur Weitergabe betreffen Verteiler, Empfänger und Partner.

Das TLP dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtlicher Belange zur Folge haben. **Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.**

Durch die Unterschrift auf der TLP-Verpflichtung erklären natürliche und juristische Personen ihre Verpflichtung, die Regeln des TLP einzuhalten. Diese Verpflichtung endet nicht mit ihrer Zugehörigkeit zu einer bestimmten am TLP-basierten Informationsaustausch teilnehmenden Organisation. Eine Verpflichtung stellvertretend für den eigenen Verantwortungs- oder Zuständigkeitsbereich ist möglich. Werden Funktionspostfächer oder Gruppenrufnummern der Organisation angegeben, sind alle potenziellen Empfänger durch den Unterzeichner auf die Einhaltung des TLP zu belehren.

[1] Verschlusssachenanweisung, www.bsi.bund.de/dok/6602050
[2] Traffic Light Protocol – FIRST Standards Definitions and Usage Guidance 2.0, www.first.org/tlp

TLP:CLEAR

Die TLP-Stufen

TLP:CLEAR **Unbegrenzte Weitergabe**

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Hinweis: TLP:CLEAR entspricht der Kennzeichnung TLP:WHITE der früheren Version 1.0 des TLP.

TLP:GREEN **Organisationsübergreifende Weitergabe**

Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe, wie beispielsweise Angehörige der Cybersecurity-Community, angehören.

TLP:AMBER **Eingeschränkte interne und organisationsübergreifende Weitergabe**

Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisation gilt das Prinzip „Kenntnis nur, wenn nötig". Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen, diese müssen eingehalten werden.

TLP:AMBER+STRICT **Eingeschränkte interne Weitergabe**

Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers, jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig". Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen, diese müssen eingehalten werden.

TLP:RED **Persönlich, nur für bekannte Empfänger**

Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.

HK2 Rechtsanwälte

Merkblatt zum sicheren Informationsaustausch mit dem Traffic Light Protocol (TLP), Version 2.0 (allianz-fuer-cybersicherheit.de)

HK2 Rechtsanwälte

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

Präambel
1. Begriffsbestimmungen
2. Geltungs- und Anwendungsbereich
3. Leistungen
4. Leistungserbringung nach dem Stand der Technik
5. Weitere Anforderungen an Leistungserbringung
6. Compliance- und KRITIS-Zulieferer-Verpflichtungen
7. Dokumentationen
8. Zertifikate, Testate und Audits
9. Unterbeauftragungen
10. Ansprechpartner, Weisungen, Mitarbeiter
11. Geheimhaltung, Datenschutz

HK2 Rechtsanwälte

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

Präambel
1. Begriffsbestimmungen
2. Geltungs- und Anwendungsbereich
3. Leistungen
4. Leistungserbringung nach dem Stand der Technik
5. Weitere Anforderungen an Leistungserbringung
6. Compliance- und KRITIS-Zulieferer-Verpflichtungen
7. Dokumentationen
8. Zertifikate, Testate und Audits
9. Unterbeauftragungen
10. Ansprechpartner, Weisungen, Mitarbeiter
11. Geheimhaltung, Datenschutz
12. Vertragsstrafen
13. Änderungen der Leistungspflichten während der Laufzeit (Change Request)
14. Überleitungskooperation
15. Change of control
16. Auslegung
17. Anlagen

Sonderregeln für MSP, MSSP, CSP und andere!

Durchführungsrechtsakt-E der EU Kommission
Entwurf vom 27.06.2024

HK2 Rechtsanwälte

Ref. Ares(2024)4640447 - 27/06/2024

EUROPEAN COMMISSION

Brussels, XXX
[…](2024) XXX draft

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of XXX

laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

Significant incidents with regard to managed service providers and managed security service providers

With regard to managed service providers and managed security service providers, an incident shall be considered significant under Article 3 where it fulfils one or more of the following criteria:

(a) one or more of the managed services or managed security services is completely unavailable for more than 10 minutes;

(b) for one or more of the managed services or managed security services provided, the customer service level agreement is not met for more than 5 % of the service users in the Union, or for more than 1 million of the service users in the Union, whichever number is smaller, for a duration of more than one hour;

(c) the availability of one or more of the managed or managed security services of a provider that has no customer service level agreement in place is impacted by the incident;

(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the managed service or the managed security service is compromised as a result of a suspectedly malicious action,

(e) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the managed service or the managed security service, is compromised with an impact on more than 5 % of the managed service or the managed security service users in the Union.

DRAFT

Durchführungsrechtsakt der EU Kommission – Annex-E
Entwurf vom 27.06.2024

HK2 Rechtsanwälte

Ref. Ares(2024)4640447 - 27/06/2024

EUROPEAN COMMISSION

Brussels, XXX
[…](2024) XXX draft

ANNEX

ANNEX

to the

Commission Implementing Regulation

laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

5.1. Supply chain security policy

5.1.1. For the purpose of Article 21(2), point (d) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply a supply chain security policy which governs the relations with their direct suppliers and service providers in order to mitigate the identified risks to the security of network and information systems. In the supply chain security policy, the relevant entities shall identify their role in the supply chain and communicate it to their direct suppliers and service providers.

5.1.2. As part of the supply chain security policy referred to in point 5.1.1, the relevant entities shall lay down criteria to select and contract suppliers and service providers. Those criteria shall include the following:

(a) the cybersecurity practices of the suppliers and service providers, including their secure development procedures;

(b) the ability of the suppliers and service providers to meet cybersecurity specifications set by the entities;

(c) the overall quality and resilience of ICT products and ICT services and the cybersecurity risk-management measures embedded in them, including the risks and classification level of the ICT products and ICT services;

(d) the ability of the relevant entities to diversify sources of supply and limit vendor lock-in.

HK2
Rechtsanwälte

§ 2 BSIG-E

*25. „**Managed Security Service Provider**“ oder „MSSP“ ein MSP, der Unterstützung für Tätigkeiten im Zusammenhang mit dem Risikomanagement im Bereich der Cybersicher-heit durchführt oder erbringt;*

*26. „**Managed Service Provider**“ oder „MSP“ ein Anbieter von Diensten im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, -Netzen, -Infrastruktur, -Anwendungen oder jeglicher anderer Netz- und Informations-systeme durch Unterstützung oder aktive Verwaltung in den Räumlichkeiten der Kunden oder aus der Ferne;*

HK2
Rechtsanwälte

§ 30 BSIG-E

(3) Der von der Europäischen Kommission gemäß Artikel 21 Absatz 5 Unterabsatz 1 der NIS-2-Richtlinie erlassene Durchführungsrechtsakt zur Festlegung der technischen und methodischen Anforderungen an die in Absatz 1 genannten Maßnahmen in Bezug auf DNS-Diensteanbieter, Top Level Domain Name Registries, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Content Delivery Networks, Managed Service Provider, Managed Security Service Provider, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter hat für die vorgenannten Einrichtungsarten Vorrang.

(4) Sofern die Europäische Kommission einen Durchführungsrechtsakt gemäß Artikel 21 Absatz 5 Unterabsatz 2 der NIS-2-Richtlinie erlässt, in dem die technischen und methodischen Anforderungen sowie erforderlichenfalls die sektoralen Anforderungen der in Absatz 2 genannten Maßnahmen festgelegt werden, so gehen diese Anforderungen den in Absatz 2 genannten Maßnahmen vor, soweit sie diesen entgegenstehen.

(5) Sofern die Durchführungsrechtsakte der Europäischen Kommission nach Artikel 21 Absatz 5 der NIS-2-Richtlinie keine abschließenden Bestimmungen über die technischen und methodischen Anforderungen sowie erforderlichenfalls über die sektoralen Anforderungen an die in Absatz 2 genannten Maßnahmen in Bezug auf besonders wichtige Einrichtungen und wichtige Einrichtungen enthalten, können diese Bestimmungen vom Bundesministerium des Innern und Heimat im Benehmen mit den jeweils betroffenen Ressorts durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, unter Berücksichtigung der möglichen Folgen unzureichender Maßnahmen sowie der Bedeutung bestimmter Einrichtungen präzisiert und erweitert werden.

HK2
Rechtsanwälte

Auswirkungen auf Verträge zur IT-Sicherheit nach DSGVO

AV-Vereinbarung nach Art. 28 Abs. 3 DSGVO

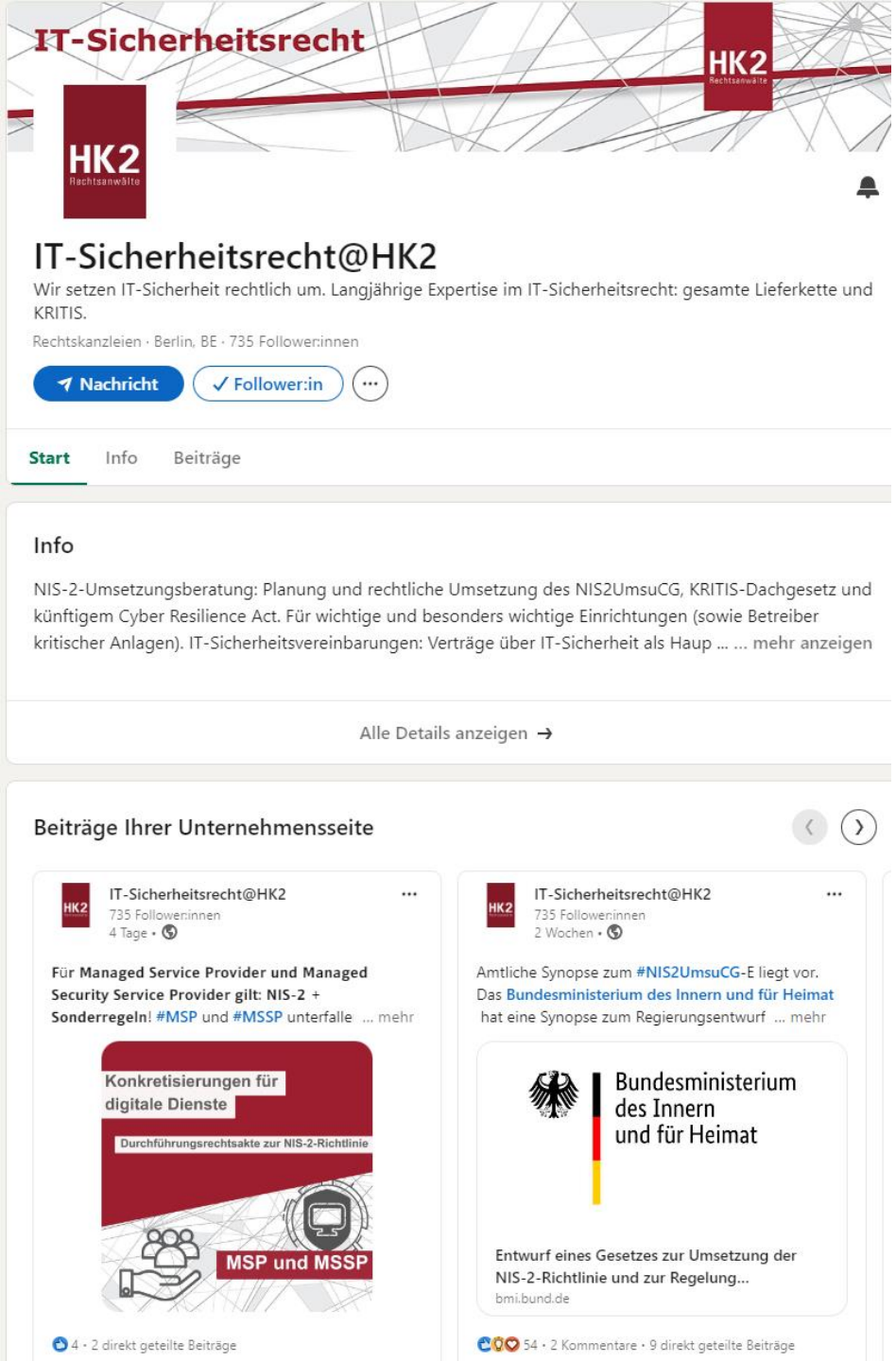
HK2 Rechtsanwälte

a) „… nur auf dokumentierte Weisung des Verantwortlichen verarbeitet …“
b) Gewährleistung von Vertraulichkeitsverpflichtungen oder gesetzliche Verschwiegenheitspflicht
c) alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift
d) „… Bedingungen für die Inanspruchnahme … eines weiteren Auftragsverarbeiters …“
e) Unterstützung des Verantwortlichen bei dessen Pflicht zur Beantwortung von Betroffenenanträgen
f) Unterstützung des Verantwortlichen bei dessen Einhaltung der Pflichten aus Art. 32 - 36
g) Löschung/ Rückgabe nach Abschluss der Verarbeitungsleistungen, sofern keine Verpflichtung zur Speicherung
h) Informationen zum Nachweis der Einhaltung von Art. 28 oder/ und Überprüfungen ermöglichen und unterstützen

HK2
Rechtsanwälte

IT-Sicherheitsvereinbarungen

… werden (immer) komplexer.
… haben selbst *state of the art* zu sein.
… entstehen und wirken interdisziplinär.



HK2 Rechtsanwälte

LinkedIn-Fokusseite

HK2
Rechtsanwälte

Kontakt

www.hk2.eu

www.comtection.de

linkedin.com/in/karstenbartels

Karsten U. Bartels LL.M.*

- Rechtsanwalt/ Partner bei HK2
- Geschäftsführer HK2 Comtection GmbH
- Lehrbeauftragter für IT-Sicherheitsrecht, Ludwig-Maximilians-Universität München
- Vorsitzender Arbeitsgemeinschaft IT-Recht (davit) im Deutschen Anwaltverein
- Stellv. Vorstandsvorsitzender Bundesverband IT-Sicherheit (TeleTrusT)
- Leiter AG IT-Sicherheitsrecht TeleTrusT
- Zert. Datenschutzbeauftragter (TÜV)

*Rechtsinformatik