Herzlich willkommen zur BaFinTech

TIBER-DE
Cyber-Resilienz-Tests im Finanzsektor

Dr. Miriam Sinn
TIBER Cyber Team, Deutsche Bundesbank

BaFinTech2022

In Kooperation mit der Deutschen Bundesbank

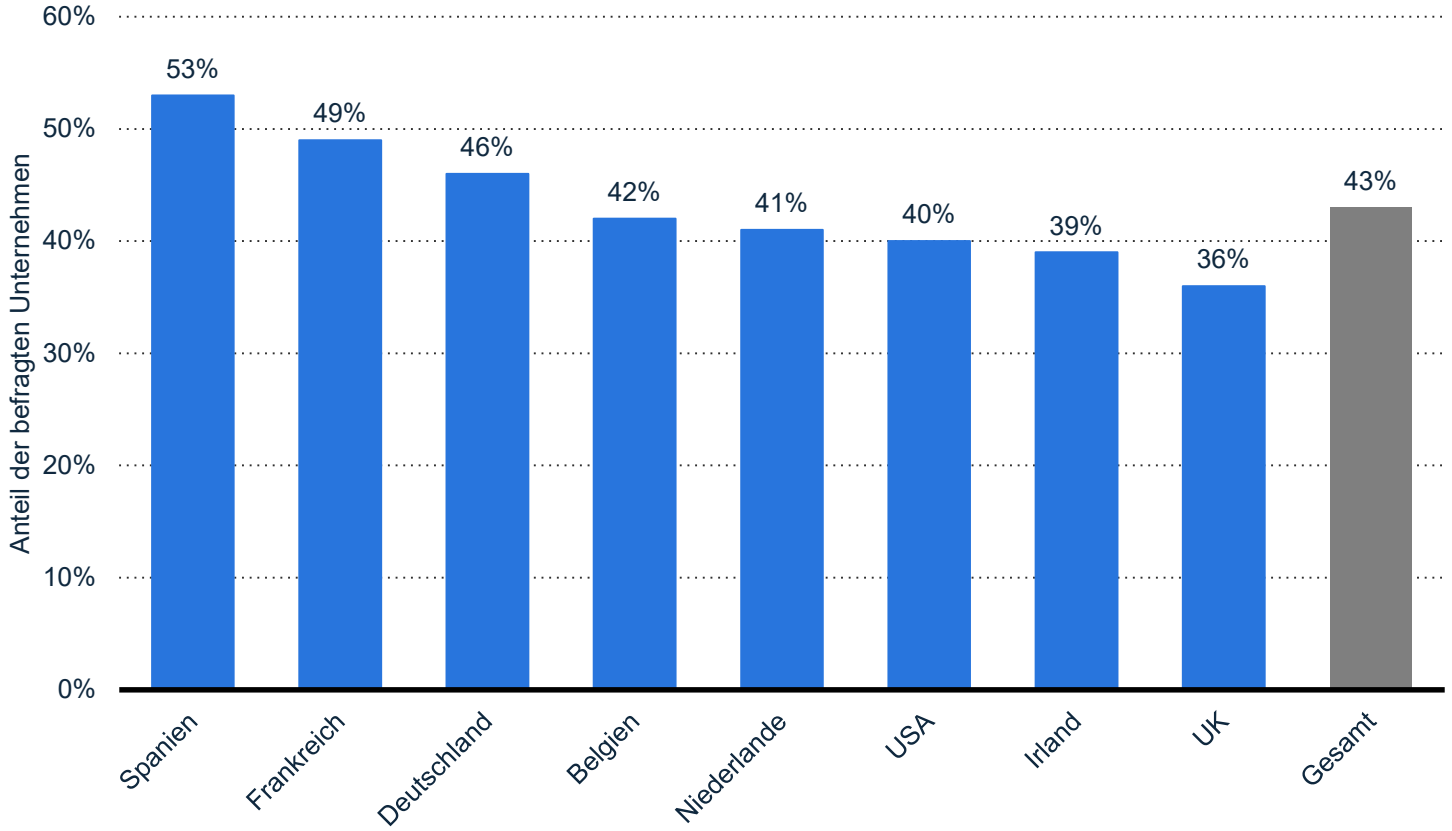
1. Warum TIBER-Tests?

Nur ein Angriff unter vielen…

Quelle: © Rawf8/stock.adobe.com

Die wachsende Gefahr

Unternehmen, die 2021 eine Cyber-Attacke erlebt haben



Quelle: Hiscox;

Hinweis(e): Weltweit, Belgien, Frankreich, Deutschland, Irland, Niederlande, Spanien, Vereinigtes Königreich, USA; 5. November 2020 bis 8. Januar 2021; 6.043 Befragte; Cybersecurity-Personal

Inhalt

Agenda

1 Warum TIBER-Tests?

2 TIBER-EU als elaboriertes Rahmenwerk für Cyber-Resilienz-Tests in Europa

3 TIBER-DE: Umsetzung in Deutschland

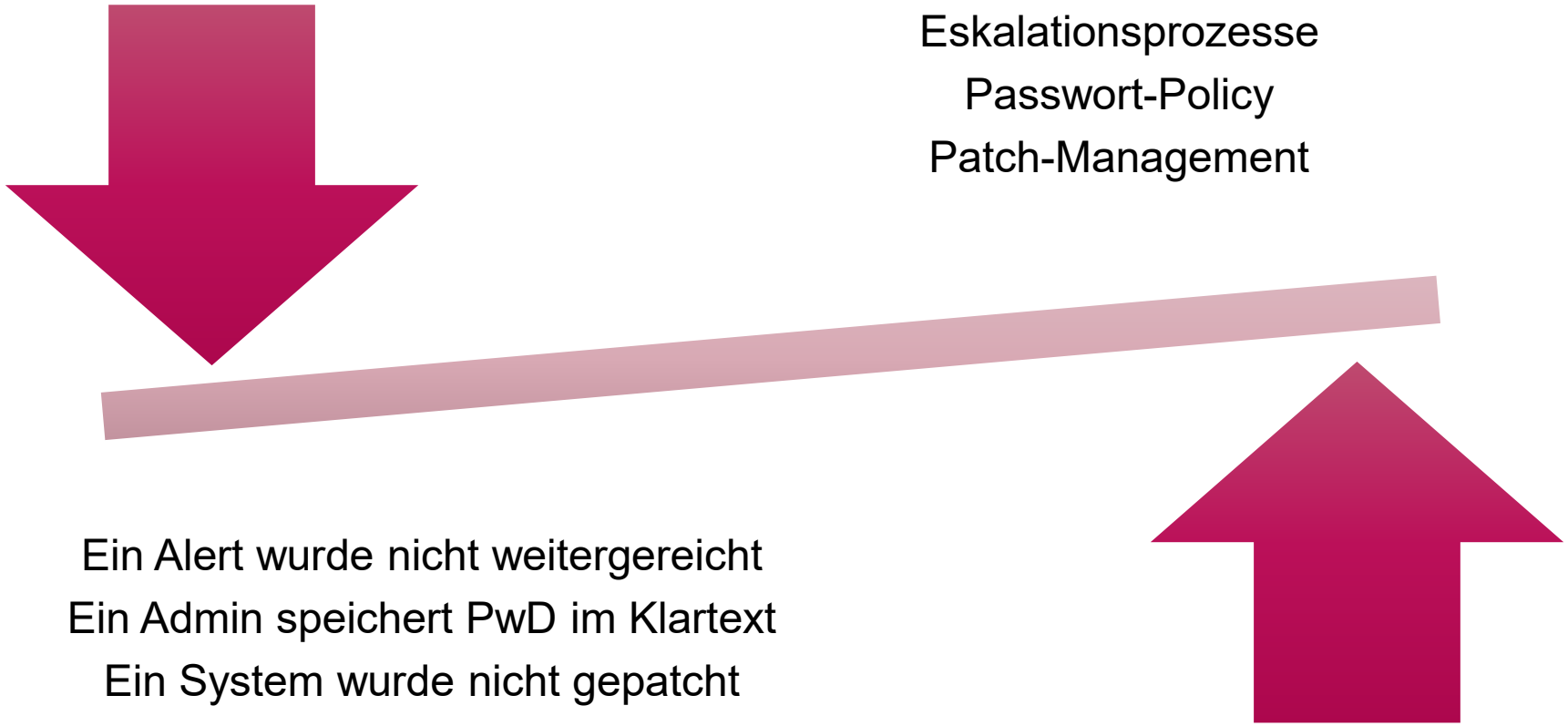
4 Funktionsweise eines TIBER-Tests

5 Erfahrungen aus TIBER-Tests

6 Fragen und Diskussion

1. Testen als wichtige Ergänzung zur konzept. Ausrichtung

Top-down vs. Bottom-up



1. Testen als wichtige Ergänzung zur konzept. Ausrichtung

Aktuelle Testmöglichkeiten für Cyberwiderstandsfähigkeit

Penetrationstest

- Überprüfung bekannter Schwachstellen
- Fokus: ausgewählte Systeme
- Einsatz von (automatisierten) Werkzeugen

Red Teaming

- Fokus: gesamtes Unternehmen
- Bedrohungsgeleitete Angriffe
- Werkzeuge:
  - Penetrationstest
  - Social Engineering
  - Physisches Testen
  - …

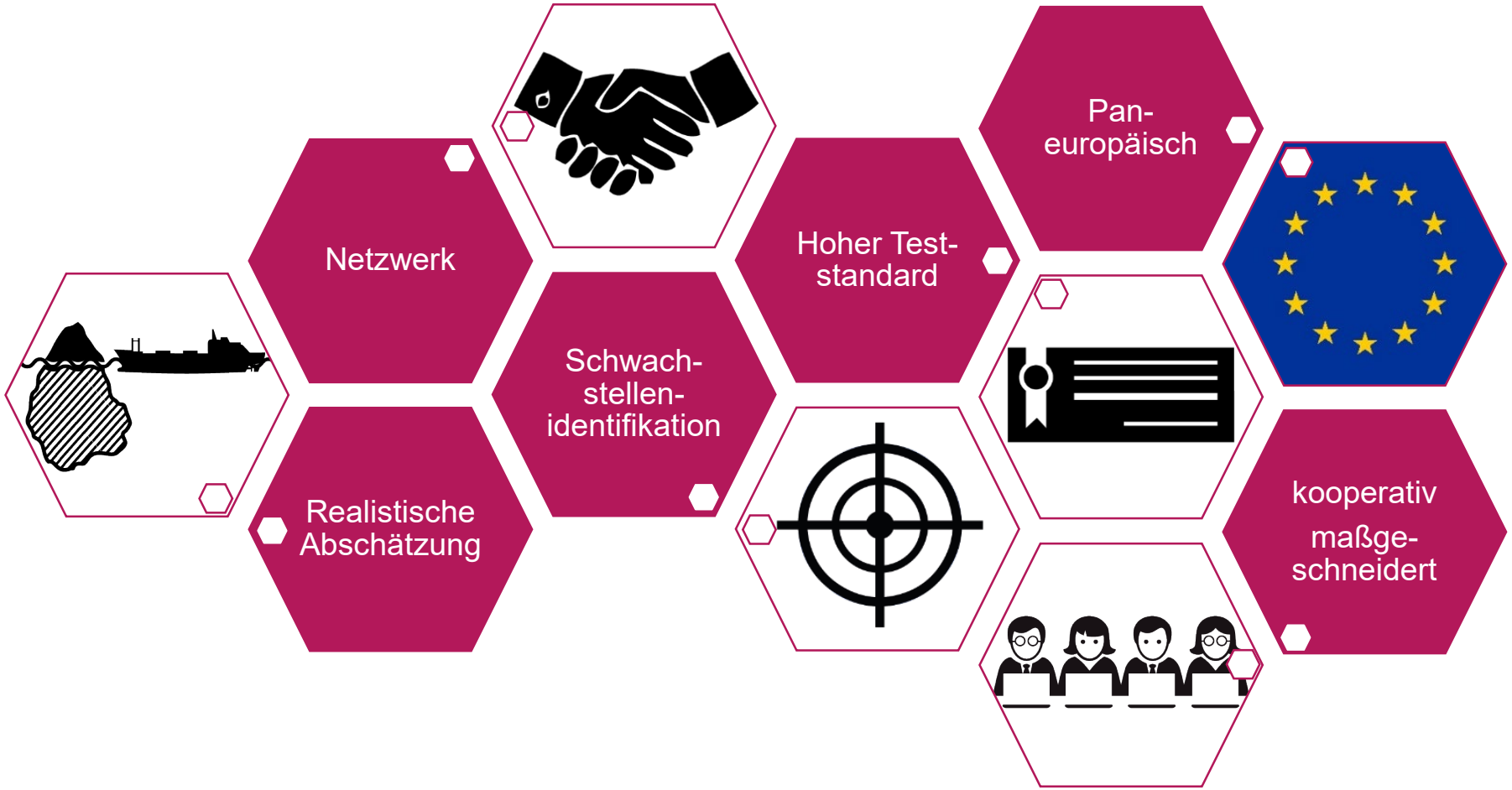
Threat Intelligence-Based Ethical Red Teaming (TIBER)

- Europaweite Harmonisierung von RT-Tests
- Hoher Teststandard:
  - Produktivsysteme
  - Externe Angriffsteams
- Länderübergreifende Tests
- Pan-europäische Anerkennung

zunehmende Test-Intensität

1. Testen als wichtige Ergänzung zur konzept. Ausrichtung

Warum ein TIBER-Test?



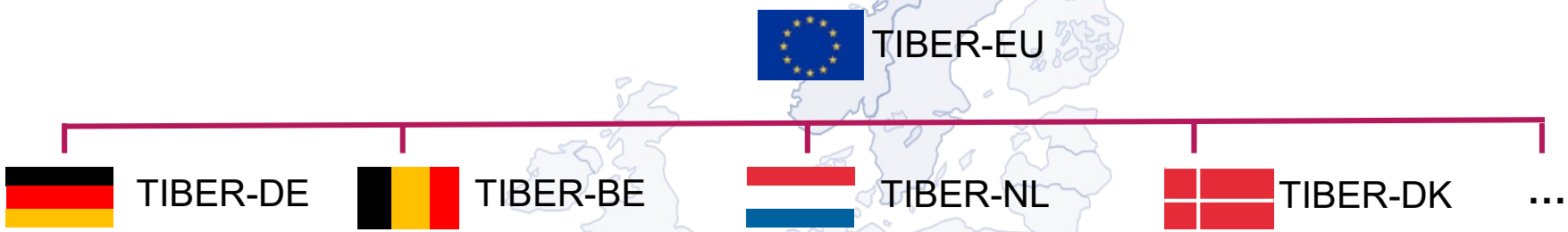
2. TIBER-EU als elaboriertes Rahmenwerk für Cyber-Resilienz-Tests in Europa

2. TIBER-EU als elaboriertes RW für Cyber-Resilienz-Tests

TIBER-EU Struktur

Threat Intelligence Based Ethical Red-Teaming

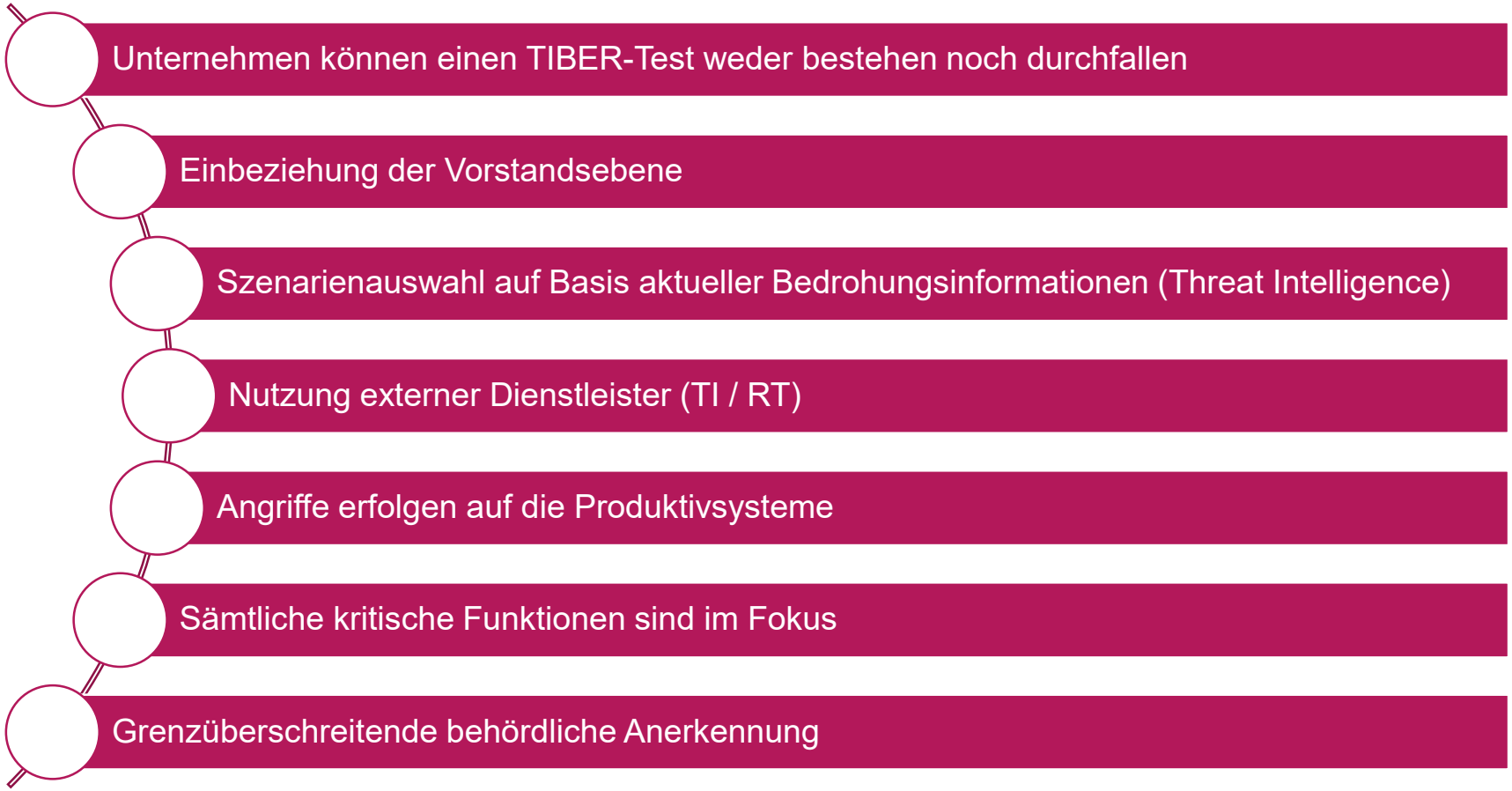
TIBER-EU ist ein Meta-Rahmenwerk für bedrohungsgeleitete Red-Teaming-Übungen



- Entwickelt von den Zentralbanken des Eurosystems (eingeführt 2018)
- Implementierung auf nationaler Ebene erforderlich
- Verpflichtende Elemente für eine europaweite Harmonisierung sowie optionale Elemente für nationale Besonderheiten

2. TIBER-EU als elaboriertes RW für Cyber-Resilienz-Tests

Zentrale Eigenschaften eines TIBER-Tests



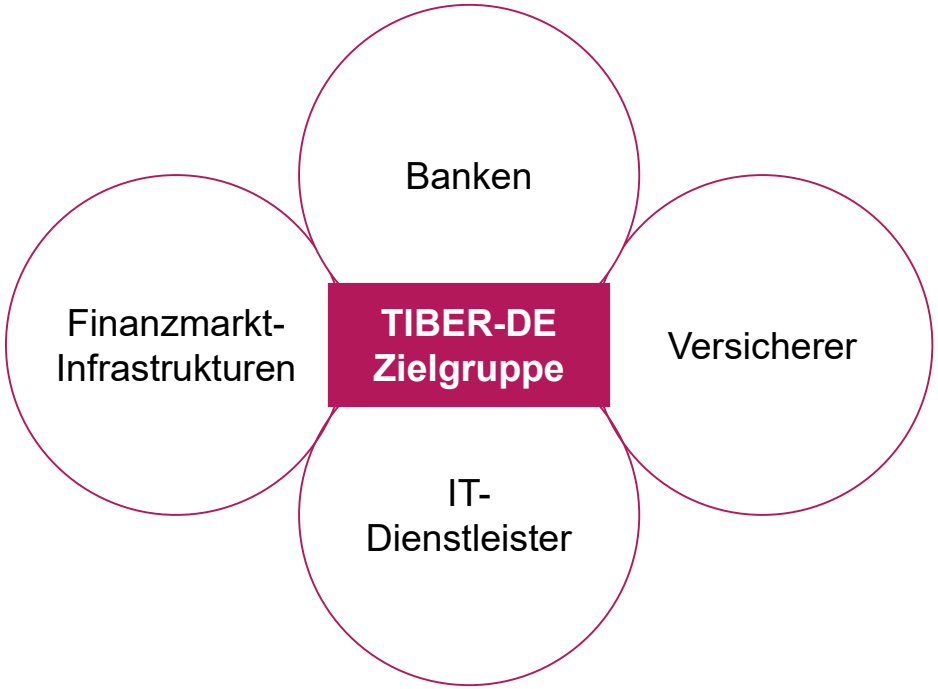
3. TIBER-DE: Umsetzung in Deutschland

- Eckdaten
- Governance
- White Team Lead- und Dienstleister-Community

3. TIBER-DE: Umsetzung in Deutschland

Eckdaten

- Nationales Kompetenzzentrum **(TIBER Cyber Team – TCT)** im Bereich Zahlungsverkehr und Abwicklungssysteme bei der Bundesbank
- Teilnahme der Unternehmen als **freiwillige Selbstverpflichtung** (kooperativer Ansatz)
- **Attestierung** der erfolgreichen Durchführung und **grenzüberschreitende behördliche Anerkennung**



3. TIBER-DE: Umsetzung in Deutschland

Governance

- strategische Steuerung

- Kontaktstelle für konkrete TIBER-Tests
- operative Betreuung der Tests
- kontrolliert Einhaltung der Vorgaben

Kein TIBER ohne TCT!

- betreut ein spezifisches Unternehmen
- ist in alle Treffen und Absprachen eingebunden

3. TIBER-DE: Umsetzung in Deutschland

White Team Lead- und Dienstleister-Community

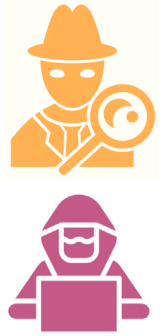
Aufbau einer TIBER-DE-Community

WTL-Community

- Cybersecurity-Community aller TIBER-DE White Team-Manager und CISOs
- Plattform für den regelmäßigen Informations- und Erfahrungsaustausch
- Weiterentwicklung des TIBER-DE-Rahmenwerks

Dienstleister-Community

- Austauschplattform für Anbieter von Threat Intelligence- und Red Teaming-Dienstleistungen
- Austausch zu Best Practices für TIBER-DE-Tests
- Weiterentwicklung des TIBER-DE-Rahmenwerks

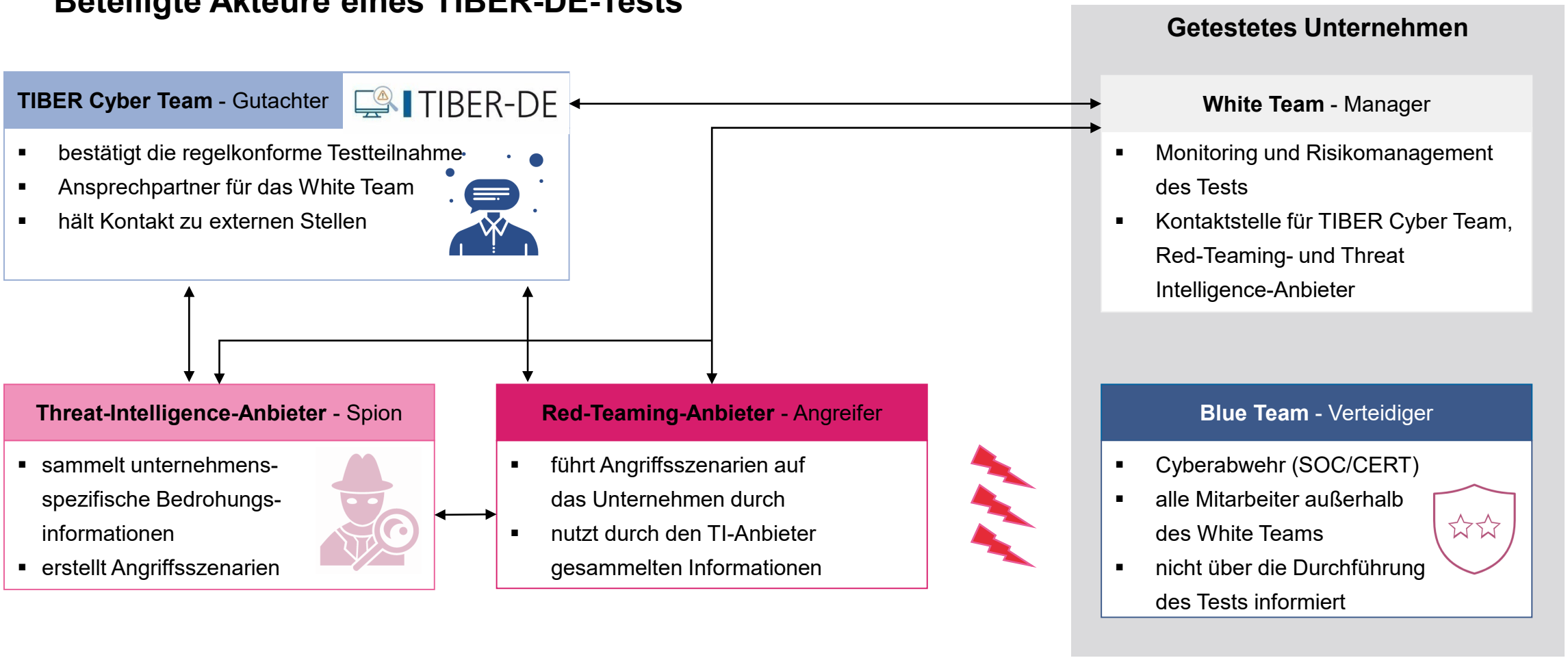


4. Funktionsweise eines TIBER-Tests

- Beteiligte Akteure eines TIBER-DE-Tests
- Ablauf eines TIBER-DE-Tests und Ressourcenaufwand

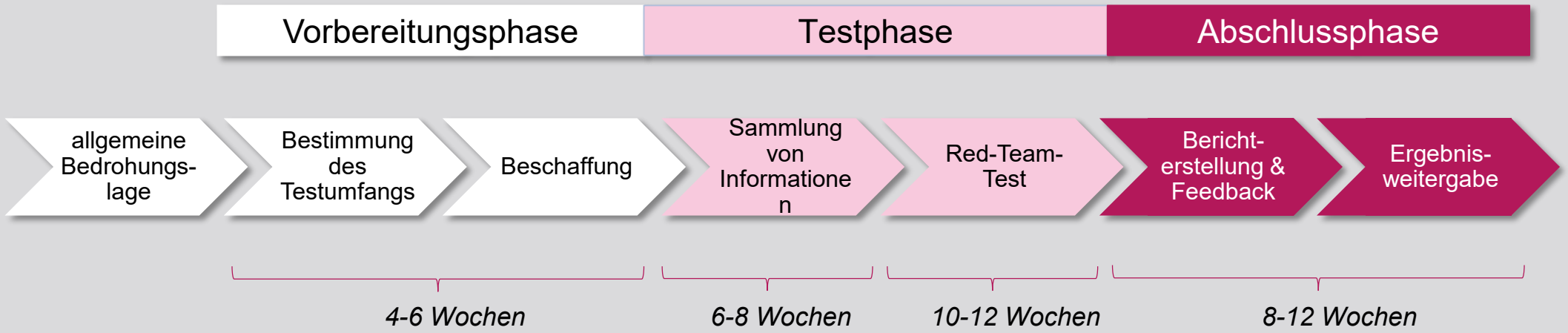
4. Funktionsweise eines TIBER-Tests

Beteiligte Akteure eines TIBER-DE-Tests

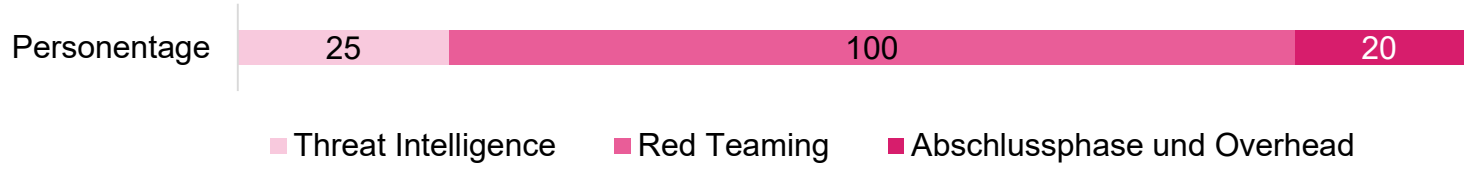


4. Funktionsweise eines TIBER-Tests

Ablauf eines TIBER-DE-Tests und Ressourcenaufwand



Geschätzter Ressourcenaufwand für externe Dienstleister



5. Erfahrungen aus TIBER-Tests

- Threat Intelligence
- Red Teaming
- Übergreifende Erkenntnisse aus TIBER-DE-Tests

5. Erfahrungen aus TIBER-Tests

Threat Intelligence

Pro Test werden 3-5 Szenarien verprobt.

Simulierte Angreifer sind häufig Nation States, Organized Crime Groups und Insider.

Physische Einbruchsszenarien sind ausdrücklich möglich.

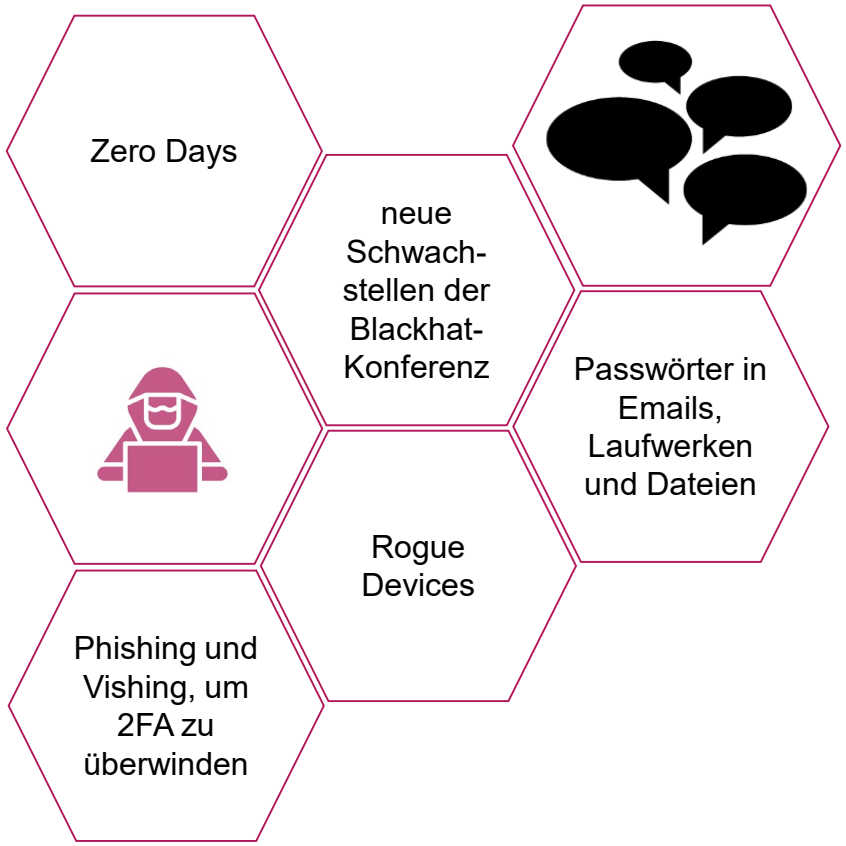
Der Threat-Intelligence-Anbieter erstellt einen unternehmensspezifischen Bericht auf Basis der GTL. Der Bericht enthält unternehmensspezifische Bedrohungen, Schwachstellen und Angriffsszenarien.

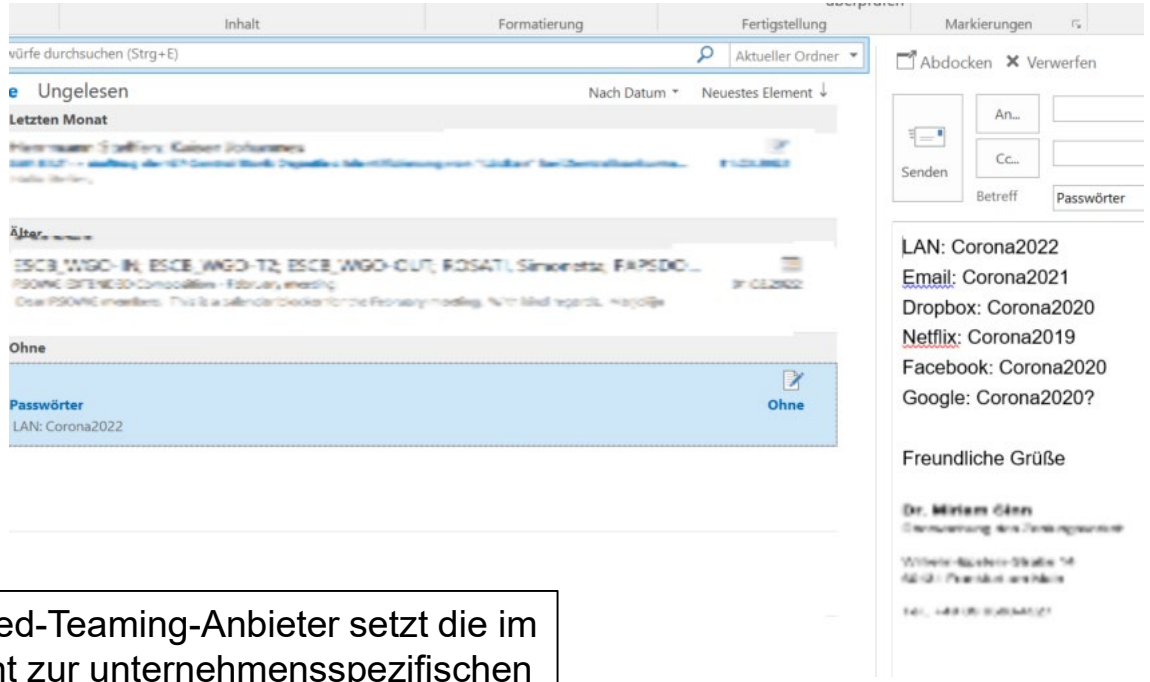
aktuelle Passwörter z.B. aus Leaks und öffentlichen GitHub Repositories

Genutzte Eindringungstechniken (Auszug): Mass-Phishing, Spear-Phishing, Password Spraying, Man-in-the-Middle, Rogue Devices

5. Erfahrungen aus TIBER-Tests

Red Teaming





Der Red-Teaming-Anbieter setzt die im Bericht zur unternehmensspezifischen Bedrohungslage genannten Angriffsszenarien um.

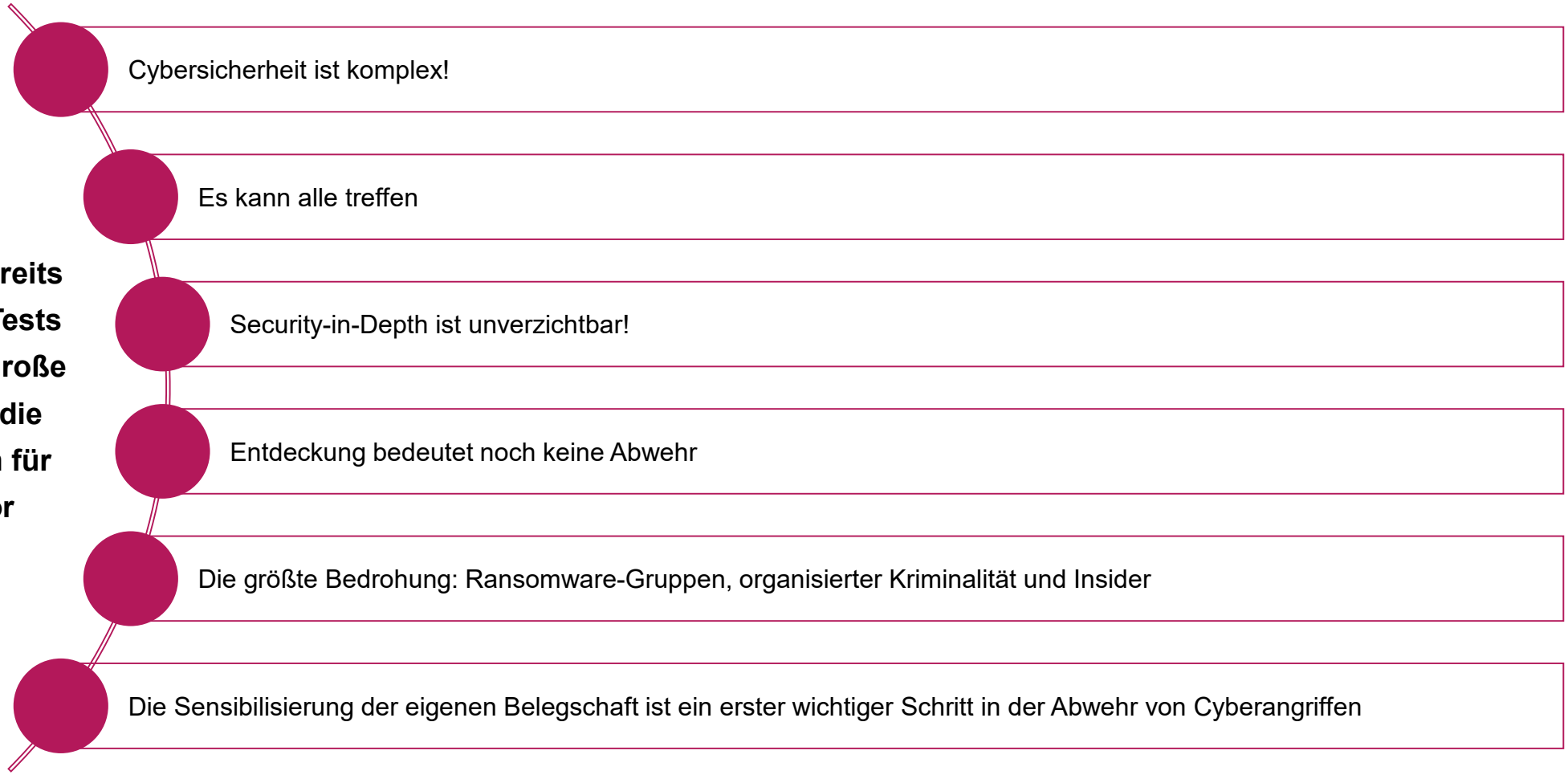
Erfahrungen aus TIBER-Tests
Der Faktor Mensch

- Mitarbeiter sind **(zu) hilfsbereit**
  - Mitarbeiter teilen auf Social Media (zu) viele unternehmensspezifische Informationen
  - Mitarbeiter lassen Türen zum Rauchen offen stehen; Mitarbeiter lassen Fenster über Nacht gekippt
  - Angreifer werden im Gebäude identifiziert, anschließend aber „laufen gelassen“
- Ablage sensibler Informationen auf **nicht gesicherten Ablageorten ohne Zugriffsbeschränkung**
- Passwort-Spray-Angriffe mit „Corona21“ und „Sommer21“ waren in mehreren Fällen erfolgreich
- Das Fehlen eines zweiten Faktors zur Authentifizierung ermöglichte den Angreifern **Zugriff auf die internen Systeme**.

5. Erfahrungen aus TIBER-Tests

Übergreifende Erkenntnisse aus TIBER-DE-Tests

Erfahrungen aus bereits begleiteten TIBER-Tests unterstreichen die große Herausforderung, die durch Cyberrisiken für den Finanzsektor entstehen.



Vielen Dank für Ihre Aufmerksamkeit!

Dr. Miriam Sinn
TIBER Cyber Team, Deutsche Bundesbank

BaFinTech2022

In Kooperation mit der Deutschen Bundesbank