Pinnipedia Technologies

Assistierte Erstellung von IT Sicherheitskonzepten

OMNISECURE®

Startup-Arena

Berlin, den 20. Januar 2025

Pinnipedia Technologies

Die Gewährleistung von IT-Sicherheit ist von zunehmender Dringlichkeit

LIDL-KONZERNMUTTER

Schwarz-Gruppe wehrt 350.000 Hackerangriffe ab – pro Tag

Die Schwarz-Gruppe sieht sich einer extrem gestiegenen Zahl von Cyberangriffen ausgesetzt, vor allem aus

Ein Pfleger arbeitet in einem Krankenhaus an einem Computer | dpa

Hackerangriffe auf Kliniken

"Nur eine Frage der Zeit"

Stand: 29.01.2024 10:11 Uhr

Krankenhäuser und Pflegeeinrichtungen werden immer häufiger zum Ziel von Cyberattacken. Ein großflächiger Angriff mit vielen Ausfällen ist ein denkbares Szenario. Viele Einrichtungen sind schlecht vorbereitet.

24.10.2024, 18:37 Uhr · Audiobeitrag

> Hackerangriff auf sieben Schulen im Landkreis Kitzingen

Hackerangriff auf sieben Schulen im Landkreis Kitzing

Gleich sieben weiterführende Schulen auf einmal sind im Landkreis Kitz Hackerangriff betroffen. Der Unterricht ist dadurch aber nicht eingesch Schulen zum Ziel für die Hacker wurden, ist noch unklar.

kerangriffe auf Autos

Vehe, wenn da uto gehackt w

yberkriminalität

Italienische Polizei ermittelt we- gen prorussischer Hackerangriffe

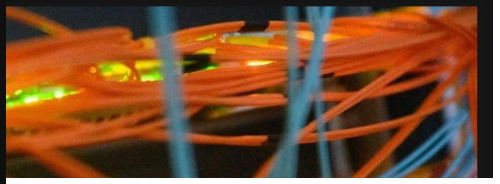
urden in den letzten Tagen das Außenministerium, Flughäfen rssysteme gehackt. Laut Polizei bekannte sich e den Angriffen.

INTERNETKRIMINALITÄT

+ Bochum kämpft gegen Hackerangriffe: Was nun zu tun ist

08.01.2025, 09:00 Uhr • Lesezeit: 3 Minuten

Von **Andreas Rorowski**
Redakteur Lokal



Nach simuliertem Angriff

Lauterbach: EPA-Start nur bei er Sicherheit

Hacker mögliche Sicherheitslücken der elektronischen Patientenakte (EPA) t haben, die 70 Millionen Digitalakten betreffen könnten, hat undheitsminister Karl Lauterbach (SPD) angekündigt, mit dem EPA-Start so lange bis die Mängel beseitigt sind. Dass damit der Start der Testphase infrage steht, die Gematik nicht.

Persönliche Daten betroffen

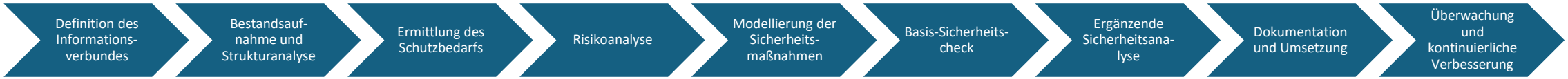
Hackerangriff auf Reha-Klinik in Bad Wildungen

Unbekannte Hacker haben eine Reha-Klinik in Bad Wildungen angegriffen. Die Klinik geht davon aus, dass sie an persönliche Daten gelangten. Der Betrieb sei aber davon nicht betroffen.

Quelle: Presse, Pinnipedia Technolgies GmbH

Pinnipedia Technologies

IT-Sicherheit beginnt mit einer Analyse der Situation und einem IT-Sicherheitskonzept



Die Erstellung eines IT-Sicherheitskonzepts ist ein Prozeß der für

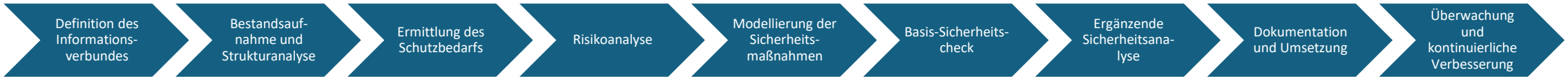
- KMU mindestens vier bis sechs Monate
- größere Unternehmen mehr als 1 Jahr

dauert.

Die Kosten hängen von der Komplexität des Informationsverbunds ab und betragen zwischen €10.000 und €x00.000.

Pinnipedia Technologies

IT-Sicherheit beginnt mit einer Analyse der Situation und einem IT-Sicherheitskonzept



Die Erstellung eines IT-Sicherheitskonzepts ist ein Prozeß der für

- KMU mindestens vier bis sechs Monate
- größere Unternehmen mehr als 1 Jahr

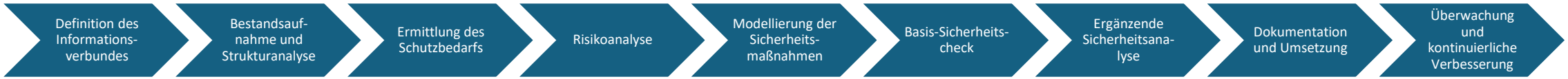
dauert.

Die Kosten hängen von der Komplexität des Informationsverbunds ab und betragen zwischen €10.000 und €x00.000.

Cyber Resiliance Act (CRA):
25.000 bis 40.000 Unternehmen in Deutschland

Pinnipedia Technologies

IT-Sicherheit beginnt mit einer Analyse der Situation und einem IT-Sicherheitskonzept



Die Erstellung eines IT-Sicherheitskonzepts ist ein Prozeß der für

- KMU mindestens vier bis sechs Monate
- größere Unternehmen mehr als 1 Jahr

dauert.

Die Kosten hängen von der Komplexität des Informationsverbunds ab und betragen zwischen €10.000 und €x00.000.

Cyber Resiliance Act (CRA):
25.000 bis 40.000 Unternehmen in Deutschland

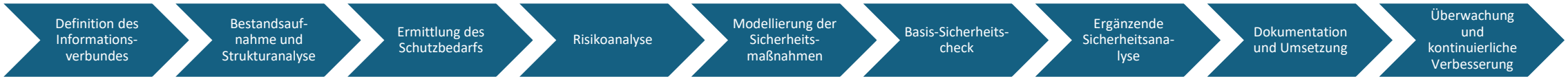
Die Erstellung eines IT-Sicherheitskonzepts benötigt Fachexpertise die

- KMUs in der Regel nicht vorhalten
- Behörden, größere Unternehmen und Service Provider nur schwer am Markt finden

Dieser Mangel führt zu einem erheblichen Backlog in der Erstellung und damit gerade bei Vorhaben der öffentlichen Hand auch zu Verzögerungen in der Umsetzung von Projekten.

Pinnipedia Technologies

IT-Sicherheit beginnt mit einer Analyse der Situation und einem IT-Sicherheitskonzept



Die Erstellung eines IT-Sicherheitskonzepts ist ein Prozeß der für

- KMU mindestens vier bis sechs Monate
- größere Unternehmen mehr als 1 Jahr

dauert.

Die Kosten hängen von der Komplexität des Informationsverbunds ab und betragen zwischen €10.000 und €x00.000.

Cyber Resiliance Act (CRA): 25.000 bis 40.000 Unternehmen in Deutschland

Die Erstellung eines IT-Sicherheitskonzepts benötigt Fachexpertise die

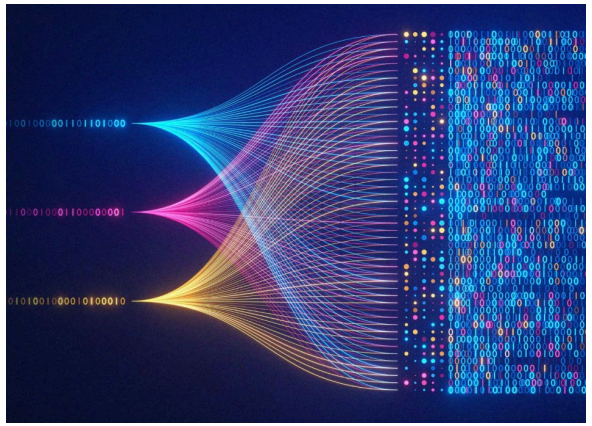
- KMUs in der Regel nicht vorhalten
- Behörden, größere Unternehmen und Service Provider nur schwer am Markt finden

Dieser Mangel führt zu einem erheblichen Backlog in der Erstellung und damit gerade bei Vorhaben der öffentlichen Hand auch zu Verzögerungen in der Umsetzung von Projekten.

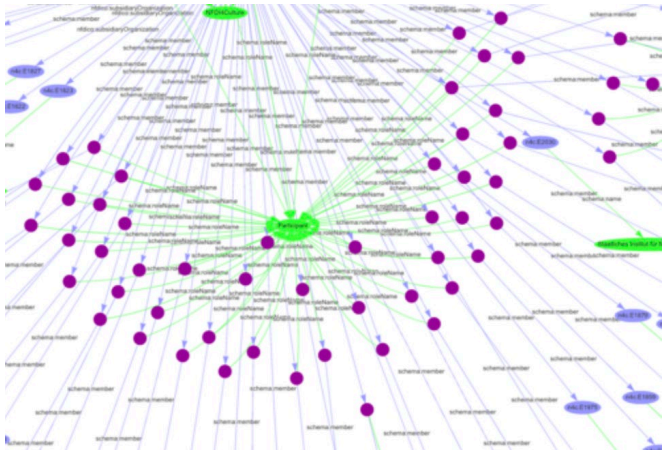
Pinnepedia Technologies schafft automatisierte Lössungen mit KI!

Pinnipedia Technologies

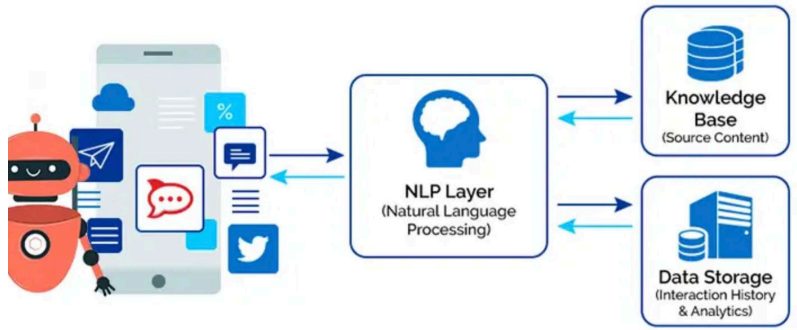
Pinnipedia nutzt moderne KI und Datentools …



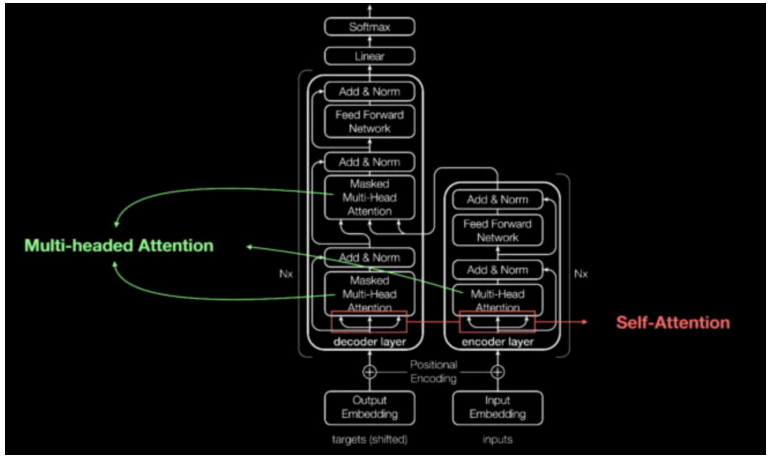
Komplexe Datenaufarbeitung und Analyse von Unternehmensdokumente



Graphentheorie zur Analyse und Trennung von Datensätzen



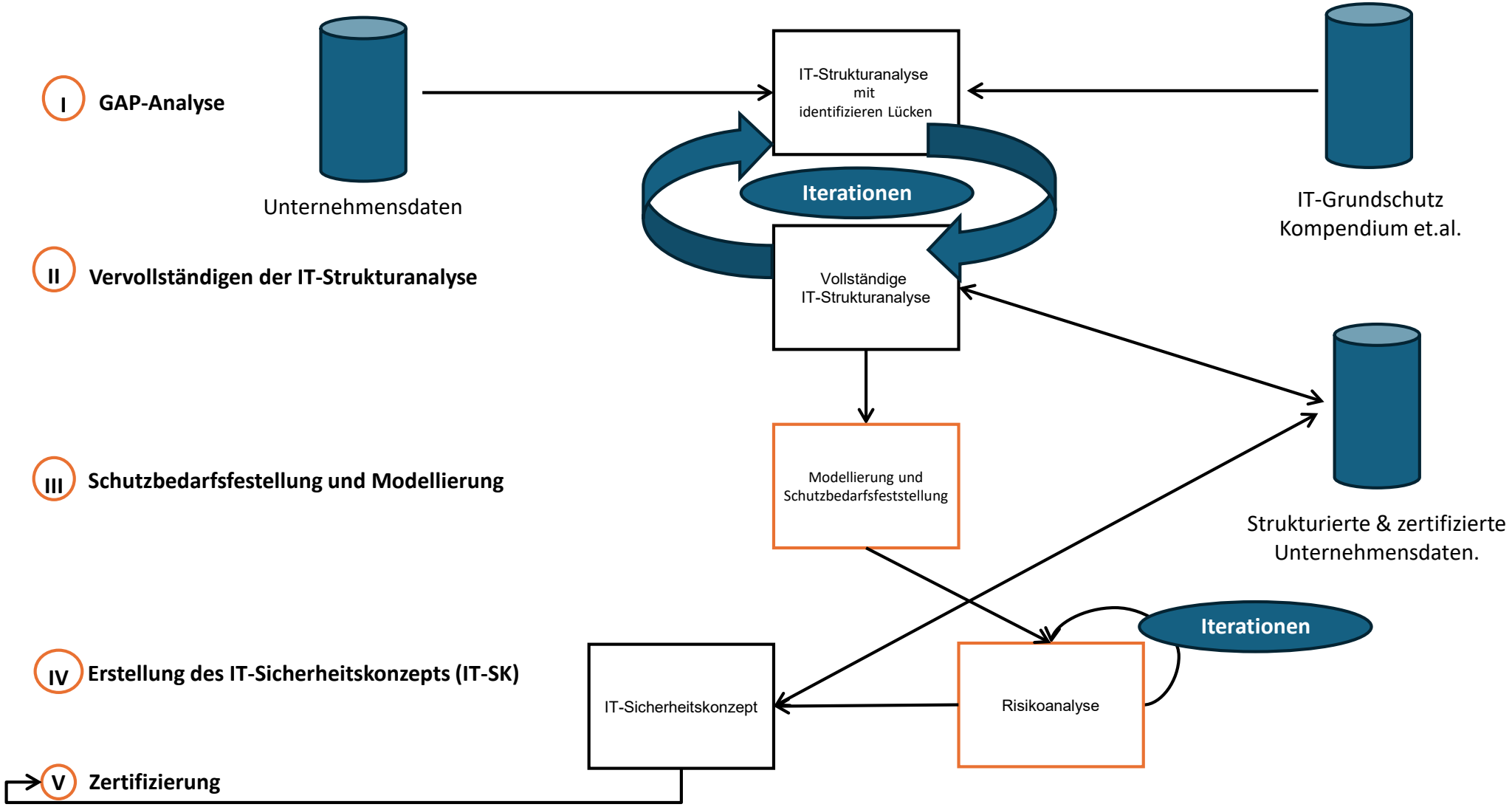
Chat-Bot zur Vervollständigung der Analyse



Generative KI zur Textgenerierung und Graphenerstellung

… zur Automatisierung und Assistierung der Erstellung von IT-Sicherheitskonzepten

Pinnipedia Technologies



Source: Pinnipedia Technolgies GmbH

Pinnipedia Technologies

Geschäftsmodell: IT-Sicherheitskonzept in fünf Stufen als assistiertes SaaS-Modell

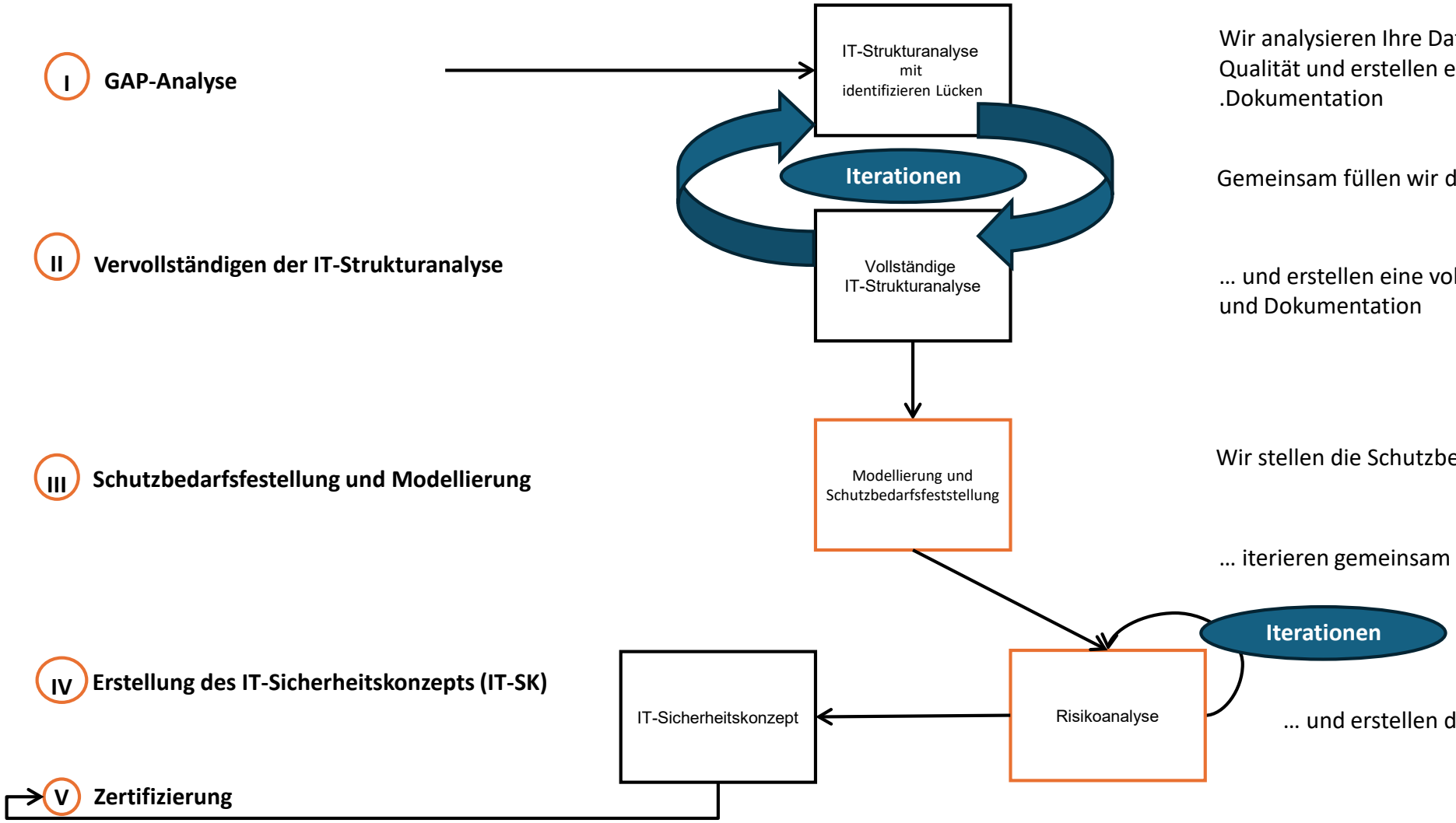
I **GAP-Analyse**

II **Vervollständigen der IT-Strukturanalyse**

III **Schutzbedarfsfestellung und Modellierung**

IV **Erstellung des IT-Sicherheitskonzepts (IT-SK)**

V **Zertifizierung**



Wir analysieren Ihre Daten auf Vollständigkeit und Qualität und erstellen eine IT-Strukturanalyse .Dokumentation

Gemeinsam füllen wir die Lücken …

… und erstellen eine vollständige IT-Strukturanalyse und Dokumentation

Wir stellen die Schutzbedarfe fest und …

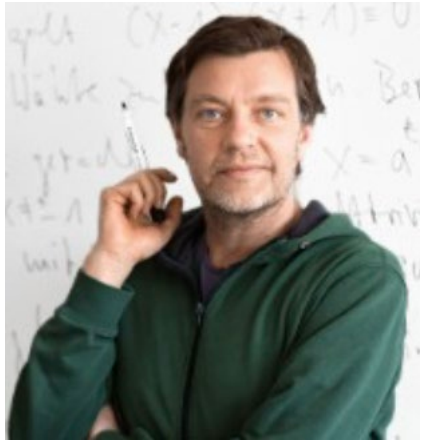
… iterieren gemeinsam die Risikoanalyse

… und erstellen das Sicherheitskonzept

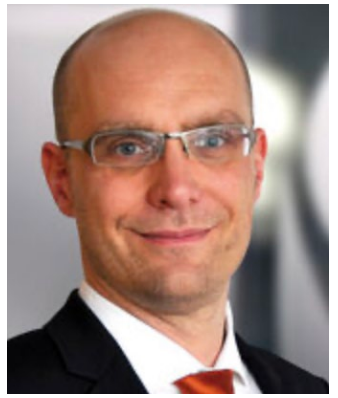
Das Gründerteam

Pinnipedia Technologies

Gerhard Wunder ist Professor für Cybersicherheit und KI an der Freien Universität Berlin. Zu seinen Forschungsschwer-punkten gehören u.a. LLMs, Erklärbarkeit von KI und KI mit Datenschutz. Gerhard Wunder ist Heisenberg-Stipendiat der DFG und wurde zusammen mit Dr. Müller (BOSCH Stuttgart) und Prof. Paar (Ruhr-Universität Bochum) für den Deutschen Zukunftspreis 2017 für seine Arbeit im Bereich innovativer Sicherheitsver-fahren nominiert.



Marian Margraf ist Professor für Informationssicherheit an der Freien Universität Berlin und Abteilungsleiter am Fraunhofer Institut AISEC. Er verfügt über mehr als 20 Jahre Erfahrung auf dem Gebiet der Informationssicherheit. Zunächst als Kryptologe im Bundesamt für Sicherheit in der Informationstechnik und dann als Regierungsdirektor im Bundesministerium des Innern. Seit 2013 ist er Professor an der Freien Universität Berlin mit Forschungsschwerpunkt Usable Privacy and Security, Kryptografie, insb. Post-Quanten-Kryptografie, elektronische Identitäten und Informationssicherheitsmanagement.



Sören Werth ist Professor für IT-Sicherheit an der Berliner Hochschule für Technik. Von 2008 bis 2012 entwickelte er im Bundesamt für Sicherheit in der Informationstechnik Ende-zu-Ende Verschlüsselungs-systeme. Dann wechselte er in das Bundesministerium des Innern und war an der Entwicklung und Umsetzung politischer Strategien für IT-Sicherheit in kritischen beteiligt. Seine Schwerpunkte in Forschung, Lehre und Praxis liegen in den Bereichen Kryptographie und Maschinelles Lernen.

Jürgen Laartz ist unabhängiger Berater mit Fokus auf der Realisierung von digitalen Geschäfts-strategien. Er verfügt über mehr als dreißig Jahre Beratungserfahrung, davon 24 Jahre mit McKinsey & Company, wo er in vielfältigen Funktionen die Technolgieberatung in Skandinavien, Deutschland, Osteuropa und dem mittleren Osten geleitet hat. Er hat über 15 Jahre eine jährliche anwender zentrierte Konferenz zum Thema IT-Architektur ausgerichtet. Ein Schwerpunkt seiner Beratungs-arbeit ist IT-Risk Management, Cybersecurity und sichere Softwareentwicklungsprozesse.