IT-Sicherheit@Mittelstand 3.0

Unter der Schirmherrschaft des

Bundesministerium
für Wirtschaft
und Energie

DIHK

DsiN Deutschland sicher im Netz

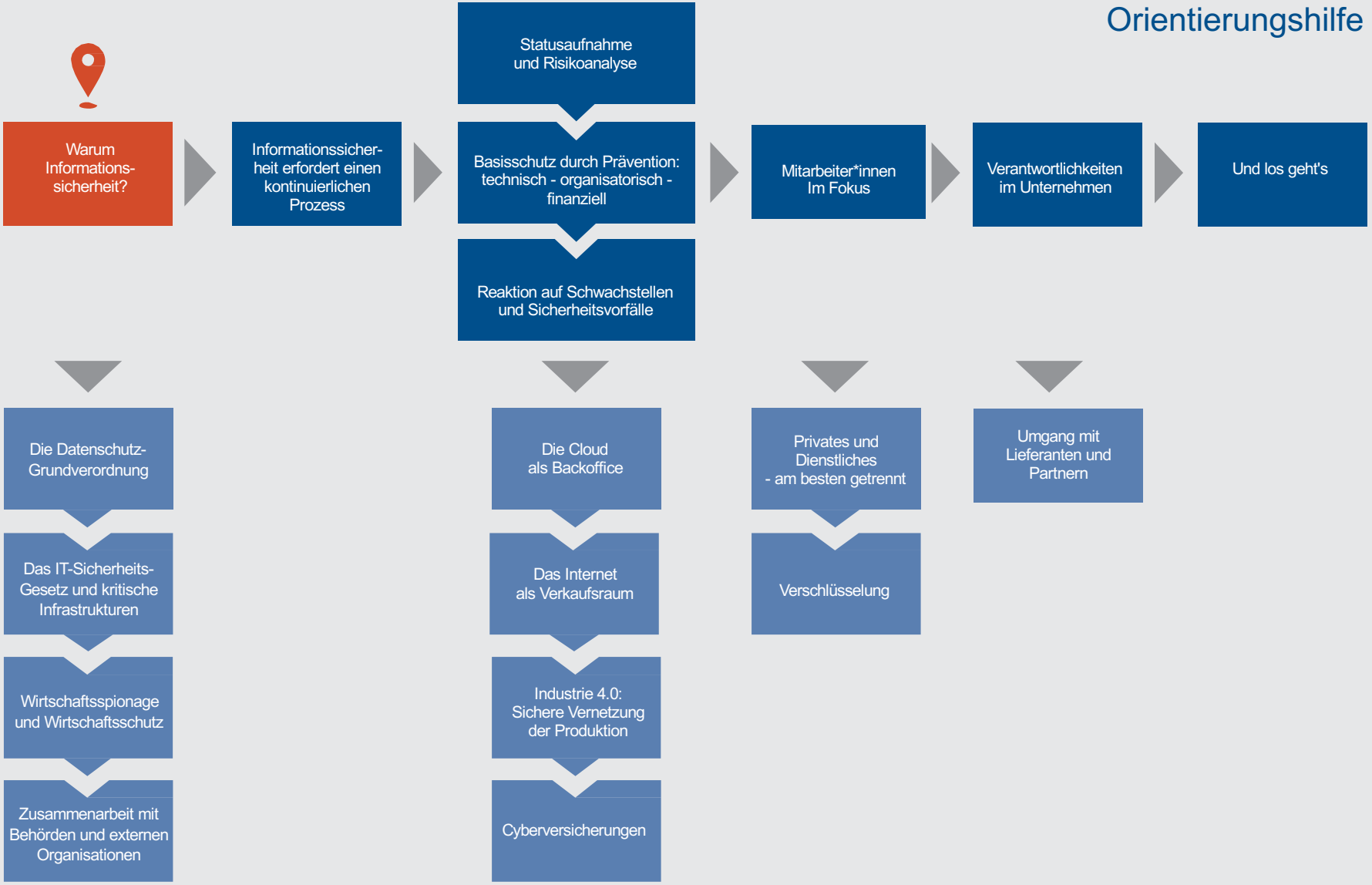
„Anwender müssen nicht nur Sicherheit haben wollen, sondern auch eigenständig beurteilen können, was sie wirklich benötigen. Dafür sind Kompetenzen erforderlich. Die Workshops liefern einen ersten Einstieg für Geschäftsführer kleinerer Unternehmen."

Klemens Gutmann
Mitgründer und Geschäftsführer der regiocom-Gruppe

DIHK

DsiN Deutschland sicher im Netz

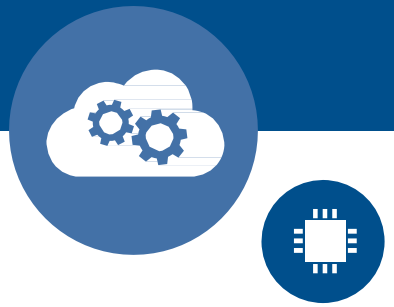
Orientierungshilfe



DIHK

DsiN Deutschland sicher im Netz

Warum Informationssicherheit?
1. Nutzen Sie die Vorteile der Digitalisierung



Aktuelle Situation

- Digitalisierung ist nur sinnvoll, wenn Sie dabei keine unangemessenen Risiken eingehen!
- In vielen Fällen sind – richtig eingesetzt und mit einem Basisschutz versehen – die digitalen Lösungen besser und sicherer.
- Beispiele:
  - Buchführung
  - Maschinensteuerung
  - Kommunikation mit Geschäftspartnern

Empfehlung

- Stellen Sie einen Basisschutz für sämtliche Informationen her:
  - für Ihre eigenen,
  - für die Informationen Ihrer Mitarbeiter*innen,
  - und für den Input Ihrer Kund*innen und Partner!
- Schützen Sie Ihre Kronjuwelen mit besonderen Maßnahmen
- Wichtigste Frage: Wo ist IT Teil des Kerngeschäfts?

DIHK

DsiN Deutschland sicher im Netz

Warum Informationssicherheit?
2. Halten Sie die Gesetze ein!

Gesetze mit Bezug zur Informationssicherheit

- Datenschutz-Grundverordnung der EU
  - Direkt geltendes Gesetz in den Mitgliedsstaaten
- IT-Sicherheitsgesetz
  - Schutz kritischer Infrastrukturen
  - Schutz von Internet-Diensten
- Sorgfaltspflicht der Geschäftsleitung
  - GoB – korrekte Rechnungslegung
  - GmbHG – Verletzung Geheimhaltungspflicht

Was fordern diese Gesetze?

Fast jeder ist betroffen!

DIHK

DsiN Deutschland sicher im Netz

Warum Informationssicherheit?
3. Reduzieren Sie die persönliche Haftung der Geschäftsführung

Bewertung der Rechtslage

- Fahrlässig oder grob fahrlässig ist es, wenn man den „Stand der Technik“ nicht einsetzt
- Der „Stand der Technik“ ist gleichzusetzen mit dem Einsatz eines Management- Systems für Informationssicherheit

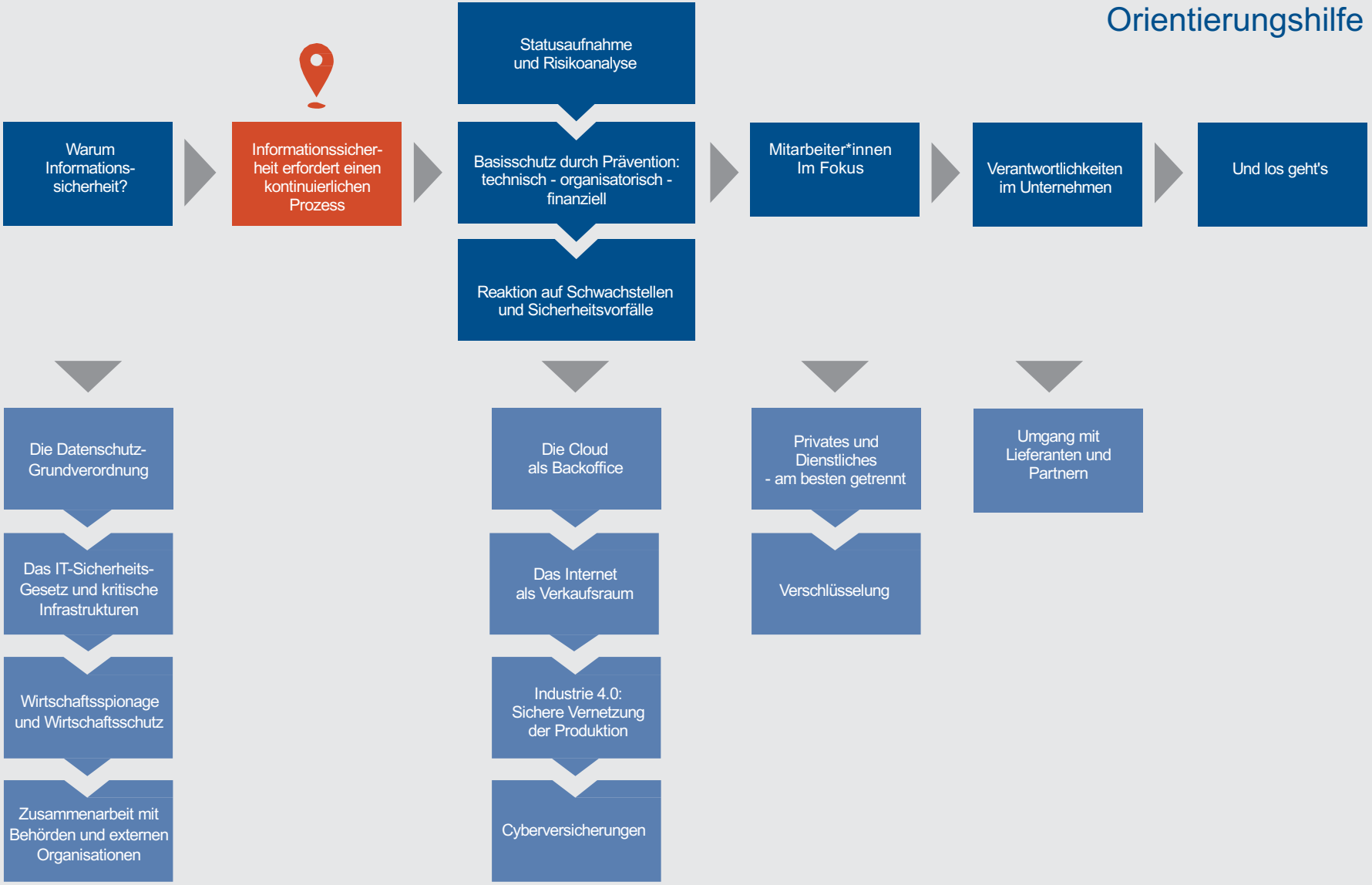
Empfehlung

- Nicht nur wegen Digitalisierung oder Datenschutz: ein angemessener, nachhaltiger Schutz der Informationen mit einem Management-System ist notwendig, um persönliche Konsequenzen für die Geschäftsleitung zu vermeiden!

DIHK

DsiN Deutschland sicher im Netz

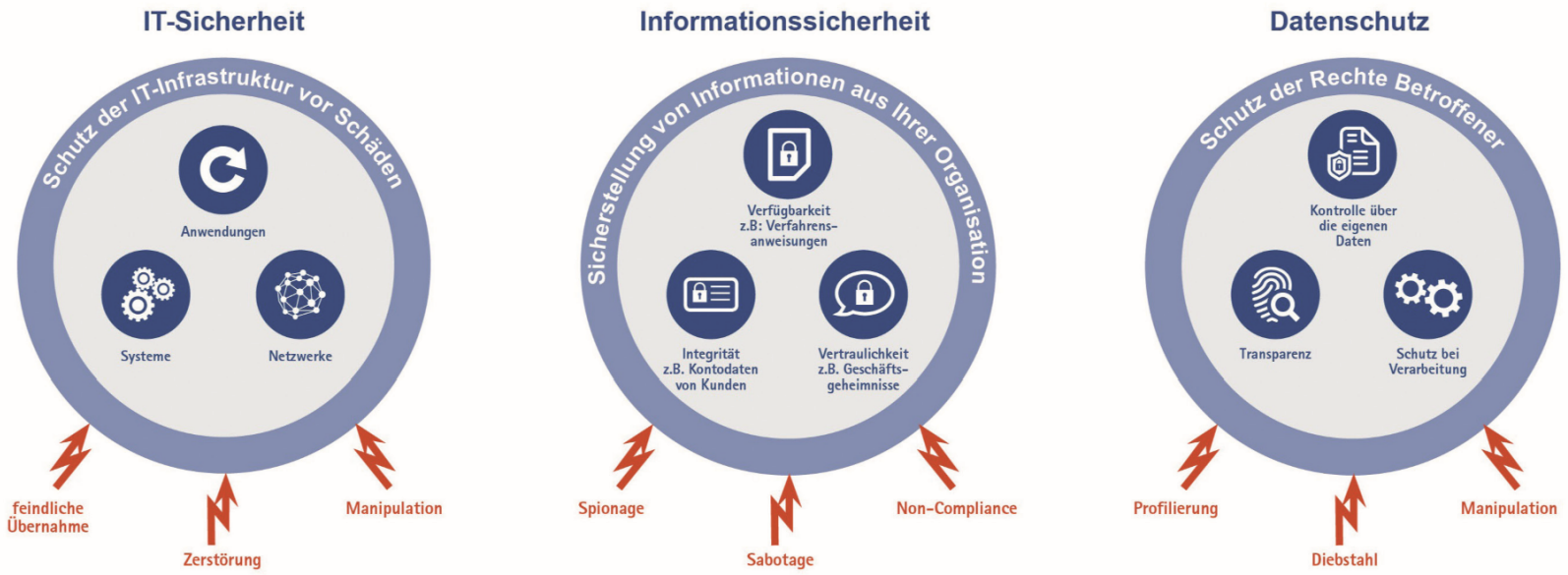
Orientierungshilfe



DIHK

DsiN Deutschland sicher im Netz

Was ist Informationssicherheit?



DIHK

DsiN Deutschland sicher im Netz

Sicherheit aus zwei unterschiedlichen Perspektiven

Sicherheit ist ein unstabiler Zustand

- Die Bedrohungssituation kann sich ständig ändern
- Die Wirksamkeit der Schutzmaß- nahmen kann sich ständig ändern
- Der Schutzbedarf kann sich ständig ändern

  > der Zustand der Sicherheit ist volatil

Sicherheit ist ein Prozess

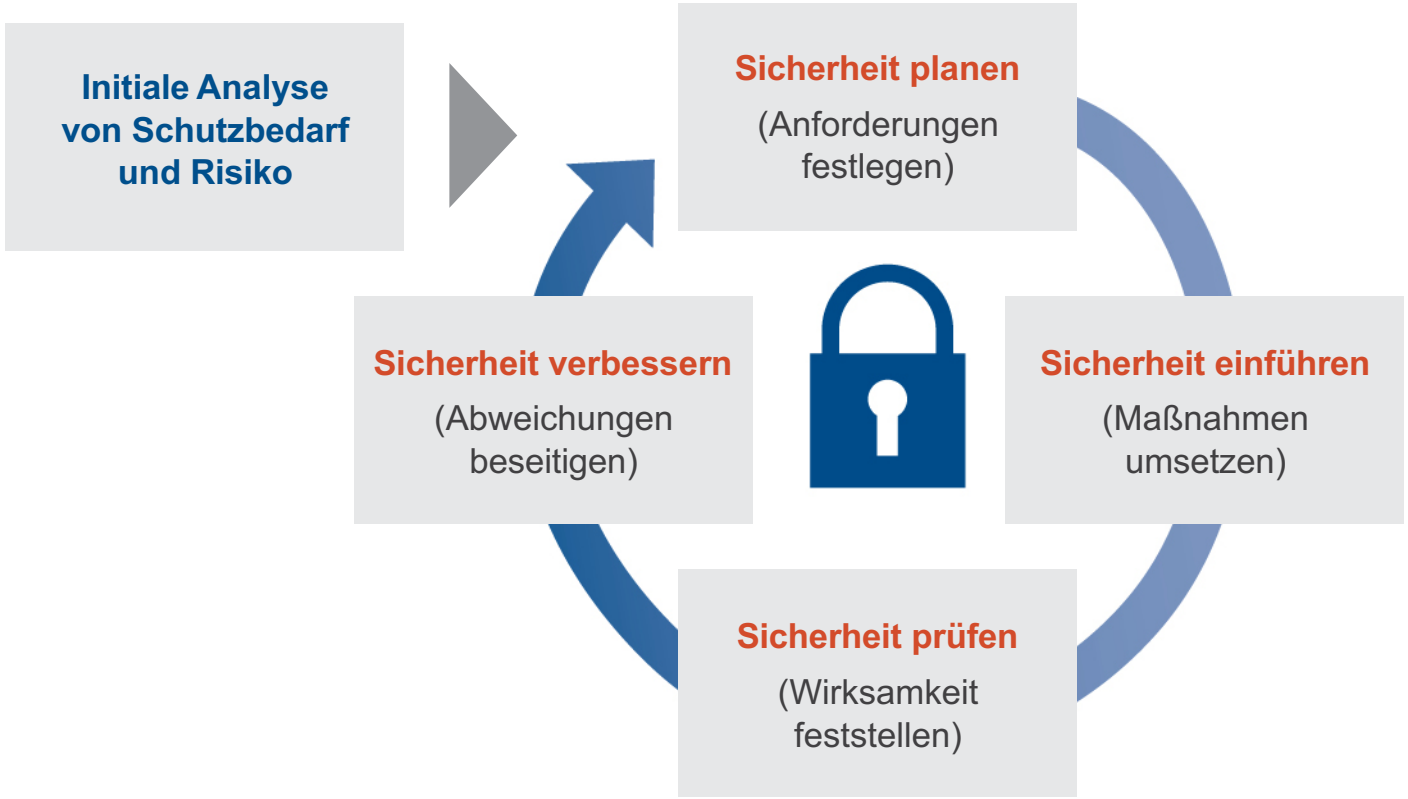
- Nur mit einem
  - nachhaltigen,
  - immer wiederkehrenden,
  - sich ständig verbessernden

Prozess kann man die erforderliche Sicherheit von Informationen sicher-stellen

DIHK

DsiN Deutschland sicher im Netz

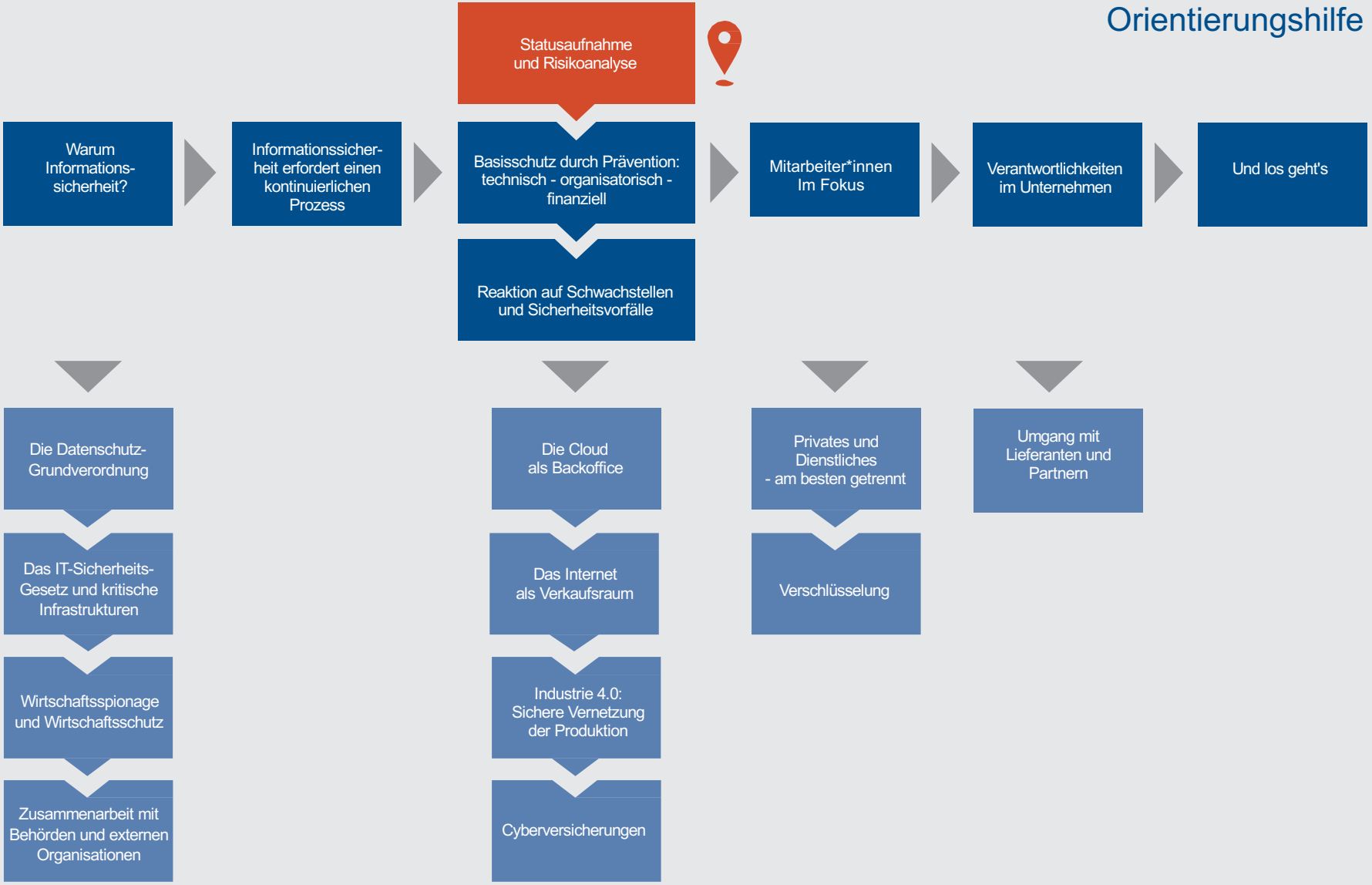
Der Informationssicherheitsprozess



DIHK

DsiN Deutschland sicher im Netz

Orientierungshilfe



DIHK

DsiN Deutschland sicher im Netz

Schutzbedarf und Risiko ermitteln

Schutzbedarf: Identifizieren Sie Ihre „Kronjuwelen“

- Welche Informationen müssen absolut vertraulich / integer / verfügbar sein, damit Ihre Firma weiter existieren kann?
- Dann ist der Schutzbedarf dieser Informationen **sehr hoch**
- **Achtung**: Personenbezogene Daten haben immer **hohen** Schutzbedarf

Identifizieren Sie Ihre TOP Risiken für die Kronjuwelen

Eintrittswahrscheinlichkeit

x

Schadenshöhe

Risiko

Welche Schadensfälle können für diese Informationen eintreten?
Wie oft, schätzen Sie, wird dies in 3 Jahren eintreten?
Wie hoch wäre der Schaden für Ihr Unternehmen (in €)?

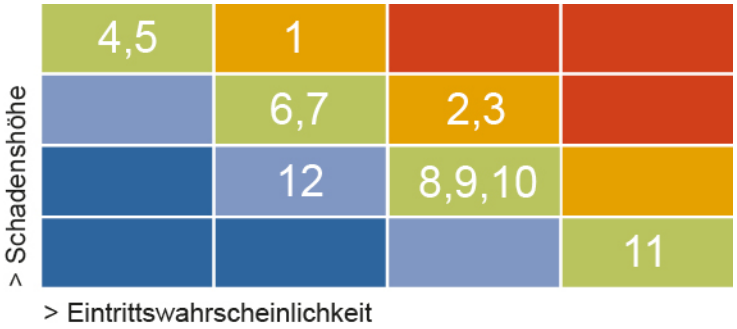
Für den Anfang sind auch Stufen (z.B. niedrig – mittel – hoch) angemessen

DIHK

DsiN Deutschland sicher im Netz

Darstellung der TOP Risiken

Risikomatrix



Risikotabelle

Nr.	Risiko	EW	SH
1	Verschlüsselungstrojaner	2	4
2	Identitätsdiebstahl durch Phishing	3	3
3	Spionage durch Praktikanten	3	3
4	Firma brennt ab	1	4
5	Server fallen komplett aus	1	4
6	...		

DIHK

DsiN Deutschland sicher im Netz

Optionen für den Umgang mit Risiken

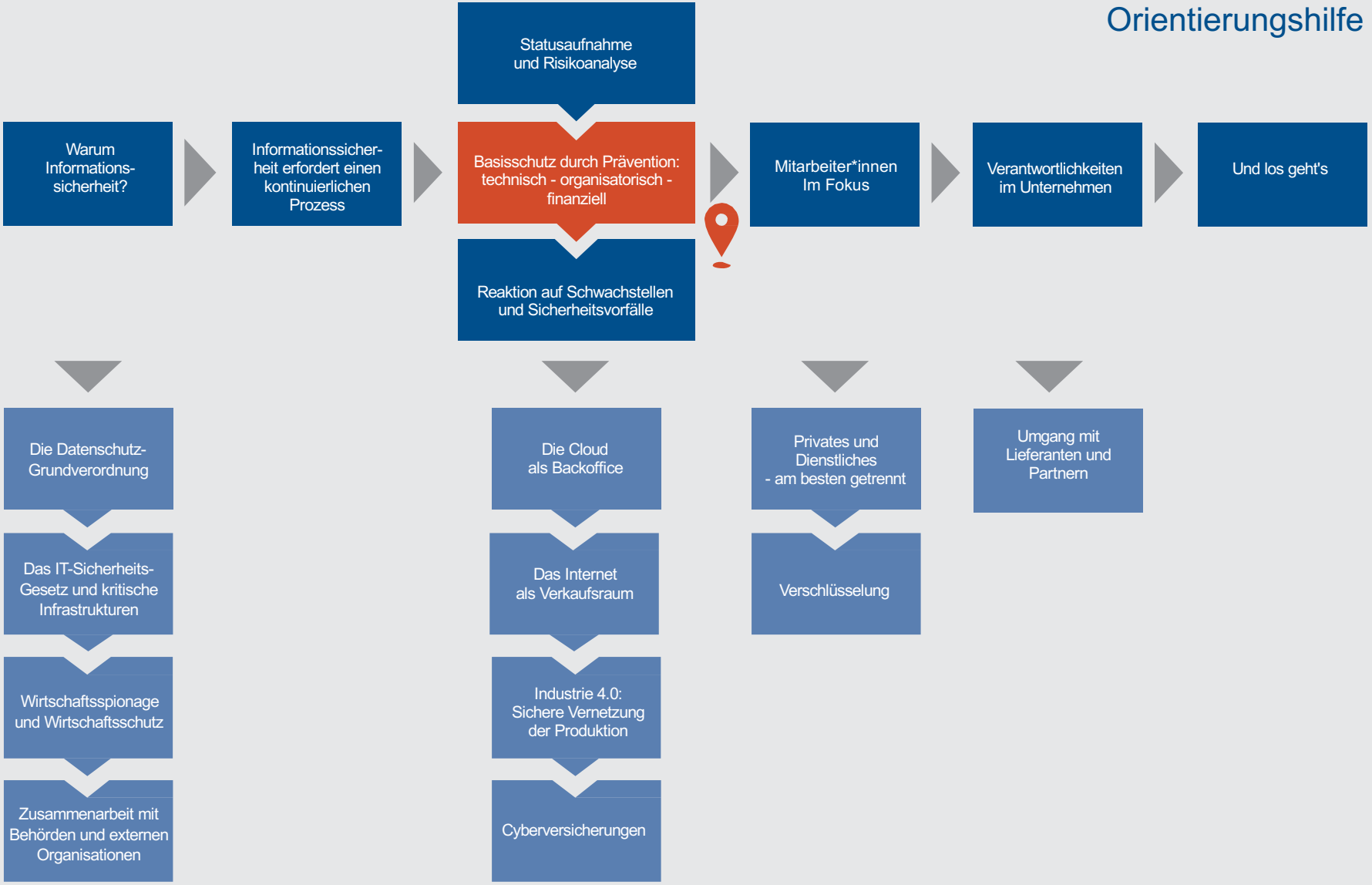
Vermeiden
- Dann: Risikoreiche Tätigkeit unterlassen!

Minimieren
- Geeignete Auswahl von Maßnahmen erforderlich

Überwälzen
- Restrisiken versichern, wenn möglich

Akzeptieren
- Wenn das Risiko klein genug ist

Orientierungshilfe



DIHK

DsiN Deutschland sicher im Netz

Präventionsmaßnahmen

Prävention erfolgt auf verschiedenen Ebenen:

technisch

- Endgeräte
- Infrastruktur

Organisatorisch

- Verhaltensvorgaben
- Dienstaufgaben

Finanziell

- Rückstellungen
- Cyberversicherungen

Empfehlungen

Bei präventiven Maßnahmen wichtig:

- **Angemessenheit** (Kosten-Nutzen-Verhältnis): Ist eine Vereinzelungsanlage zum Zugang in den Bürotrakt angemessen?
- **Nebenwirkungen** und **Aktzeptanz** (Maßnahmen können zu ungewollten Effekten führen): Gibt es zu viele Anforderungen an Passwörter, werden sie aufgeschrieben, und es gibt erkennbare Muster

Tipps aus der Praxis

Bei präventiven Maßnahmen wichtig:

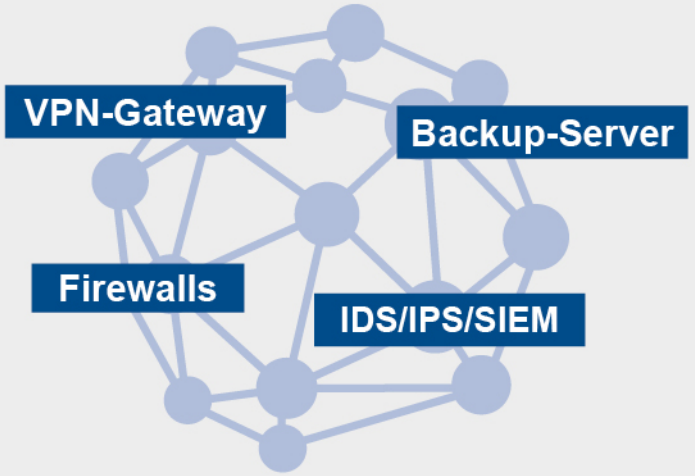
- Informationssicherheitsrisiken mit **hoher Eintrittswahrscheinlichkeit** sollte auf jeden Fall präventiv begegnet werden!
- Risiken mit **hohem Schaden** (und geringer Wahrscheinlichkeit) sollte tendenziell eher mit einer **guten Reaktionsfähigkeit** begegnet werden (und, wenn möglich, einer Versicherung)

Technische Präventionsmaßnahmen

Endgeräte

- Am Wichtigsten: Aktuelle Betriebssysteme und Anwendungen
  - Hilfreich bei größeren Firmen: Patchmanagement
- Anti-Malware-Lösungen
  - Anti-Virus ist immer noch notwendig – aber nicht mehr ausreichend!
- Backup-Lösung
  - Wichtig: regelmäßig einspielen!

Infrastruktur



Meist werden Basisdienste hierfür schon von guten DSL-Gateways mitgeliefert.

Tipp: Verwenden Sie Cloud-Services, diese bringen viel Sicherheit von Anfang an mit!

DIHK

DsiN Deutschland sicher im Netz

Organisatorische Präventionsmaßnahmen

Verhaltensvorgaben ggf. in eigenen Richtlinien

- Nutzung von Anwendungen / technischen Systemen, z.B.
  - Keine offenen WLAN-Hotspots!
  - Mobile Endgeräte: Was darf damit gemacht werden?
  - WhatsApp, Chat-Programme: Was soll freigegeben werden?
  - Dropbox, Foren: Dürfen diese verwendet werden? Wofür?
- Keine zusätzlichen Netzwerk-Schnittstellen, da damit neue Angriffspunkte entstehen
  - Insbesondere in der Produktion: keine Geräte mit „eigener“ Internet-Anbindung
- Keine ungeprüfte Verbindung von Firmen-Endgeräten (Laptops, Smartphones) mit anderen WLAN-Netzen
  - Besser: Flatrate bei Mobilfunk-Dienstleister buchen!

Sicherheits-Dienstleistungen

Die folgenden Tätigkeiten eignen sich für das Outsourcing:

- Wachschutz
- Penetrationstests
- Angriffserkennung
- Notfallmanagement

Achten Sie dabei darauf, dass Ihre Sicherheitsanforderungen auch durch den Dienstleister erfüllt werden.

Finanzielle Präventionsmaßnahmen

Rückstellung

- Nach Minimieren der Risiken durch geeignete Maßnahmen legen Sie Rückstellungen in der Höhe der Restrisiken an
- Umgekehrt sollten Maßnahmen nie mehr kosten als die damit verbundene Risikosenkung (über 3 Jahre)
  - Und speziell nie mehr als die möglichen Wiederherstellungskosten bei Schäden!

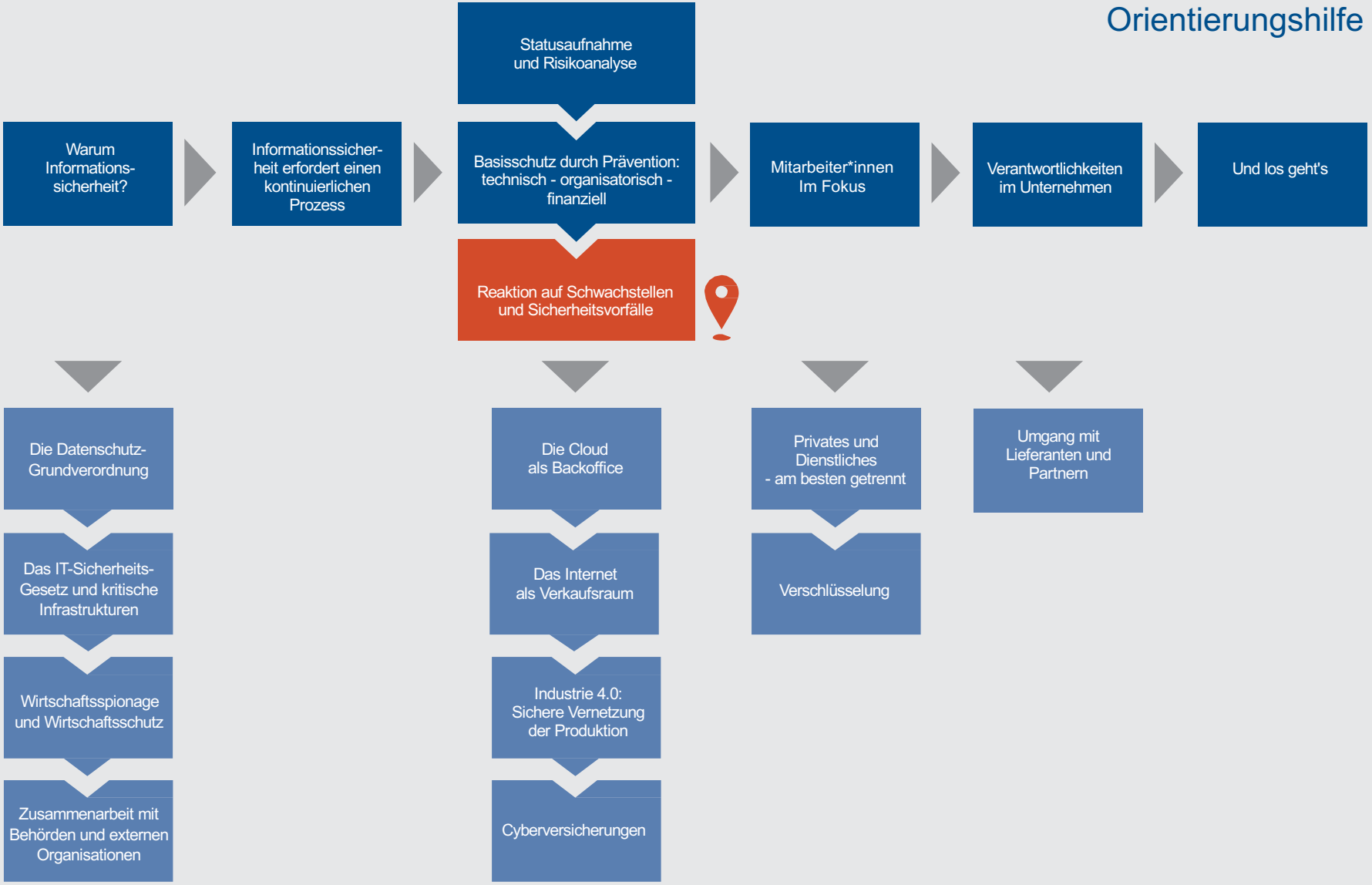
Cyberversicherungen

- Sind dazu da, die Restrisiken nach Ergreifen von Sicherheitsmaßnahmen finanziell abzusichern
- Setzen unterschiedliche Maßnahmen voraus
  - Basisschutz-Maßnahmenpaket
  - Informationssicherheits-Managementsystem
- Helfen bei der Sofortreaktion / dem Notfallmanagement

DIHK

DsiN Deutschland sicher im Netz

Orientierungshilfe



DIHK

DsiN Deutschland sicher im Netz

Schwachstellen vs. Vorfälle

Schwachstelle

- Ist latent vorhanden
- Bietet Hacker*innen die Möglichkeit anzugreifen
  - z.B. durch Verwendung von „Exploits“
- Kann aber auch ein „Fehler“ in einem Sicherheitskonzept sein
- Müssen gemanagt werden, um die aktuelle Risikolage einschätzen zu können
  - Und ggf. kompensierende Maßnahmen zu ergreifen

Vorfall („Incident“)

- Hier besteht akute Gefahr
- Beispiele: Abhören, Datendiebstahl, Sabotage, Identitätsklau, CEO Fraud
- Schwachstellen werden ausgenutzt
- Müssen aktiv bearbeitet werden (wie gerade ausgebrochenes Feuer)
  - Sonst kann der Schaden evtl. nicht mehr begrenzt werden

DIHK

DsiN Deutschland sicher im Netz

Umgang mit Schwachstellen und Vorfällen

Schwachstellen vermeiden

- Betriebssysteme und Anwendungen möglichst aktuell halten
- Dafür: aktuelle Patches und Updates der Hersteller schnellstmöglich einspielen
- Sicherheitskonzepte regelmäßig überprüfen

Betroffenheit feststellen

- Informationen über Schwachstellen auch aus anderen Quellen sichten
- **Dafür: Informationsdienste abonnieren und Empfehlungen prüfen**
  - **DsiN Sicherheitsbarometer**
  - **BSI BürgerCERT**
- Sofortmaßnahmen einleiten, wenn sehr hohes Risiko gegeben

Angriffe erkennen

- Software und Hardware mit Sonden versehen
- Auffälligkeiten analysieren (lassen)
  - Für KMU: am besten als Dienstleistung beauftragen
- Sofortmaßnahmen ergreifen (Notfallplan)
- Forensische Beweismittelsicherung beauftragen
  - Schalten Sie Experten, ggf. auch Polizei und BKA ein!

Schaden begrenzen

- Notfallpläne entwickeln
- Erstreaktion trainieren
- Digitale Ersthelfer*innen bestimmen
- Das Einspielen von Backups regelmäßig testen

DIHK

DsiN Deutschland sicher im Netz

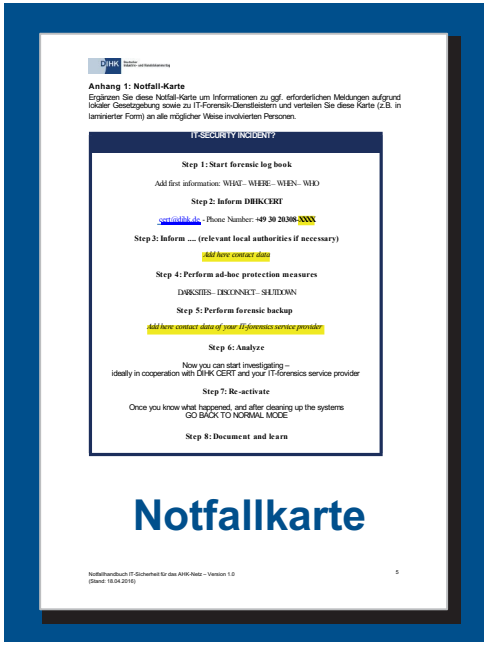
Angriffe erkennen und bearbeiten

IT-Sicherheitsangriffe sind normal – lernen Sie, damit umzugehen!

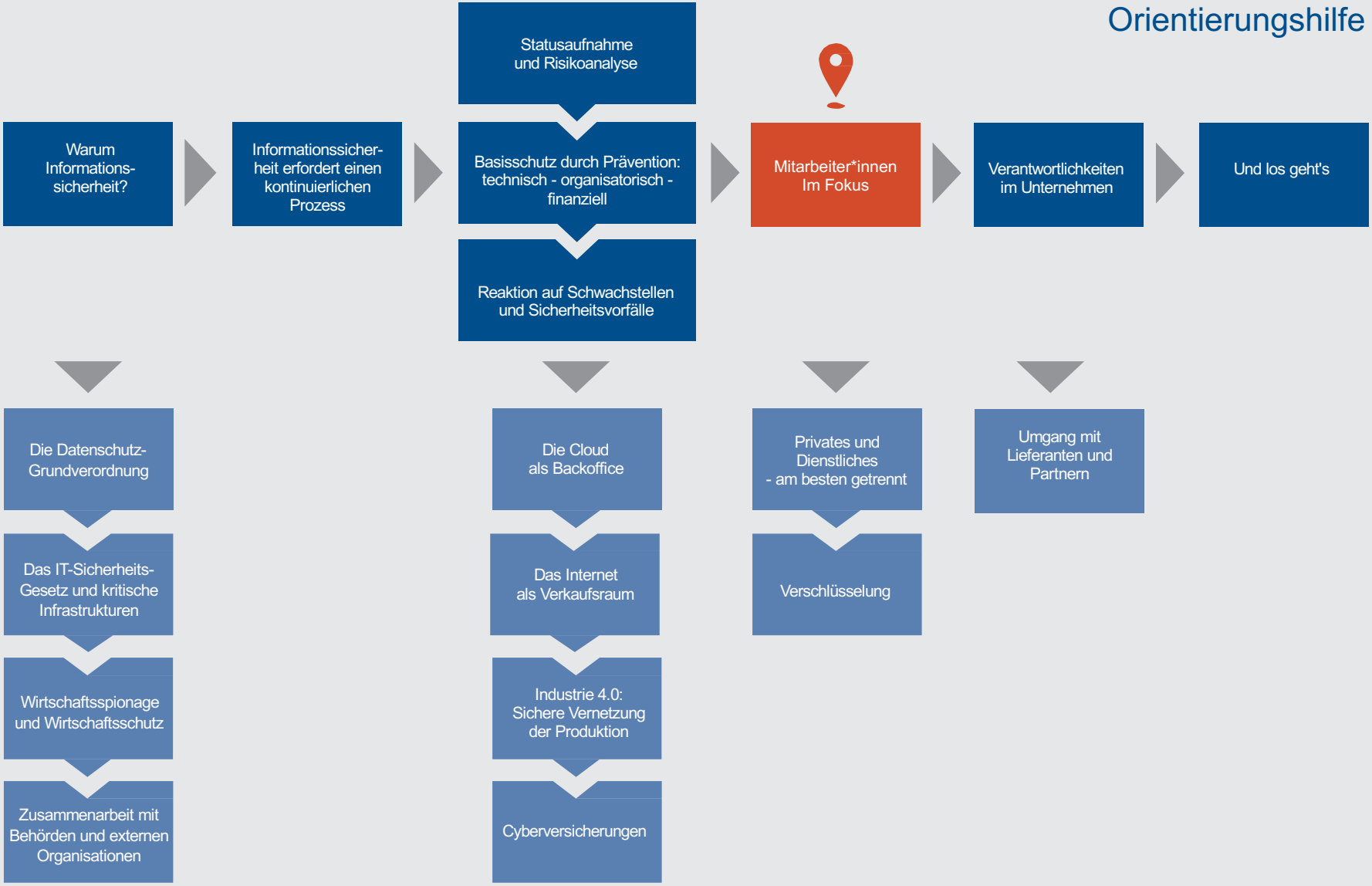
Netzwerkangriffe: Arbeiten Sie mit einem professionellen Dienstleister zusammen („Security Intelligence“) – oft zusammen mit Netzwerk-Dienstleistungen im Angebot

Angriffe auf **Anwendungen**: Regelmäßige Prüfungen von Log-Dateien sind PFLICHT

Angriffe auf **Menschen**: Verdachtsmomente sollten gemeldet werden – keine Angst vorm Anschwärzen!



Orientierungshilfe



DIHK

DsiN Deutschland sicher im Netz

Die Mitarbeiter*innen: die beste Sicherheitsmaßnahme

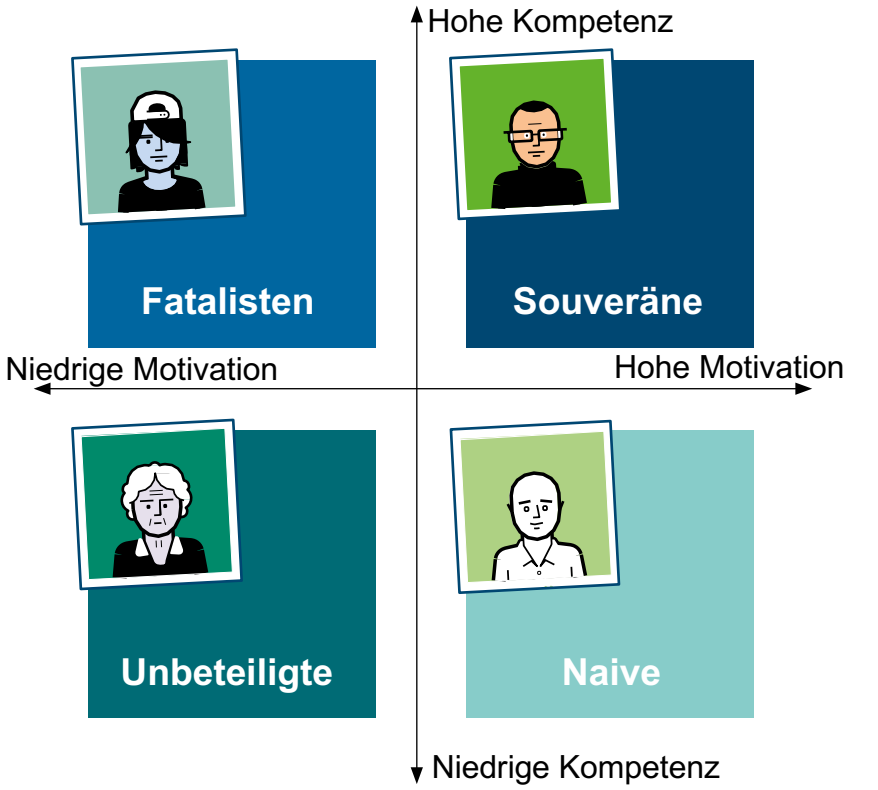
Vom Risiko zur Maßnahme

- Menschen sind (immer noch) die entscheidenden Faktoren für die Sicherheit Ihrer Informationen
- Kein Sicherheitsbewusstsein sowie Unkenntnis bilden ein großes Risiko
- Aufmerksame und geschulte Mitarbeiter*innen können sicher mit den Systemen umgehen

Es gibt unterschiedliche kritische Gruppen von Mitarbeiter*innen

- Zentrale Leitfiguren (haben strategische Informationen)
- Umsetzungschampions (Vernetzung operativer Kenntnisse und Zugänge)
- Vagabunden (BA-Studierende, Trainees, ...) mit „gesammelten“ Berechtigungen

Verschiedene Nutzertypen



Sensibilisierung und Kompetenzentwicklung

Steigerung der Sensibilität

Unterbewusstsein

- Durch Awarenesskampagnen
  - Poster, Flyer,...
  - Veranstaltungen
  - Gamification
- Zielgruppenspezifische Gestaltung
  - Für Führungskräfte
  - Für Techniker*innen
  - ...
- Ansprechen des *Unterbewusstseins*

Entwicklung des Wissens

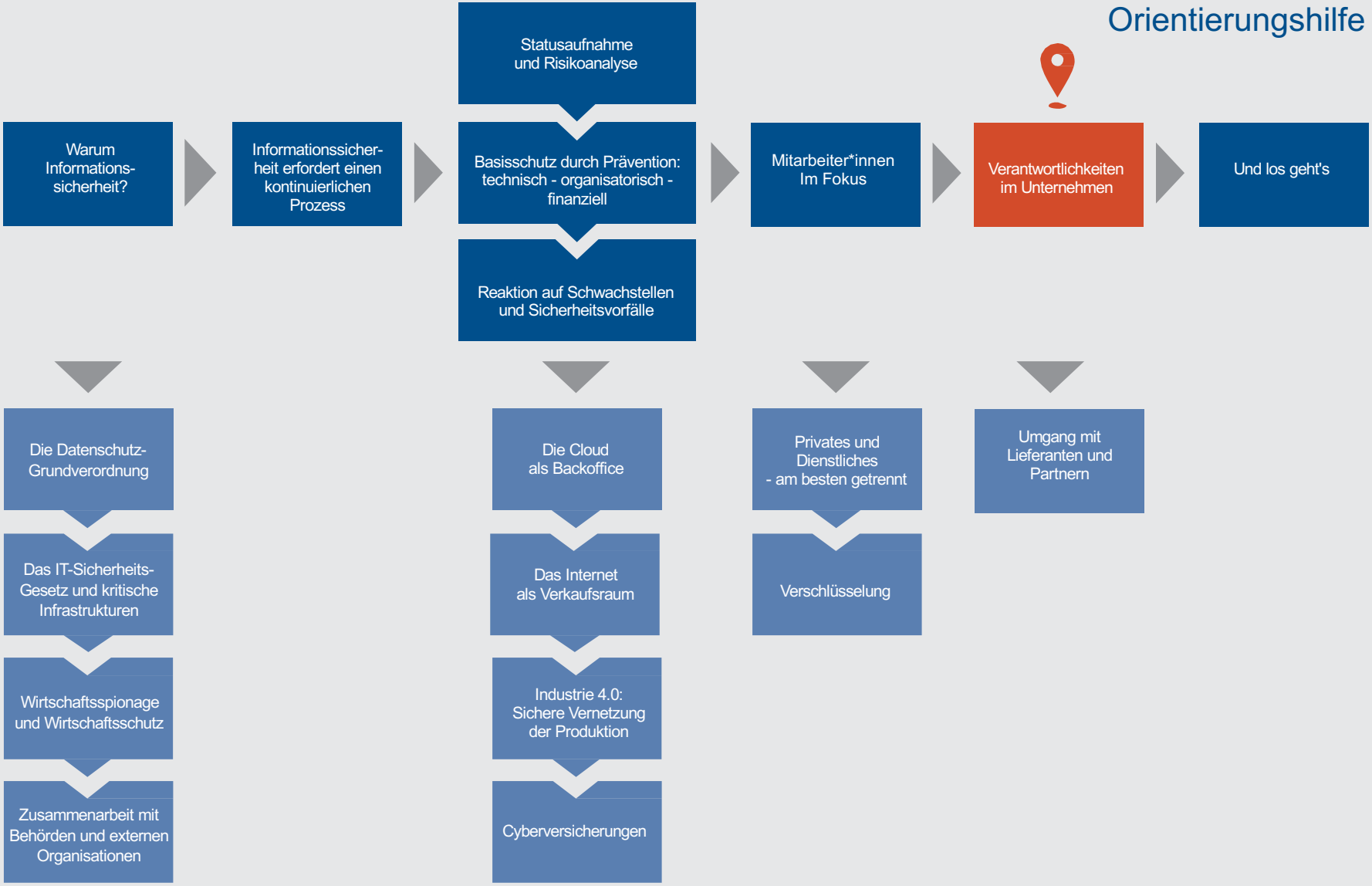
Bewusstsein

- Durch Training
  - Online-Module
  - Seminare
  - Lernmaterial
- Themenspezifische Zusammenstellung
  - Smartphone-Gefahren
  - Vertrauliche Dokumente
  - ...
- Ansprechen des *Bewusstseins*

DIHK

DsiN Deutschland sicher im Netz

Orientierungshilfe



DIHK

DsiN Deutschland sicher im Netz

Verantwortlichkeiten

Geschäftsleitung, Führungskräfte

- Sind für die Sicherheit verantwortlich
- Entscheiden über den Umgang mit Risiken
- Entscheiden über das Ergreifen von Maßnahmen

Informationssicherheitsbeauftragte

- Werden von Geschäftsleitung benannt
- Haben direkten Berichtsweg zur Geschäftsleitung
- Sorgen für Risikotransparenz
- Schlagen Maßnahmen vor
- Organisieren Awareness und Training

DIHK

DsiN Deutschland sicher im Netz

Erstellen Sie eine Sicherheitsleitlinie

Achtung Betriebsrat!
Je nachdem, was in der Richtlinie steht, ist sie ggf. mitbestimmungspflichtig:
- Arbeitsanweisungen
- Informationen, die Leistungskontrolle dienen könnten
- Datenschutzbezogene Aspekte

Inhalte

- Sicherheitsziele
- Verantwortlichkeiten
- Sicherheitsprozess
- Wichtige Maßnahmen
- Konsequenzen

Tipps aus der Praxis

- Diese Richtlinie muss von der Geschäftsleitung beschlossen und an alle Mitarbeiter*innen aktiv kommuniziert werden
- Sie muss regelmäßig (z.B. jährlich) auf Aktualität überprüft werden
- Lassen Sie sich eine Richtlinie von externen Expert*innen für Ihr Unternehmen erstellen
- Kosten: ca. 3 Tage

Ach ja: die Rolle der IT-Abteilung

IT-Abteilung / IT-Dienstleister*innen

- Setzen Maßnahmen um
- Müssen Sicherheitsvorgaben umsetzen
- Definieren NICHT die Sicherheit
- Grund: haben Schutz ihrer Dienste im Blick, nicht den Schutz der Informationen

IT-Dienstleistung:

- Leistungserbringung für allgemeine Tätigkeiten
- Leistungserbringung für Geschäftsprozesse
- Hier treten **Bedrohungen** und **Schwachstellen** auf

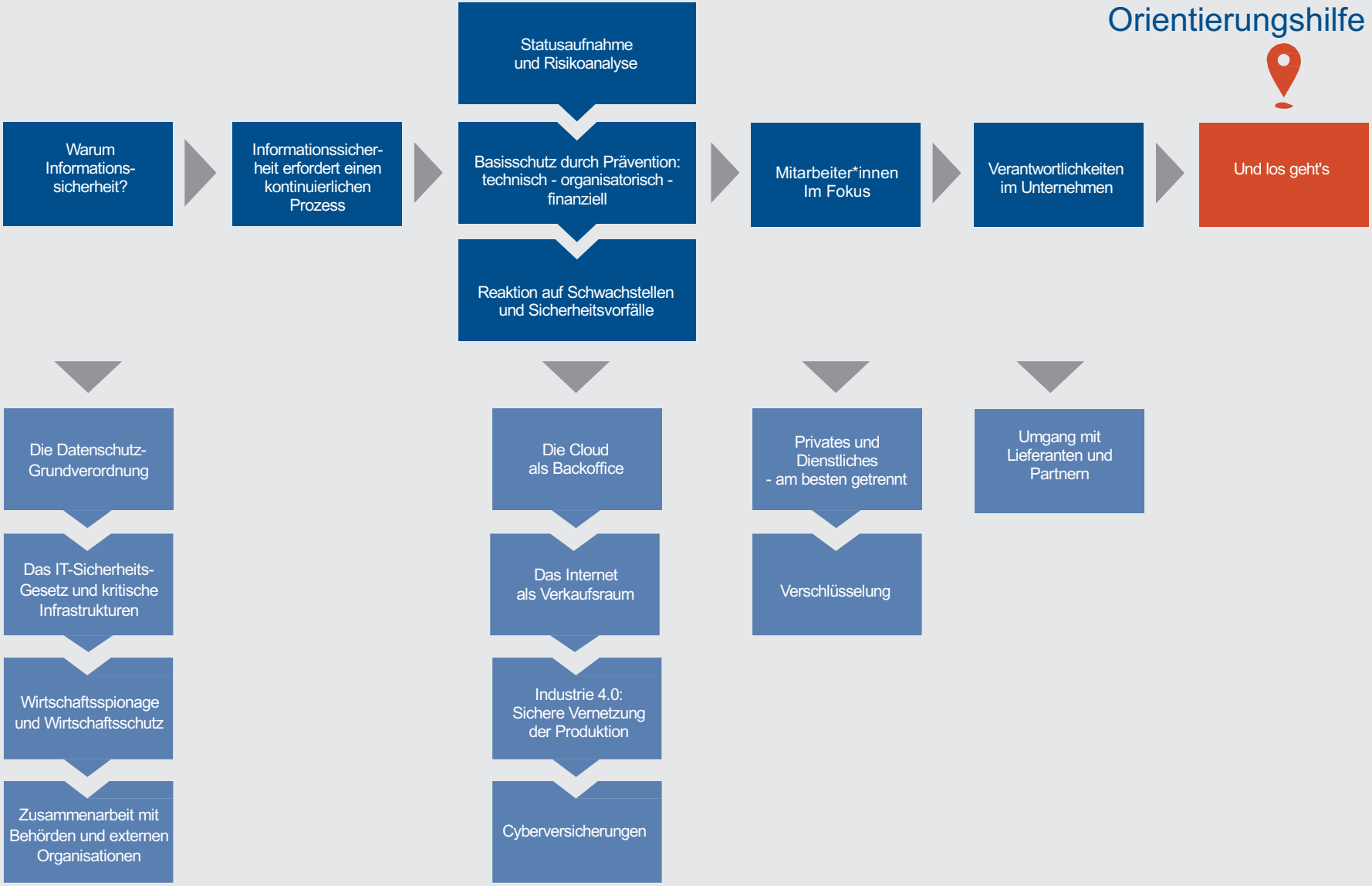
Geschäftsbereich:

- Verwendung von IT für eigene Leistungerbringung
- Hier können entstehende **Risiken bewertet** werden

DIHK

DsiN Deutschland sicher im Netz

Orientierungshilfe



DIHK

DsiN Deutschland sicher im Netz

Wie fange ich an?

Erste Schritte

- Risikoanalyse
- Erste präventive Maßnahmen bestimmen
- Verantwortlich-keiten festlegen
- Sicherheitsleit-linie erstellen und veröffentlichen
- Awareness planen
- Notfallplan erstellen

Ziele für das erste Jahr

- Risiken sind transparent
- Bestehende Maßnahmen sind in ihrer Wirkung verstanden
- Alle Bereiche sind Verantwortlichen zugeordnet
- Mitarbeiter*innen kennen alle die Leitlinie
- Awareness-Konzept erstellt
- Digitale Erst-Helfer*innen ernannt

DIHK

DsiN Deutschland sicher im Netz

Wo bekomme ich Hilfe?

Verschiedene Berater:

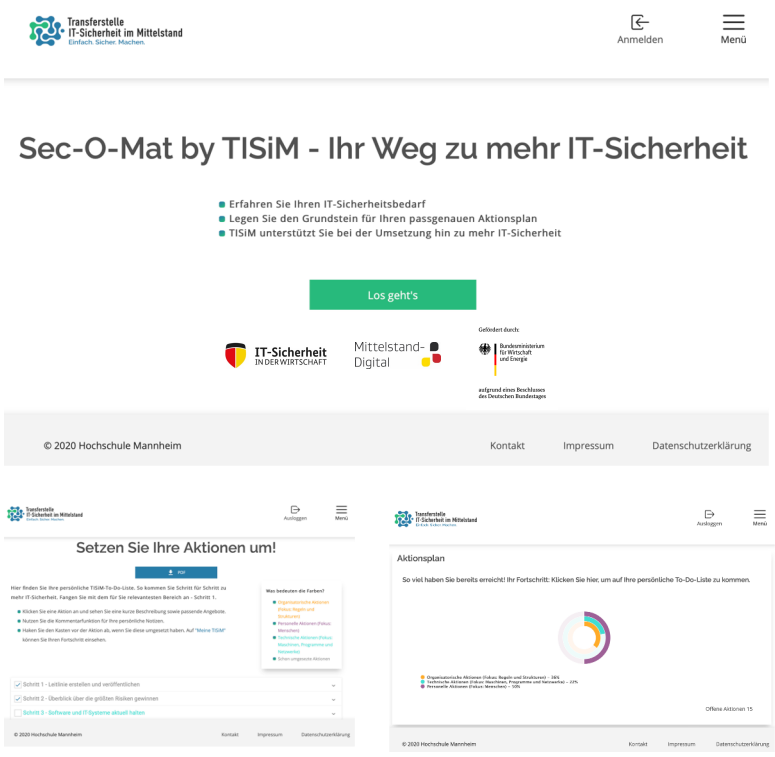
- IHK & DsiN
- E-Business-Lotsen
- Wirtschaftsprüfer*innen
- IT-Systemhäuser
- TISiM: tisim.de
- Externe Berater haben
  - hohes Fachwissen und Branchen-Know-How...
  - ...kennen aber die unternehmensinternen Zusammenhänge nicht
  - Zudem geht Wissen oft verloren

Tipps aus der Praxis

- Führen Sie **Tandem-Teams** ein:
  Jede externe Expertise muss intern begleitet werden
- Umsetzungsverantwortung bleibt immer intern
- Vereinbaren Sie keine Werksverträge, auch wenn es finanziell attraktiver erscheint
- U.U. wird an der Qualität gespart
- Etablieren Sie eine langfristige Partnerschaft
- Nutzen Sie den Berater/die Beraterin als „Teilzeit“-Experten/Expertin
- Nutzen Sie Plattformen für die geeignete Berater*innen-Auswahl z.B. den IT-Sicherheits-Navigator des BMWi

Welche Hilfe bieten DsiN / DIHK?

Sec-O-Mat (www.sec-o-mat.de)



Vorlagen-Dokumente für

- Leitlinie
- Nutzungsrichtlinie
- IT-Sicherheitshandbuch
- Risikoanalyse
- Notfall-Karte
- Regelmäßiger Risikobericht

Datenschutz:

- Verzeichnis der Verarbeitungstätigkeiten
- Datenschutzfolgeabschätzung
- Antrag Betroffenenrechte
- Auskunft Verarbeitung von Daten
- Meldung Datenpanne

DIHK

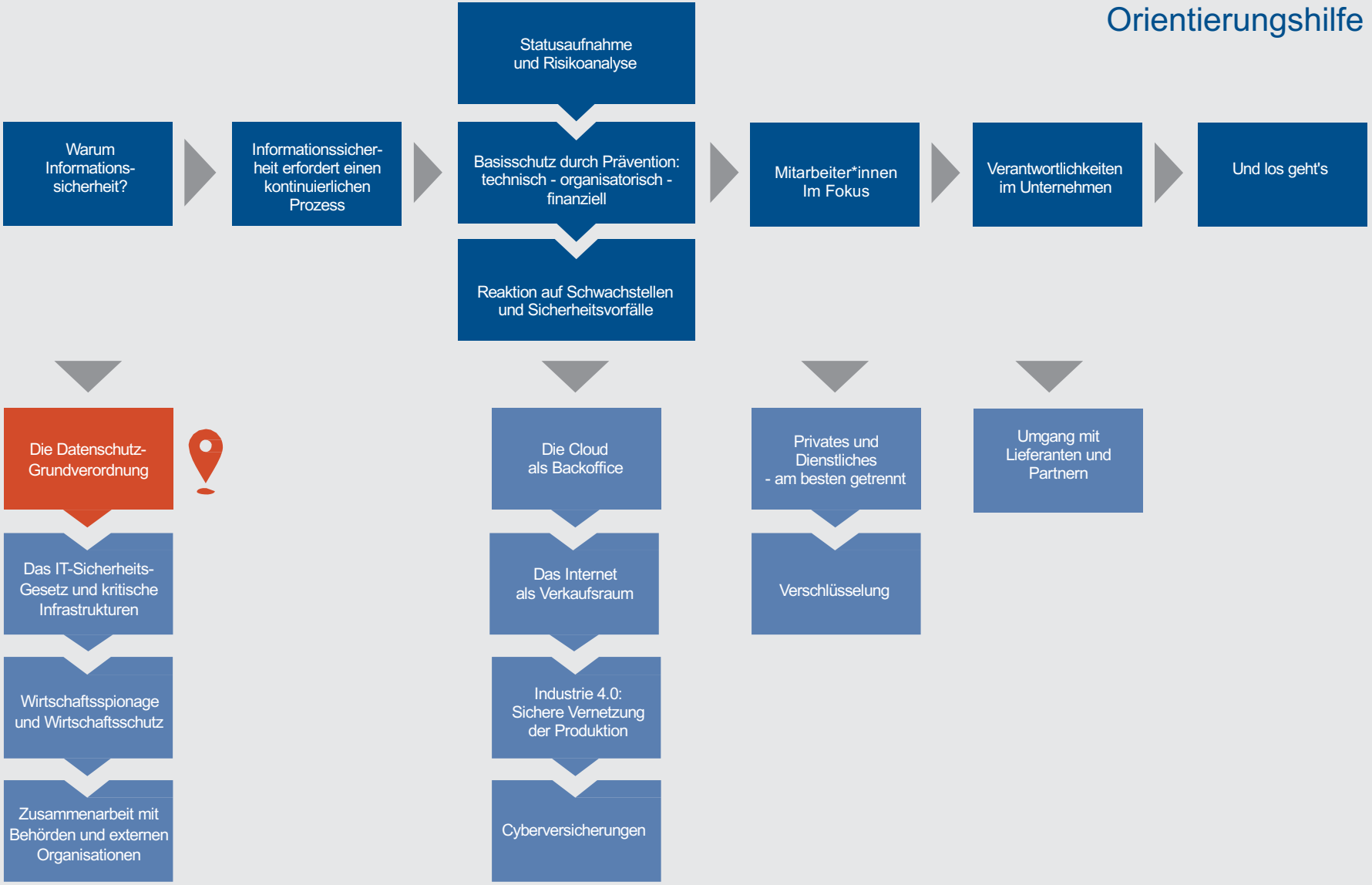
DsiN Deutschland sicher im Netz

Zusatzmodule

DIHK

DsiN Deutschland sicher im Netz

Orientierungshilfe



DIHK

DsiN Deutschland sicher im Netz

DSGVO: Gemeinsamkeiten und Unterschiede zum ISMS

ISMS

- Management-System: regelmäßige Überprüfung der Wirksamkeit und Angemessenheit der Maßnahmen
- Schutzziele definiert das Unternehmen für sich
  - Außer gesetzlich geregelt, z.B. ITSG
- Zertifizierung möglich:
  - IT-Grundschutz (BSI)
  - ISO 27001
  - VdS 3473

DSGVO

- Management-System: regelmäßige Überprüfung der Wirksamkeit und Angemessenheit der Maßnahmen
- Schutzziele gesetzlich vorgeschrieben: personenbezogene Daten (Mitarbeiter*innen, Kund*innen, ...)

☞ Empfehlung:

Nehmen Sie die DSGVO-Schutzziele in Ihr ISMS mit auf!

DIHK

DsiN Deutschland sicher im Netz

DSGVO: Was ist zu tun?

Notwendige zusätzliche Aktivitäten

- **Transparenz über Verarbeitung der Daten von Betroffenen (Mitarbeiter*innen, Kund*innen, …):**
  - Datenschutzerklärung erstellen
- **Umsetzung Rechte Betroffener:**
  - Auskunftsstelle vorsehen
  - Herausgabe / Korrektur / Löschung planen
- **Verzeichnis der Verarbeitungstätigkeiten:**
  - Mit Risikobewertung aus Sicht der Betroffenen und ggf. ADV-Verträgen
  - Bei hohem Risiko: Datenschutz-Folgeabschätzung
- **Löschprozess einführen:**
  - Nach Aufbewahrungsfrist Daten löschen!

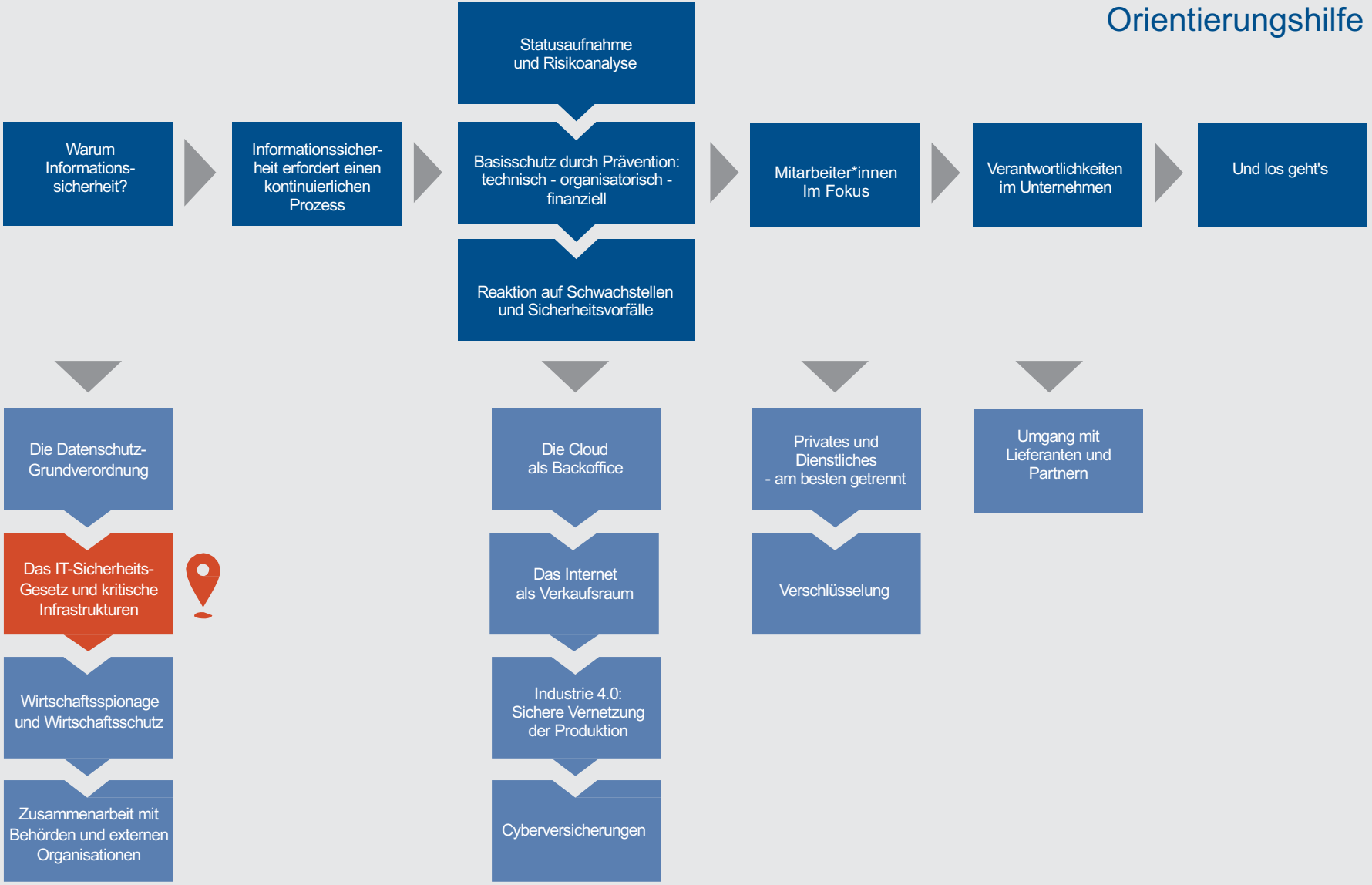
Wer ist betroffen?

- **Alle Unternehmen**
  - Seit Mai 2018 Übergangsfrist abgelaufen
  - Produkthersteller: „Privacy by design“ beachten
  - Muss mein Unternehmen einen Datenschutzbeauftragten stellen?

DIHK

DsiN Deutschland sicher im Netz

Orientierungshilfe



DIHK

DsiN Deutschland sicher im Netz

Das IT-Sicherheitsgesetz

Was wird geregelt?

- Einführung eines ISMS zum Schutz kritischer Infrastrukturen verpflichtend
- Schutzziele gesetzlich vorgegeben
- Ggf. zusätzliche Anforderungen an Schutzmaßnahmen pro Branche

Wer ist betroffen?

- Alle, die Zugang zu Netzdiensten anbieten (E-Mail, Telefonie, etc.)
- Alle die Informationen und Dienste online anbieten (Websites, Online-Shops, etc.)
- Betreiber*innen kritischer Infrastrukturen mit einem Wirkungskreis von > 500.000 Bürgern

DIHK

DsiN Deutschland sicher im Netz

Das IT-Sicherheitsgesetz – was ist zu tun?

Für alle Betroffenen

- Einführung eines Informations-sicherheits-Management-Systems
  - Beachtung der im Gesetz formulierten Schutzziele
- Bestätigung der Wirksamkeit durch eine Zertifizierung (nach ISO 27001 oder IT-Grundschutz)

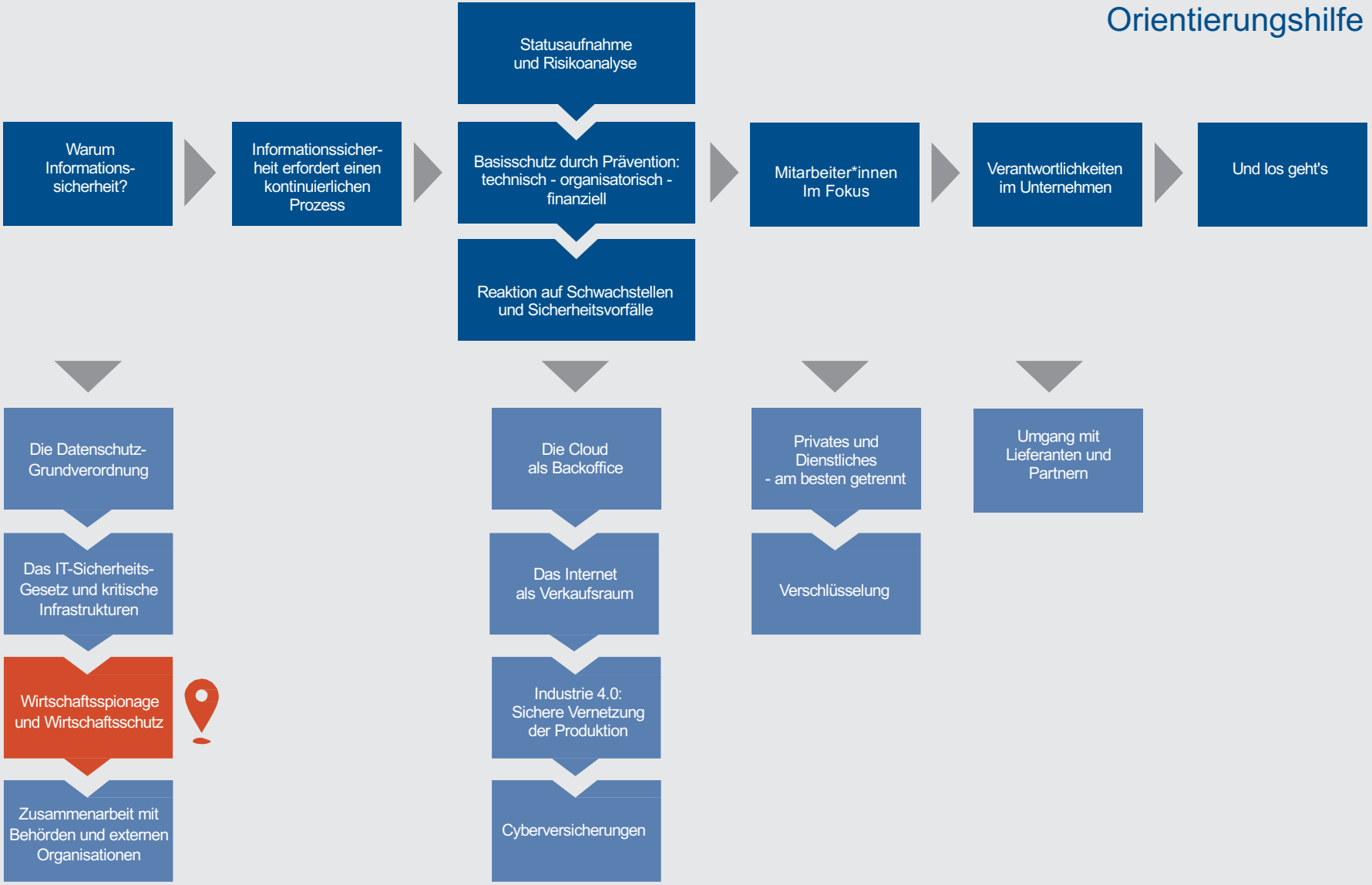
Branchenspezifische Zusatzanforderungen

- Meldestelle einrichten
- Meldung von kritischen Schwach-stellen und Vorfällen
- Ggf. Umsetzung weiterer Schutzmaß-nahmen („Maßnahmenkataloge“)
- Für Produkthersteller*innen: Mitwirkung bei der Bewertung und Beseitigung von Schwachstellen
- Für Telemediendienste-Anbieter: Websites nach Stand der Technik

DIHK

DsiN Deutschland sicher im Netz

Orientierungshilfe



DIHK

DsiN Deutschland sicher im Netz

Wirtschaftsspionage

Wie erkenne ich Wirtschaftsspionage?

- Nicht an einzelnen Aspekten – ausschließlich in der Korrelation verschiedener Beobachtungen
- Das Ergebnis hingegen kann man oft gut an internationalen Konkurrenten erkennen:
  - Sehr ähnliche Produkte
  - Innovationsbeschleunigung
  - Marktanteile stark ansteigend

Was kann ich tun? Wo bekomme ich Hilfe?

- Es gibt keine offizielle behördliche Unterstützung
  - Außer für geheimschutzbetreute Unternehmen
- Hilfe gibt es:
  - Bei den Landesämtern für Verfassungsschutz (LfV)
  - Bei den Verbänden für Sicherheit in der Wirtschaft (VSW)

DIHK

DsiN Deutschland sicher im Netz

Neue EU-Richtlinie zum Geheimnisschutz (Juni 2016)

Was wird geregelt?

- Einheitliche Europäische Mindest-standards zum Schutz von Betriebs- und Geschäftsgeheimnissen
- Einheitliche Definition eines „Geschäftsgeheimnisses“
- Angemessene Schutzmaßnahmen Voraussetzung für Schadensersatz-ansprüche

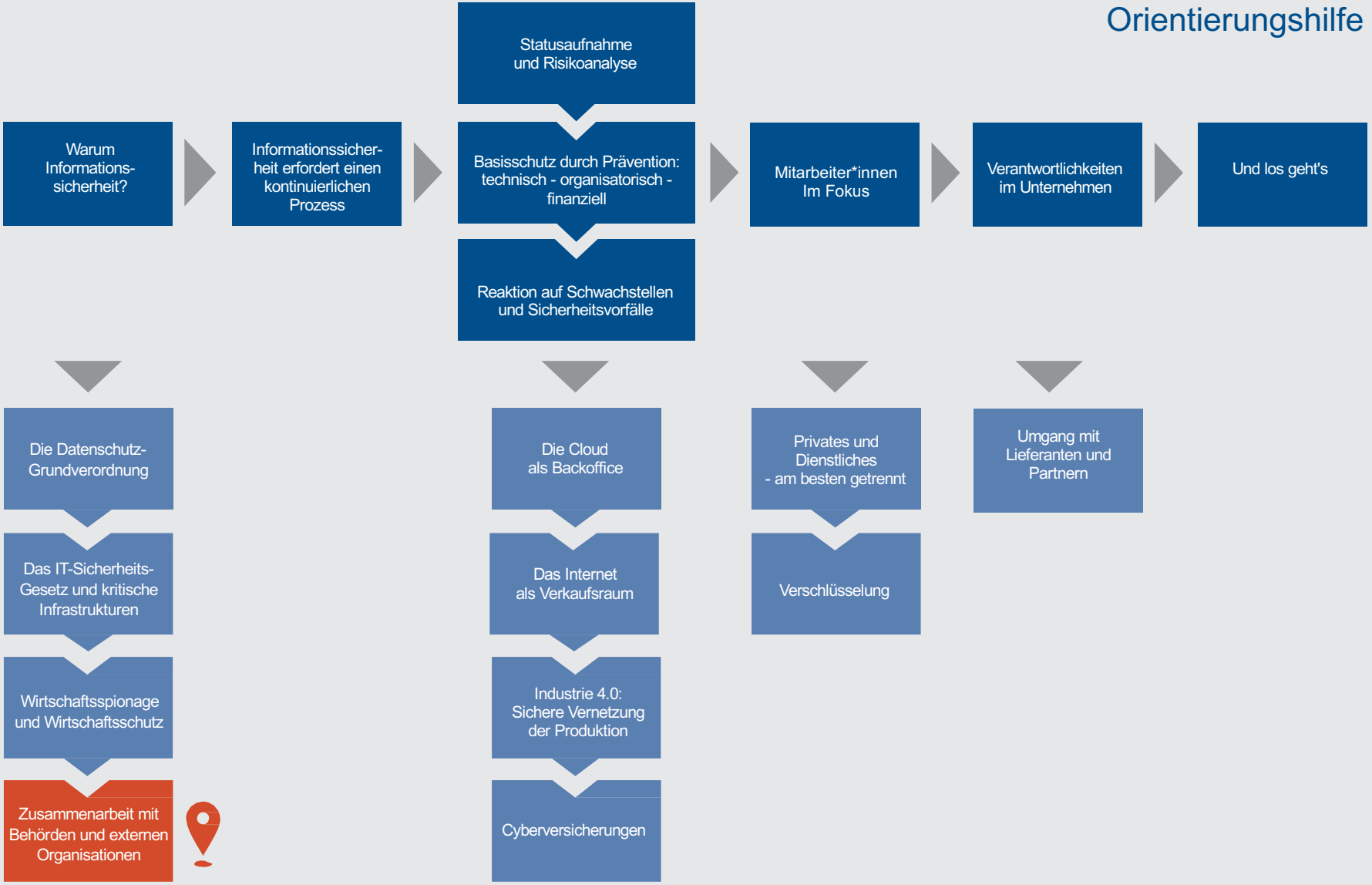
Was bedeutet dies für mich?

- Verschiedene Gesetze (UWG, BGB, …) müssen in Deutschland geändert werden
- Reverse Engineering eines öffentlich erhältlichen Produkts ist nicht mehr strafbar (!)
- Wirksames ISMS bildet Grundlage für Schadensersatz

DIHK

DsiN Deutschland sicher im Netz

Orientierungshilfe



DIHK

DsiN Deutschland sicher im Netz

Zusammenarbeit mit Behörden

Wer hat welche Aufgabe? (u.a.)

- Polizei: Strafverfolgung
- Anwälte: Interessensvertretung im Zivilrecht
- Landeskriminalamt: Gefahrenabwehr
- Verfassungsschutz: Informationssammlung zu sicherheitsgefährdenden Entwicklungen für fremde Mächte
- BSI: technische Kompetenz (für Behörden (u.a.) bindende Vorgaben)

Was kann ich von wem erwarten?

- Polizei: Beweisaufnahme
- Anwälte: Prüfen und Durchführen von Zivilklagen wg. Schadensersatz
- LKA: Ermittlungen bei Verdacht auf Organisierte Kriminalität
- LfV: Unterstützung bei Wirtschaftsspionage
- BSI: Best Practices, aktuelle (technische) Sicherheitsinformationen

DIHK

DsiN Deutschland sicher im Netz

Zusammenarbeit mit anderen Organisationen

Wer hat welches Ziel?

Deutschland sicher im Netz:
Unterstützung im sicheren Umgang mit digitalen Anwendungen und Technologien zur Erhöhung des Sicherheitsbewusstseins

IHK:
Vermittlung von Sicherheits-kompetenz für ihre Mitglieder

Allianz für Cybersicherheit:
Erfahrungsaustausch und Erhöhung der technischen Sicherheitskompetenz (PPP)

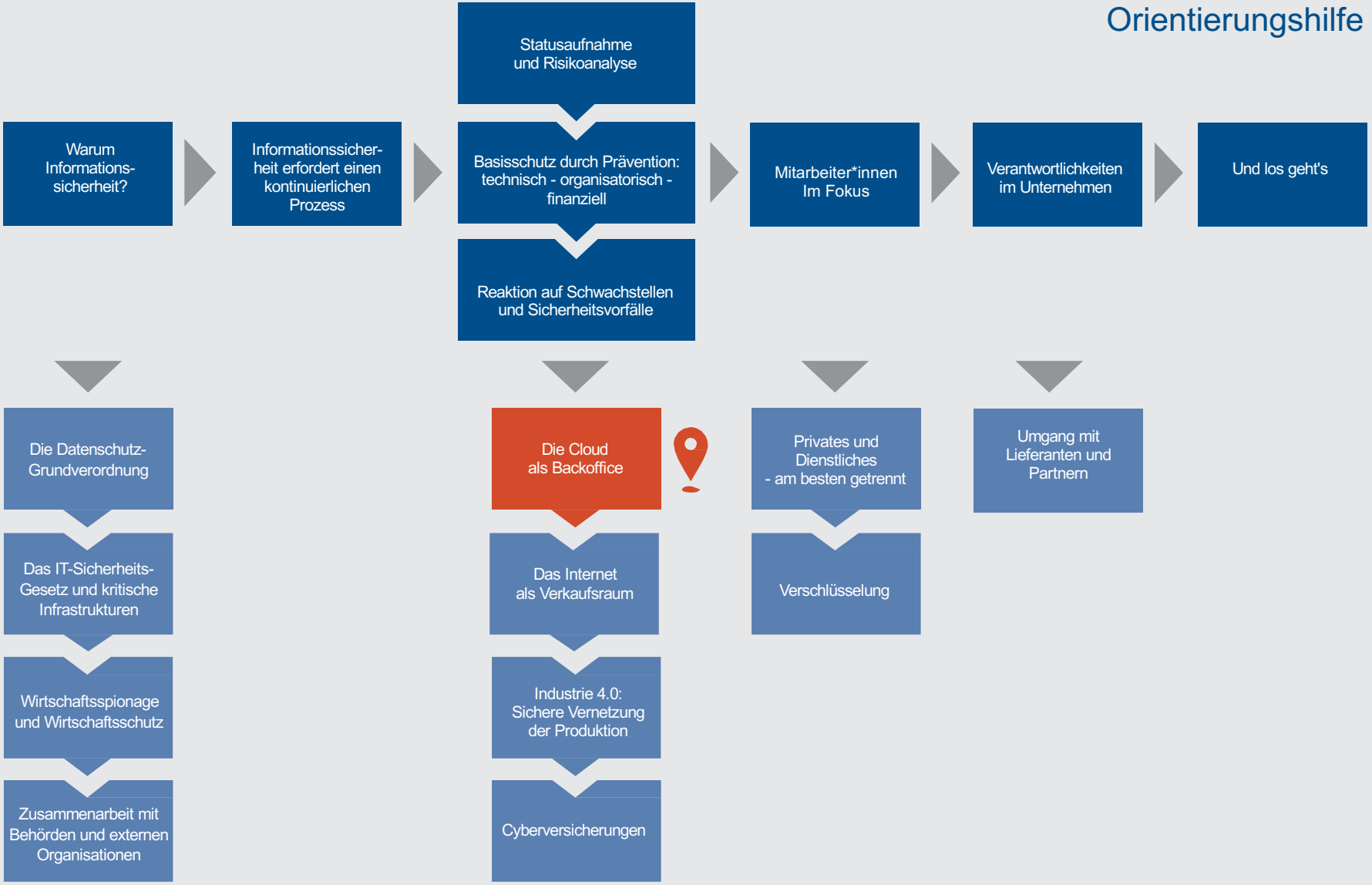
Was kann ich erwarten?

Praxisnahe Aufklärungs- und Schulungsanbegote für Unternehmen im Verbund mit DsiN-Partnern

Weiterbildungen, Werkzeuge. Erfahrungsaustausch mit anderen Unternehmen, Kontakte zu Sicherheitsbehörden

Austausch mit Leidens-genossen, konkrete Handlungsempfehlungen

Orientierungshilfe



DIHK

DsiN Deutschland sicher im Netz

Die Cloud als Backoffice – Risiko oder Segen?

Backoffice als Eigenbetrieb

- Eigener Mail-Server
- Dokumentenablage auf eigenem Netzwerk-Laufwerk
- Eigener Web-Server (intern und extern)
- Eigener Betrieb eines ERP-Systems
- Eigenes Backup-Programm für alle notwendigen Systeme

Backoffice in der Cloud

- E-Mail, Dokumente, Ablage aus der Cloud
- Web-Server werden professionell gehostet
- ERP-Systeme als Web-Anwendung ebenfalls aus der Cloud möglich
- Backup immer vollständig Teil der Leistung
- Managed Security Services

DIHK

DsiN Deutschland sicher im Netz

Eigenbetrieb oder Cloud?

Risiken durch den Eigenbetrieb

- Hohe Kompetenz erforderlich für sicheren Betrieb von allen Servern und Anwendungen
- Hoher Aufwand erforderlich für die kontinuierliche Prüfung und Aufrechterhaltung der Sicherheit
- Oft hohe Aufwände bei Versions-wechsel oder Upgrades
- Backup aus Ressourcengründen oft nicht getestet

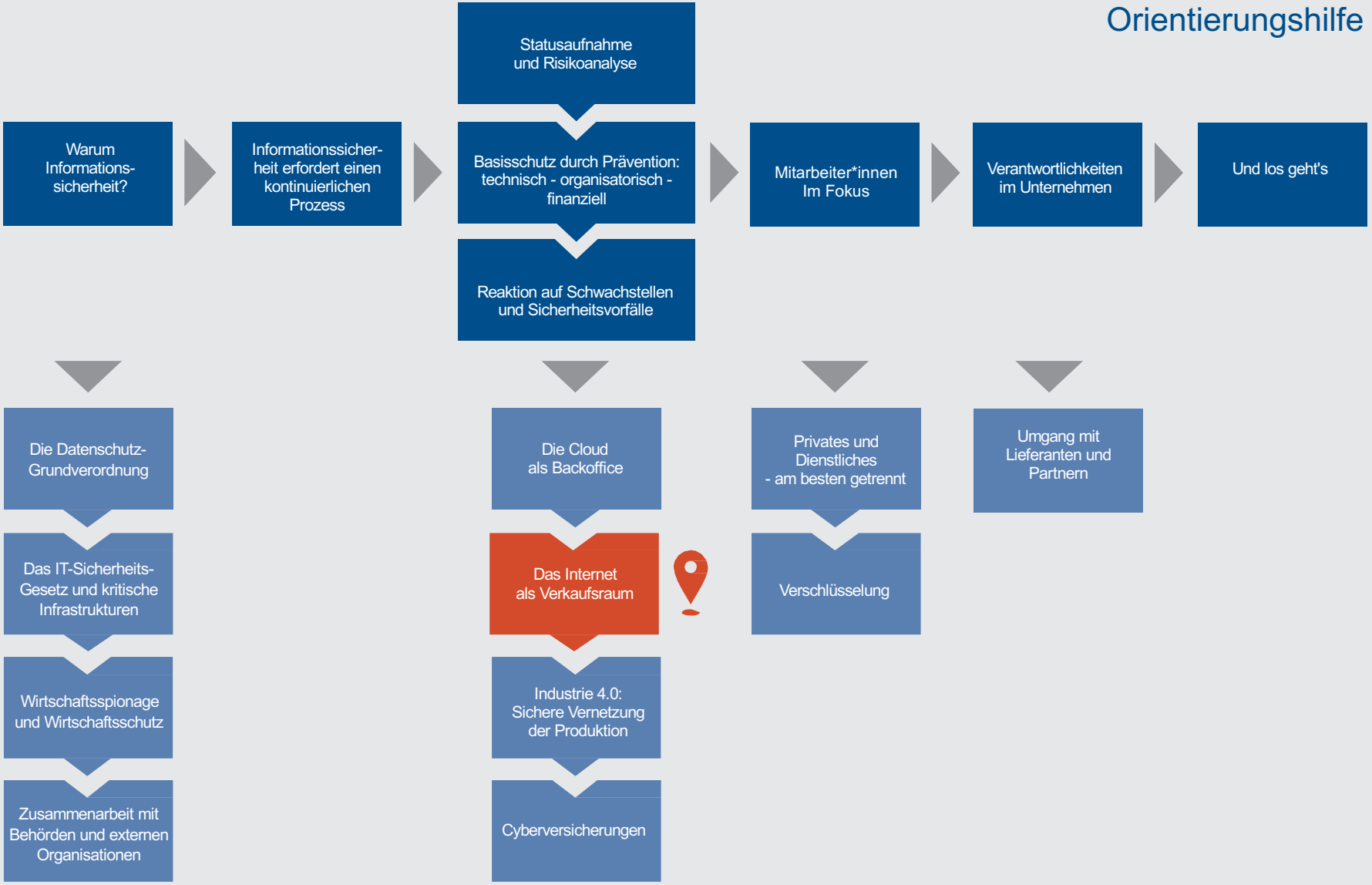
Risiken durch die Cloud

- Vertrauen in Cloud-Service-Anbieter erforderlich
  - Große Anbieter haben oft sehr hohe Kompetenz
  - Nationale Anbieter in Bezug auf Wirtschaftsspionage vertrauenswürdig
- Verfügbarkeit der Daten und Anwendungen von Internet-Anbindung abhängig
- Rückkehr zu Eigenbetrieb oder Wechsel zu anderen Anbietern möglicherweise schwieriger („Lock-In-Effekt“)
- Ggf. keine Datenschutz-Konformität

DIHK

DsiN Deutschland sicher im Netz

Orientierungshilfe



DIHK

DsiN Deutschland sicher im Netz

Das Internet als Verkaufsraum – was ist zu beachten?

Website = Schaufenster

- Hinweis auf die Verwendung von Cookies erforderlich
- Bei Login-Möglichkeit: Beachtung der Datenschutzgesetze
- Website muss sicher sein gegen Malware-Befall (aktuell halten, Schwachstelleninfos beobachten...)
- Umsetzung der Anforderungen des IT-Sicherheits-Gesetzes
- Umsetzung der DSGVO
    - Einwilligung für Werbe-E-Mails vorsehen

Internet-Shop = Ladengeschäft

- Zusätzlich:
    - Umsetzung der Sicherheitsanforderungen bei Zahlungsverkehr
    - Berücksichtigung der Regelungen des Fernabsatzgesetzes
    - Website muss sicher sein gegen aktive Angriffe auf die Verkaufs-Anwendung (aktuell halten, regelmäßige Penetrations-tests,…)
    - DSGVO: Löschprozess für Kundendaten berücksichtigen

DIHK

DsiN Deutschland sicher im Netz

Eigenbetrieb oder Teilnahme an Marktplätzen?

Risiken des Eigenbetriebs

- Aktualität nicht nur von Produkten, auch von Design und Bestellvorgang erforderlich
- Verfügbarkeit durch Serverkapazität selbst sicherstellen
- Unterstützung von vielen Bezahl- und Auslieferungsoptionen erforderlich

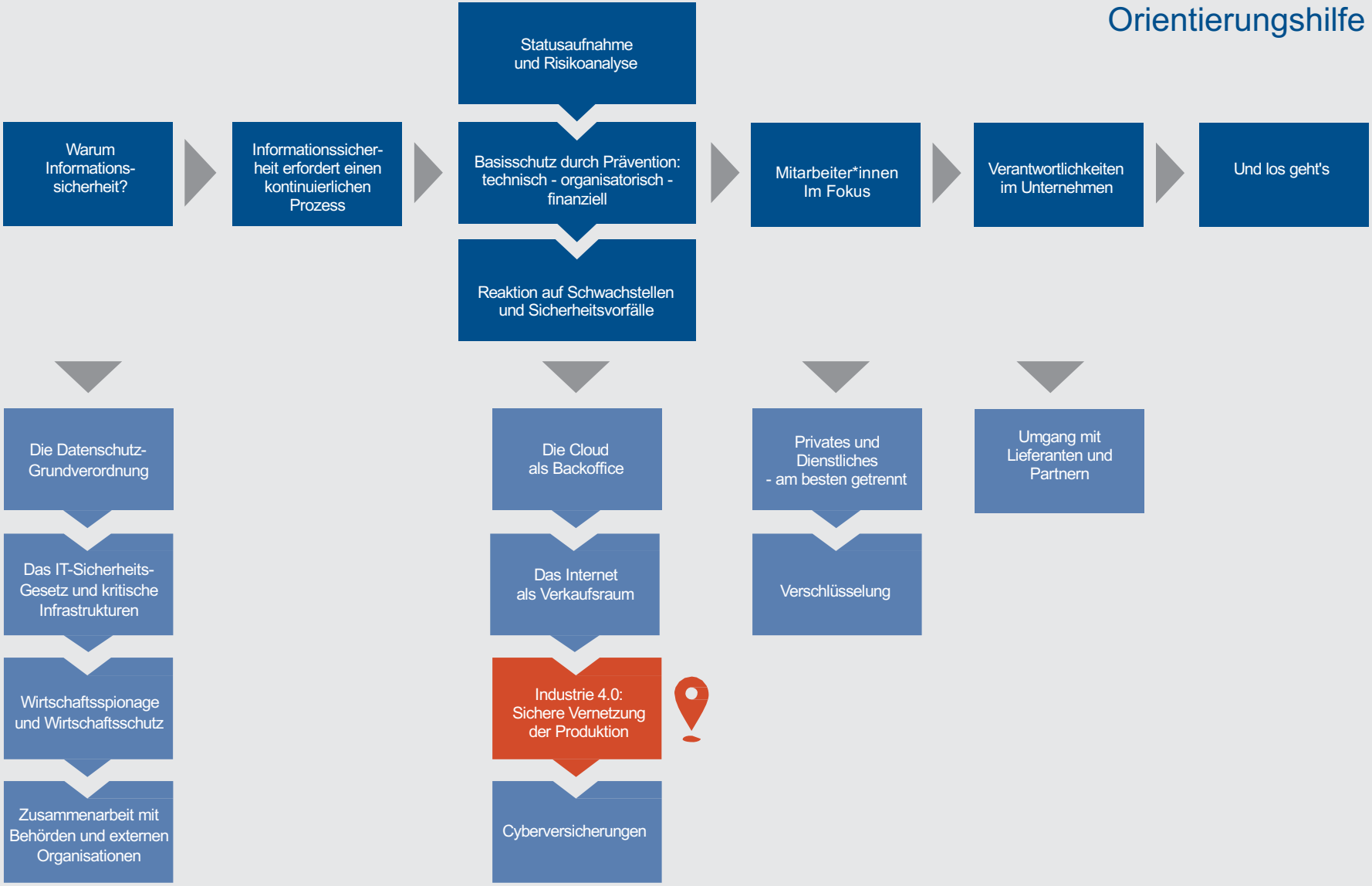
Risiken bei Marktplätzen

- Produkte leicht und schnell durch Konkurrenten auffind- und durchsuchbar = hohe Transparenz
- Abhängigkeit vom Marktplatzbetreiber
  - insbesondere auch hinsichtlich Sicherheitsaspekten

DIHK

DsiN Deutschland sicher im Netz

Orientierungshilfe



DIHK

DsiN Deutschland sicher im Netz

Sichere Vernetzung der Produktion

Besondere Herausforderungen im Vergleich zu „Office IT“

- Produktions-IT oft nicht auf dem aktuellen Stand
- Patchen nicht / nur selten möglich
- Benötigt oft deutlich höhere Verfügbarkeit
- Betreuung meist durch Hersteller der Maschine

Empfehlungen und erste Maßnahmen

Produktionsnetz und Office-Netz trennen

+

Schwachstellen-Management für Produktions-IT einführen

+

Produktions-IT in ISMS aufnehmen

DIHK

DsiN Deutschland sicher im Netz

Anforderungen an Maschinen-Software-Hersteller / -Dienstleister

...in Bezug auf die Software

- Aktuelle Betriebssysteme verwenden, so dass diese gepatcht werden können
- Standardisiertes Identitätsmanagement verwenden, um den Wildwuchs von Konten/technischen Benutzern einzudämmen
- Kommunikationsstrecken mit TLS verschlüsseln

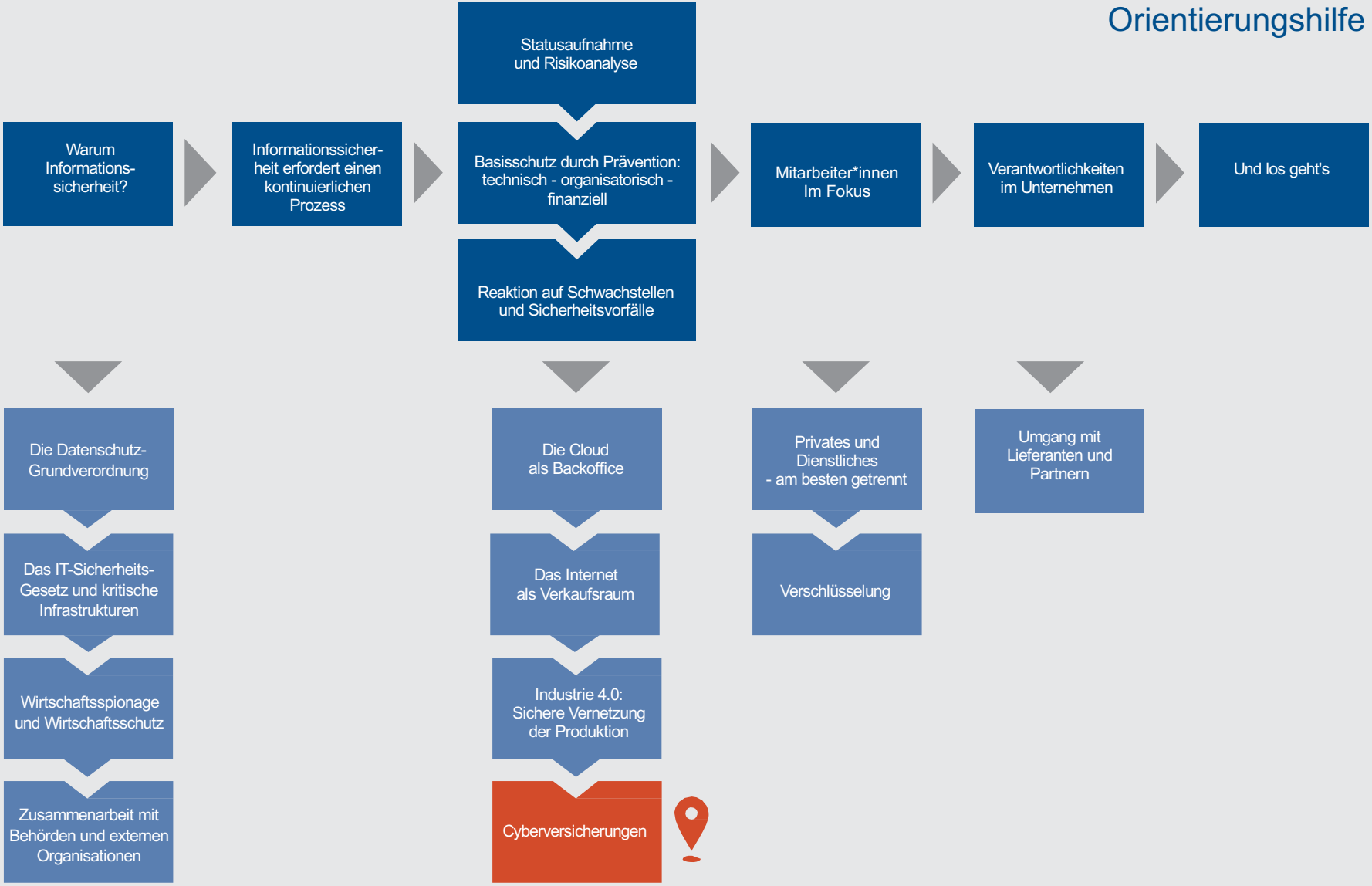
… in Bezug auf Wartung und Dienstleistungen

- Remote-Zugang so gestalten, dass die Aktivitäten „mitverfolgt“ werden können
- Nur geeignet qualifiziertes Personal einsetzen
- Bei kritischen Schwachstellen und Vorfällen beim Hersteller/Dienstleister die Kunden unverzüglich informieren

DIHK

DsiN Deutschland sicher im Netz

Orientierungshilfe



DIHK

DsiN Deutschland sicher im Netz

Wie funktionieren Cyberversicherungen?

Sie versichern die „Verletzung der Informationssicherheit“…

- Durch Eingriffe in Informations-verarbeitende Systeme
- Durch unberechtigte Zugriffe auf elektronische Daten
- Durch Angriffe auf Systeme oder Daten
- Durch Schadprogramme, die auf Systeme oder Daten wirken
- Durch Handlung oder Unterlassung mit Verletzung der Datenschutz-pflichten

Sie bieten folgende Leistungen

Vermögensschäden

- Datenwiederherstellung
- Haftpflicht des Versicherungsnehmers
- Betriebsunterbrechung

Kostenpositionen

- Forensik
- Krisenmanagement
- Benachrichtigungskosten

DIHK

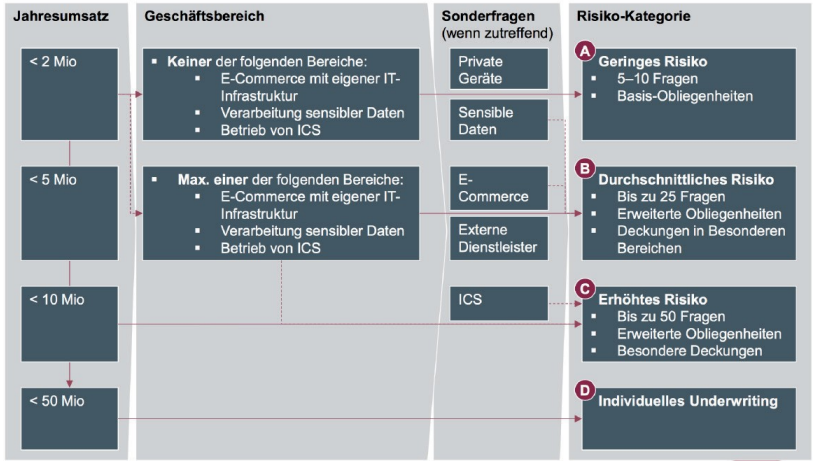
DsiN Deutschland sicher im Netz

Cyberversicherungen: Entscheidungshilfe

Welche Anforderungen stellt der Versicherer („Obliegenheiten“)?

- Ein Mindeststandard der IT-Sicherheit ist Voraussetzung für den Versicherungsschutz
- Einteilung in Risikoklassen über Risikofragebogen
- Anpassung der Obliegenheiten entlang der Risikoklassen
- Immer ist die Basis ein **Informations-sicherheits-Management-System**!

Beispiel: Risiko-Fragen-Konzept des GDV



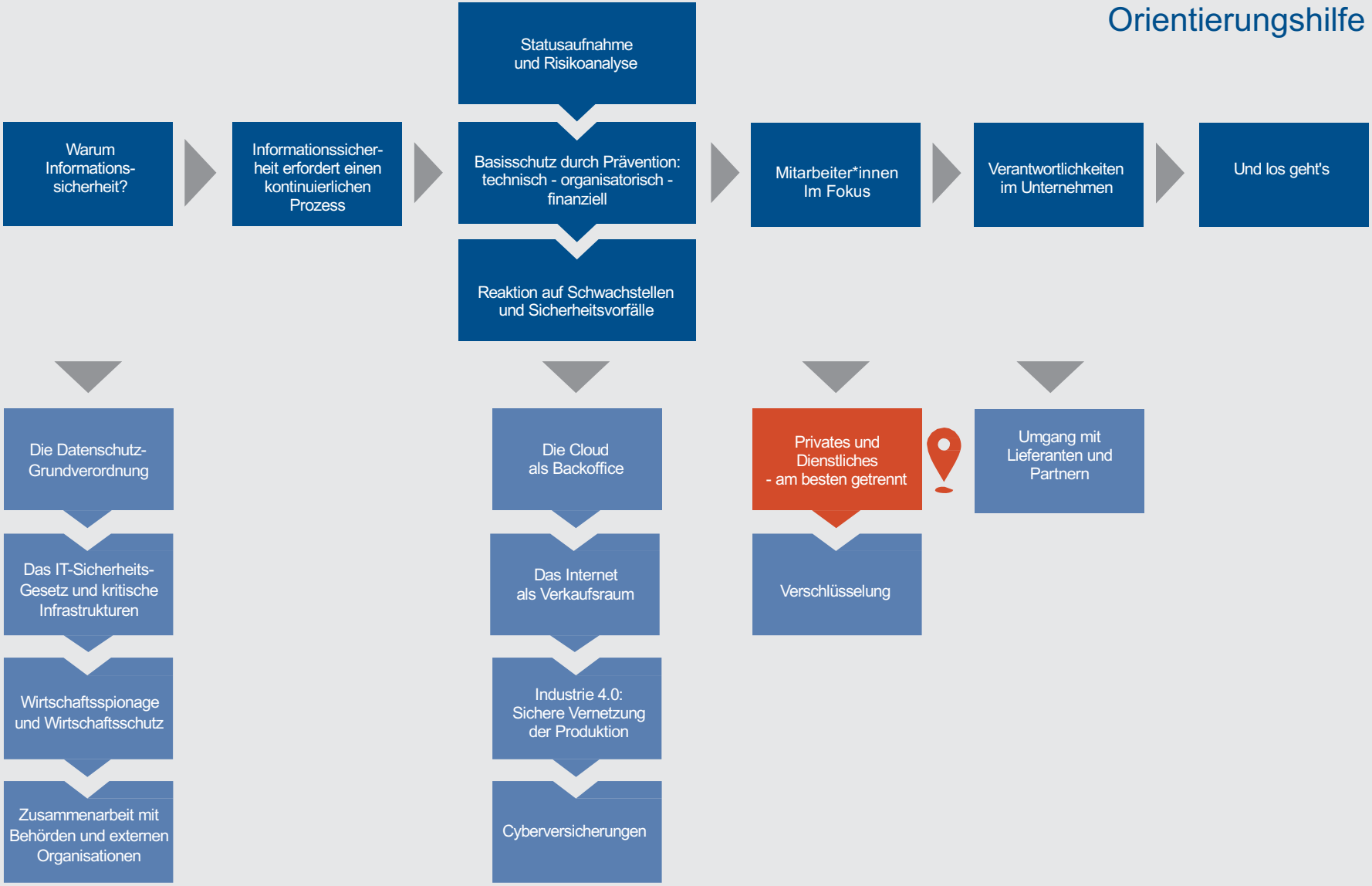
Hinweis: Als Risikofragebogen für Versicherer kann der VdS Quick Check (GDV) dienen. Unternehmen bietet dieser Fragebogen eine weitere Standortbestimmung der eigenen Risikosituation: www.vds-quick-check.de

Tipp: Gegen „CEO Fraud“ kann eine Vermögensschadensversicherung helfen!

DIHK

DsiN Deutschland sicher im Netz

Orientierungshilfe



DIHK

DsiN Deutschland sicher im Netz

Bring Your Own Device (BYOD)

Vorteile

- Kosteneinsparung bei Anschaffungen und IT-Dienstleistungen
- Hohe Mitarbeiter*innenzufriedenheit durch Selbststeuerung und Integration von Berufs- und Privatleben
- Hohe Erreichbarkeit der Mitarbeiter*innen
- Hohe Flexibilität der IT-Architektur (als Folge)

Nachteile

- Vermischung von Berufs- und Privatleben kann gesundheitlich gefährlich sein (Work-Life-Balance)
- Trennung von Firmendaten und privaten Daten nur sehr schwer umsetzbar
- Kontrolle der Firmeninformationen aufgrund von Datenschutz fast nicht realisierbar

DIHK

DsiN Deutschland sicher im Netz

Privates und Dienstliches am besten getrennt

Risiken von BYOD

- Nicht-Konformität zu Datenschutz-Vorgaben
- Kein Schutz der Informationen vor Innentätern und Wirtschaftsspionage
- Keine Kontrolle der Herausgabe von Informationen

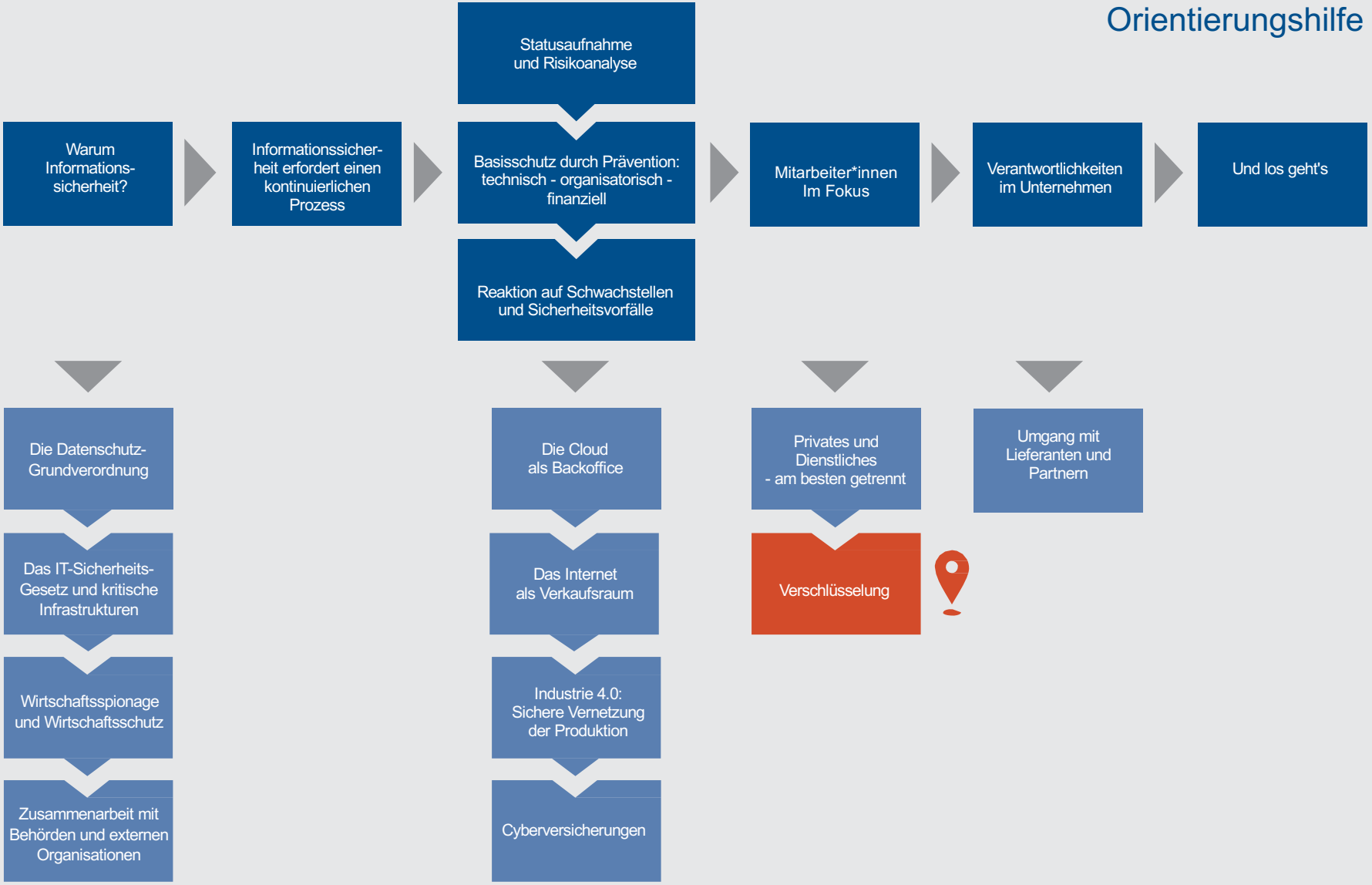
Empfehlungen

- Zwei Geräte:
  - Eines für Firmendaten
  - Eines für private Daten
- Verwendung des privaten Geräts für dienstliche Belange (z.B. Whats-App-Kontaktpflege) tolerieren, solange keine vertraulichen Informationen darüber verbreitet werden

DIHK

DsiN Deutschland sicher im Netz

Orientierungshilfe



DIHK

DsiN Deutschland sicher im Netz

Verschlüsselung und Co. – leicht gemacht

Verschlüsselungsarten

- Symmetrische Verschlüsselung (SV)
- Asymmetrische Verschlüsselung (AV)
- Hybride Verschlüsselung (HV)
- Integritätssicherung
- Durch Digitale Signaturen (DS)
- Durch Blockchain-Technologien

Optionen für das Schlüsselmanagement

- SV: Symmetrischer Schlüssel muss ausgetauscht werden
- AV, HV, DS: Öffentlicher Schlüssel muss validiert werden (i.d.R. durch Trust Center)
- Blockchain: kein (explizites) Schlüsselmanagement erforderlich!

Empfehlungen zum Einsatz von Verschlüsselung

Festplatten-verschlüsselung

- Bestandteil jedes Betriebssystems – muss eingeschaltet werden!
- Wichtig: Recovery-Konzept bedenken (für PC-Crash)

Dokumenten-verschlüsselung

- Nur für ausgewählte Dokumente und Dokumentenarten
- Sehr einfach bei PDF und MS-Office-Dateien
- Ablage / Übermittlung des Passworts sicher gestalten!

E-Mail-Verschlüsselung

- Wird von allen gängigen E-Mail-Programmen unterstützt (S/MIME)
- Verschlüsselung durch Antwort auf signierte E-Mail

Verschlüsselung beim Surfen

- Beim Surfen auf das Schloss im Browser achten! (https)
- Bei eigenen Websites: beantragen!

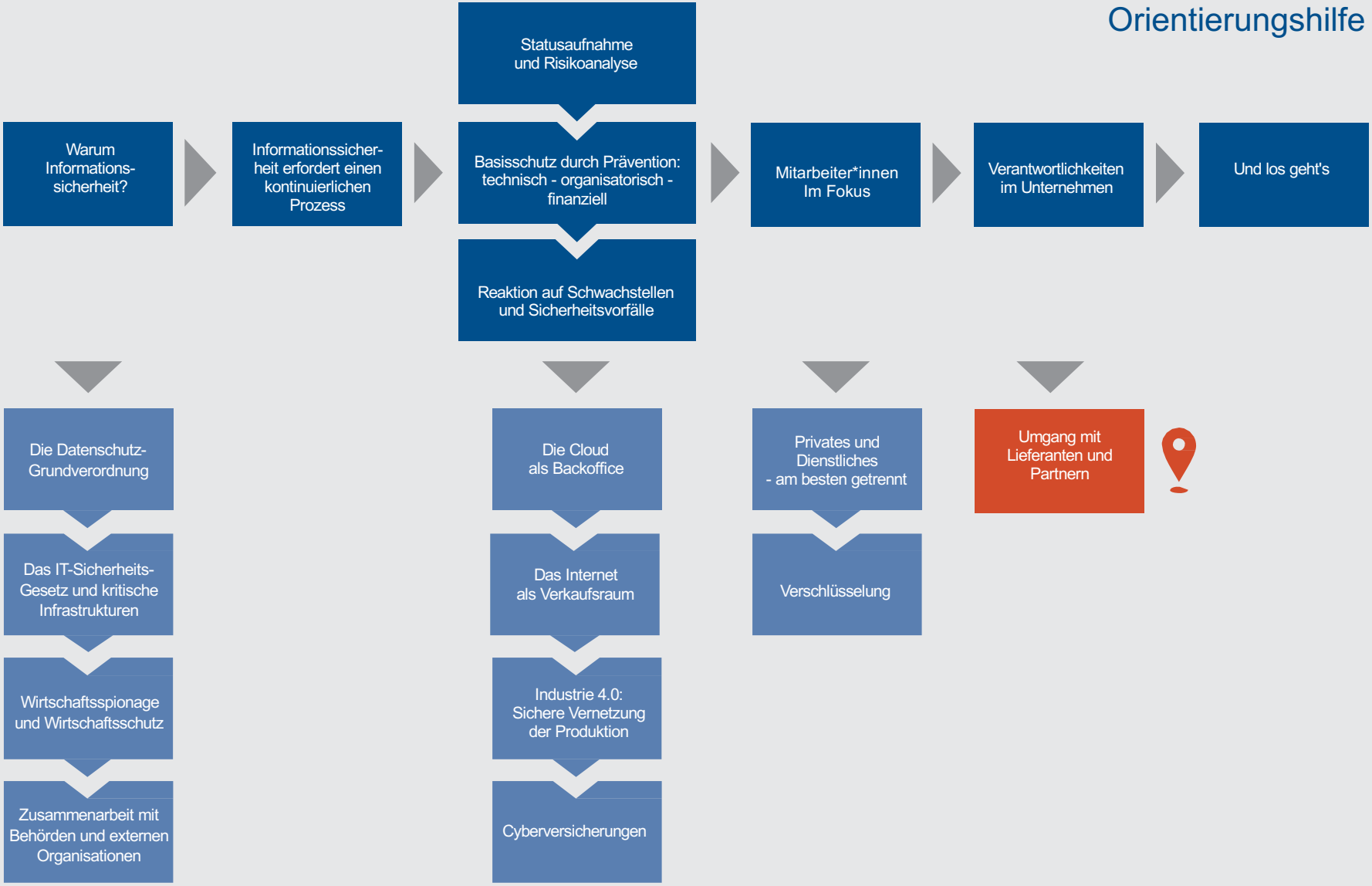
Verschlüsselung in der Cloud

- Inzwischen für alle gängigen Cloud-Ablagen verfügbar

DIHK

DsiN Deutschland sicher im Netz

Orientierungshilfe



DIHK

DsiN Deutschland sicher im Netz

Sicherheitsanforderungen an Lieferanten und Partner

In Bezug auf die Sicherheit der Dienstleistung

- Bei Schwachstellen und Vorfällen in Bezug auf die Dienstleistung die Kunden unverzüglich informieren und die Schwachstellen beheben
- Bei Remote-Verbindungen „Mitverfolgen“ ermöglichen
- Nur Einsatz von geeignet qualifiziertem Personal
- Dokumentation der Umsetzung der (funktionalen) Sicherheitsanforde-rungen

In Bezug auf die Sicherheit in dessen Organisation

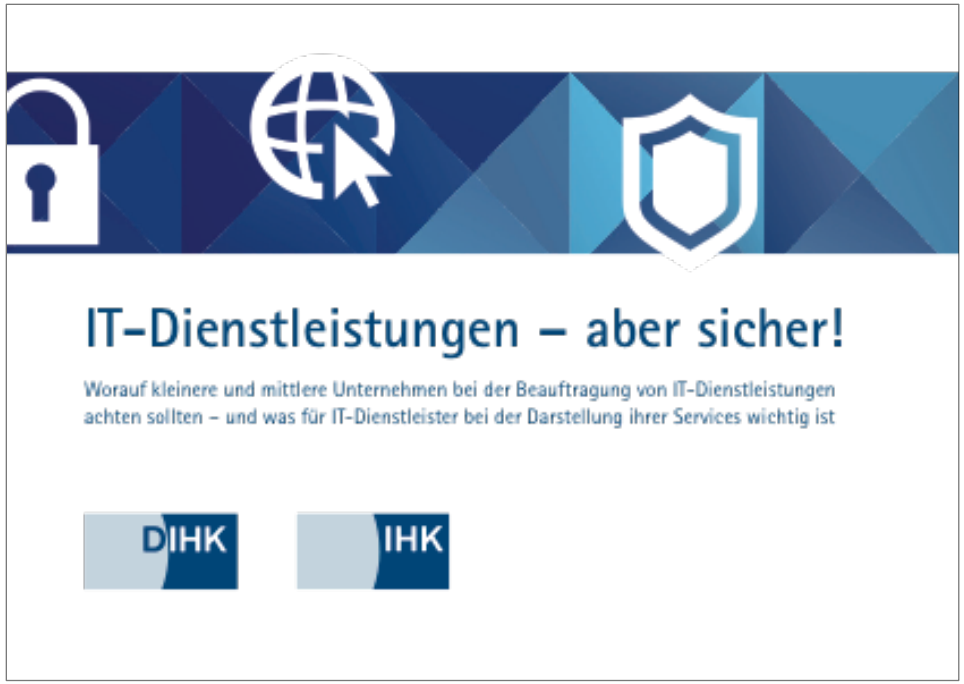
- Bei für Kund*innen möglicherweise kritischen Schwachstellen und Vorfällen in eigenen Systemen die Kund*innen unverzüglich informieren
- Eigenes ISMS
- Möglichkeit, Lieferantenaudits durchzuführen

DIHK

DsiN Deutschland sicher im Netz

Mit Sicherheit die richtigen Partner und Lieferanten finden

Auswahl von (IT-) Dienstleistern anhand von Sicherheitskriterien



Umsetzung in der Praxis

- Formulieren von Sicherheits-aspekten im Standard-Vertrag
- Prüfen der zugesagten Sicherheitsaspekte

Hier finden Sie weitere Erläuterungen zu den aufgeführten Kriterien

http://www.ihk.de/it-sicherheits-kriterien

DIHK

DsiN Deutschland sicher im Netz

VIELEN DANK!

Deutschland sicher im Netz e.V.
Leitung Mittelstand: Sandra Balz und Markus Burke
Projektverantwortliche: Clara Schaksmeier
c.schaksmeier@sicher-im-netz.de
dsin.de

IHK
Name Ansprechpartner
E-Mail-Adresse
Internetseite

Unter der Schirmherrschaft des

Bundesministerium für Wirtschaft und Energie

Mit freundlicher Unterstützung der DsiN-Mitglieder

Avira
Deutscher Sparkassen- und Giroverband e. V.
VdS Schadenverhütung

Ein Projekt von

DIHK

DsiN Deutschland sicher im Netz