aruna FACHMESSE KOMPOSIT 2024

baloise

KI – DIE neue Gefahr?

Referentin

Julia Nebe
Branchenleiterin Cyber

T +49 9231 8799 190
M +49 151 1741 3151
julia.nebe@baloise.de

linkedin.com/in/julia-nebe-cyber

Quelle: REMA 1000 - YouTube

Agenda

1. Geschichte / Entstehung künstlicher Intelligenz
2. Veränderung von Cyber-Angriffsmustern durch künstliche Intelligenz
3. Auswirkungen auf die Versicherbarkeit

Was ist künstliche Intelligenz?

„Künstliche Intelligenz ist die Eigenschaft eines IT-Systems *menschenähnliche* Verhaltensweisen zu zeigen.“

bitkom e.V. und deutsches Forschungszentrum für künstliche Intelligenz

„Die künstliche Intelligenz ist ein *Teilgebiet der Informatik*, welches sich mit der *Forschung* von Mechanismen des intelligenten menschlichen Verhaltens befasst (…).“

Spektrum der Wissenschaft, Lexikon der Neurowissenschaften

„Unter künstlicher Intelligenz verstehen wir Technologien, die *menschliche Fähigkeiten* im Sehen, Hören, Analysieren, Entscheiden und Handeln *ergänzen und stärken*.“

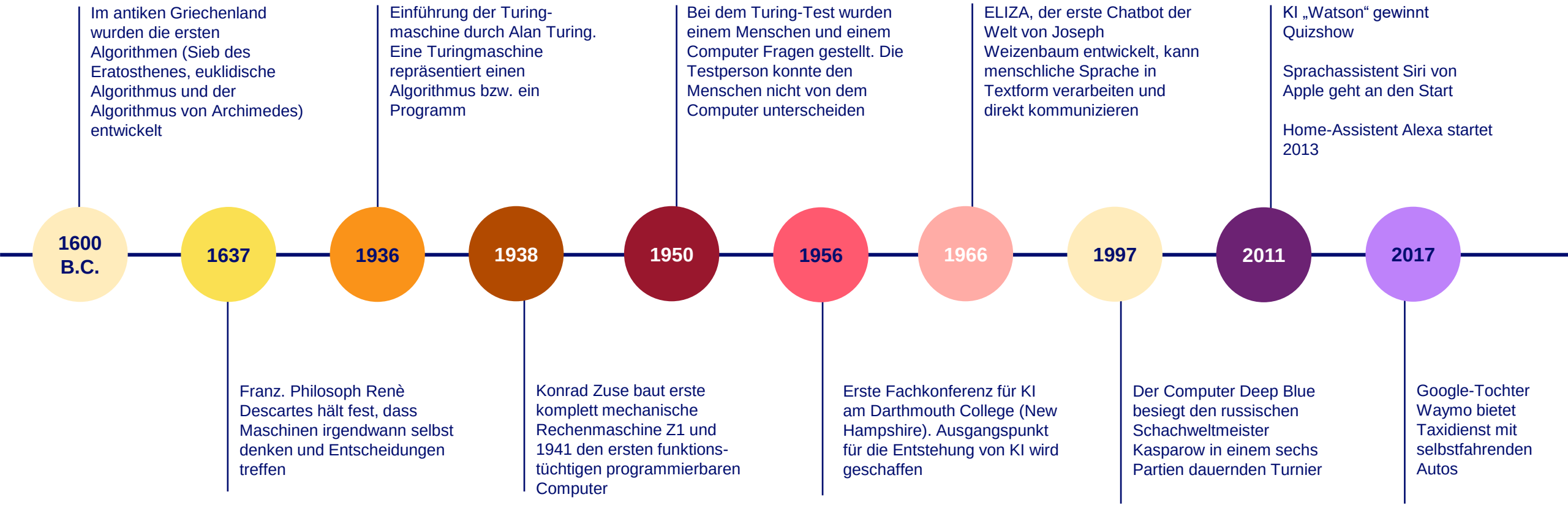
Microsoft Corp

„Künstliche Intelligenz ist die Fähigkeit einer Maschine, *menschliche Fähigkeiten* wie logisches Denken, Lernen, Planen und Kreativität zu *imitieren*.“

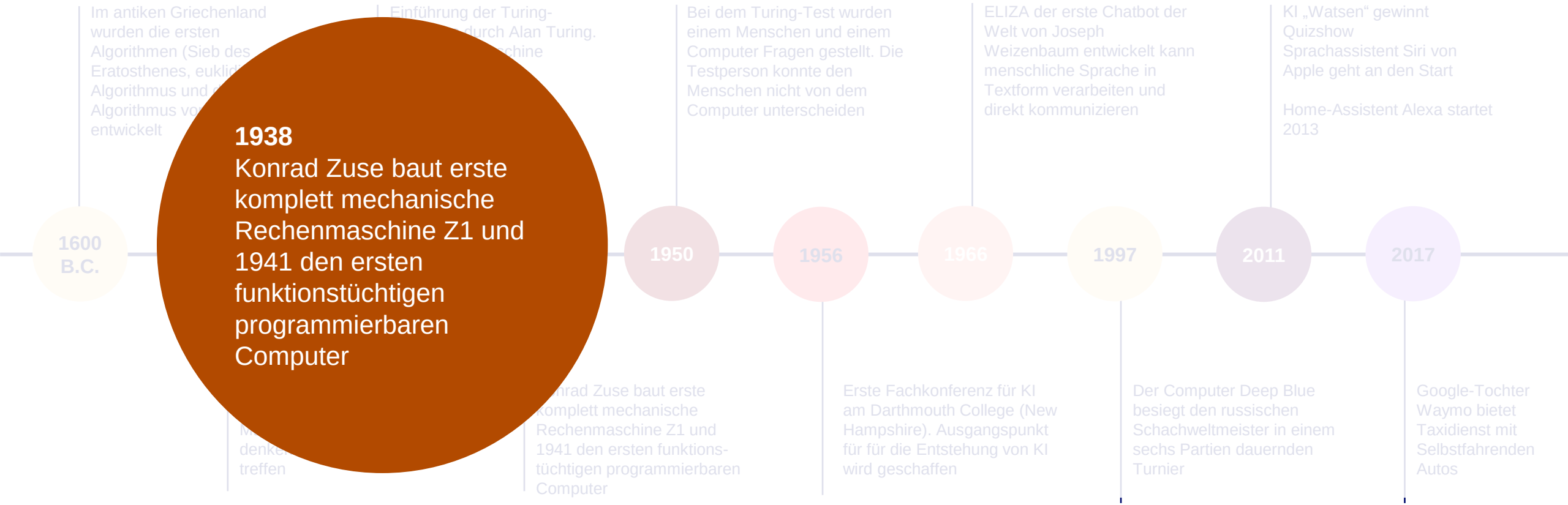
Europäisches Parlament

01 Geschichte / Entstehung künstlicher Intelligenz

Entstehung von künstlicher Intelligenz / Meilensteine der Entwicklung



Entstehung von künstlicher Intelligenz / Meilensteine der Entwicklung



Entstehung von künstlicher Intelligenz / Meilensteine der Entwicklung

1600 B.C.
Im antiken Griechenland wurden die ersten Algorithmen (Sieb des Eratosthenes, euklidische Algorithmus und der Algorithmus von Archimedes) entwickelt

1637
Franz. Philosoph Renè Descartes hält fest, dass Maschinen irgendwann selbst denken und Entscheidungen treffen

1936
Einführung der Turing-maschine durch Alan Turing. Eine Turingmaschine repräsentiert einen Algorithmus bzw. ein Programm

1950
Bei dem Turing-Test wurden einem Menschen und einem Computer Fragen gestellt. Die Testperson konnte den Menschen nicht von dem Computer unterscheiden

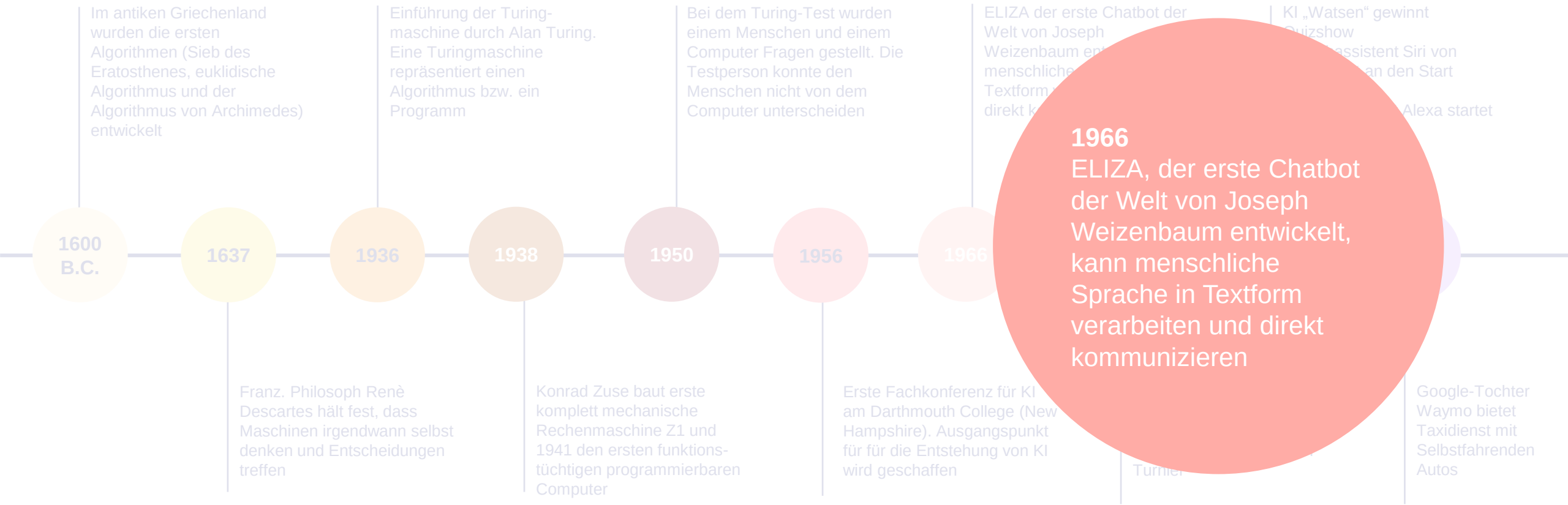
1997
Der Computer Deep Blue besiegt den russischen Schachweltmeister in einem sechs Partien dauernden Turnier

2011
KI „Watsen“ gewinnt Quizshow
Sprachassistent Siri von Apple geht an den Start

Home-Assistent Alexa startet 2013

2017
Google-Tochter Waymo bietet Taxidienst mit Selbstfahrenden Autos

Entstehung von künstlicher Intelligenz / Meilensteine der Entwicklung



1966
ELIZA, der erste Chatbot der Welt von Joseph Weizenbaum entwickelt, kann menschliche Sprache in Textform verarbeiten und direkt kommunizieren

Entstehung von künstlicher Intelligenz / heute und morgen

Heutige KI-Anwendungen:

- Beautiful-ai, presentations.ai, Gamma zur Erstellung von PPTs
- PopAi für Textzusammenfassungen und PPTs
- Dall-E, Jasper Art zur Generierung von Bildern
- GrammarlyGo für Rechtschreib- und Grammatikprüfung
- Automatisierter Aktienhandel

02 Veränderung von Cyber-Angriffsmustern durch künstliche Intelligenz

Veränderung von Cyber-Angriffsmustern durch künstliche Intelligenz

Veränderung von Angriffsmustern

Adaptive Angriffe

- KI-gestützte Malware
- Adaptive Phishing-Angriffe
- Dynamische DDoS-Angriffe

Gezielte Phishing-Kampagnen

- CEO-Betrug
- Lieferantenbetrug
- Spear-Phishing

Automatisierte Schwachstellen-Identifizierung

- Schwachstellen-Scanner
- Penetration Testing Tools
- Code-Analyse-Tools

Veränderung von Cyber-Angriffsmustern durch künstliche Intelligenz

KI-gestützte Malware: Schadsoftware, die mithilfe von künstlicher Intelligenz ihre Verhaltensmuster anpasst, um dadurch vorhandene Sicherheitsmaßnahmen zu umgehen.

Adaptive Phishing-Angriffe: Generell gezielteres und personalisiertes Vorgehen. Phishing-Email wird an die betroffene Person (Position, Namen, etc.) angepasst. Außerdem Reaktion auf Echtzeit-Informationen, um so technischen Gegenmaßnahmen zu entgehen.

Dynamische DDoS-Angriffe: Um die Auswirkungen zu maximieren, variieren die Angriffe ihre Intensität und die Angriffsvektoren basierend auf den erkannten Verteidigungsmaßnahmen.

Adaptive Angriffe

Angriffsmethoden, die sich dynamisch an Sicherheits-maßnahmen anpassen, um die Erfolgschancen zu erhöhen.

Durch den Einsatz von KI können Angriffe deutlich optimiert werden.

Einer KI ist es möglich, sich während eines Angriffs dynamisch an Gegenmaß-nahmen anzupassen

Veränderung von Cyber-Angriffsmustern durch künstliche Intelligenz

CEO-Betrug: Zum Beispiel werden Mitarbeiter durch Voice Cloning getäuscht, um diese anzuweisen, eine Geldtransaktion vorzunehmen. Oder es wird telefonisch auf die Dringlichkeit einer betrügerischen Email verwiesen.

Lieferantenbetrug: Ein Angreifer gibt sich als legitimer Lieferant oder Vertragspartner aus, um so eine Überweisung von Geldern auf ein gefälschtes Konto zu fordern.

Spear-Phishing: Personalisierte Phishing-Emails inkl. dazugehöriger Hintergrundinformationen, um an vertrauliche Informationen zu gelangen.

Gezielte Phishing-Kampagnen

Bei Verwendung einer KI können personalisierte Nachrichten erstellt werden, die speziell auf die Interessen und das Verhalten des Opfers angepasst werden.

Deutlich höhere Erfolgsquote durch perfektionierte Phishing-Nachrichten, welche in Echtzeit angepasst (Schreibstil, Kommunikationsmuster) werden können. Ein Erkennen wird immer schwieriger.

Veränderung von Cyber-Angriffsmustern durch künstliche Intelligenz

Schwachstellen-Scanner (Nutzung von KI): Datensammlung (installierte Software, Betriebssystemdetails, etc.) eines anvisierten Ziels. Nutzung von fortschrittlichen Algorithmen zur gezielten Schwachstellensuche (z.B. veraltete Software). Bewertung der festgestellten Schwachstellen sowie ihrer potentiellen Auswirkung.

Penetration Testing Tools: Automatisierte Penetrationstests können Schwachstellen in Systemen identifizieren, indem sie simulierte Angriffe durchführen, um potenzielle Eintrittspunkte zu entdecken.

Code-Analyse-Tools: Identifizierung vorhandener Sicherheitslücken oder fehlerhafter Programmierung durch die Verwendung von automatisierten Tools, die den Quellcode von Anwendungen oder Software durchsuchen.

Automatisierte Schwachstellen-Identifizierung

Bei einer automatisierten Schwachstellen-Identifizierung findet der Einsatz von Tools und Technologien (ohne menschliches Eingreifen) statt, um gezielt Schwachstellen in Computersystemen, Netzwerken oder Anwendungen ausfindig zu machen. Das wiederrum erleichtert es Cyber-Kriminellen potenzielle Ziele zu identifizieren.

Zukünftige Entwicklungen

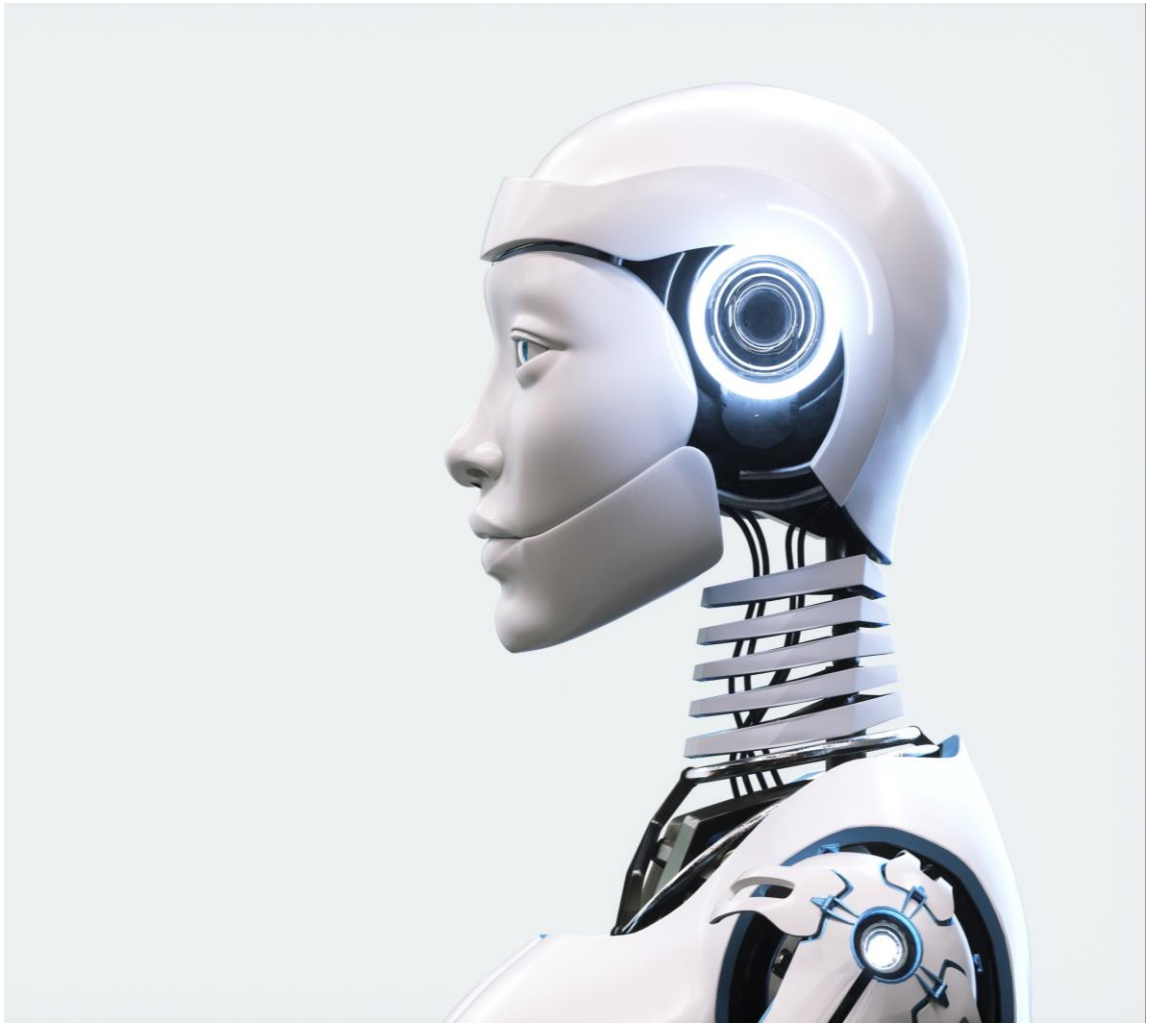
Quantentechnologie: Quantencomputer sind eine komplett neue Art von Computersystemen, die eine neue Dimension von Rechenleistung eröffnen.

Durch die Nutzung von Quantentechnologie können herkömmliche Verschlüsslungsmethoden sehr schnell durchbrochen werden.

Biometrische Datenmanipulation: Vorstellbar ist eine deutliche Zunahme von Angriffen auf biometrische Daten (Gesichtserkennung, Fingerabdruck), um an sensible Daten zu gelangen oder Identitäten zu stehlen.

Zunahme von **komplexen**, gegebenenfalls auch staatlich motivierten, **Angriffen** auf kritische **Infrastrukturen**.

KI kann aber auch helfen…



Verhaltensanalyse: KI-Systeme können für die Überwachung von normalem Verhalten von Nutzern und Systemen eingesetzt werden, um so Anomalien zu erkennen, die durch einen Angriff entstehen können.

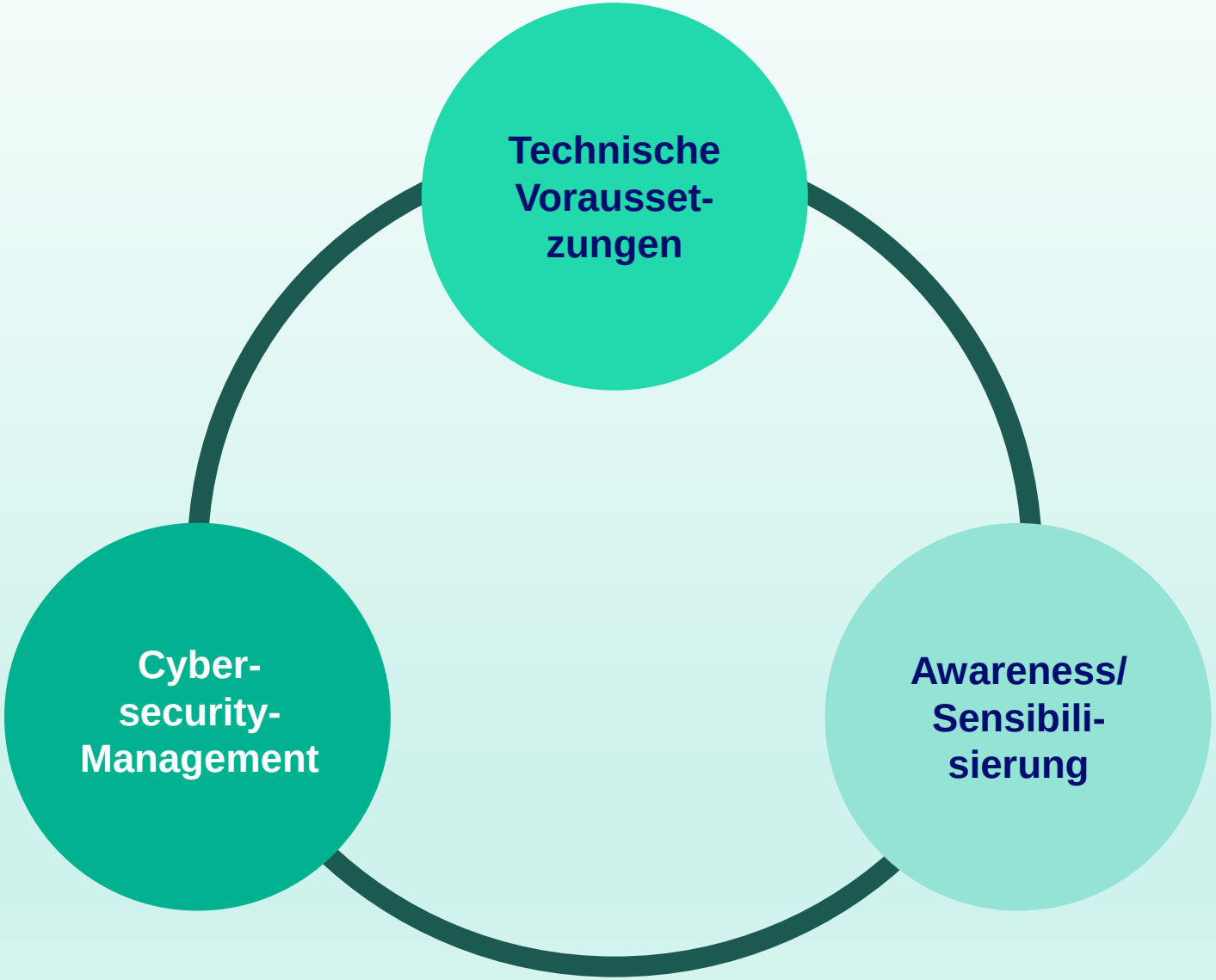
Anti-Malware: KI kann zur Unterstützung von Antivirensoftware beitragen und es ermöglichen, neue Arten von Malware zu erkennen. Da eine KI zwischen „gute“ von „bösen“ Daten unterscheiden kann.

Schnelligkeit: KI ermöglicht Warnungen vor Bedrohungen in Echtzeit. Aber auch autonome Gegenmaßnahmen können durch eine KI eingeleitet werden.

03 Auswirkungen auf die Versicherbarkeit

Im Zusammenhang mit KI müssen alle noch eine ordentliche Schippe drauflegen!

Auswirkungen auf die Versicherbarkeit



Auswirkungen auf die Versicherbarkeit

Technische Voraussetzungen: Sicherheitsupdates (Patches) unverzüglich aufspielen um vorhandene Sicherheitslücken zu schließen. Außerdem Antiviren-software auf dem aktuellsten Stand halten und Firewalls entsprechend konfigurieren. Regelmäßige Datensicherungen vornehmen und diese sicher aufbewahren. Je nach Risiko eine Netzwerksegmentierung vornehmen. Altsysteme nicht mehr verwenden.

Awareness: Regelmäßige Nutzer- / Mitarbeiterschulungen hinsichtlich aktueller Angriffsszenarien und Gefahren zur Erkennung von Phishing-Emails, entsprechender Betrugsmaschen, etc.

Cyber-Security-Management: Notfall- / Wiederanlaufpläne erstellen und schriftlich fixieren. Dokumentation von IT-Strukturen. Wichtige Dokumente nicht nur auf dem Rechner sichern. Frühzeitig Zuständigkeit klären und benennen. Backup-Konzepte entwickeln und Adminrechte reglementieren.

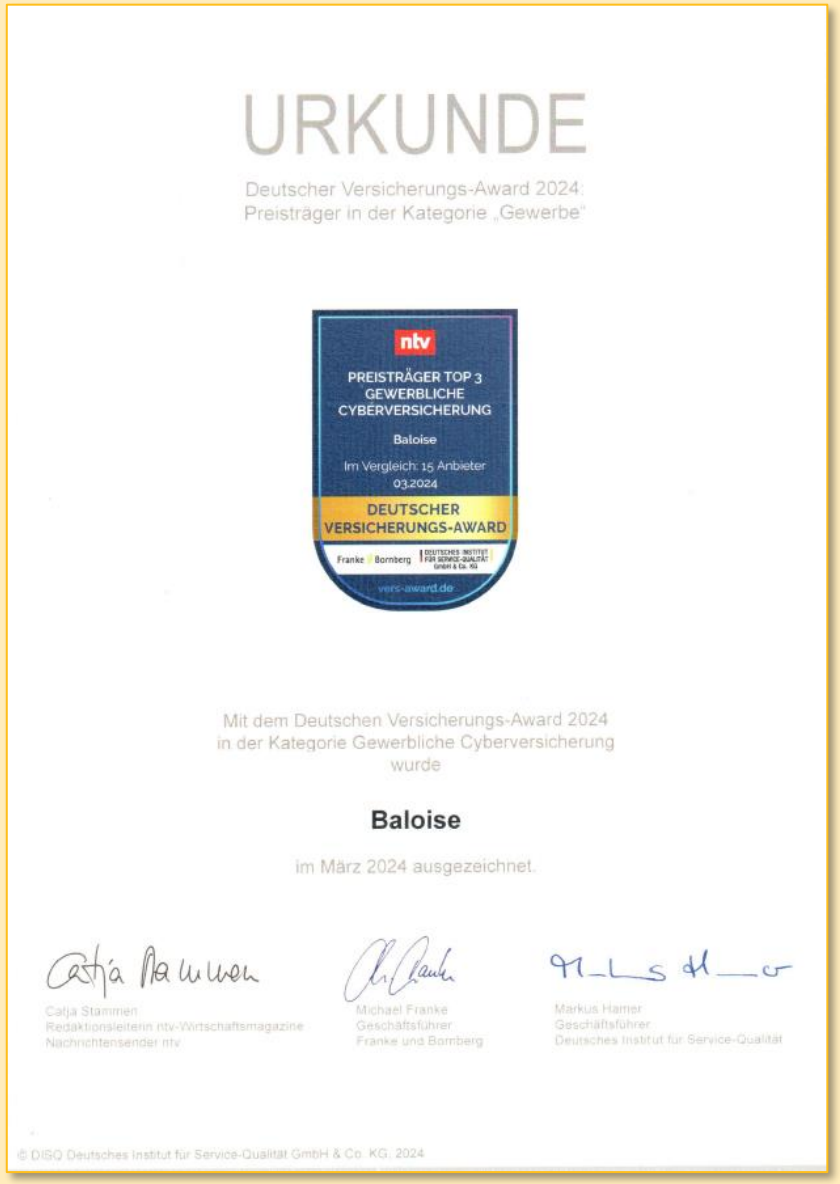
04 Baloise Cyber-Police Baloise Cyber-Basisrisiko 2024

Baloise Cyber-Police 2024

- Aufnahme **Kulanz**gutscheine
- Klarstellung **BU** durch Ausfall Dienstleister von **ent-** und **unentgeltlichen** Dienstleistern **(Cloud)**
- Überarbeitung der **Zielbranchen** (einfacherer Abschluss über das Antragsmodell)
- **15%** Prämien**nachlass** bei Abschluss **Awareness-**Maßnahmen über perseus
- **Sachverständigen**verfahren
- Consumer Redress Fund
- u.v.m.

Highlights der Baloise Cyber-Police

- Elektronische und **analoge Daten**
- **Bedienfehler**
- «**Kleine** Repräsentantenklausel»
- **Vorsätzliche Schäden** durch Mitarbeiter
- **Cysmo**-Report
- Unbegrenzte **Rückwärtsdeckung** für **alle** Bausteine
- **Abschließende** Gefahrerhöhung
- Leistungs-Update-**Garantie**


URKUNDE

Deutscher Versicherungs-Award 2024:
Preisträger in der Kategorie „Gewerbe"

ntv
PREISTRÄGER TOP 3
GEWERBLICHE
CYBERVERSICHERUNG
Baloise
Im Vergleich: 15 Anbieter
03.2024
DEUTSCHER
VERSICHERUNGS-AWARD
Franke und Bornberg
vers-award.de

Mit dem Deutschen Versicherungs-Award 2024
in der Kategorie Gewerbliche Cyberversicherung
wurde

Baloise

im März 2024 ausgezeichnet.

Catja Stammen
Redaktionsleiterin ntv-Wirtschaftsmagazine
Nachrichtensender ntv

Michael Franke
Geschäftsführer
Franke und Bornberg

Markus Hamer
Geschäftsführer
Deutsches Institut für Service-Qualität

Cyber Basisrisiko

- **Baustein** innerhalb der **Betriebshaftpflicht**versicherung
- Abschließbar bis zu einem Jahresumsatz von **10 Mio. EUR**
- **Fest**prämie unabhängig vom Umsatz
- Gilt für alle **Betriebsarten** analog dem **Antragsmodell**
- **24/7-Support** durch Assistance-Hotline (perseus)
- Leichter Einstieg in die Cyberversicherung

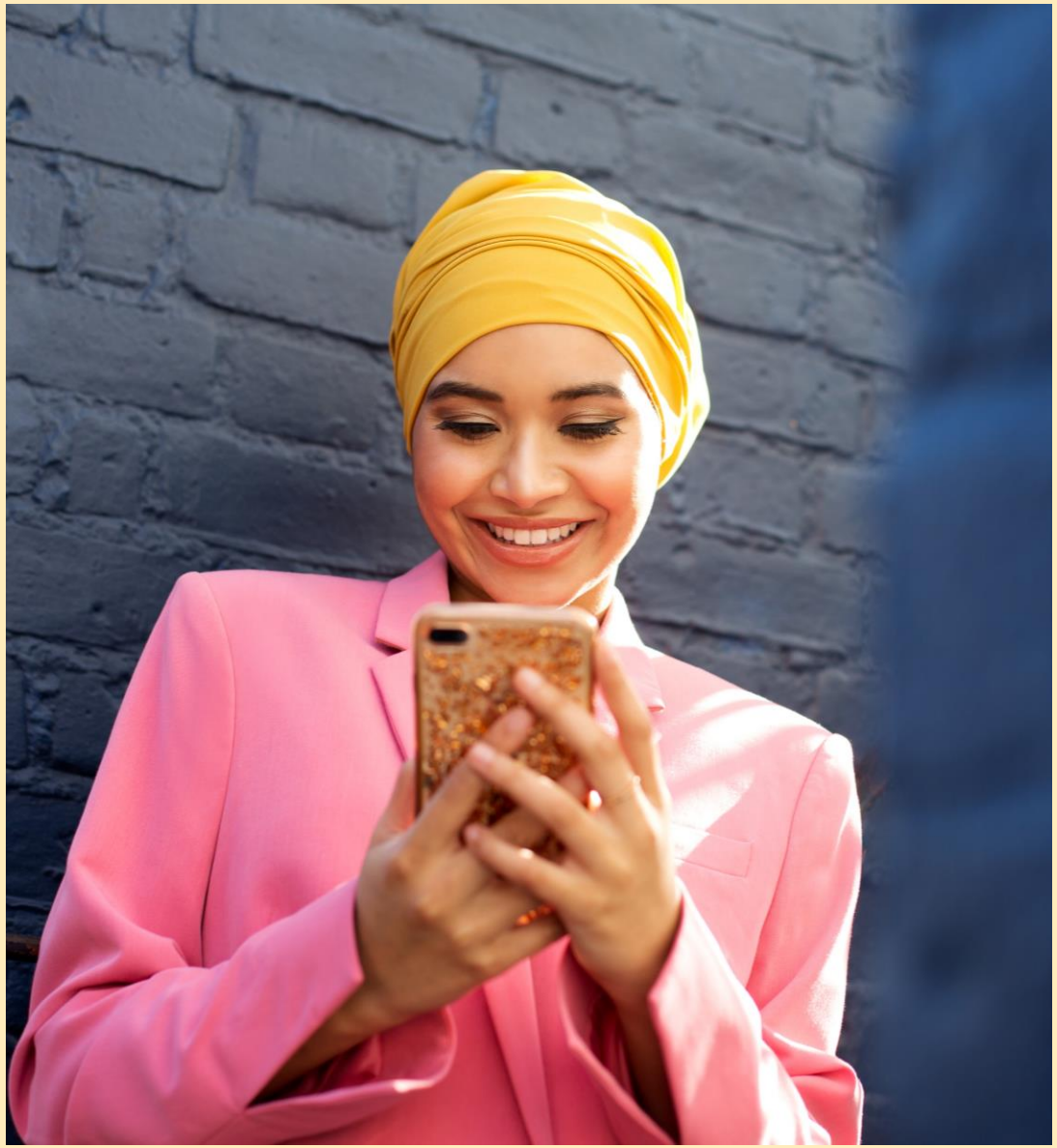
- **Cyber-Police bestehend aus den Bausteinen**
  - Kostenposition / Krisenmanagement
  - Drittschadendeckung
  - Eigenschadendeckung
- **Selbstbehalte**
  - 1.000 EUR
  - 12 Stunden
- **Haftzeit 6 Monate**
- **Versicherungssumme 50.000 EUR**

Cyber-Basisrisiko

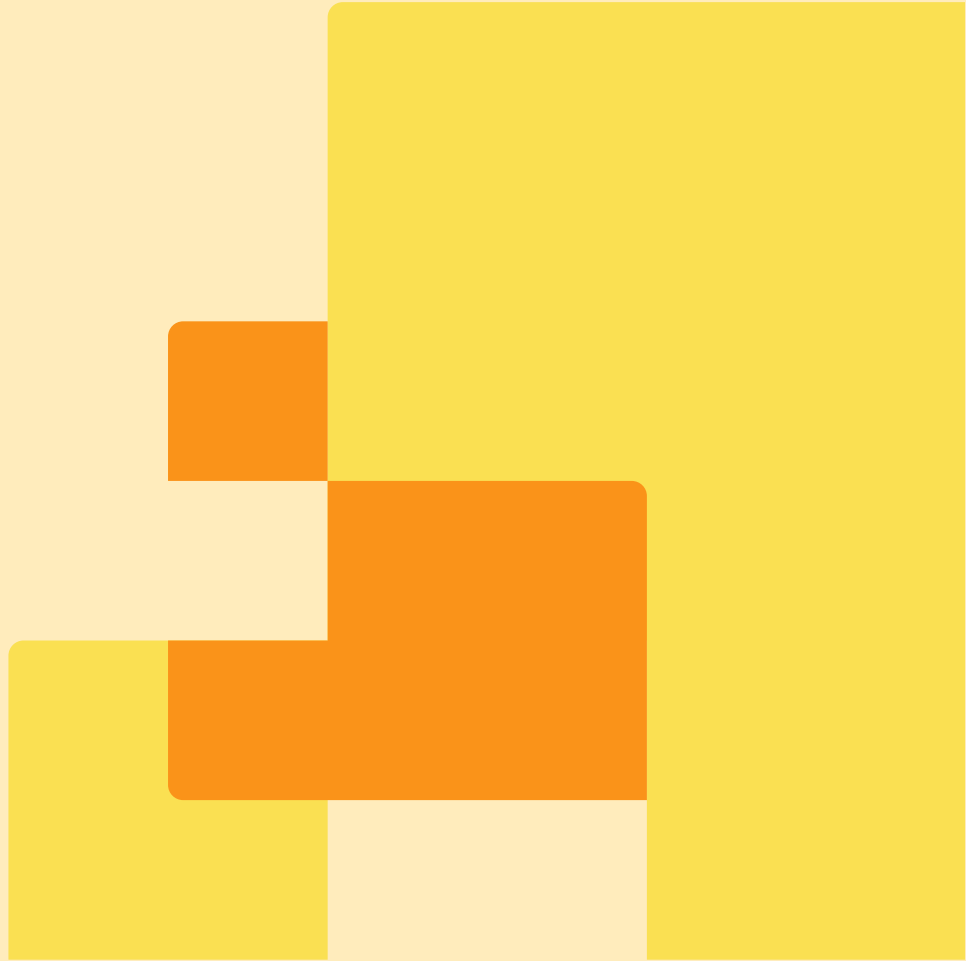
- **Versicherte Kostenschäden**
  - Forensik
  - Forensik ISV nicht feststellbar (Sublimit 25.000 EUR)
  - Krisenkommunikation und PR-Maßnahmen

- **Versicherte Drittschäden**
  - Abwehr, Prüfung von Ansprüchen
  - E-Payment
  - Rechtsverteidigungskosten

- **Eigenschäden**
  - Betriebsunterbrechung (Sublimit 10.000 EUR)
  - Mehrkosten (Sublimit 10.000 EUR)
  - Wiederherstellung von Daten (Sublimit 10.000 EUR)
  - Elektronischer Zahlungsverkehr
  - Cyber-Erpressung (Sublimit 25.000 EUR)



Vielen Dank!



Ihre Fragen ?