



BWI

IT für Deutschland



Marktdialog@BWI Cyber Security & Zero Trust – Die Zukunft der Cyber-Security 23.01.2025, ab 13 Uhr

Marktdialog@BWI – V 2.2 – BWI frei verwendbar – Eine Weitergabe an Auftraggeber ist erlaubt

Bildquelle: BWI/Herdieckerhoff

Agenda

01

Begrüßung und Informationen

02

Cyber Security & Zero Trust –
Die Zukunft der Cyber-Security

03

Fragerunde und Dialog mit den BWI Experten

04

Ausblick & Verabschiedung

01 Begrüßung und Informationen



Referenten

- Peter Scaruppe, Leiter CRO Procurement
- Martina Kotalla, CRO P Business Partnering
- Andreas Ritschel, Leiter Security Program Management & Cross Functions
- Milan Göllner, Lead Security Expert



Agenda

01

Begrüßung und Informationen

02

Cyber Security & Zero Trust –
Die Zukunft der Cyber-Security

03

Fragerunde und Dialog mit den BWI Experten

04

Ausblick & Verabschiedung



02 Cyber Security & Zero Trust – Die Zukunft der Cyber-Security

Marktdialog@BWI – V 2.2 – BWI frei verwendbar – Eine Weitergabe an Auftraggeber ist erlaubt

Bildquelle: BWI/Herdieckerhoff



Andreas Ritschel



Milan Göllner

CDO CCITS SecProgrMgmt&Cross Fct

Kontaktieren Sie uns gerne persönlich
bei Fragen und Anregungen.

Sie erreichen uns unter:
milan.goellner@bwi.de



Marktdialog 2025

Zero Trust für die Bundeswehr

Marktdialog@BWI - V 2.2 - BWI frei verwendbar - Eine Weitergabe an Auftraggeber ist erlaubt

Bildquelle: Andreas Ritschel (privat)

Zero Trust Struktur

Zero Trust ist ein modernes Sicherheitsrahmenwerk, welches antritt, mit den mannigfaltigen aktuellen und zukünftigen Bedrohungsszenarien für Informationssysteme Schritt zu halten. Zero Trust strebt dabei Veränderungen in 3 Bereichen an:

Kultur

Der Bereich Kultur umfasst die Menschen, welche die Zero Trust tauglichen, ressourcenzentrischen Informationssysteme der Zukunft verantworten, entwickeln, testen, in Betrieb nehmen und schlussendlich nutzen.

Governance

Der Bereich Governance hat das Ziel, über die gesamte Organisation hinweg eine einheitliche und stimmige Prozess- und Vorgabenlandschaft zu etablieren und die Anwendung dieser Prozesse und Vorgaben sicherzustellen.

Technologie

Der Bereich Technologie befasst sich mit der konkreten Entwicklung und Operationalisierung von aus Zero Trust Prinzipien basierenden Fähigkeiten sowohl bei Neuentwicklung als auch während des Lebenszyklus von Bestandsfähigkeiten.

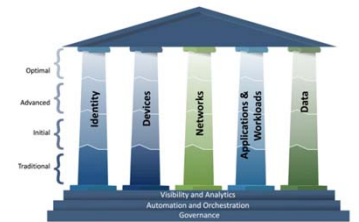
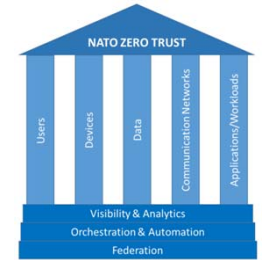
Die BWI befasst sich mit dem dritten Bereich von Zero Trust, der Technologie. Der Bundeswehr sollen Wege aufgezeigt werden, wie das Zero Trust Rahmenwerk in den Betriebsumgebungen der Bundeswehr im Inland, im Ausland, bei Einsätzen und kooperativ mit Verbündeten wirken und umgesetzt werden kann.

Zero Trust – Was machen wir eigentlich?

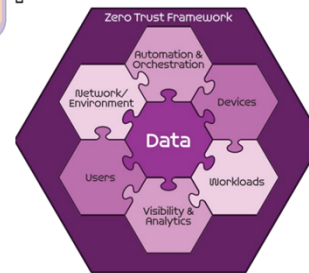
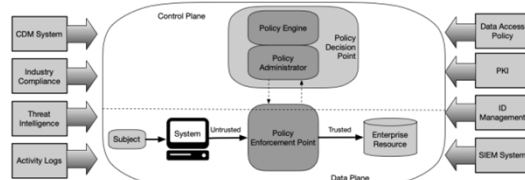
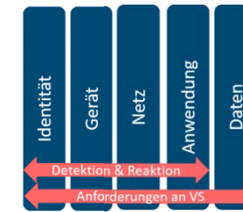
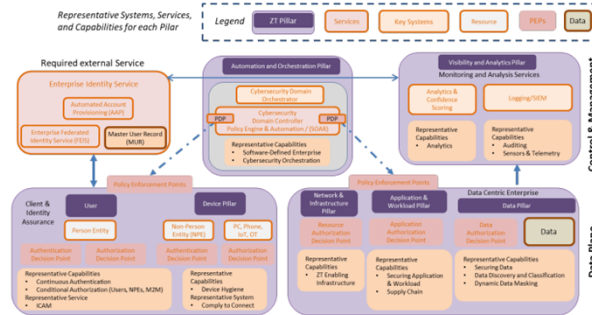
Zero Trust wird in vielen Dokumenten auf sehr hoher Flughöhe beschrieben und bewertet. Dabei ergeben sich nicht nur eine Vielzahl an Widersprüchen, sondern eine wesentliche Frage wird nicht beantwortet: WARUM werden diese Schritte/Schnitte/Fähigkeiten etc. eigentlich so empfohlen/festgelegt/vorgegeben?

Die BWI versuchte zunächst, das WARUM für die Bundeswehr in Form von Wirkweisen so zu beantworten, das sie den Wunsch des Kunden nach spürbaren Verhaltensweisen einer Zero Trust befähigten Infrastruktur beschreiben und die so ein angepeiltes Zielbild aufmalen.

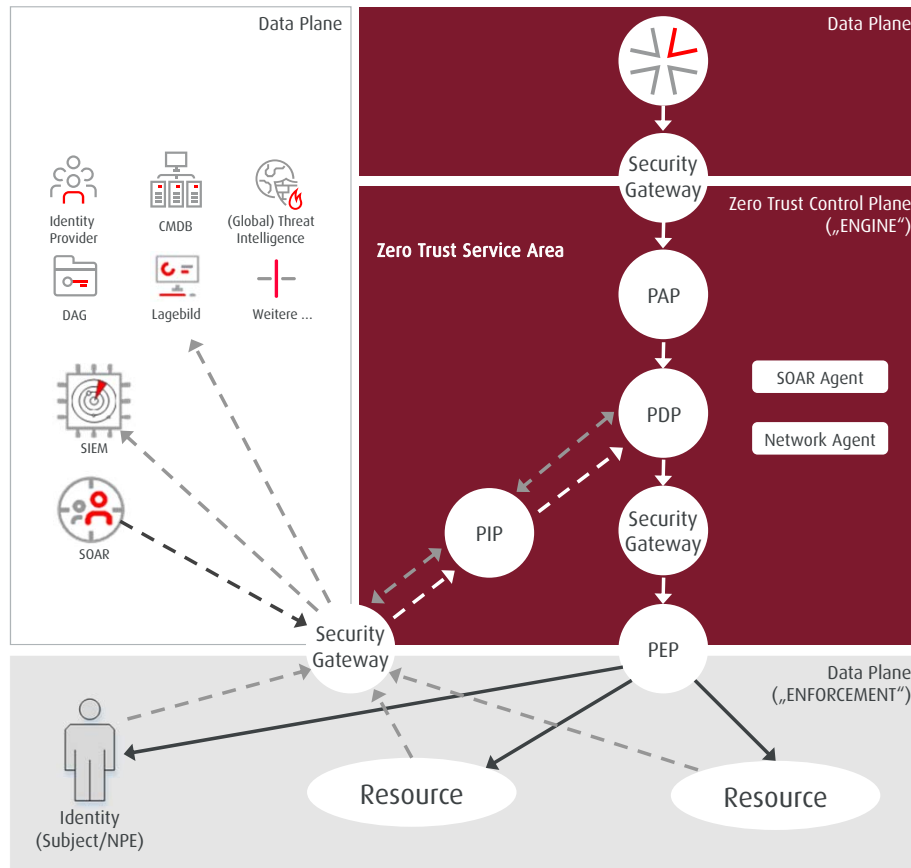
Die BWI hat dabei darauf verzichtet, künstliche Limitationen oder Gedankenbarrieren aufzubauen, um das Thema einfacher oder übersichtlicher zu gestalten. So gehören beispielsweise sämtliche Aspekte der Thematik Data Centric Security zweifelsfrei in das Zero Trust Zielbild, werden aber oft separat behandelt, BWI betrachtet DCS hingegen als ein zwangsläufiges Resultat einer umfassenden Implementierung von Zero Trust.



	Identity	Devices	Networks	Applications and Workloads	Data
Optional	• Continuous authentication • User behavior analytics • Adaptive authentication • Threat intelligence • Risk-based authentication	• Device posture assessment • User and device authentication • Device health monitoring • Device compliance • Device management • Device lifecycle management	• Network segmentation • Network access control • Network anomaly detection • Network intrusion detection • Network intrusion prevention • Network traffic analysis • Network traffic monitoring	• Application security • Application vulnerability assessment • Application performance monitoring • Application log management • Application log analysis • Application log correlation	• Data classification • Data loss prevention • Data retention • Data archiving • Data backup • Data recovery
Advanced	• Privileged user access • User behavior analytics • User risk management • User session monitoring • User session recording • User session replay	• Device posture assessment • User and device authentication • Device health monitoring • Device compliance • Device management • Device lifecycle management	• Network segmentation • Network access control • Network anomaly detection • Network intrusion detection • Network intrusion prevention • Network traffic analysis • Network traffic monitoring	• Application security • Application vulnerability assessment • Application performance monitoring • Application log management • Application log analysis • Application log correlation	• Data classification • Data loss prevention • Data retention • Data archiving • Data backup • Data recovery
Initial	• User authentication • User authorization • User session management • User session recording • User session replay	• Device posture assessment • User and device authentication • Device health monitoring • Device compliance • Device management • Device lifecycle management	• Network segmentation • Network access control • Network anomaly detection • Network intrusion detection • Network intrusion prevention • Network traffic analysis • Network traffic monitoring	• Application security • Application vulnerability assessment • Application performance monitoring • Application log management • Application log analysis • Application log correlation	• Data classification • Data loss prevention • Data retention • Data archiving • Data backup • Data recovery
Traditional	• User authentication • User authorization • User session management • User session recording • User session replay	• Device posture assessment • User and device authentication • Device health monitoring • Device compliance • Device management • Device lifecycle management	• Network segmentation • Network access control • Network anomaly detection • Network intrusion detection • Network intrusion prevention • Network traffic analysis • Network traffic monitoring	• Application security • Application vulnerability assessment • Application performance monitoring • Application log management • Application log analysis • Application log correlation	• Data classification • Data loss prevention • Data retention • Data archiving • Data backup • Data recovery



Zero Trust – Wie machen wir was wir machen



BWI hat folgendes Zero Trust Model als Detaillierungsschritt des NIST Model vorläufig festgelegt. Das Kommunikationsmodell ist hier logisch dargestellt.

Die Zero Trust Control Plane ist im Regelbetrieb von außerhalb für zwei Kategorien von Kommunikationspartnern erreichbar:

1. Administrativ zum Policy Administration Point zur Regelmodellierung
2. Funktional über den Policy Information Point um
 - I. Empfang von Anforderungen zur Bewertung von Ressourcennutzungsanfragen aus dem Enforcement
 - II. Empfang von Informationen von externen Datenquellen
 - III. Empfang von priorisierten Sofortmaßnahmen des Security Operations Centers

Der Enforcement Bereich mit seinen Policy Enforcement Points wird in diesem Model als eine verteilte Sammlung von unterschiedlichen Verwaltungswerkzeugen verstanden, welche die Regelentscheidungen des Policy Decision Point für die jeweiligen Plattformen umsetzen. Pro Verwaltungswerkzeug ist zu klären, wie diese durch den externen Policy Enforcement Point konfiguriert werden können (API).

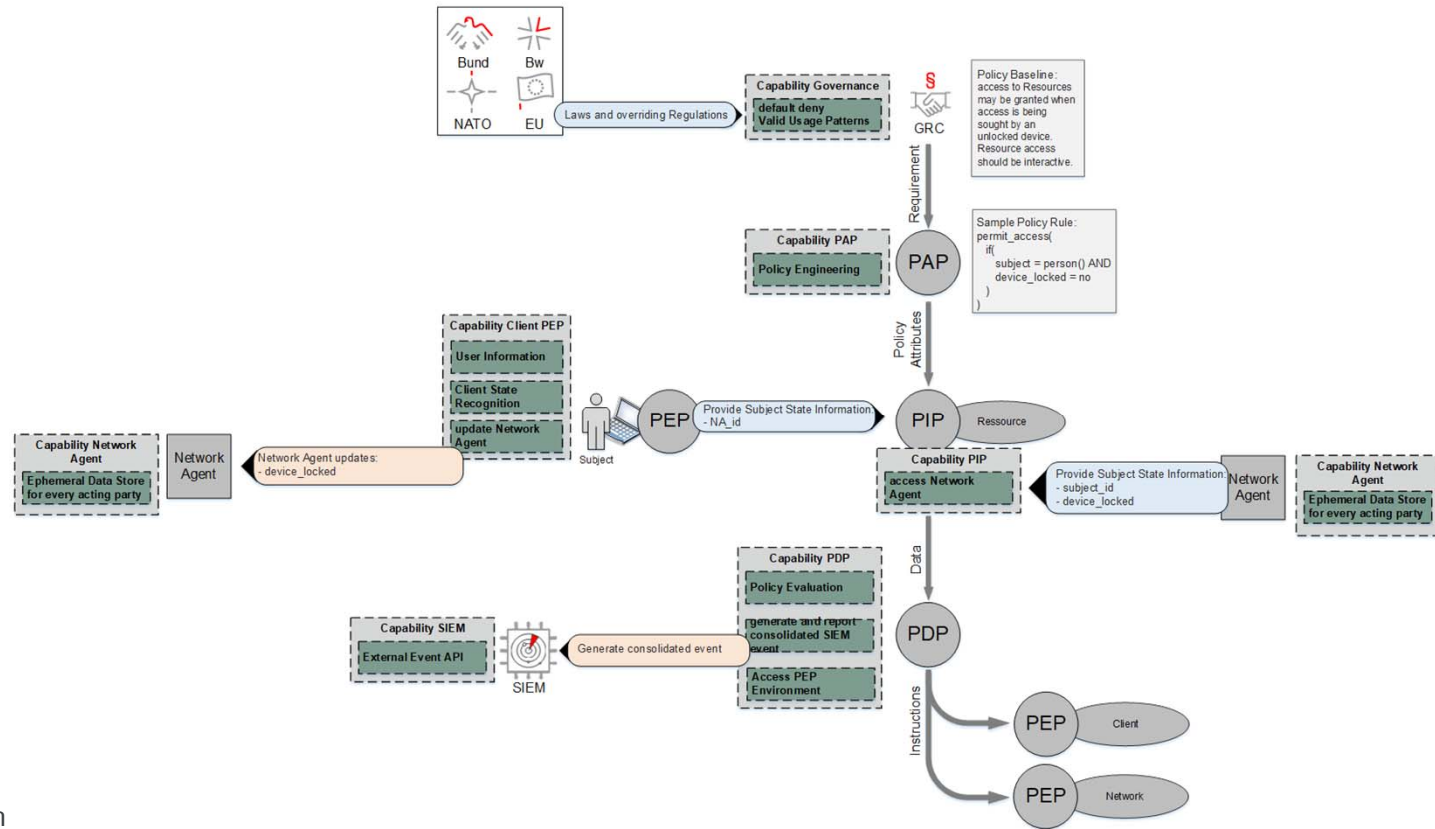
Zero Trust – Warum machen wir was wir machen

Wirkweisen beschreiben die Möglichkeiten der Ressourcennutzung (i.d.R. Daten) durch Konsumenten innerhalb einer Zero Trust Umgebung.

Wirkweisen werden in Fähigkeiten und Funktionen heruntergebrochen, um einen iterativen Lösungsansatz basierend auf marktverfügbaren und/oder neu zu erstellenden Produkten in unterschiedlichen Reifegraden zu beschreiben.

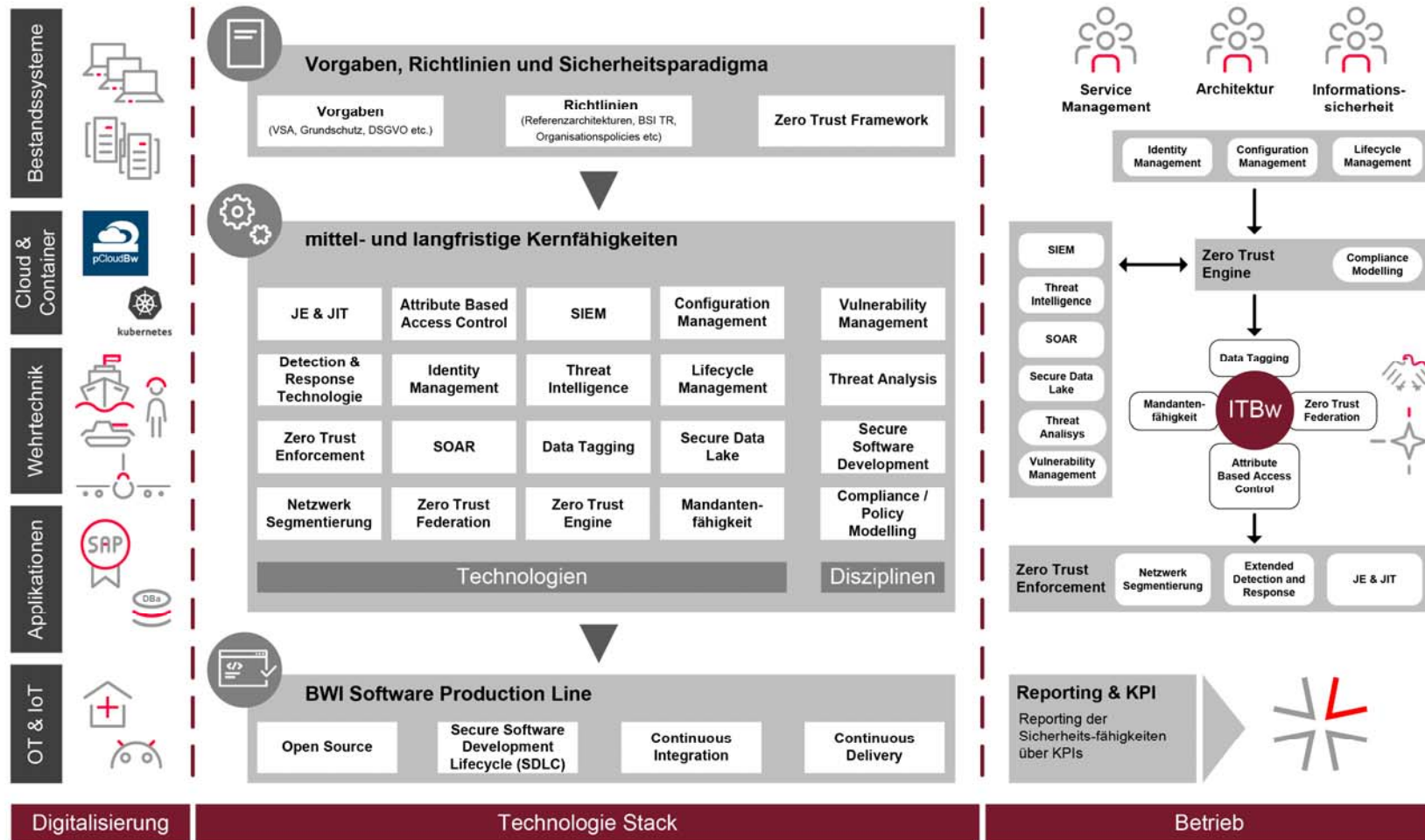
Eine Wirkweise wird in Form eines beispielhaften Anwendungsfalls verdeutlicht, jedoch sind die für die Wirkweise benötigten Fähigkeiten mit Blick auf das Zielbild wiederverwertbar und übergreifend zu designen.

Dieser Lösungsansatz kann einen Satz Werkzeuge zur Verfügung stellen, welcher geeignet wäre, die Kontrolle über und Zulässigkeit der Nutzung von Daten in Form von Regeln mit dynamischen Bedingungen flexibel zu modellieren und durchzusetzen.



Beispiel-Darstellung: Wirkweisenanalyse

Zero Trust Fähigkeiten Zielbild



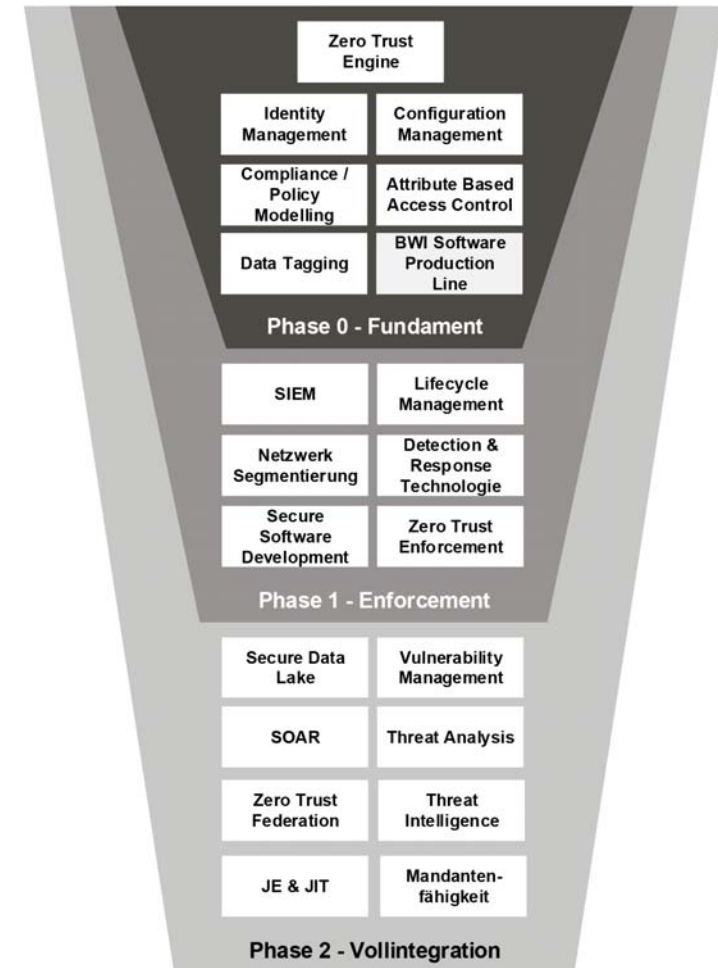
Operationalisierungsphasen

Zero Trust stellt für die BWI ein zweiteiliges Operationalisierungsprogramm dar.

Teil 1 muss die Engine entwickeln und Schnittstellen und Standards zur Automatisierung etablieren.

Teil 2 integriert bestehende Fähigkeiten so miteinander, dass die für die angestrebte Wirkung erforderlichen Rahmenbedingungen geschaffen werden. Diese Integration beinhaltet die Nutzung sowie die Weiterentwicklung von Bestandsfähigkeiten als auch die Entwicklung neuer Fähigkeiten.

Die Operationalisierung kann dann in drei elementaren Phasen erfolgen, welche darauf ausgerichtet sind, sukzessiv Fähigkeiten nach Wirkbedarf zu integrieren. Es ist davon auszugehen, dass es innerhalb dieser Phasen weitere Detaillierungsgrade geben wird und dass die Abgrenzungen zwischen Phasen schwimmend sein können. So wird beispielsweise die Entwicklung der Engine nicht in Phase 0 abgeschlossen werden können, sondern zunächst so weit voran gebracht werden, dass Phase 1 initiiert werden kann.



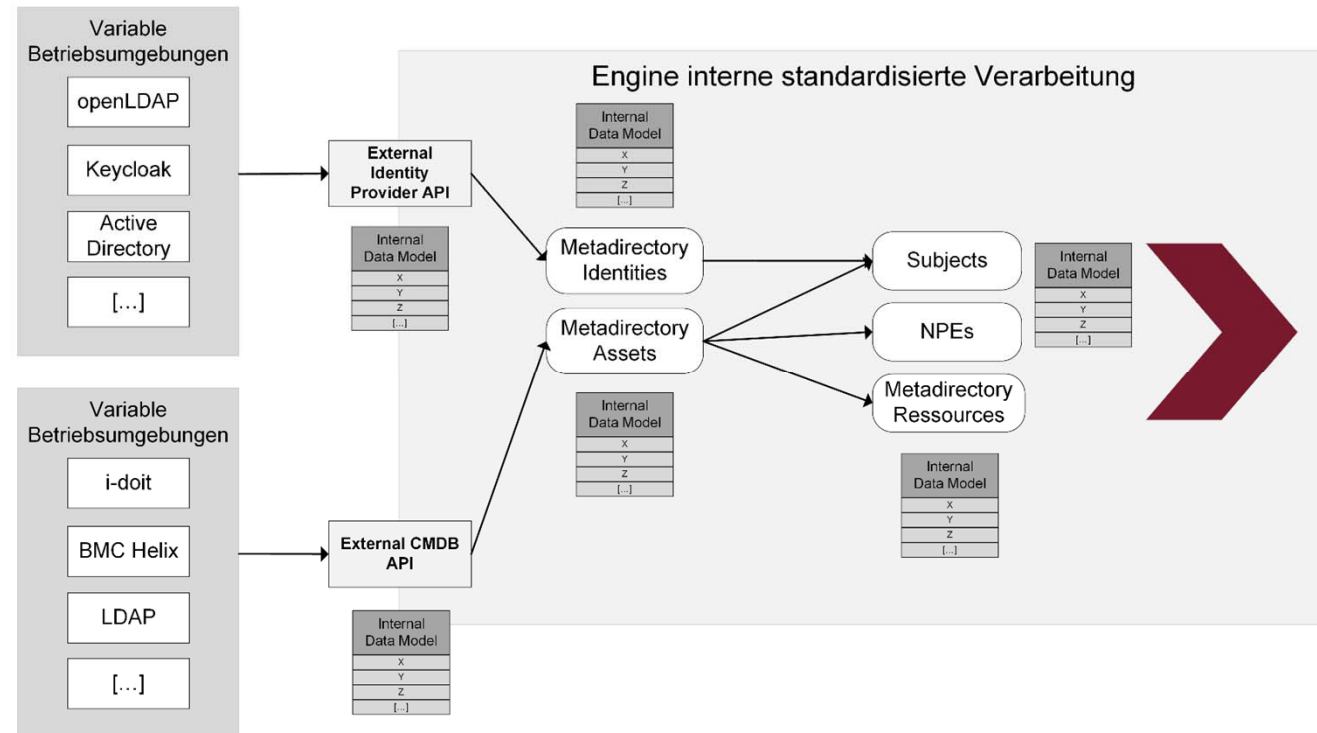
Standardisierung und Flexibilität am Beispiel Identitäten und Assets

Die avisierte Zero Trust Umgebung verfolgt das Ziel, sowohl flexibel einsetzbar bei gleichzeitiger maximaler Standardisierung zu sein.

Um dies zu erreichen verwendet die Zero Trust Engine intern Metaverzeichnisse, um Abbilder der primären Datenquellen nach einem standardisierten Datenmodell aufzubauen. Ausgehend von diesen Daten erfolgt dann die interne Weiterverarbeitung.

Nach Außen bietet die Zero Trust Engine hierfür APIs an, welche durch die primären Datenquellen zu bedienen sind, um die Metaverzeichnisse zu befüllen.

Somit können Datenquellen theoretisch unbegrenzt flexibel und produktunabhängig sein, so lange sie die Zero Trust API bedienen und Daten in der gemäß Reifegrad festgelegten Qualität und Umfang liefern können.



Umfrage per TedMe

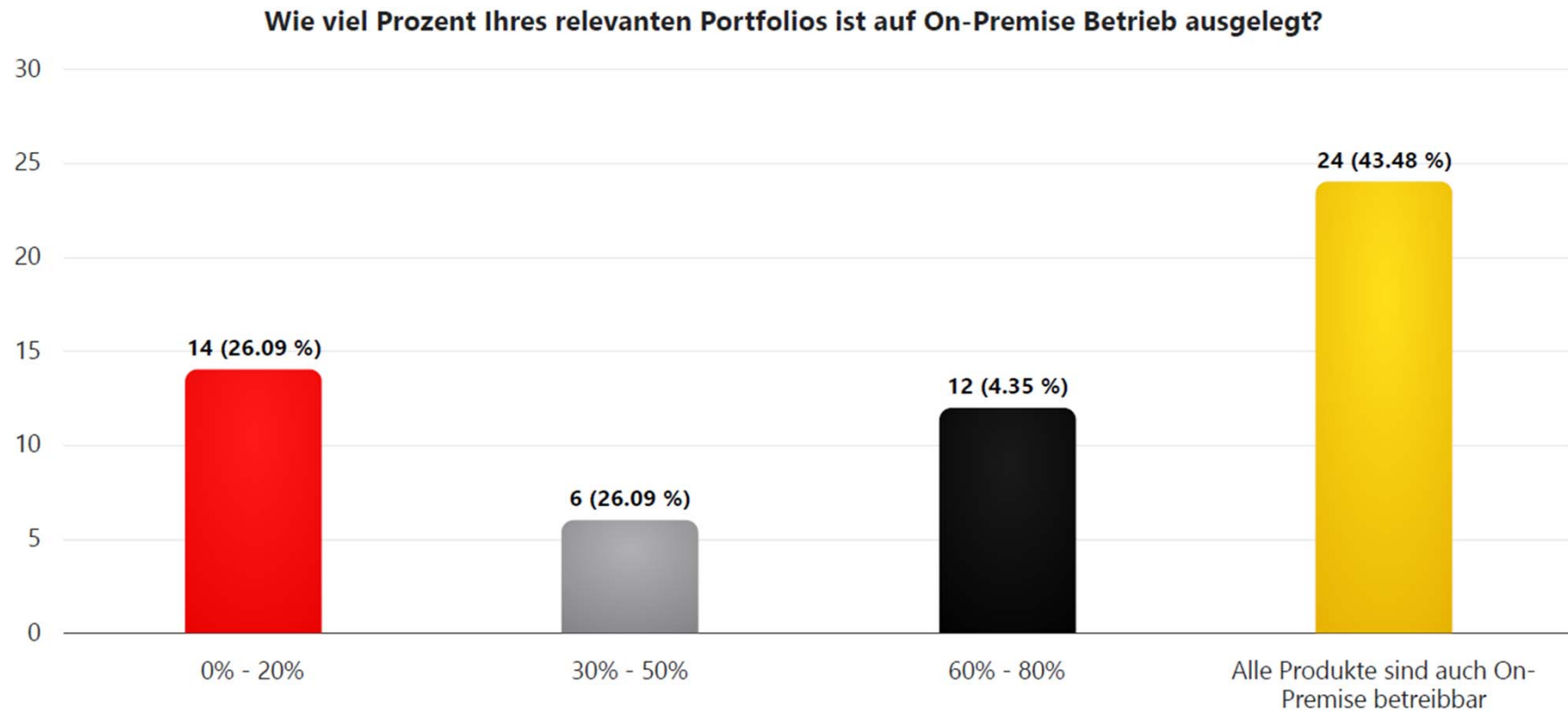
TEDME

Bitte öffnen Sie
www.tedme.com
und geben folgende
Raumnummer ein:
MD25

ODER scannen Sie diesen QR-Code
mit ihrem Mobiltelefon



Umfrage per TedMe - Ergebnis

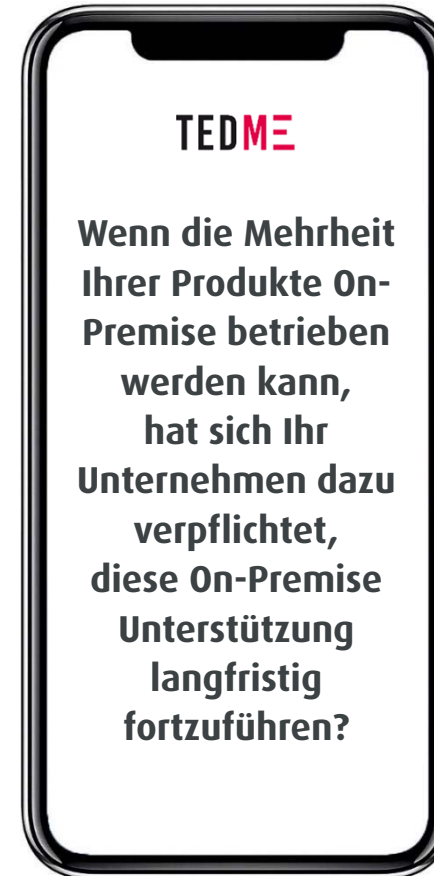


Umfrage per TedMe

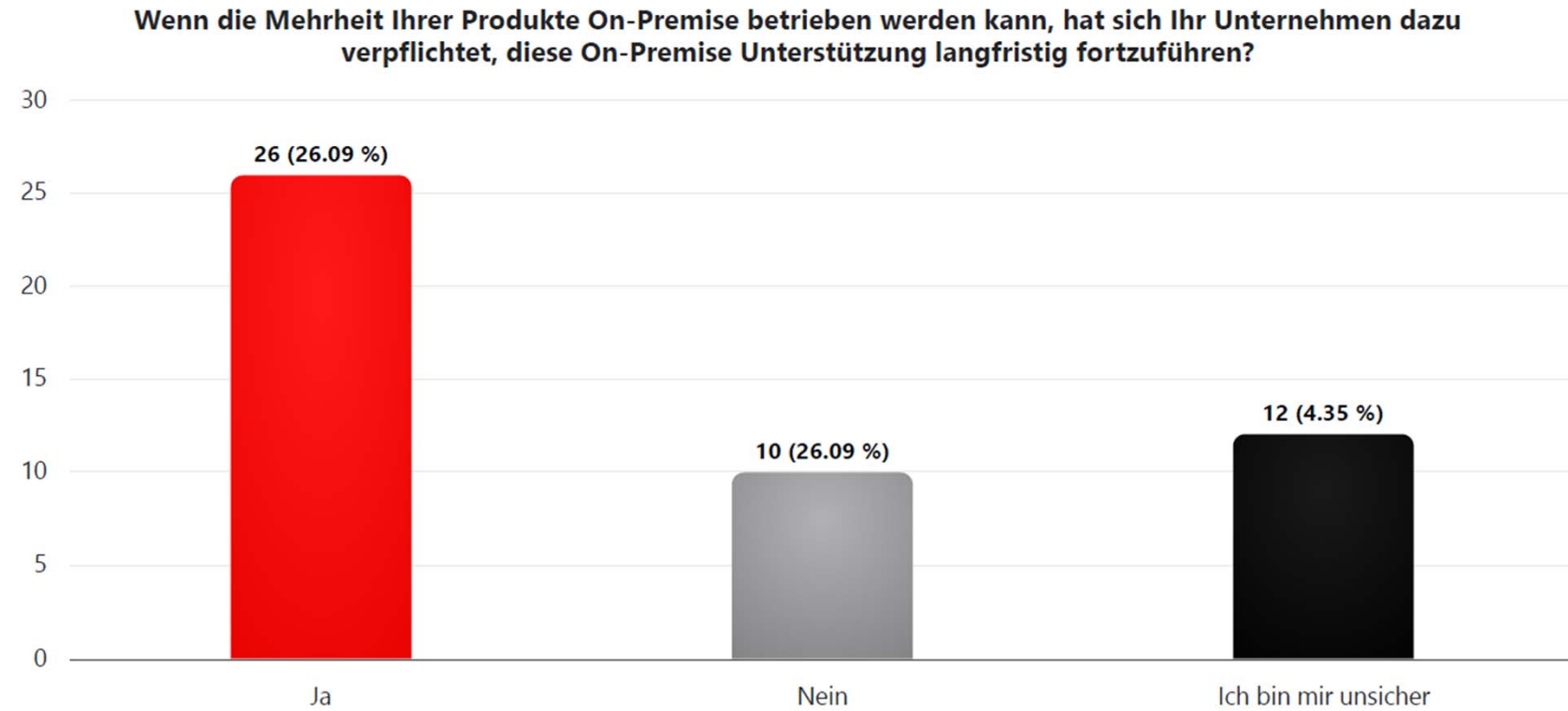
TEDME

Bitte öffnen Sie
www.tedme.com
und geben folgende
Raumnummer ein:
MD25

ODER scannen Sie diesen QR-Code
mit ihrem Mobiltelefon



Umfrage per TedMe - Ergebnis

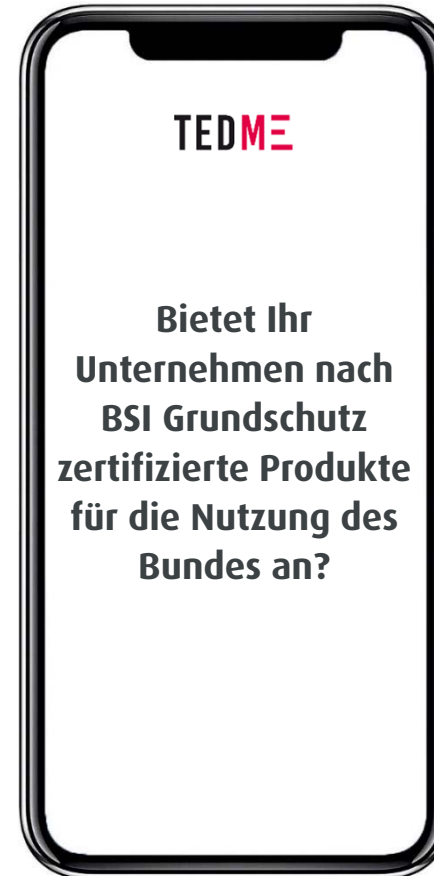


Umfrage per TedMe

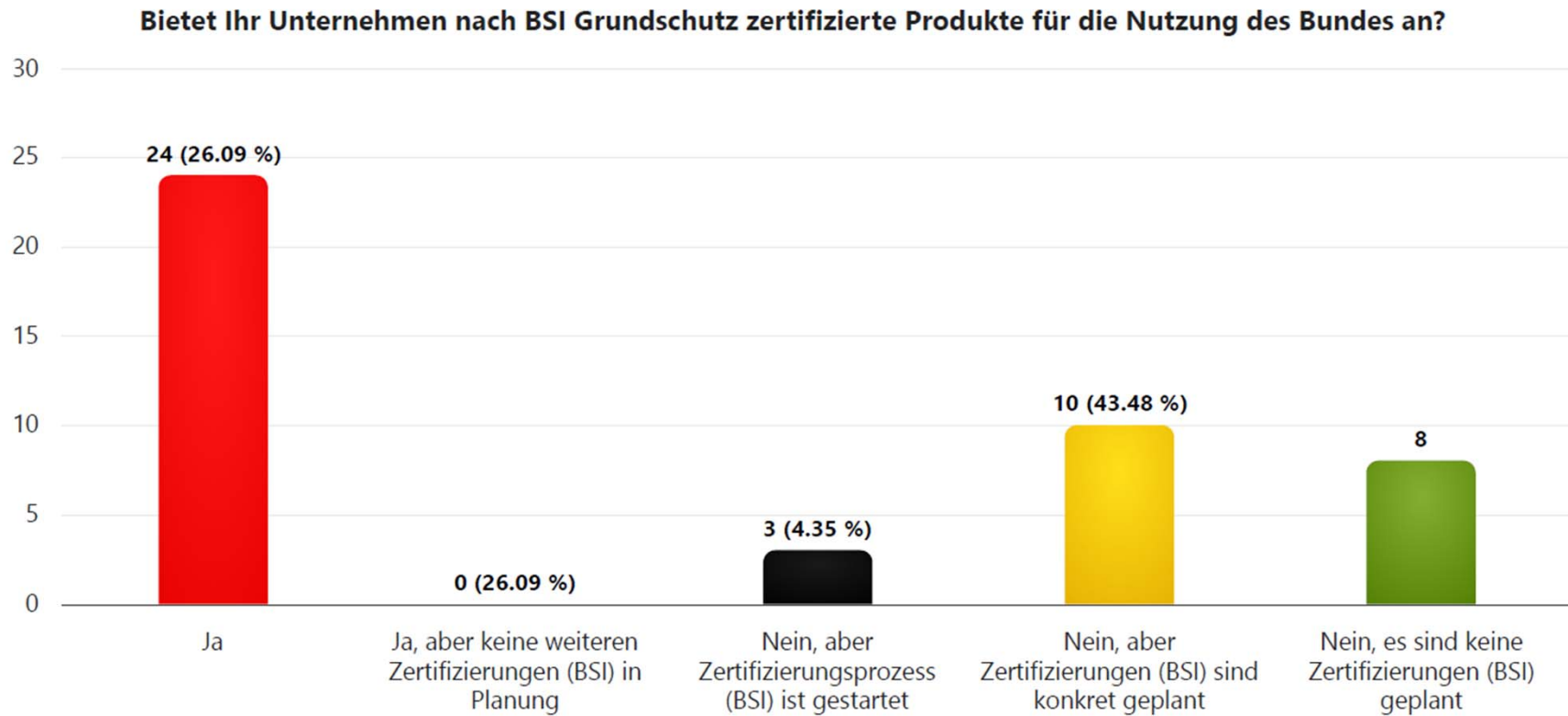
TEDME

Bitte öffnen Sie
www.tedme.com
und geben folgende
Raumnummer ein:
MD25

ODER scannen Sie diesen QR-Code
mit ihrem Mobiltelefon



Umfrage per TedMe - Ergebnis

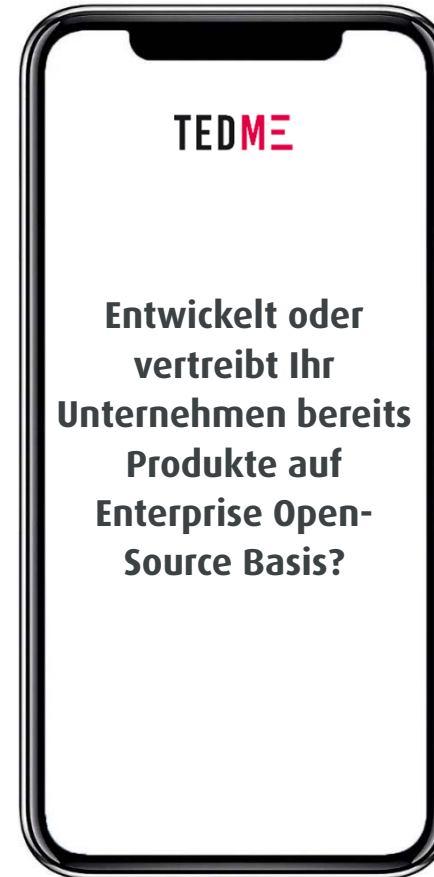


Umfrage per TedMe

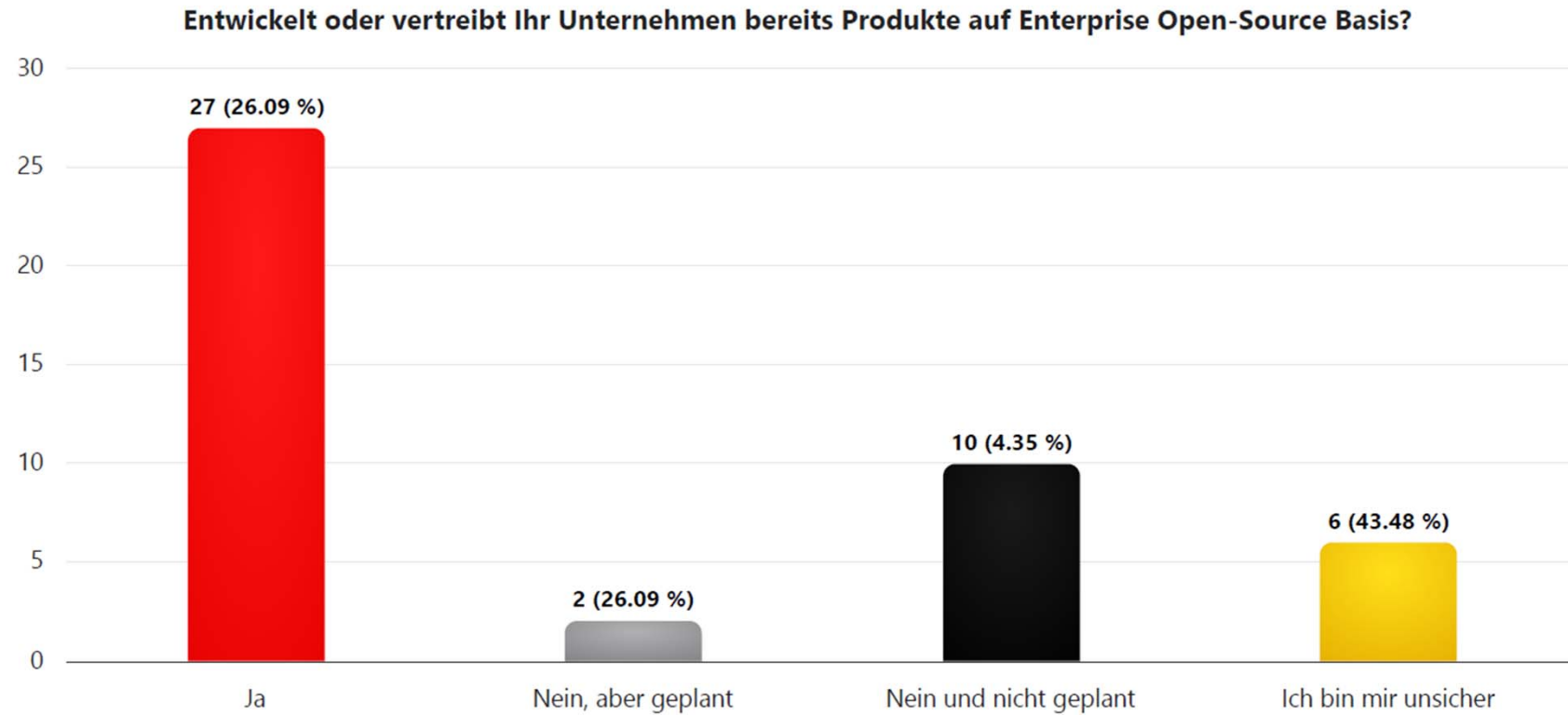
TEDME

Bitte öffnen Sie
www.tedme.com
und geben folgende
Raumnummer ein:
MD25

ODER scannen Sie diesen QR-Code
mit ihrem Mobiltelefon



Umfrage per TedMe - Ergebnis



Umfrage per TedMe

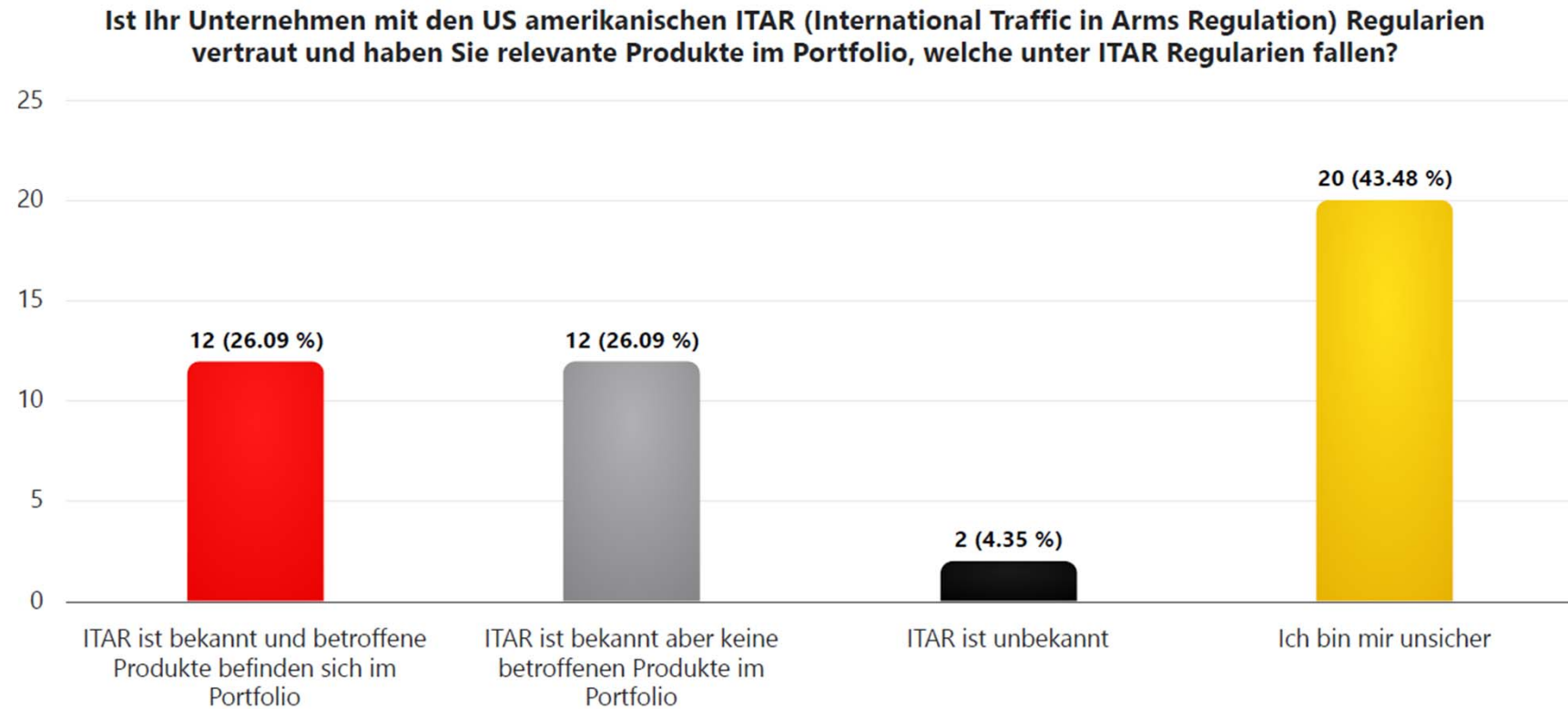
TEDME

Bitte öffnen Sie
www.tedme.com
und geben folgende
Raumnummer ein:
MD25

ODER scannen Sie diesen QR-Code
mit ihrem Mobiltelefon



Umfrage per TedMe - Ergebnis



Agenda

01

Begrüßung und Informationen

02

Cyber Security & Zero Trust –
Die Zukunft der Cyber-Security

03

Fragerunde und Dialog mit den BWI Experten

04

Ausblick & Verabschiedung

03 Fragerunde mit den Experten – Dialog zwischen der BWI und dem Markt



Umfrage per TedMe

TEDME

Bitte öffnen Sie
www.tedme.com
und geben folgende
Raumnummer ein:
MD25

ODER scannen Sie diesen QR-Code
mit ihrem Mobiltelefon



Umfrage per TedMe - Ergebnis

Was hat Ihnen am Marktdialog@BWI zum Thema "Cyber Security & Zero Trust" gut gefallen?

Informativ und Transparent Präsentatoren Mehr und genauer auf die Produkte die Zero Trust haben sollen eingehen
Security Prozess Wertigkeit sehr grob OFFENHEIT Intensiver Austausch
Sehr guter Mix Erläuterung technischer Themen + Diskussion dazu + Sensibilisierung für wichtige Features
Sinnvolle Weiterentwicklung der Sicherheit Klare Aussagen, kein Geschwurbel
Oberflächlichkeit Know-How der Vortragenden Präsentationsform
Wenig Tiefgang Kompetenz **Informativ** Q&A ist sinnvoll sehr oberflächlich
Der Grobüberblick zu Zero Trust Detailtiefe des Vortrages Status Details Einblicke
angenehme technische Tiefe Perspektiven für die Marktteilnehmer Austausch
Mehr Sicherheit für die Bundeswehr Ein konkretes Thema mit Tiefgang, gut
Transparenz von Status und Zielbild Sehr informativ. Ich weiß jetzt wo die Reise hier in der nächsten Zeit hingeht.
Klare Anforderungen unverbindlich Gute Information Sehr informativ und transparent
Gute Darstellung und klare Kommunikation der Anforderungen.

Umfrage per TedMe

TEDME

Bitte öffnen Sie
www.tedme.com
und geben folgende
Raumnummer ein:

MD25

ODER scannen Sie diesen QR-Code
mit ihrem Mobiltelefon



Umfrage per TedMe - Ergebnis

Was können wir beim nächsten Marktdialog@BWI besser machen?

Ausblick für die nächsten Schritte Ausblick der Zusammenarbeit mit Industrie

Bezugnahme auf Umsetzbarkeit im lfd Geschäftsjahr

Ich wünsche mir die Präsentation ;-)

Die überlegene Sicherheit der Public Cloud im Vergleich zu On-Premises-Lösungen wurde nicht thematisiert – ein wichtiger Vorteil, der noch hervorgehoben werden könnte.

Den linken Kollegen austauschen , der rechte war gehaltvoller

Benennung von Zeiträumen Folien parallel zum Video zeigen

Roadmap Zerotrust Der rechte Herr muss das nächste mal mehr Redezeit bekommen

zeitliche Relevanz des besprochenen Themas für mögliche Beschaffungen

Agenda

01

Begrüßung und Informationen

02

Cyber Security & Zero Trust –
Die Zukunft der Cyber-Security

03

Fragerunde und Dialog mit den BWI Experten

04

Ausblick & Verabschiedung

04 Ausblick auf kommende Informationsveranstaltungen

BWI Industry Days

02./03. September 2025
Berlin
KOSMOS

Marktdialog@BWI

Themenvorschläge für den
Marktdialog@BWI sind
willkommen

Wir freuen uns über
Ihre Anregungen!



Feedback

Feedback via E-Mail
an das Funktionspostfach
bwi.fp.marktdialog@bwi.de





Danke für Ihr Interesse & bis zum nächsten Marktdialog@BWI!

Die gezeigte Präsentation, Ihre Fragen und unsere Antworten sowie den Link zu der Vergabe-Plattform finden Sie in kurzer Zeit unter <https://www.bwi.de/partner-oekosystem>.

Marktdialog@BWI – V 2.2 – BWI frei verwendbar – Eine Weitergabe an Auftraggeber ist erlaubt

Bildquelle: BWI/Herdieckerhoff