Zero Trust
Wie sieht die Umsetzung in der chemisch-pharmazeutischen Industrie aus?

22.10.2026: 10:00 - 11:00
VCI und PwC Webinar-Serie

Ausblick auf die PwC Webinar-Serie mit IT-Security Impulsen für die chemisch-pharmazeutische Industrie



Webinar Teil 1

„KI Security – welche Maßnahmen sollten heute umgesetzt werden, um KI-Bedrohungen zu antizipieren?“

KI-Lösungen wie das Anthropic Modell „Mythos“ reduzieren die Zeit in den Schwachstellen ausgenutzt werden können von Tagen zu Stunden.

Gleichzeitig nimmt die Nutzung von KI in Unternehmen massiv zu, was neue Security-Herausforderungen erzeugt. Lernen Sie in unserem Webinar, was Sie heute angehen, sollten.

17.09.26: 10.00 – 11.00 Uhr



Webinar Teil 2

„Zero Trust: Wie sieht die Umsetzung in der chemisch-pharmazeutischen Industrie aus?“

Zero Trust ist mehr als ein Schlagwort, es beschreibt einen grundlegenden Paradigmenwechsel in der IT-Sicherheit.

Dieser Kurzvortrag erklärt die Funktionsweise der Zero Trust Architektur und ordnet sie in den Kontext der chemischen Industrie ein:

Welche spezifischen Herausforderungen gibt es, und wie gelingt eine praxisnahe Umsetzung?

22.10.26: 10.00 – 11.00 Uhr



Webinar Teil 3

„OT Security: Welche OT-Bedrohungen existieren für die chemisch-pharmazeutische Industrie?“

Industrielle Steuerungssysteme und Produktionsumgebungen stehen zunehmend im Fokus von Cyberangriffen.

Wir beleuchten die Besonderheiten der OT-Security, analysieren aktuelle Bedrohungsszenarien für die chemisch-pharmazeutische Industrie und stellen bewährte Ansätze zur technischen Absicherung vor.

19.11.26: 10.00 – 11.00 Uhr

Heute für Sie im Termin



Jan-Hinrich Schierhölter
Senior Associate
Zero Trust

Frankfurt am Main
+49 69 95855555
jan-hinrich.schierhoelter@pwc.com

- B.Sc. Wirtschaftsinformatik, Universität Mannheim
- Certified Information Security Manager (CISM)
- ISO/IEC 27001 Implementer
- BSI BCM Praktiker
- Unternehmensberater für Cyber Security & Resilience
    - Zero Trust Architekturen, Security Transformationen
    - IT Service Continuity und (Cyber-) Desaster Recovery

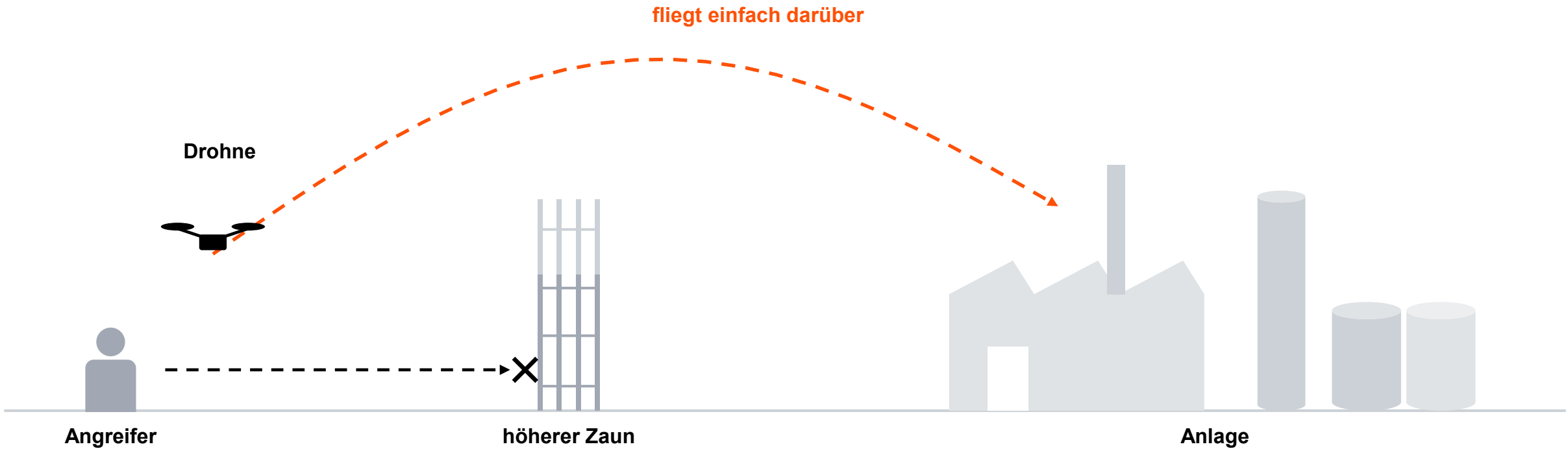
Agenda

1. Warum ein neues Sicherheitsverständnis nötig ist
2. Zero Trust als neues Vertrauensmodell
3. Anwendungsbeispiel Fernwartung
4. Wo Sie heute anfangen können
5. Fragen & Diskussion

1

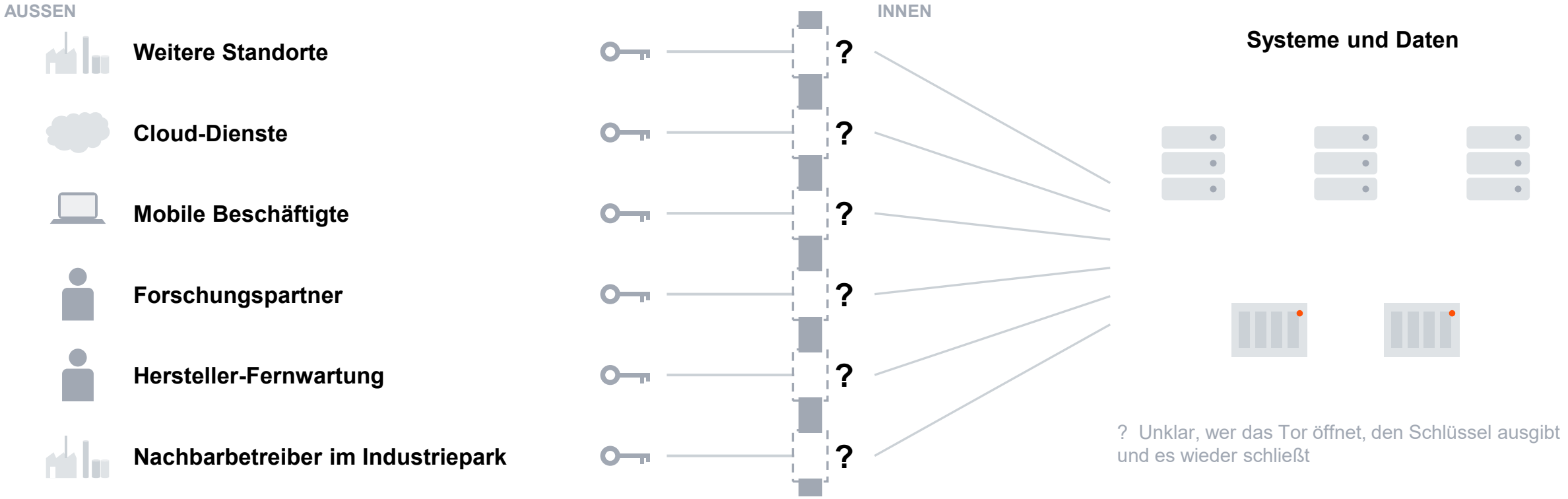
Warum ein neues Sicherheitsverständnis nötig ist

Höhere Zäune schützen nicht vor Drohnen: Mehr vom Gleichen reicht nicht



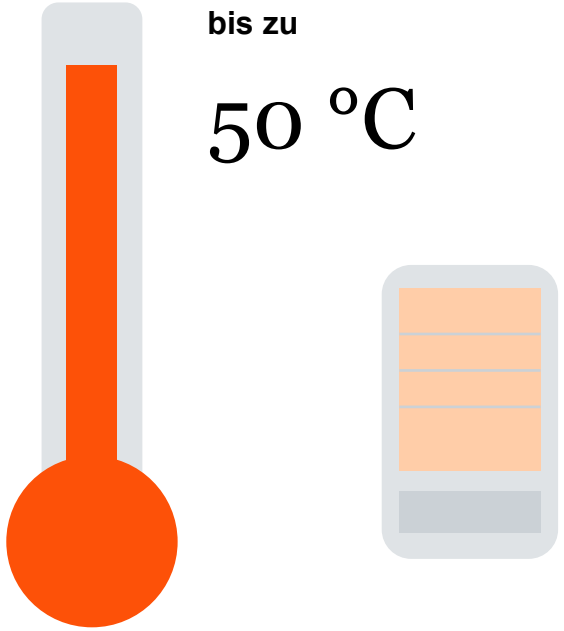
> Der Zaun bleibt richtig. Gegen den neuen Angriffsweg hilft er nicht, auch nicht, wenn er höher wird.

Digital hat unser Zaun längst viele Tore, und viele Beteiligte haben einen Schlüssel



> Jedes Tor ist gewollt. Offen ist oft nur, wer dafür zuständig ist.

Angriffe finden statt: Im Oktober 2026 heizte die Kühlung in Hunderten Supermärkten auf bis zu 50 °C



bis zu

50 °C

Gezielt geht es auch: Stuxnet (2010) manipulierte Steuerungen einer Urananreicherung.

OKTOBER 2026 · FRANKREICH · HUNDERTE SUPERMÄRKTE

Steuerung am Internet

Ältere Kühlsteuerungen mehrerer Hersteller direkt am Internet

Aus der Ferne verändert

Abtau- und Temperatureinstellungen über Nacht umgestellt

Ware vernichtet

Schäden in Millionenhöhe, vereinzelt Brände

WARUM ES FUNKTIONIERT HAT

Am Internet

Verwaltungsoberflächen direkt erreichbar, auch nach dem Angriff noch rund 2.700

Ohne Updates

Ältere Modelle bekommen seit Jahren keine Sicherheitsupdates mehr

Unklare Zuständigkeit

Zwischen Hersteller, Dienstleister und Betreiber

Quellen: CERT-FR (CERTFR-2026-ALE-012), Herstellerangaben, Claroty, Presse; Stand 21.10.2026

> Was würde bei Ihnen passieren, wenn die Kühlung plötzlich heizt?

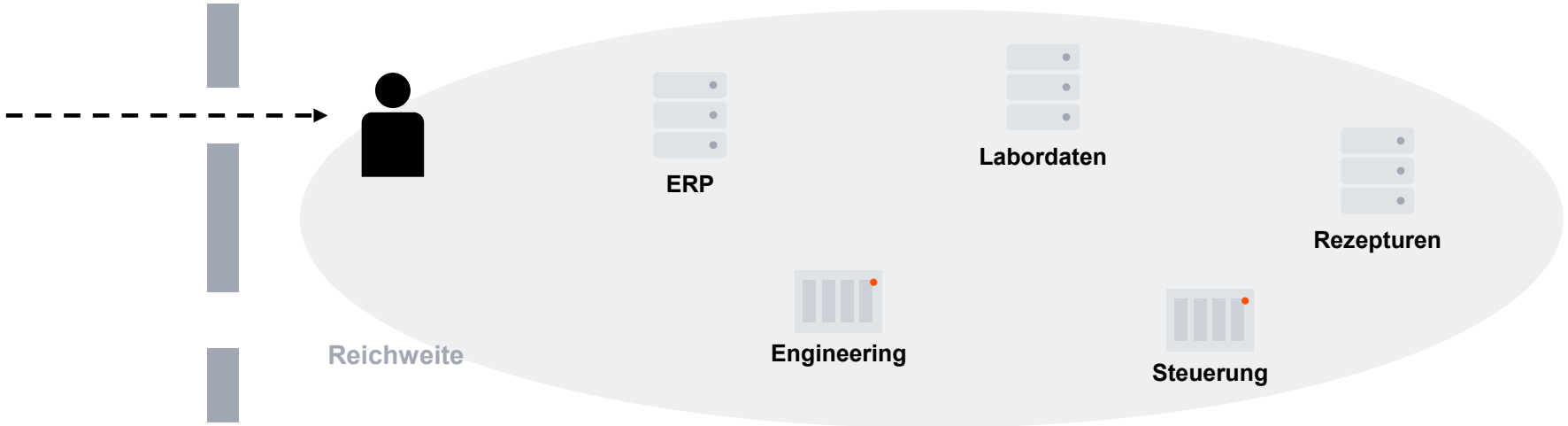
Wir können nicht jeden Einbruch verhindern: Entscheidend ist, wie weit ein Angreifer danach kommt

21. OKTOBER 2026 · WELTWEIT

Quellen: BSI, PHP-Projekt, Fachpresse (21.10.2026)

PHP2Shell: Notfall-Patches für kritische Lücken in PHP, der Grundlage vieler Webanwendungen

- **Aus der Ferne ausnutzbar, ohne Anmeldung**
- **Schweregrad 9,2 von 10**
- **Laut Entdecker mithilfe von KI gefunden**
- **Patch am selben Tag, Berichte über erste Angriffe**



FRAGE AN SIE

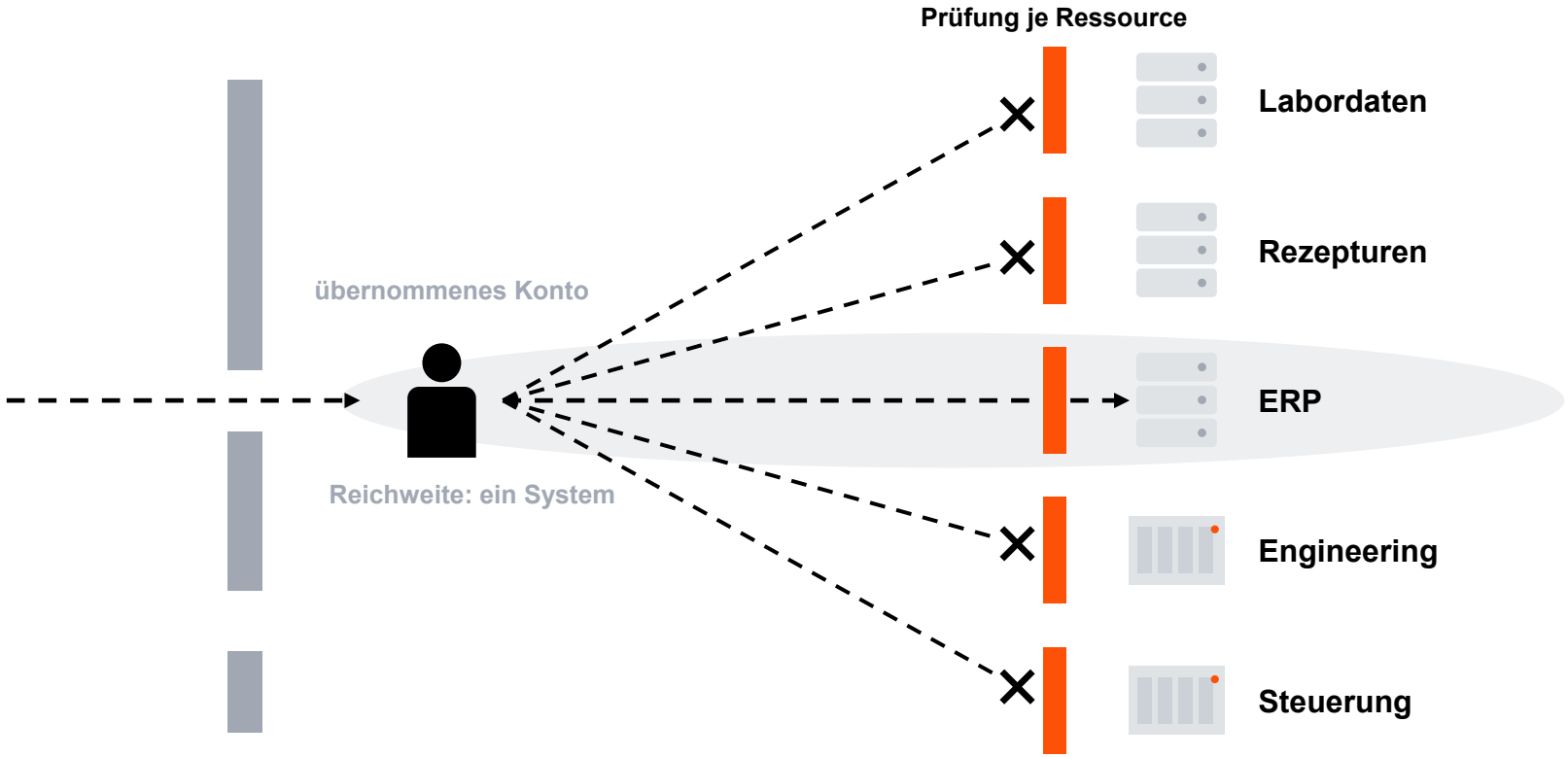
Wer hat PHP2Shell schon überall geschlossen und ist sicher, dass keine Instanz übersehen wurde und es nirgends schon zu spät war?

> Wie weit kommt ein Angreifer nach dem ersten Zugriff?

2

Zero Trust als neues Vertrauensmodell

Zero Trust heißt: Vertrauen wird nicht vorausgesetzt, sondern für jeden Zugriff begründet und begrenzt



Explizit prüfen
Verify explicitly

Jeder Zugriff wird einzeln entschieden, anhand von Identität, Gerät, Bedarf und Risiko.

Minimal berechtigen
Least privilege

Das Konto erreicht nur, wofür es berechtigt ist, und nur so lange wie nötig.

Kompromittierung einkalkulieren
Assume breach

So gebaut, dass ein übernommenes Konto nicht automatisch weitere Systeme öffnet.

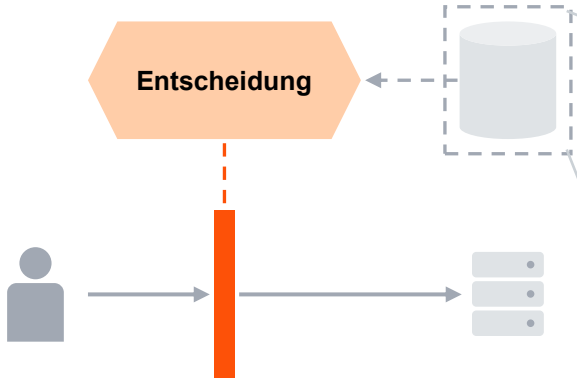
Wir misstrauen nicht unseren Mitarbeitenden, sondern ungeprüften digitalen Nachweisen.

Vor jedem Zugriff auf eine Ressource steht eine Prüfung, die anhand des Kontexts entscheidet und weiterläuft

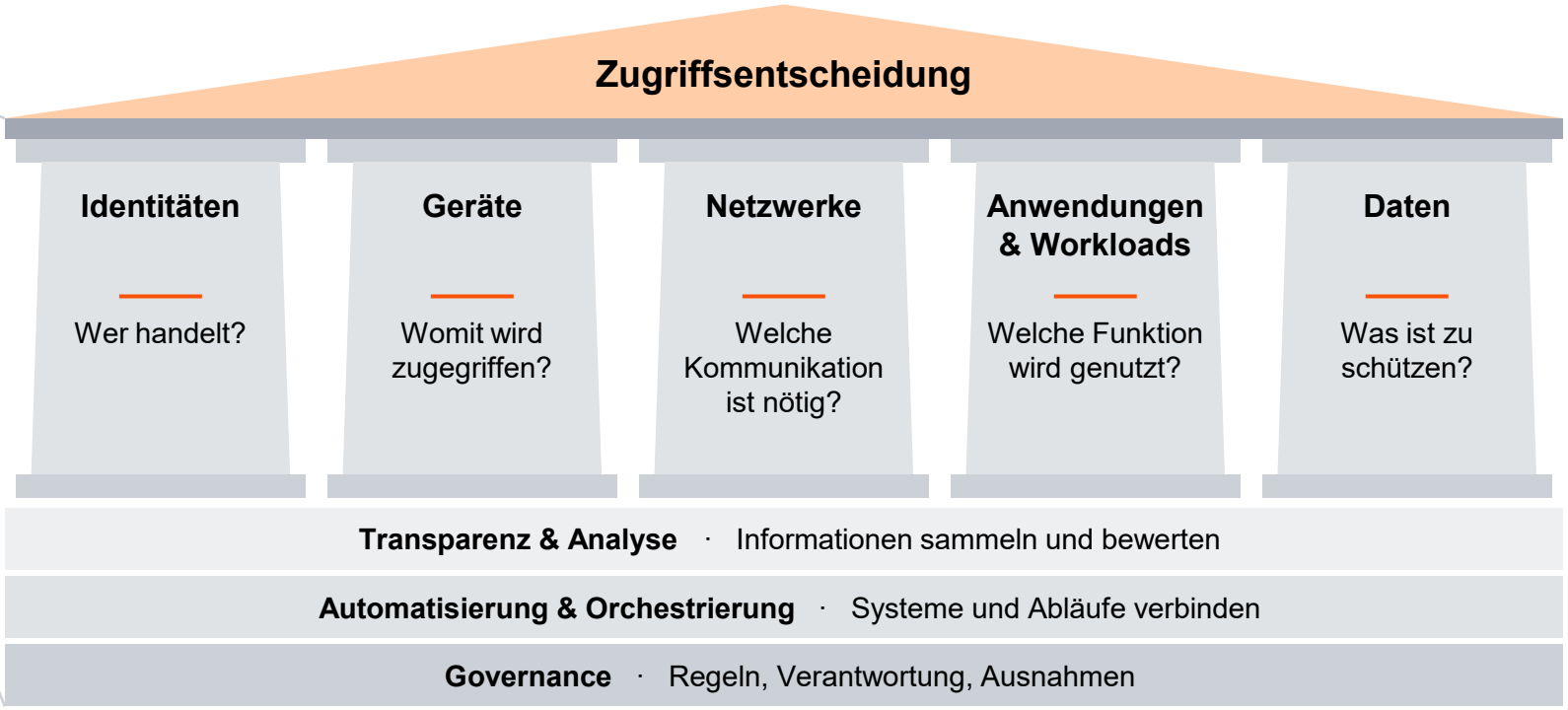


Entschieden wird nicht einmal am Eingang, sondern bei jedem Zugriff, und fortlaufend.

Die Prüfung ist nur so gut wie die Informationen, die sie aus fünf Bereichen bekommt



Auf welchen Informationen beruht die Zugriffsentscheidung?



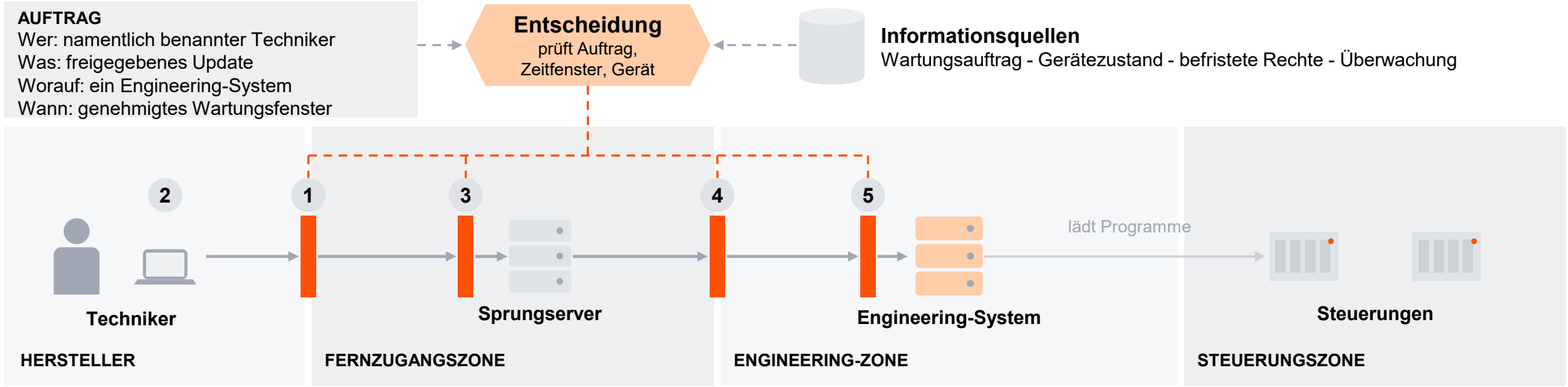
Nach CISA ZTMM 2.0

Erst wenn die fünf Säulen zusammenspielen, entsteht eine wirksame Zugriffsentscheidung.

3

Anwendungsbeispiel Fernwartung

Der Techniker erhält genau den Zugriff, den sein Auftrag erfordert



1 **Fernzugang**
Phishing-resistente MFA, nur mit freigegebenem Auftrag

2 **Gerät**
Laptop kommt nie ins Netz, nur eine Bildschirmsitzung

3 **Sprungserver**
Rechte nur im Wartungsfenster, Sitzung aufgezeichnet

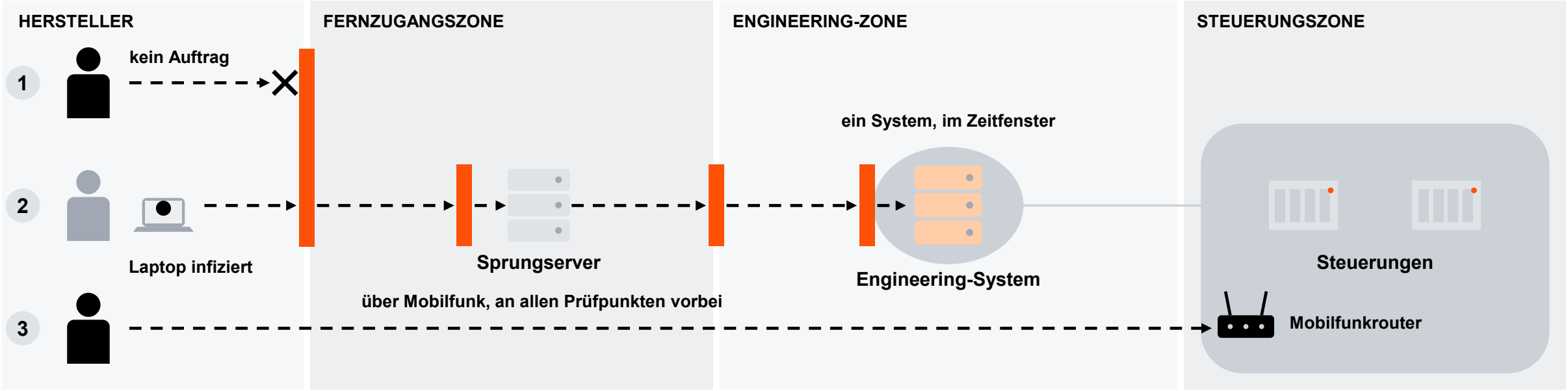
4 **Zonenübergang**
Nur das Engineering-System, nur nötige Protokolle

5 **Engineering-System**
Rolle passend zur Aufgabe, Änderung mit Freigabe

> Ein schmaler Weg zu genau einem System, und nur so lange, wie der Auftrag dauert.

Wird sein Konto übernommen, bleibt der Angreifer auf ein System beschränkt, solange es keinen zweiten Weg gibt

Zum Vergleich: Ein dauerhaftes Herstellerkonto ohne Zeitgrenze reicht bis in die Steuerungen.



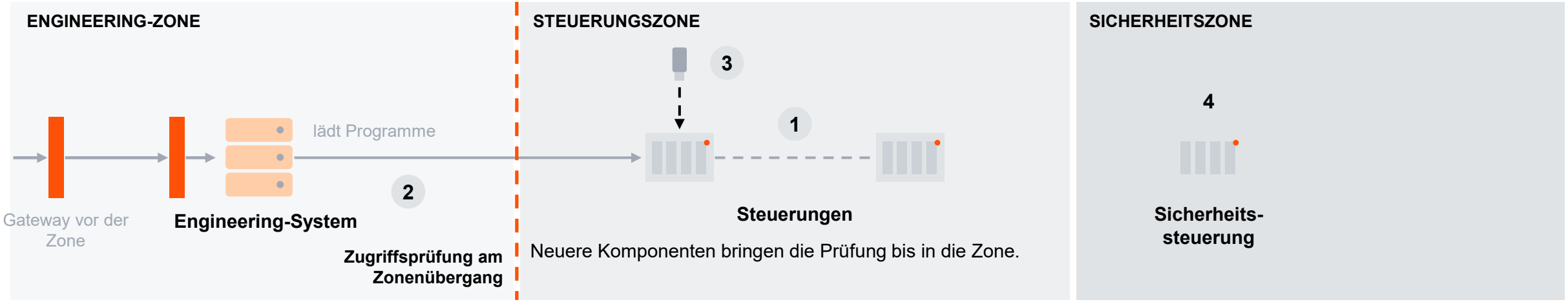
1 **Passwort gestohlen, kein Auftrag**
Reichweite: keine

2 **Laptop während der Wartung infiziert**
Reichweite: ein System, ein Zeitfenster

3 **Mobilfunkrouter im Schaltschrank**
Reichweite: die ganze Steuerungszone

Am gefährlichsten ist oft ein Zugang, den niemand kennt: Erst alle Wege erfassen, dann den Haupteingang verbessern.

In der Produktion kontrolliert Zero Trust die Zugänge, OT-Sicherheit schützt dahinter



1 **Innerhalb der Zone**
Kommunikation zwischen Steuerungen segmentieren und überwachen.

2 **Änderungen**
Programmänderungen freigeben, vergleichen und nachvollziehen.

3 **Datenträger**
Datenträger über Schleusen prüfen, denn sie umgehen das Netz.

4 **Sicherheitssteuerungen**
Abschalten funktioniert immer, unabhängig von Netz und Online-Prüfung.

VERTIEFUNG IM NÄCHSTEN WEBCAST: 19. November · OT-Sicherheit, Bedrohungen in der Produktion, Showcase

> Zero Trust kontrolliert, wer in die Produktion kommt. OT-Sicherheit schützt, was dahinter passiert.

4

Wo Sie heute anfangen können

Der erste Schritt braucht kein Projekt: Spielen Sie durch, wie weit ein Angreifer bei Ihnen käme



1 Einstieg wählen

Ein übernommenes Konto, ein Dienstleisterzugang oder ein Gerät.

2 Alle Wege erfassen

Auch Mobilfunkrouter, alte VPNs und Datenträger, nicht nur den Haupteingang.

3 Rechte und Zonen verfolgen

Welche Systeme sind erreichbar, mit welchen Rechten und wie lange?

4 Markieren, wo etwas aufhält

Und wo nicht: Diese Stellen sind Ihre Prioritäten.

WER DABEI SEIN MUSS

IT-Sicherheit
kennt Konten und Zugänge

OT und Produktion
kennt Anlage und Zonen

Dienstleistersteuerung
kennt Verträge und Fernzugänge

> Wo nichts den Angreifer aufhält, beginnt Ihre Roadmap.

Ein strukturiertes Vorgehen führt vom Startpunkt zur priorisierten Roadmap

VORGEHEN IN PROJEKTEN

1 Startpunkt bestimmen

Kritische Prozesse und Zugänge erfassen (Rapid Discovery)



z. B. der Reichweitencheck

2 Ist-Stand bewerten

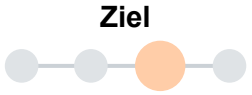
Reifegrad je CISA-Säule, einschließlich Zusammenspiel



Traditional → Optimal

3 Ziel-Reifegrad festlegen

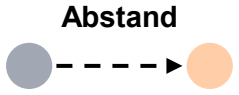
Risikobasiert je Säule, nicht überall Optimal



Traditional → Optimal

4 Lücken und größte Risiken

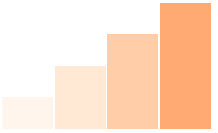
Wo ist der Abstand groß und das Risiko hoch?



größte Risiken zuerst

5 Maßnahmen festlegen

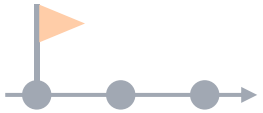
Riskanteste Zugänge zuerst, dann Vorhandenes nutzen



Details auf der nächsten Folie

6 Roadmap aufsetzen

Priorisiert nach Risiko und Aufwand, Pilot zuerst

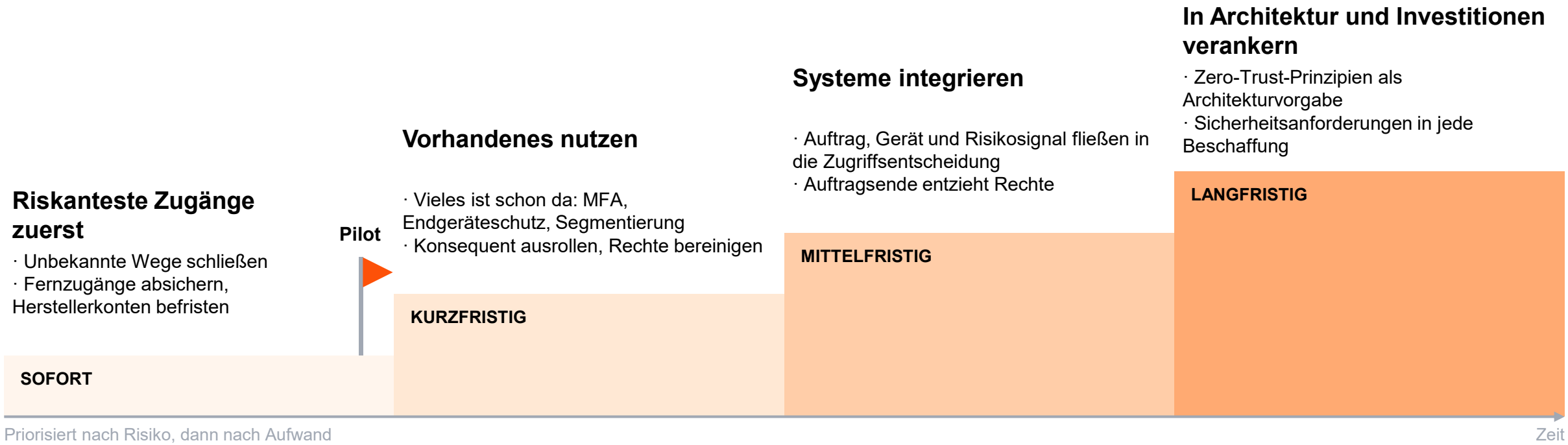


Pilot zuerst, dann ausrollen

umsetzen, Wirkung prüfen, nachsteuern

> Entscheidend ist nicht der Reifegrad an sich, sondern ob ein Angreifer nachweisbar weniger weit kommt.

Maßnahmen beginnen bei den riskantesten Zugängen und münden in Architektur- und Investitionsentscheidungen



> Zero Trust ist kein Tool und morgen nicht fertig: Es gehört in jede Architektur- und Investitionsentscheidung.

Der Perimeter bleibt notwendig, aber Sicherheit darf nicht davon abhängen, dass niemand ihn überwindet



DREI FRAGEN FÜR IHR UNTERNEHMEN

1 Wie weit käme ein Angreifer bei uns mit einem gestohlenen Dienstleisterkonto?

2 Welche Wege in unsere Anlagen kennen wir noch nicht?

3 Welchen kritischen Zugriff sichern wir als Erstes vollständig ab?



Fragen & Diskussion



Q&A

Wir laden Sie ein zum Dialog!

Ausblick auf die PwC Webinar-Serie mit IT-Security Impulsen für die chemisch-pharmazeutische Industrie



Webinar Teil 1

„KI Security – welche Maßnahmen sollten heute umgesetzt werden, um KI-Bedrohungen zu antizipieren?“

KI-Lösungen wie das Anthropic Modell „Mythos“ reduzieren die Zeit in den Schwachstellen ausgenutzt werden können von Tagen zu Stunden.

Gleichzeitig nimmt die Nutzung von KI in Unternehmen massiv zu, was neue Security-Herausforderungen erzeugt. Lernen Sie in unserem Webinar, was Sie heute angehen, sollten.

17.09.26: 10.00 – 11.00 Uhr



Webinar Teil 2

„Zero Trust: Wie sieht die Umsetzung in der chemisch-pharmazeutischen Industrie aus?“

Zero Trust ist mehr als ein Schlagwort, es beschreibt einen grundlegenden Paradigmenwechsel in der IT-Sicherheit.

Dieser Kurzvortrag erklärt die Funktionsweise der Zero Trust Architektur und ordnet sie in den Kontext der chemischen Industrie ein:

Welche spezifischen Herausforderungen gibt es, und wie gelingt eine praxisnahe Umsetzung?

22.10.26: 10.00 – 11.00 Uhr



Webinar Teil 3

„OT Security: Welche OT-Bedrohungen existieren für die chemisch-pharmazeutische Industrie?“

Industrielle Steuerungssysteme und Produktionsumgebungen stehen zunehmend im Fokus von Cyberangriffen.

Wir beleuchten die Besonderheiten der OT-Security, analysieren aktuelle Bedrohungsszenarien für die chemisch-pharmazeutische Industrie und stellen bewährte Ansätze zur technischen Absicherung vor.

19.11.26: 10.00 – 11.00 Uhr

Vielen Dank für Ihre Aufmerksamkeit.

© 2026 PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft. Alle Rechte vorbehalten. „PwC“ bezeichnet in diesem Dokument die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, die eine Mitgliedsgesellschaft der PricewaterhouseCoopers International Limited (PwCIL) ist. Jede der Mitgliedsgesellschaften der PwCIL ist eine rechtlich selbstständige Gesellschaft.

pwc.com