Univ.-Prof. Dr. Robert Koch LL.M. (McGill)
Geschäftsführender Direktor des Seminars für Versicherungswissenschaft
Fakultät für Rechtswissenschaft

Umgang mit Silent Cyber Risks

754. Mitgliederversammlung des Versicherungswissenschaftlichen Vereins in Hamburg e.V.

12. Dezember 2019

Agenda

- Einführung in die Problematik
- Position der Aufsicht, Versicherer, versicherungsnehmenden Wirtschaft
- (Silent) Cyber Risks Map
- Deckung von (silent) CyberRisks in der Nicht-/PersonenV
- Umfang der Deckung von CyberRisks in der Cyber-Versicherung
- (Beschränkte) Nullstellung von CyberRisks in den traditionellen Sach- und Haftpflichtversicherungssparten
- Einführung cyberspezifischer Obliegenheiten in traditionelle Sach- und Haftpflichtversicherungssparten
- Ausblick/Bewertung

A. Einführung in die Problematik

Silent but deadly? How cyber risk is affecting your insurance

PRA action to protect insurers from unexpected exposure to cyber risk

Not addressing 'silent cyber' could lead to ratings downgrades, Fitch warns.

Munich Re: Versicherer müssen sich mit den Silent Cyber-Risiken in ihren herkömmlichen Policen beschäftigen.

'We have to look at cyber as a peril, not an insurance product' Mark Camillo, AIG


You became victim of the PETYA RANSOMWARE!
The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.
To purchase your key and restore your data, please follow these three easy steps:
1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:
http://petya37h5tbhyvki.onion/N19fvE
http://petya5koahtsf7sv.onion/N19fvE
Petya/NotPetya
3. Enter your personal decryption code there:
If you already purchased your key, please enter it below.
Key: _

A. Einführung in die Problematik

- Versicherte Schäden aus Petya/NotPetya sollen sich auf 3,3 Mrd. US-D Schäden belaufen – davon sollen ca. 90% auf traditionelle Deckungen zurückzuführen sein, vor allem Sach- und Betriebsunterbrechung.
- Deckung von Cyberrisiken in den traditionellen Versicherungssparten nicht ausdrücklich vorgesehen und im Pricing nicht berücksichtigt.

A. Einführung in die Problematik

- Deckung von Cyberrisiken in den traditionellen Versicherungssparten **nicht ausdrücklich vorgesehen** und im Pricing nicht berücksichtigt.

Silent Cyber Risks
oder
Non-affirmative Cyber Risks

A. Einführung in die Problematik

- Silent Cyber kein neues Problem/Phänomen!
- Diskussion um Sachqualität von Daten und Ersatzfähigkeit der Wiederherstellungskosten hat VR seit 2004 dazu veranlasst, aufzunehmen
  - in der Sachversicherung
    - Klarstellung, dass Daten keine Sachen sind
    - Sonderregelung für Ersatz von Kosten der Datenwiederherstellung
  - in der Haftpflichtversicherung
    - IT-Nutzungs-Ausschluss, der nicht an Personen- und Sachschäden anknüpft, sondern an Datenveränderung und daraus resultierende weitere Schäden

B. Position der Aufsicht

- **Dr. Frank Grund**, BaFin-Jahreskonferenz am 13.11.2018:

  „Gefahren gehen nicht nur von Hackern aus, die Daten stehlen und Institutionen lahmlegen können. **Gefahren schlummern möglicherweise auch im eigenen Versicherungsbestand – und zwar auf der Deckungsseite**. Risiken aus Verträgen, in denen eine Deckung von Cyber-Risiken **nicht explizit ein- oder ausgeschlossen** wird, nennt man **‚non-affirmative Cyber-Risiken**‘‘. Im Jahr 2019 wollen wir die Branche hierfür besonders sensibilisieren.“

B. Position der Aufsicht

- **BaFin-Abfrage** „non-affirmative“ Cyber-Risks als Teil des Aufsichtsprogrammes 2019 (Fristablauf 12/2019)
  - Ziel: **Sensibilisierung** der Versicherer in Bezug auf „non-affirmative“ Cyber-Risiken
  - **Identifizierung** der „non-affirmative“ Cyber-Risiken durch Versicherer
  - Bewertung bzw. **Quantifizierung** derartiger Risiken

B. Position der Aufsicht

- **Erste Erkenntnisse** aus der Abfrage
  - Nahezu **alle Versicherungszweige der Schadenversicherung** können betroffen sein.
  - Alle befragten VR berücksichtigen „non-affirmative“ Cyber-Risiken im Risikomanagement.
  - **Anzahl der identifizierten Schadensfälle** im Bereich "non-affirmative" Cyber-Risiken **gering**.
  - Jedoch Schwierigkeiten bei der Identifizierung eines Cyber-Vorfalls als schadenauslösendes Ereignis.

C. Position der Versicherer

- Bei Cybervorfällen häufig nicht klar, ob konventionelle Sach- oder Haftpflichtpolicen die Schäden abdecken. Deckung von Cyberrisiken in den wenigsten Verträgen explizit vorgesehen.
  - „Versteckte“, nicht explizit bezeichnete Cyber-Exponierungen führten dazu, dass Kunden nicht angemessen geschützt seien und allen Beteiligten – Kunden, Makler und Versicherer – die nötige Verlässlichkeit und Transparenz fehle.

C. Position der Versicherer

- New Underwriting Strategy: “Making noise about ‘silent’ cyber” (AGCS) → “Affirmative Cyber“-Strategie:
  - Klarstellung, wie CyberRisk in herkömmlichen Policen abgedeckt werden und für welche Szenarien spezielle CyberVersicherung notwendig.
  - Cyber-Deckung ist entweder explizit ein- oder ausgeschlossen. Silent Cyber darf es nicht geben. Der Kunde muss wissen, wie viel Deckung er effektiv zur Verfügung hat.

➡ Ausschluss (Nullstellung) von CyberRisks ggf. mit standardmäßigen Wiedereinschlüssen?

C. Position der Versicherer

- **Beispiel für Komplett-Ausschluss: Data Event Exclusion Clause (AVN 124, drafted by Lloyd's Market Association)**

  "This Policy does not cover **any loss, damage, expense or liability arising out of a Data Event**.

  Data Event means any access to, inability to access, loss of, loss of use of, damage to, corruption of, alteration to or disclosure of Data.

  Data means any information, text, figures, voice, images or any machine readable data, software or programs including any person's or organisation's confidential, proprietary or personal information."

C. Position der Versicherer

- **Bsp.: Ausschluss (Nullstellung)/Wiedereinschluss elektr. Datenaustausch/Internetnutzung in der PHV/BHV**

Ziff. 7.15 AHB	Ziff. 4 BBR PHV/ZusatzBed IT
Ausgeschlossen sind Haftpflichtansprüche wegen Schäden aus Austausch, Übermittlung und Bereitstellung elektronischer Daten, soweit es sich handelt um Schäden aus	4.1 Eingeschlossen ist –insoweit abweichend von Ziff. 7.15 AHB– die gesetzl. Haftpflicht des VN wegen Schäden aus Austausch, Übermittlung und Bereitstellung elektr. Daten, z.B. im Internet, per E-Mail oder mittels Datenträger, soweit es sich handelt um

C. Position der Versicherer

- **Bsp.: Ausschluss (Nullstellung)/Wiedereinschluss elektr. Datenaustausch/Internetnutzung in der PHV**

Ziff. 7.15 AHB	Ziff. 4 BBR PHV
(1)Löschung, Unterdrückung, Unbrauchbarmachung oder Veränderung von Daten,	(1)Löschung, Unterdrückung, Unbrauchbarmachung oder Veränderung von Daten (Datenveränderung) **bei Dritten durch Computer-Viren und/oder andere Schadprogramme;**

C. Position der Versicherer

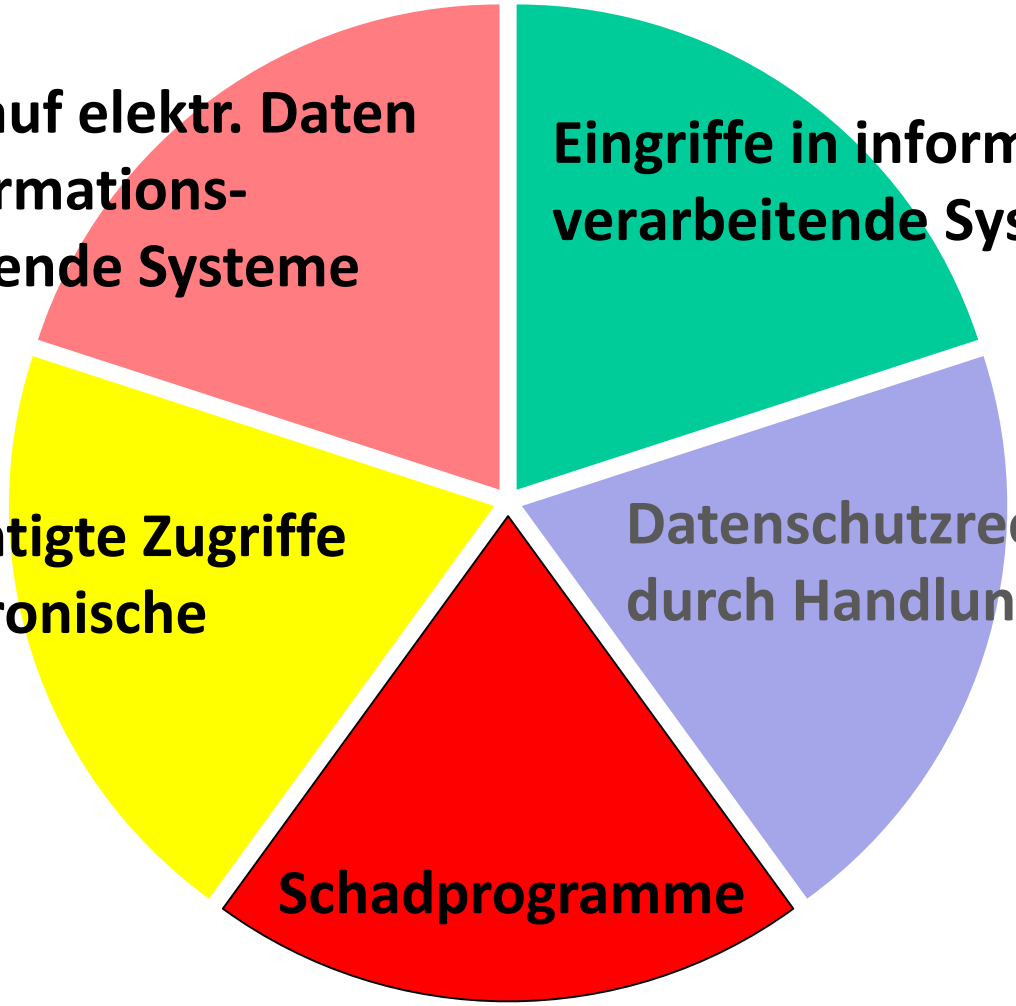
- **Bsp.: Ausschluss (Nullstellung)/Wiedereinschluss elektr. Datenaustausch/Internetnutzung in der PHV**

Ziff. 7.15 AHB	Ziff. 4 BBR PHV
(2) Nicht-erfassen oder fehlerhaftem Speichern von Daten,	(2) **Datenveränderung aus sonstigen Gründen sowie** Nichterfassung und fehlerhaften Speicherung von Daten **bei Dritten und zwar wegen** **– sich daraus ergebender Personen- und Sachschäden, nicht jedoch weiterer Datenveränderungen sowie** **– der Kosten zur Wiederherstellung veränderter Daten bzw. Erfassung/korrekter Speicherung nicht oder fehlerhaft erfasster Daten;**

D. Position der versicherungsnehmenden Wirtschaft

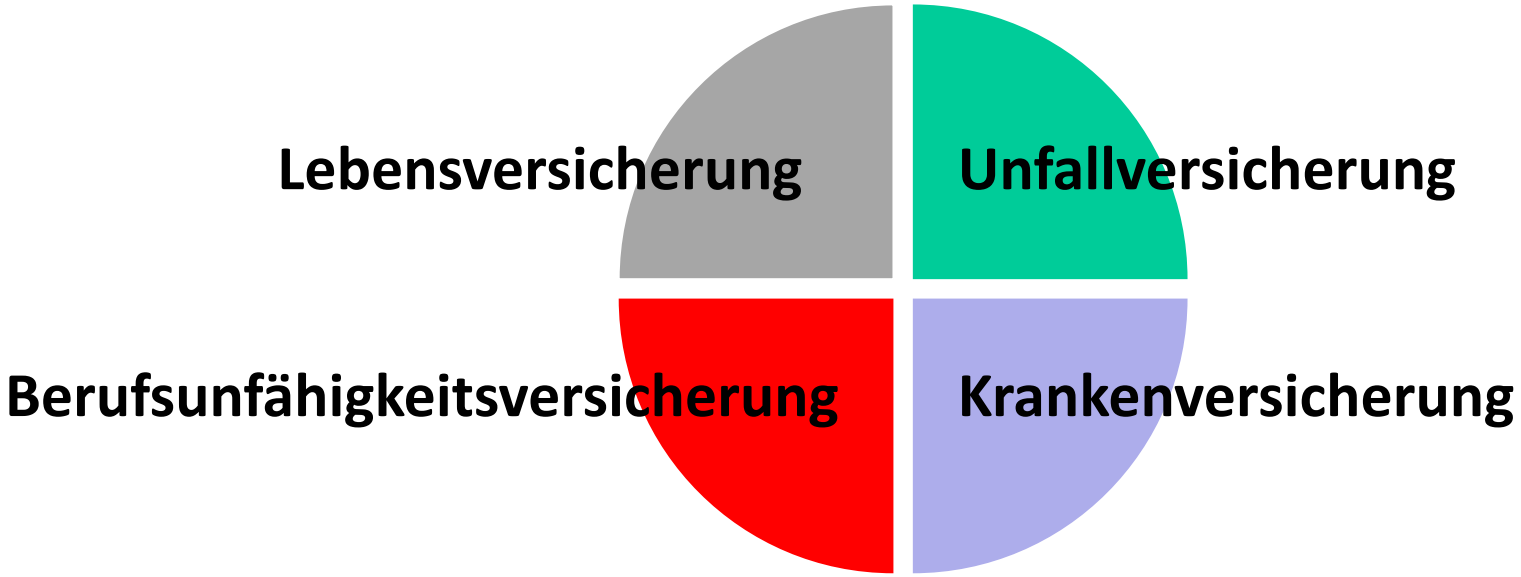
- Stellungnahme des GVNW zum „silent cyber“-Thema
  - Begrüßenswert: Klarstellung der Deckung von Cyberrisiken in herkömmlichen Policen
  - Ablehnung: pauschaler Ausschluss von Cyberrisiken
  - „Stand-alone“-Cyberversicherungen kein adäquater Ersatz für die in den herkömmlichen Policen bereits enthaltenen Deckungen von Cyberrisiken

E. (Silent) Cyber Risk Map



F. Deckung von (silent) CyberRisks in der PersonenV

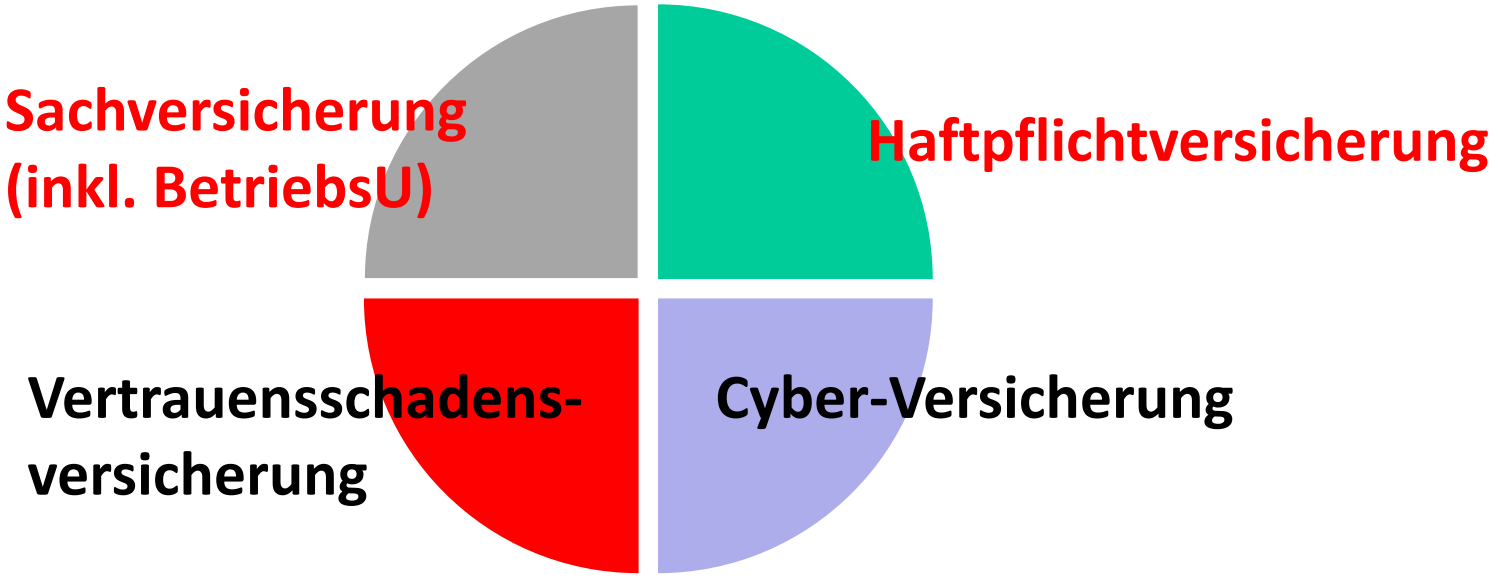
Beispiel 1: Steuerung der Aufzuganlage eines Hochhauses wird über Cyber-Angriff manipuliert. Aufzugkabine stürzt aus der 2. Etage ungebremst ab.



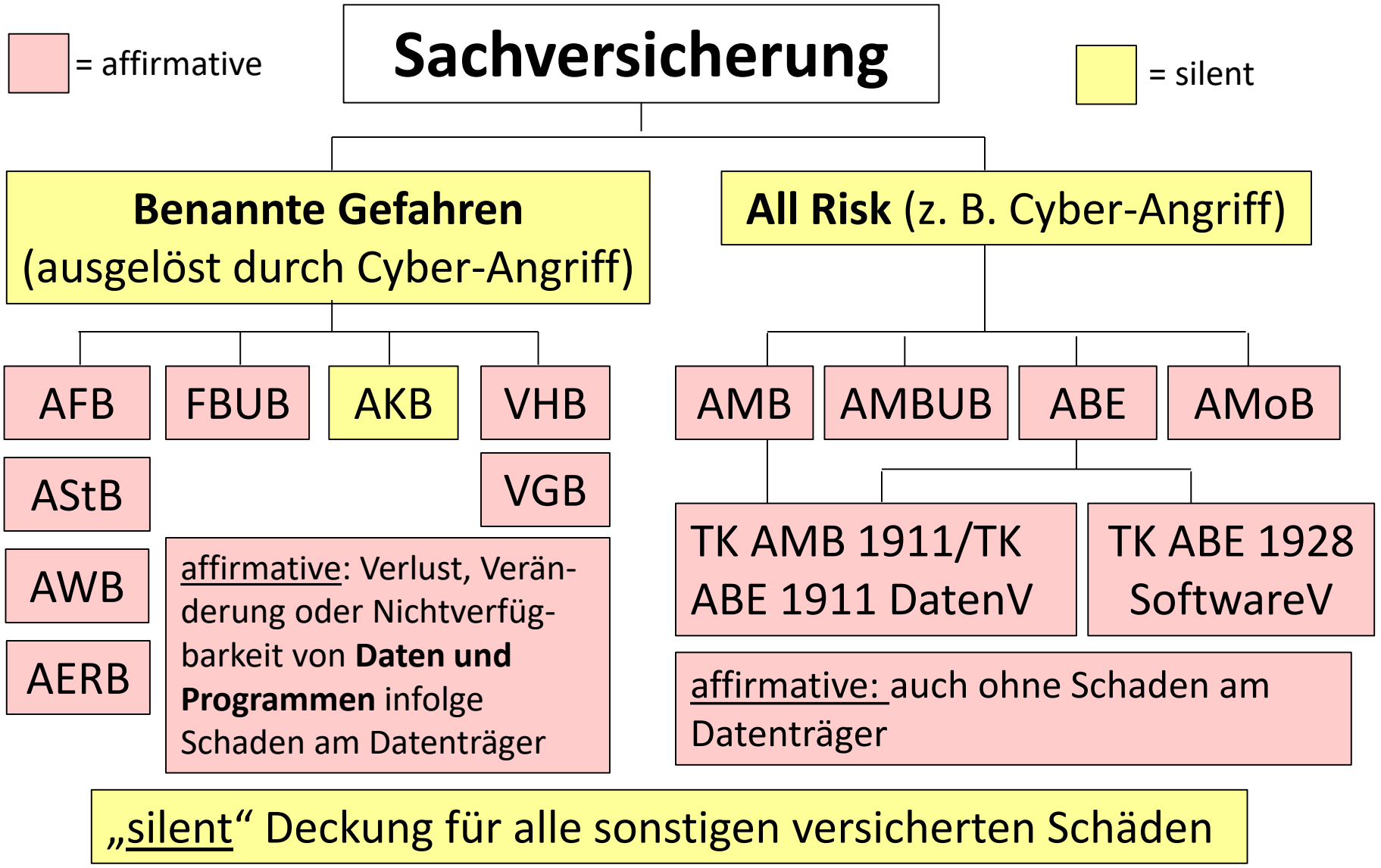
Beispiel 2: Hacker verschaffen sich Zugriff auf Medizintechnik eines Krankenhauses. Die angezeigten Funktionsdaten der Geräte weichen daraufhin von den ausgeführten Funktionsdaten ab, was zunächst nicht bemerkt wird. Es gibt Todesfälle, längere Krankenhausaufenthalte usw.

G. Deckung von (silent) CyberRisks in der NichtpersonenV

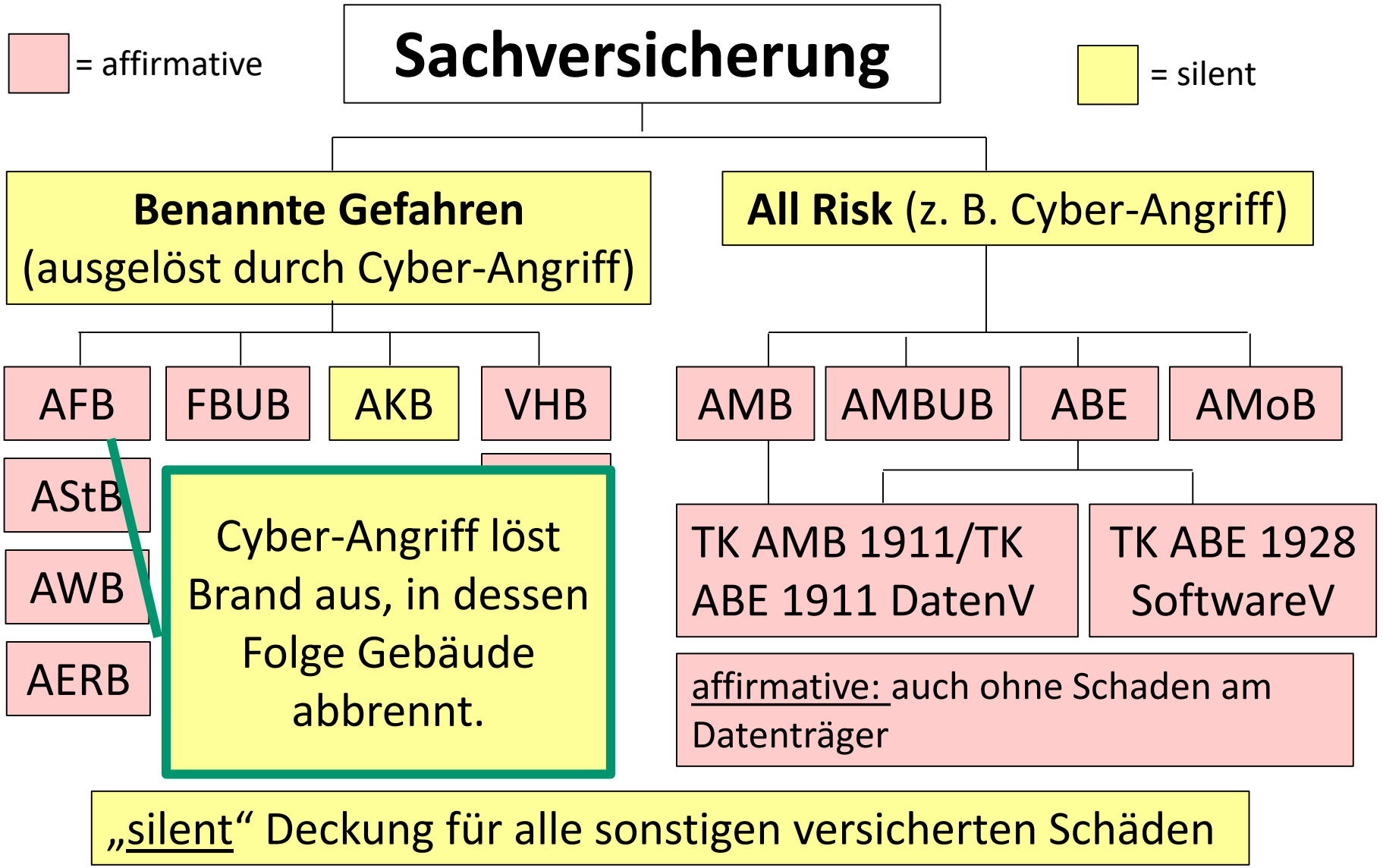
Beispiel: Aufgrund einer in die Wärmesteuerung eines Lagers für bio-technologisches Material eingeschleusten Schadsoftware, wird keine Temperaturkontrolle und Steuerung mehr vorgenommen. Es kommt zu einer Explosion, bei der **Menschen sterben** und **Maschinen besc**hädigt werden. Der **Betrieb** bleibt mehrere Monate **geschlossen**.



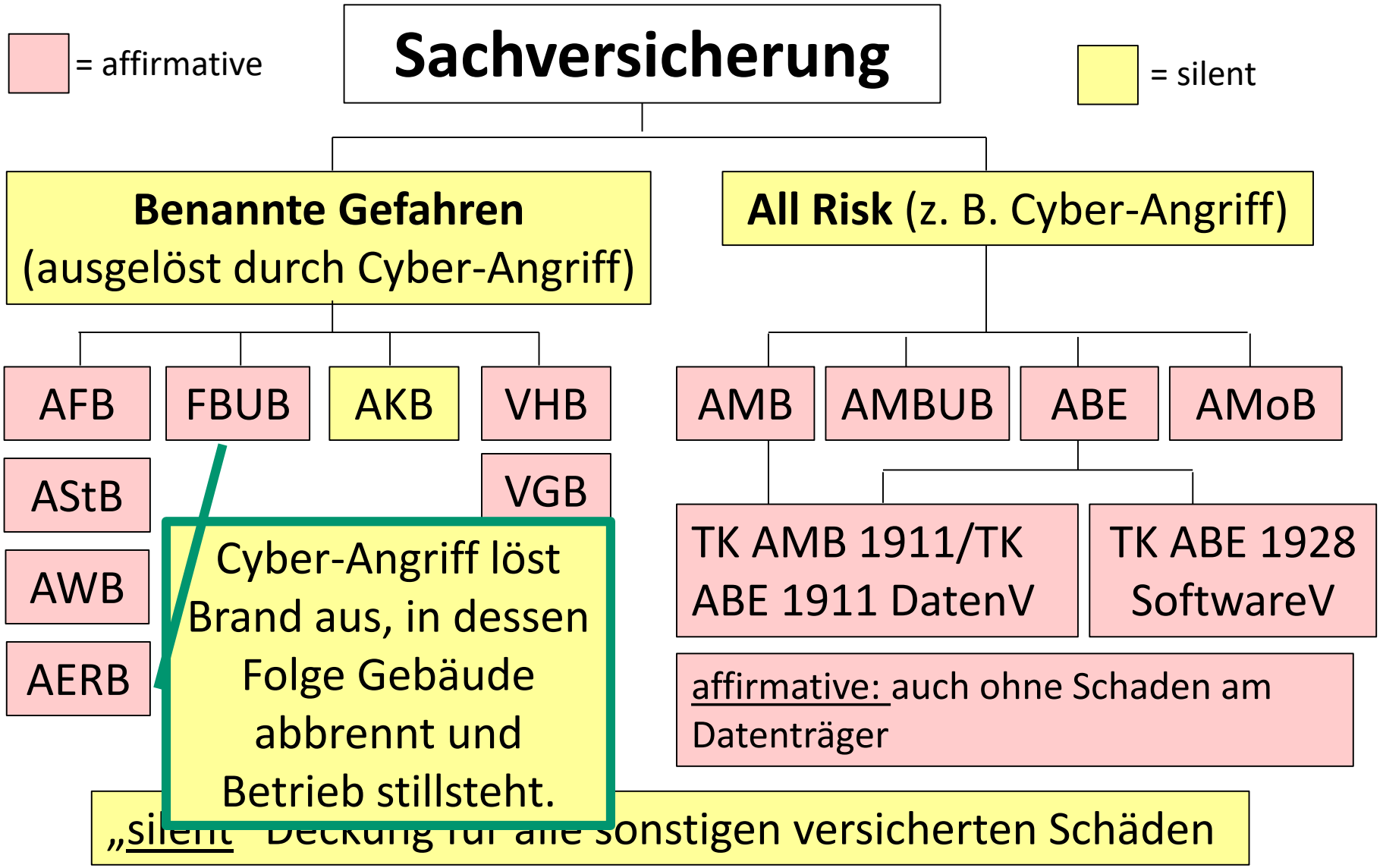
G. Deckung von (silent) CyberRisks in der NichtpersonenV



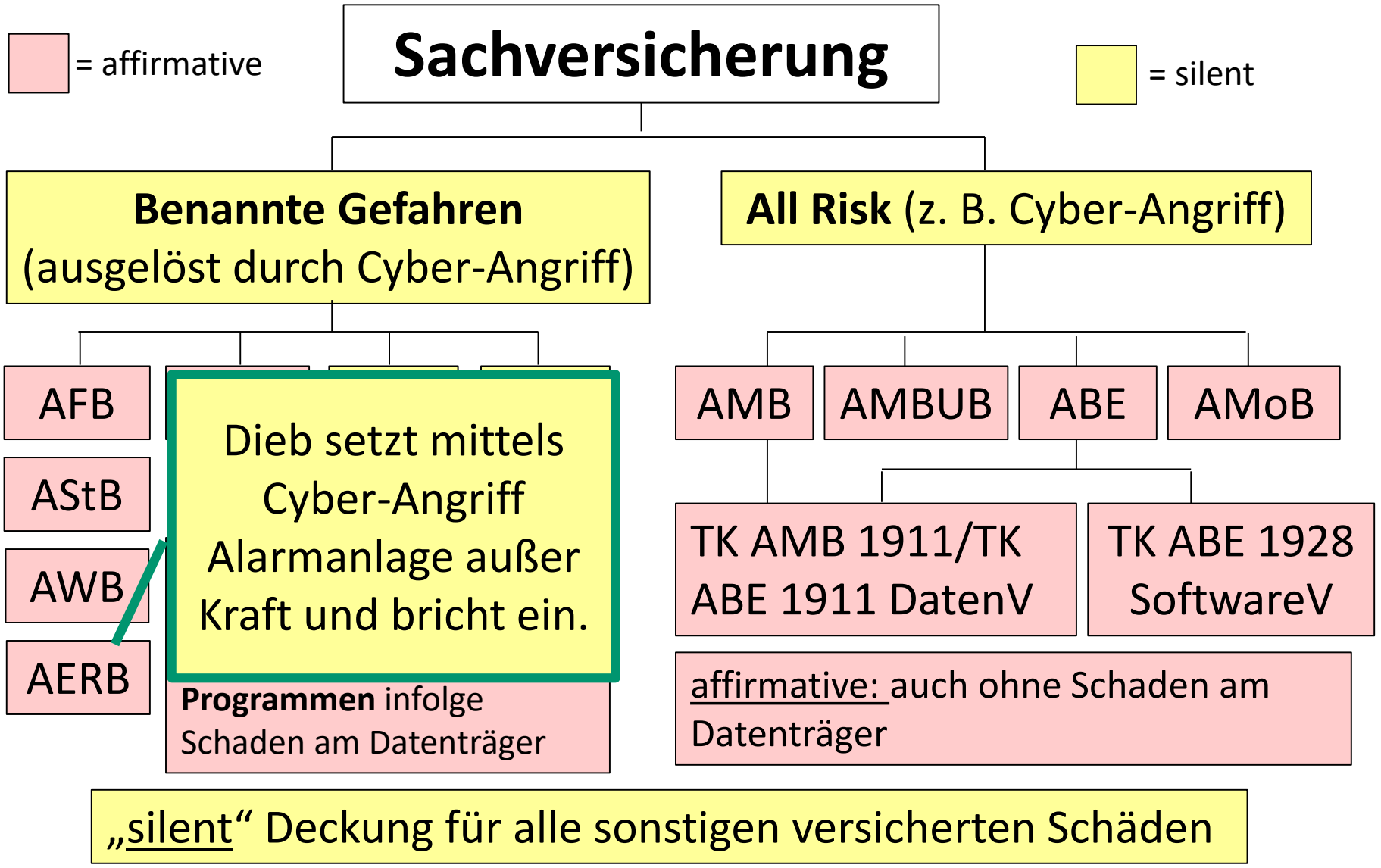
G. Deckung von (silent) CyberRisks in der NichtpersonenV



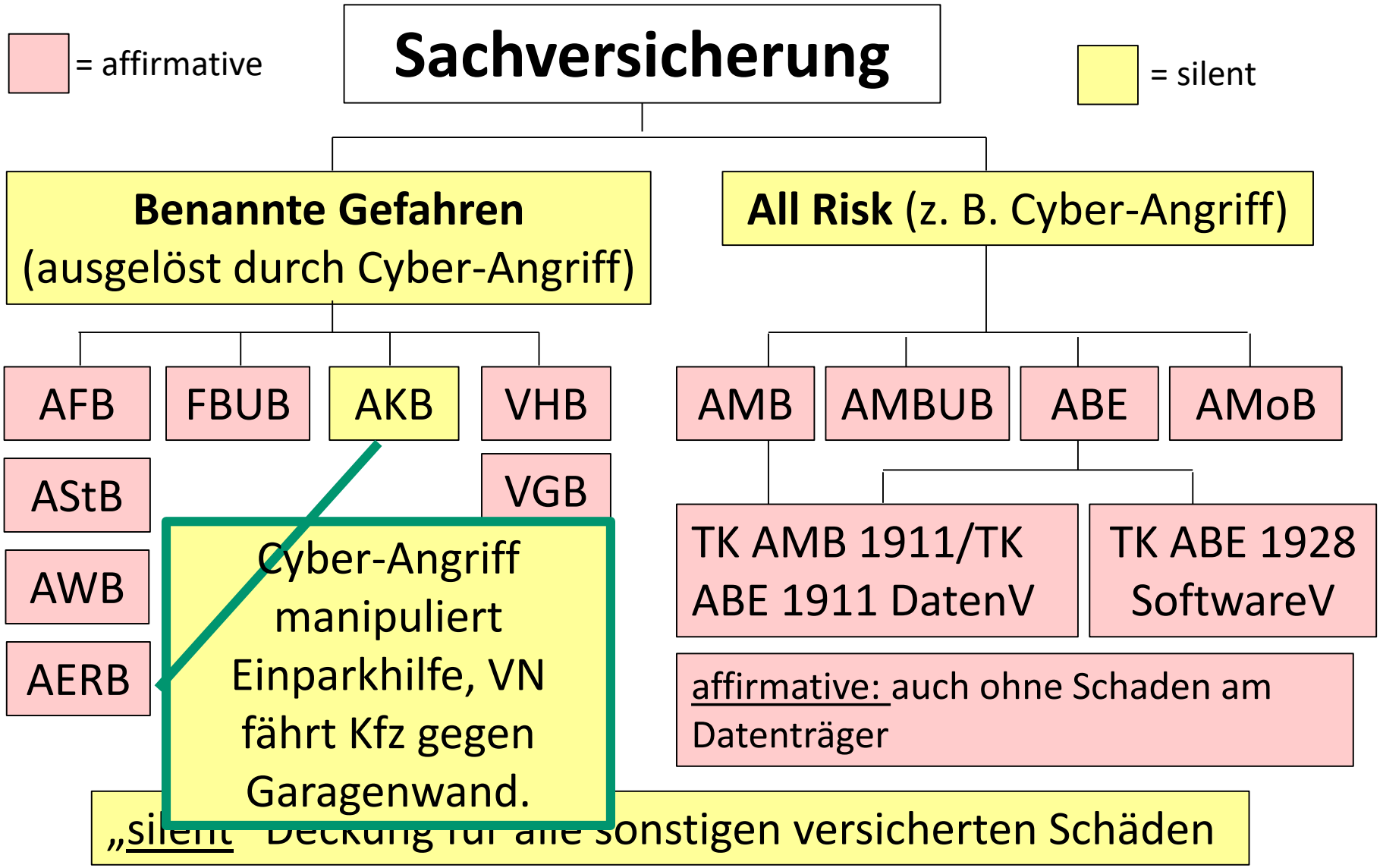
G. Deckung von (silent) CyberRisks in der NichtpersonenV



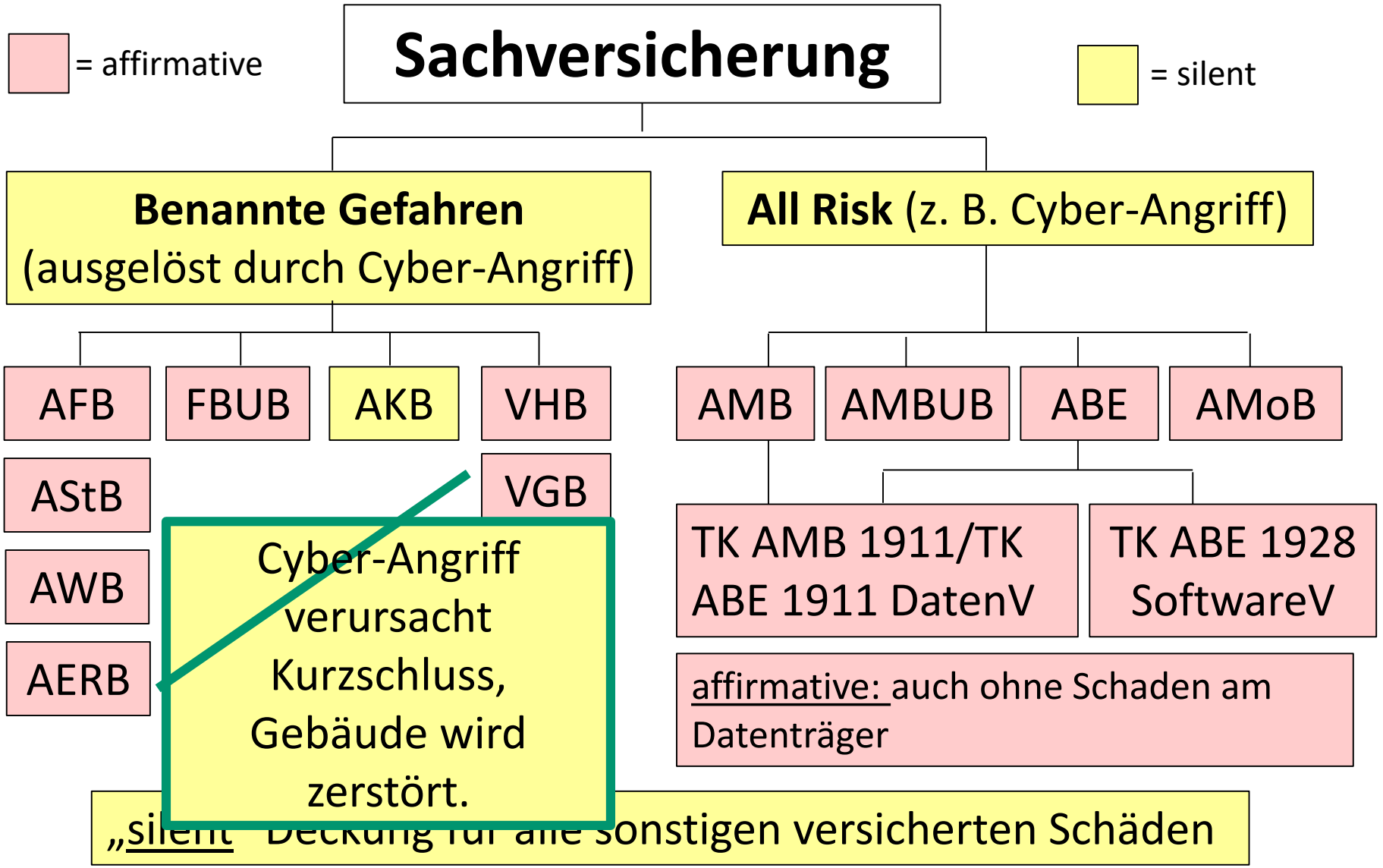
G. Deckung von (silent) CyberRisks in der NichtpersonenV



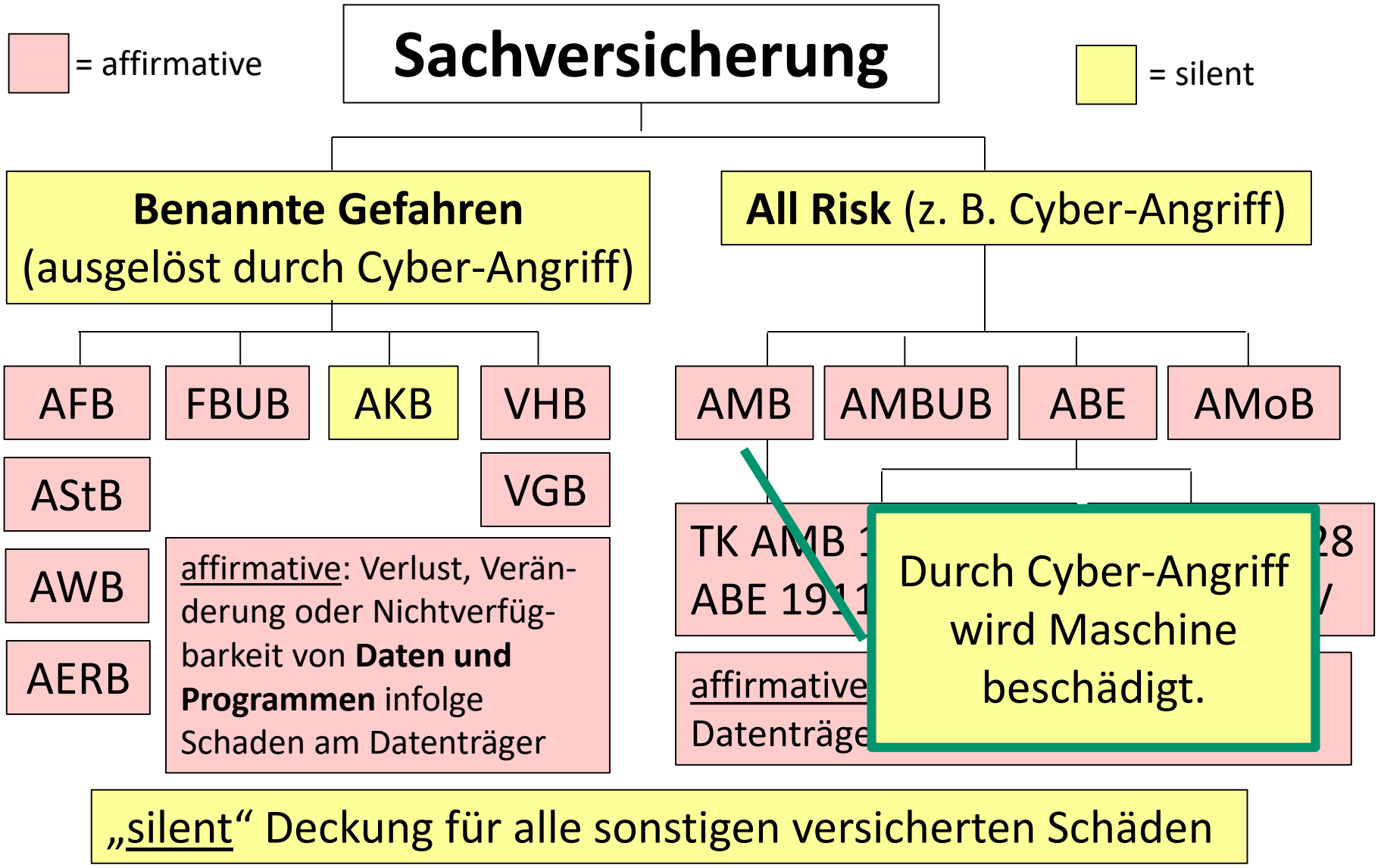
G. Deckung von (silent) CyberRisks in der NichtpersonenV



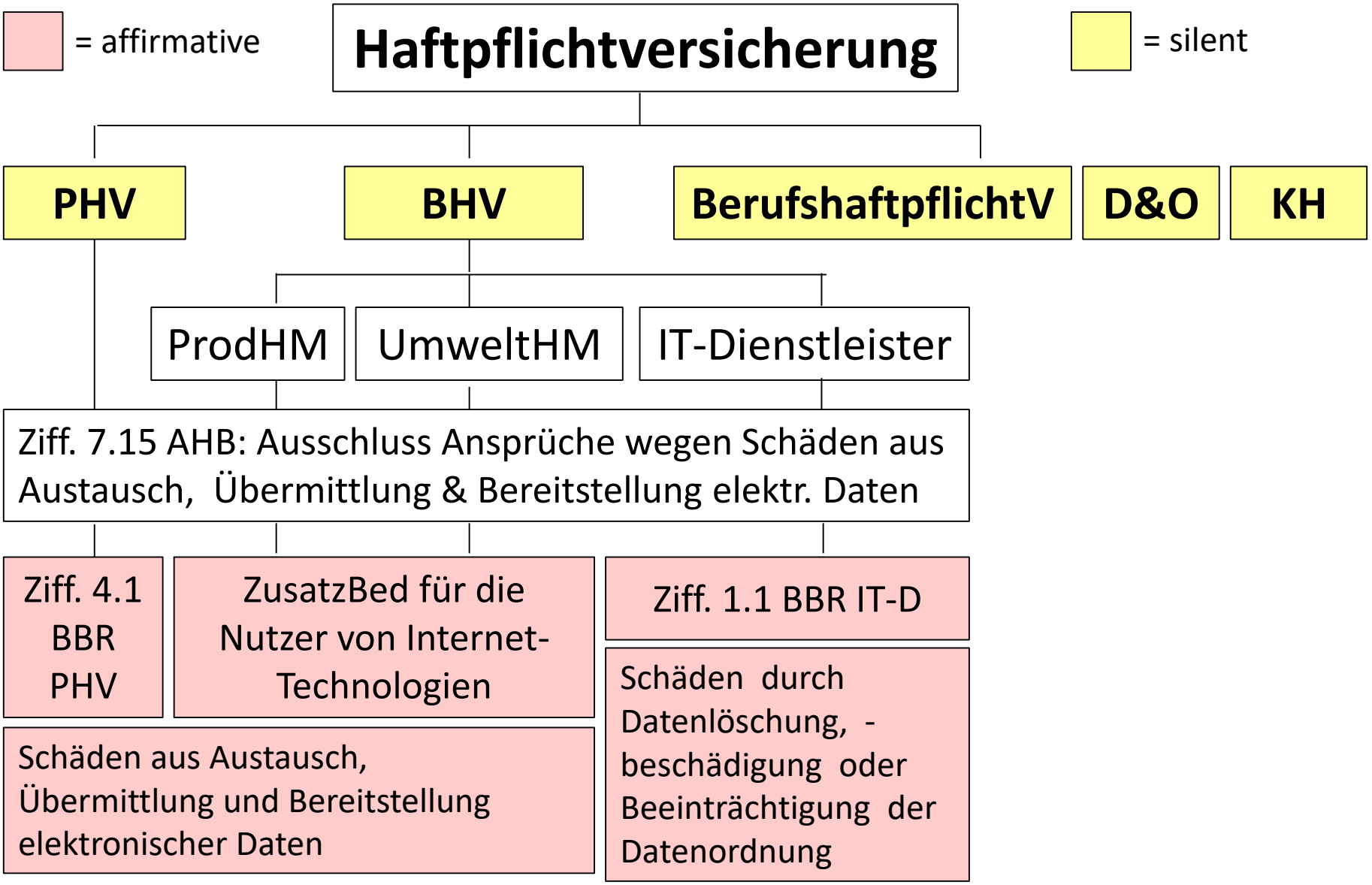
G. Deckung von (silent) CyberRisks in der NichtpersonenV



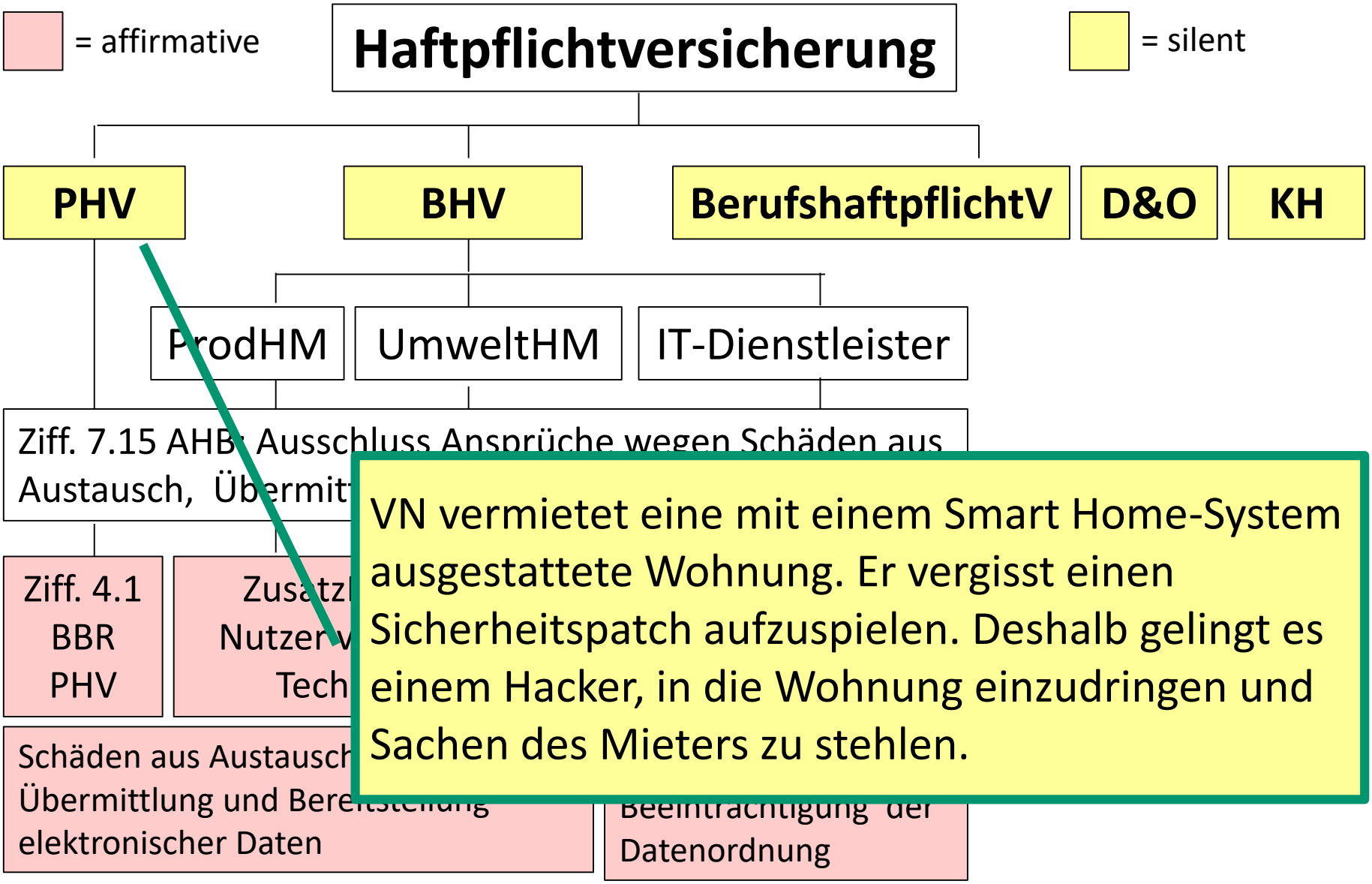
G. Deckung von (silent) CyberRisks in der NichtpersonenV



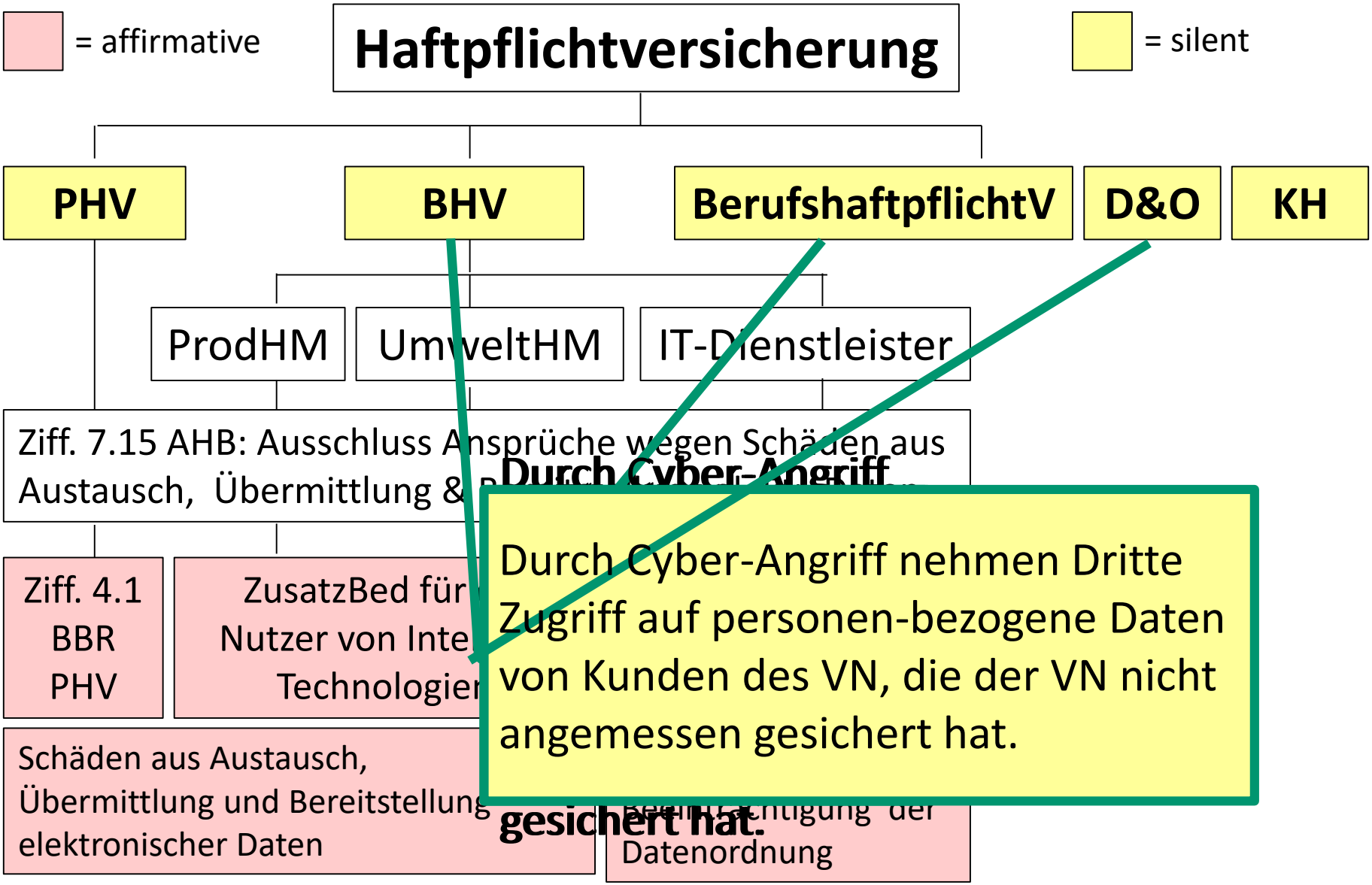
G. Deckung von (silent) CyberRisks in der NichtpersonenV



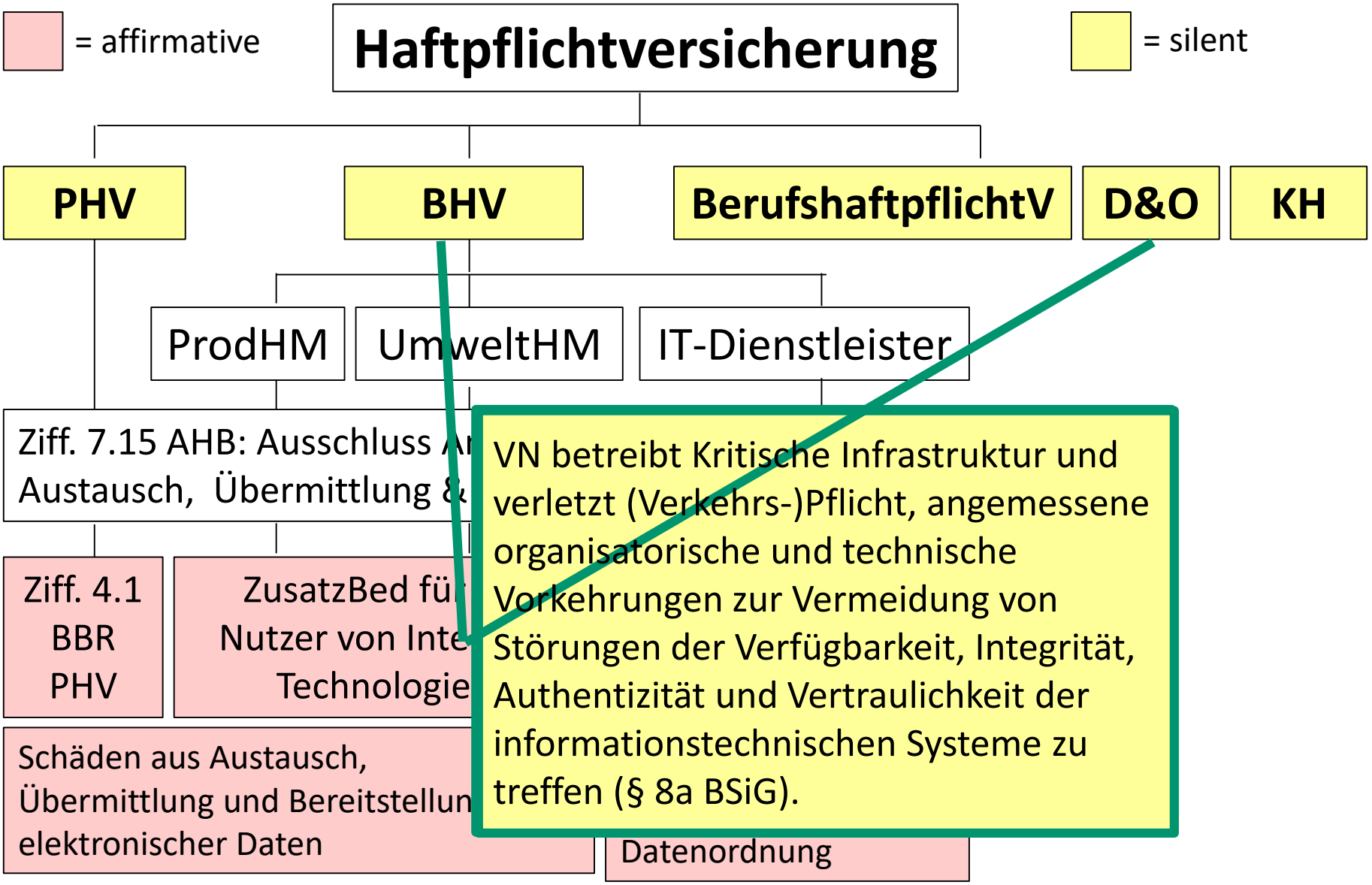
G. Deckung von (silent) CyberRisks in der NichtpersonenV



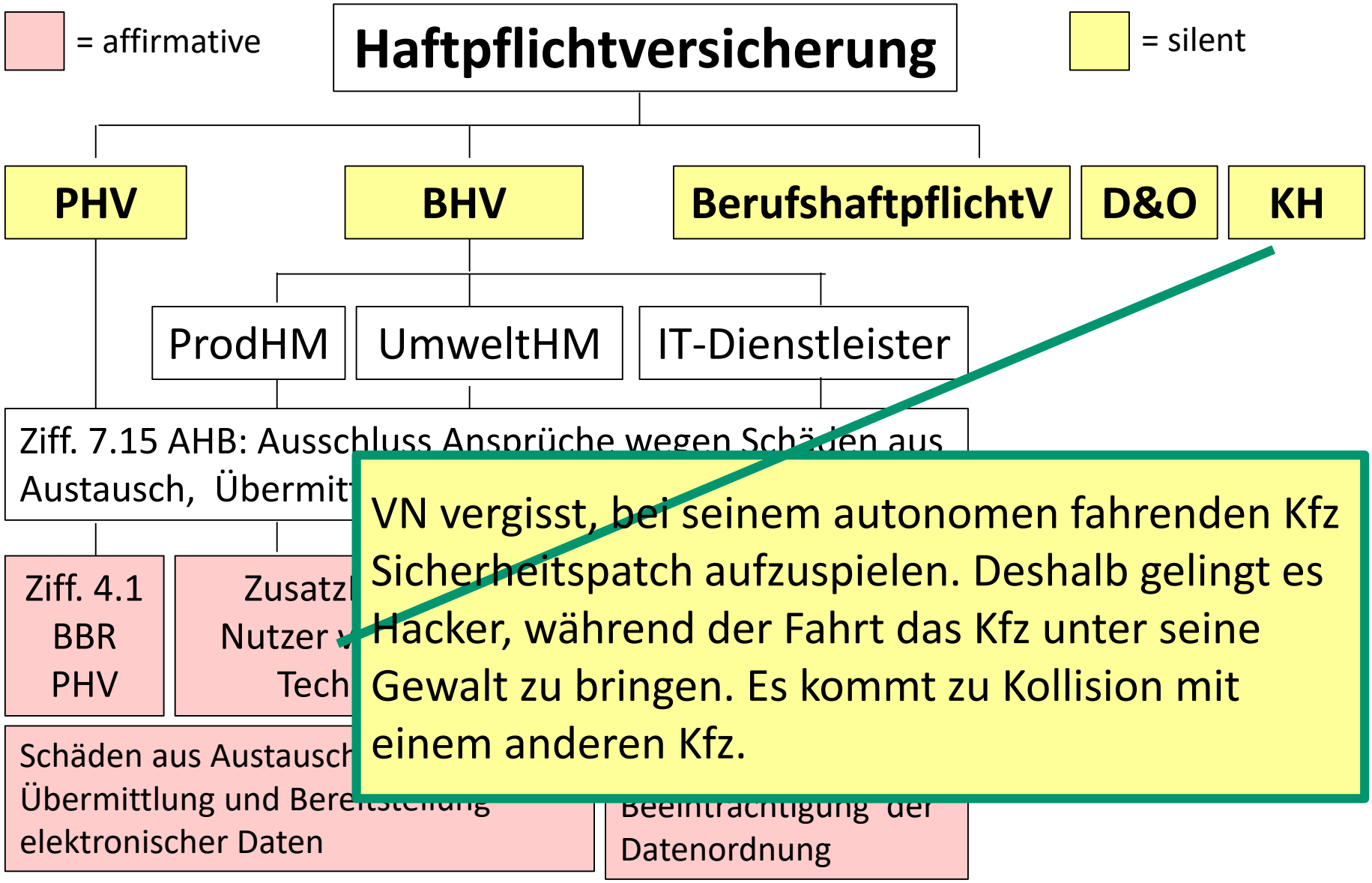
G. Deckung von (silent) CyberRisks in der NichtpersonenV



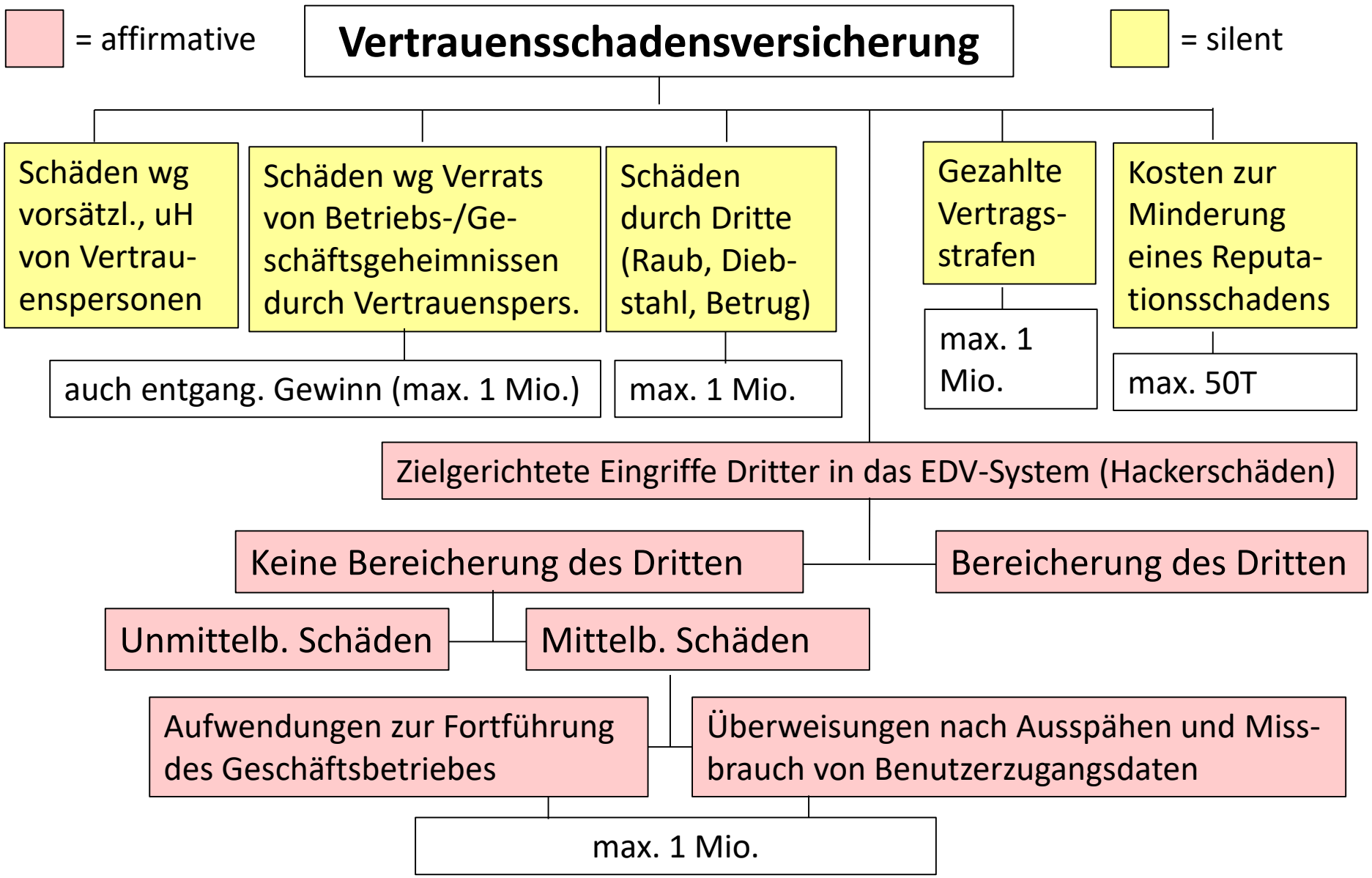
G. Deckung von (silent) CyberRisks in der NichtpersonenV



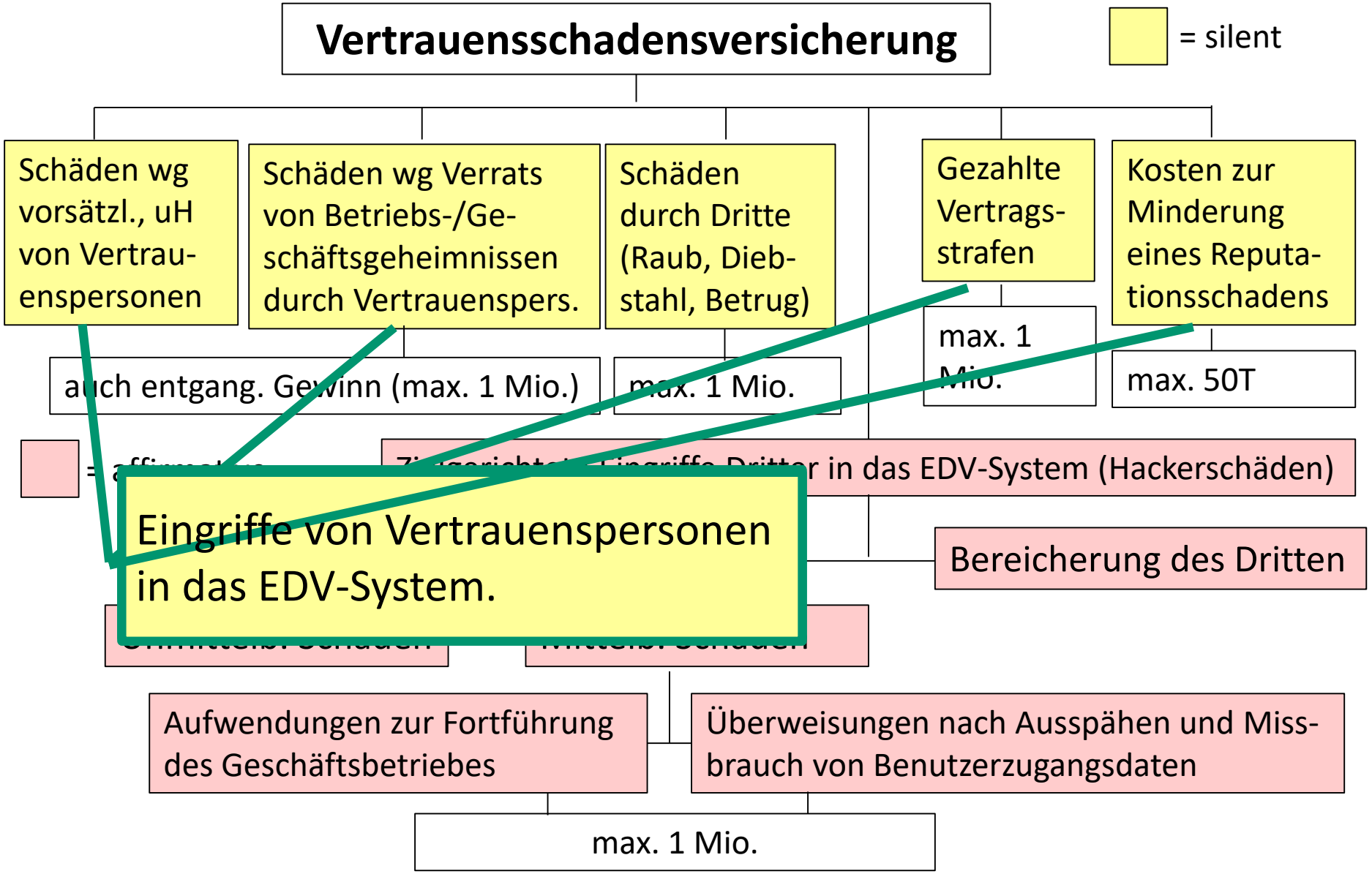
G. Deckung von (silent) CyberRisks in der NichtpersonenV



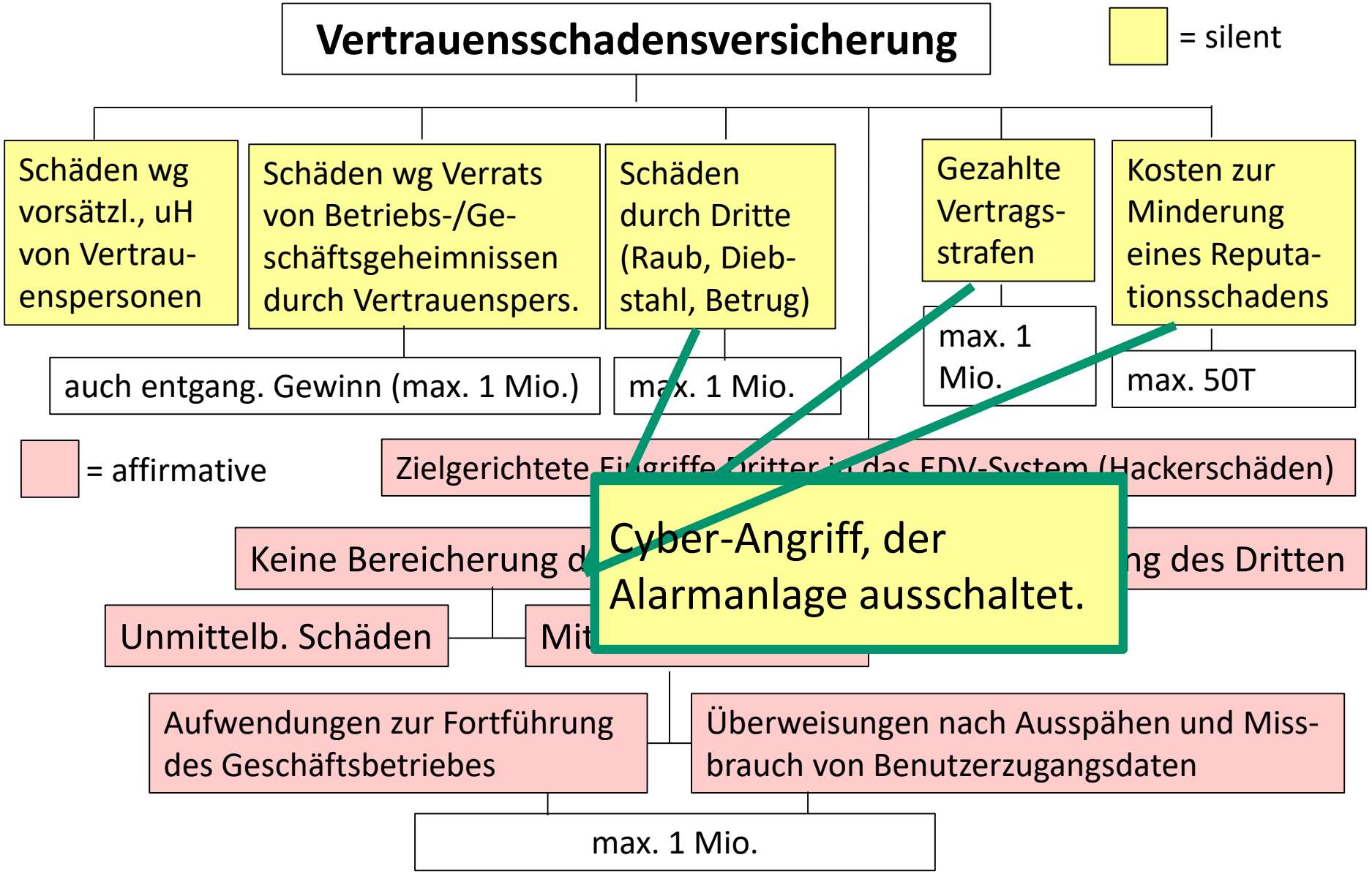
G. Deckung von (silent) CyberRisks in der NichtpersonenV



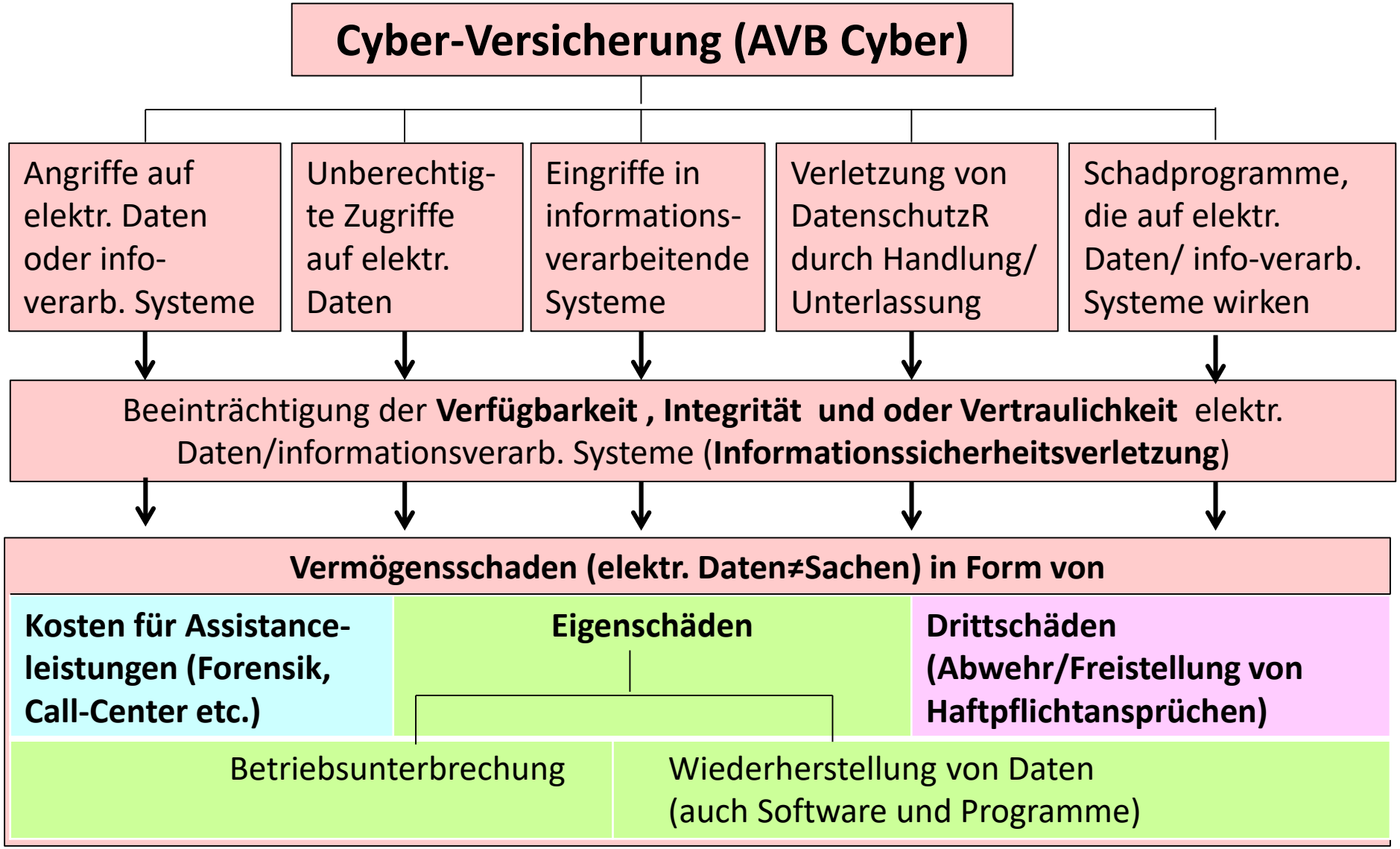
G. Deckung von (silent) CyberRisks in der NichtpersonenV



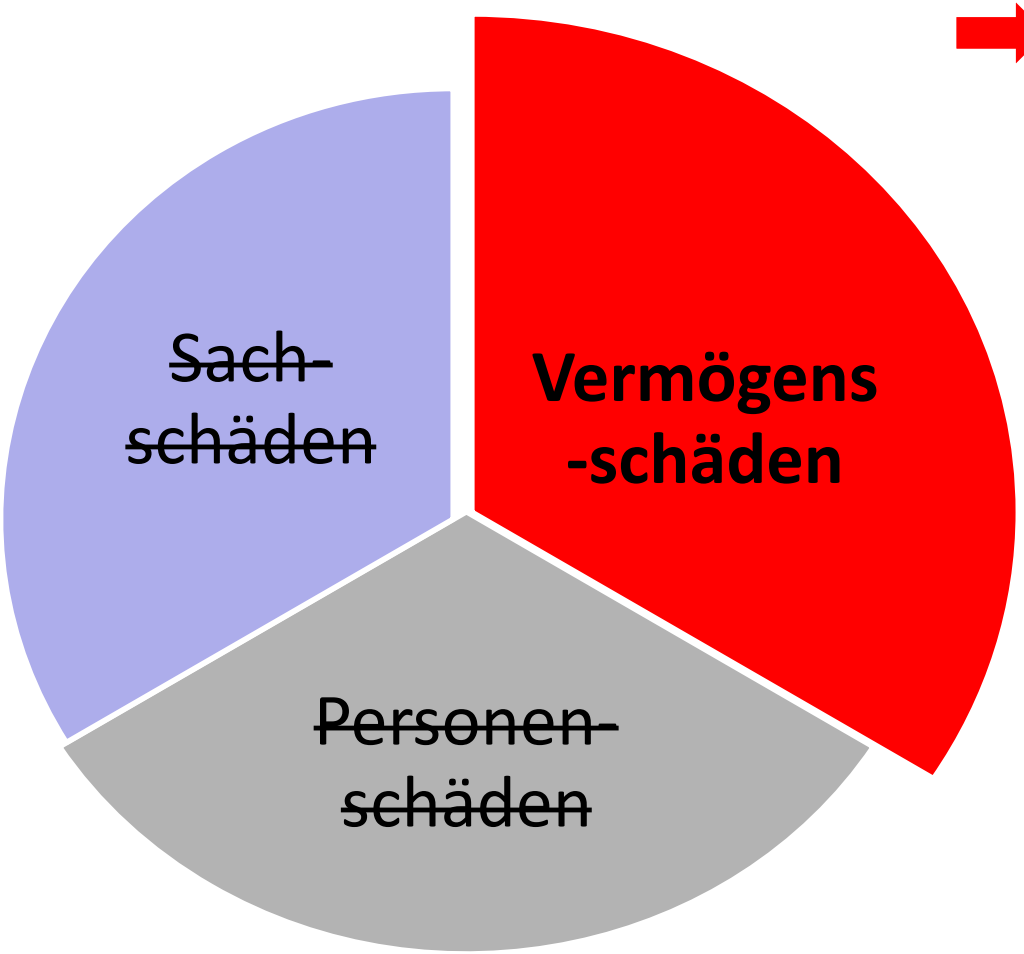
G. Deckung von (silent) CyberRisks in der NichtpersonenV



H. Umfang der Deckung von CyberRisks in der Cyber-Versicherung



H. Umfang der Deckung von CyberRisks in der Cyber-Versicherung



➡ Deckungslücke bei Nullstellung der (silent) CyberRisks

- in der Sachversicherung : Sach- und Ertragsaus-fallschäden
- in der Haftpflicht-versicherung (Inanspruchnahme wegen Sach- und Personen-schäden)

I. (Beschränkte) Nullstellung von CyberRisks in traditionellen Sach- und Haftpflichtversicherungssparten

- Ausdehnung Cyber-Versicherungsdeckung auf Sach- und Personenschäden (Kapazitätsprobleme?)
- Beschränkung der Nullstellung auf nicht zielgerichtete, d.h. gegen eine unbestimmte Zahl von Unternehmen gerichtete Cyber-Angriffe auf elektr. Daten oder informations-verarbeitende Systeme

  ➡ Versicherungsschutz besteht nur unter der Voraussetzung, dass Cyber-Angriff sich auf den VN beschränkt (keine Kumulrisiken)

I. (Beschränkte) Nullstellung von CyberRisks in traditionellen Sach- und Haftpflichtversicherungssparten

Beispiel (totale) Nullstellung in der Sachversicherung

Der VR leistet ohne Rücksicht auf mitwirkende Ursachen keine Entschädigung für Schäden durch Informationssicherheitsverletzungen, die durch folgende Ereignisse ausgelöst wird:

- Angriffe auf elektr. Daten oder informationsverarbeitende Systeme des VN;
- unberechtigte Zugriffe auf elektr. Daten des VN;
- Eingriffe in informationsverarbeitende Systeme des VN;
- eine Handlung oder Unterlassung, die zu einer Verletzung von datenschutzrechtlichen Vorschriften durch den VN führt;
- Schadprogramme, die auf elektr. Daten oder informationsverarbeitende Systeme des VN wirken.

Eine Informationssicherheitsverletzung ist eine Beeinträchtigung der Verfügbarkeit, Integrität, Vertraulichkeit von elektr. Daten des VN oder von informationsverarbeitenden Systemen, die er zur Ausübung seiner betriebl. oder berufl. Tätigkeit nutzt.

I. (Beschränkte) Nullstellung von CyberRisks in traditionellen Sach- und Haftpflichtversicherungssparten

Beispiel beschränkte Nullstellung in der Sachversicherung

Der VR leistet ohne Rücksicht auf mitwirkende Ursachen keine Entschädigung für Schäden durch Informationssicherheitsverletzungen, die resultiert aus nicht auf den VN beschränkten

- Angriffen auf elektr. Daten oder informationsverarbeitende Systeme;
- Eingriffen in informationsverarbeitende Systeme des VN;
- Schadprogrammen, die auf elektr. Daten oder informationsverarbeitende Systeme des VN wirken.

Eine Informationssicherheitsverletzung ist…

I. (Beschränkte) Nullstellung von CyberRisks in traditionellen Sach- und Haftpflichtversicherungssparten

Beispiel (totale) Nullstellung in der Haftpflichtversicherung

Vom VersSchutz sind ausgeschlossen Haftpflichtansprüche wegen Schäden durch eine Informationssicherheitsverletzungen, die durch folgende Ereignisse ausgelöst wird:

- Angriffe…;
- unberechtigte Zugriffe…;
- Eingriffe….;
- eine Handlung oder Unterlassung, die zu einer Verletzung von datenschutzrechtlichen Vorschriften durch den VN führt;
- Schadprogramme, ….

Eine Informationssicherheitsverletzung ist…

I. (Beschränkte) Nullstellung von CyberRisks in traditionellen Sach- und Haftpflichtversicherungssparten

Bsp. für beschränkte Nullstellung in der Haftpflichtversicherung

Vom VersSchutz sind ausgeschlossen Haftpflichtansprüche wegen Schäden durch Informationssicherheitsverletzungen, die resultiert aus nicht auf den VN beschränkten

- Angriffen auf elektr. Daten oder informationsverarbeitende Systeme,
- Eingriffen in informationsverarbeitende Systeme des VN,
- Schadprogrammen, die auf elektr. Daten oder informationsverarbeitende Systeme des VN wirken.

Eine Informationssicherheitsverletzung ist…

J. Einführung cyberspezifischer Obliegenheiten in traditionelle Sach- und Haftpflichtversicherungssparten

- Individuelle Zugänge zu informationsverarbeitenden Systemen, Nutzer, die mit ausreichend komplexen Passwörtern gesichert werden
- Administrative Zugänge ausschließlich für Administratoren und ausschließl. zur Erledigung administrativer Tätigkeiten
- Schutzmaßnahmen gegen unberechtigten Zugriff, zB Firewall, Verschlüsselung von Datenträgern mobiler Geräte
- Schutzmaßnahmen gegen Schadsoftware, zB Virenscanner, Firewall
- Unverzügliche Installation von relevanten Sicherheitspatches
- Erstellung von Sicherungsdatenträgern
- Sicherungsstellung, dass bei Cyber-Angriffen auf Originale und Duplikate nicht gleichzeitig zugegriffen werden kann, oder diese manipuliert, oder zerstört werden können
- Regelmäßige Prüfung der ordnungsgemäßen Funktion des Sicherungs- und Wiederherstellungsprozesses

K. Ausblick/Bewertung

- Deckungslücken im Fall der Nullstellung von CyberRisks in den traditionellen Sach- und Haftpflichtversicherungssparten werden nicht durch aktuelle Cyber-Versicherungskonzepte geschlossen
- Lückenschließung erfordert Ausdehnung der Cyber-Versicherung auf Sach- und Personenschäden
- Traditioneller Sach- und Haftpflichtversicherungsschutz muss mit Cyber-Versicherungsschutz abgestimmt werden

Vielen Dank für Ihre Aufmerksamkeit!

robert.koch@jura.uni-hamburg.de