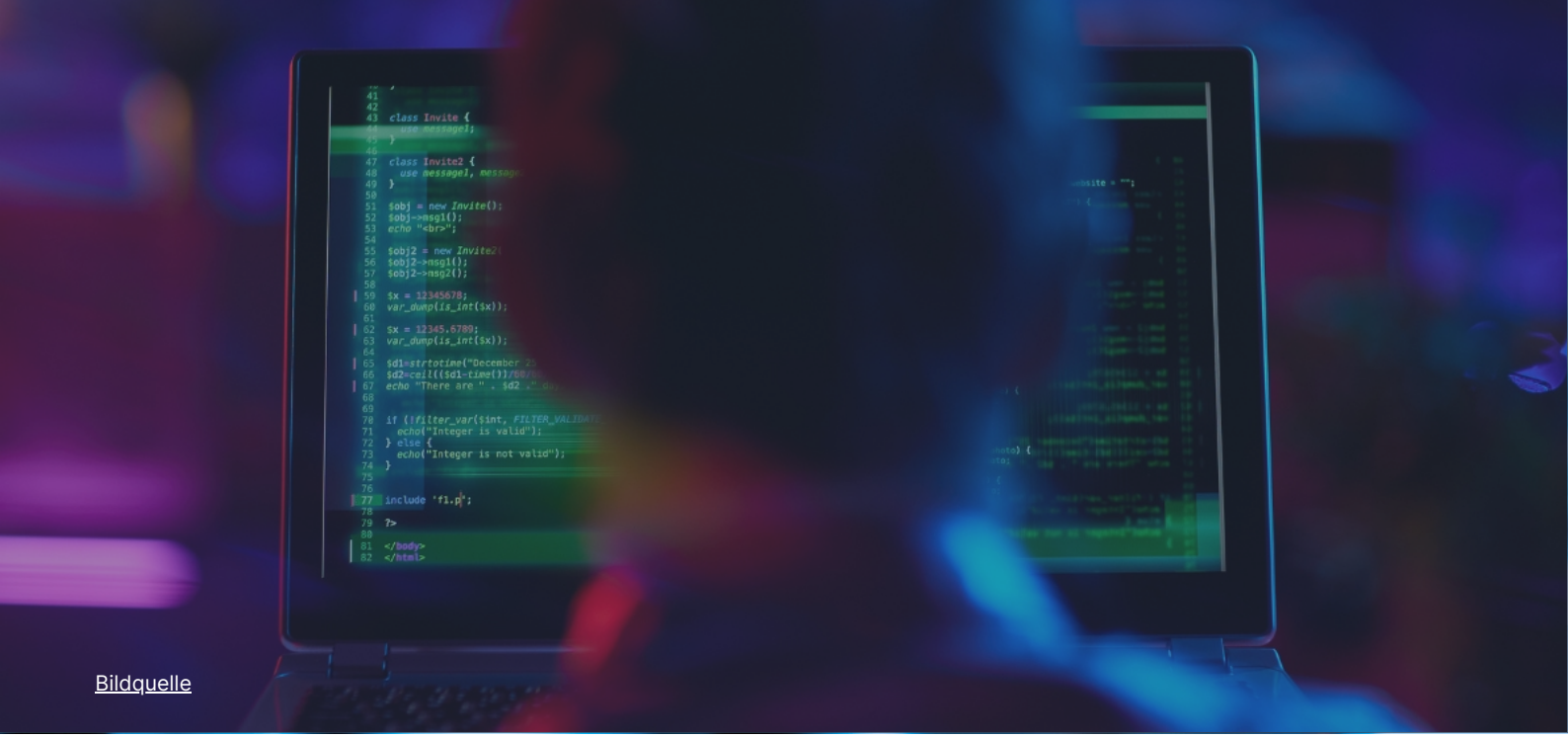
Timly

Cybersecurity Asset Management & Compliance

Register für weniger Risiken und sichere Audits

Bildquelle

Inhaltsverzeichnis



Bildquelle

Vorwort & Ziele des Reports

Wer nicht weiß, welche Assets er besitzt, kann sie nicht schützen. Genau das ist in vielen Unternehmen heute Realität: Inventare existieren, aber sie sind fragmentiert, veraltet oder ohne Sicherheitskontext.

Die Folge sind blinde Flecken in der Angriffsfläche, verzögerte Reaktionen bei Vorfällen und Compliance-Nachweise, die mühsam zusammengesucht werden müssen. Dieser Report zeigt, warum ein zentrales Asset-Register die operative Grundlage für wirksame Cybersecurity ist – und wie es sich in der Praxis aufbauen und betreiben lässt.

1.1 Warum Cybersecurity-Asset-Management jetzt ein Top-Thema ist

Die Angriffsfläche von Unternehmen wächst schneller als viele Sicherheits- und Betriebsmodelle mithalten können. Neben klassischen IT-Assets wie Laptops, Servern und Netzwerkkomponenten gehören heute auch Cloud-Ressourcen, SaaS-Anwendungen, Identitäten, externe Dienstleister, IoT-Komponenten und vernetzte OT-Systeme zur realen Sicherheitslandschaft eines Unternehmens.

Gerade in Branchen wie IT, Bau, Fertigung, Facility Management und technischen Services entstehen dadurch hochdynamische Umgebungen mit wechselnden Standorten, mobilen Geräten, temporärer Infrastruktur und gemischten Verantwortlichkeiten zwischen IT, Operations und Fachbereichen.

Das eigentliche Problem ist dabei selten nur fehlende Technologie. In vielen Unternehmen existieren bereits einzelne Inventare, CMDBs, Netzwerkscans, Cloud-Portale oder Endpoint-Tools. Doch die zentralen Fragen bleiben dennoch oft unbeantwortet: **Welche sicherheitsrelevanten Assets sind tatsächlich vorhanden, wem gehören sie, wie kritisch sind sie, und in welchem Sicherheitszustand befinden sie sich im Moment?**

Genau diese Lücke macht aus normalem Inventarmanagement ein wichtiges Cybersecurity-Thema. Die Relevanz ist messbar.

- Laut Verizons „Data Breach Investigations Report 2025" sind 46 Prozent der kompromittierten Systeme mit möglichen Unternehmens-Logins in einem untersuchten Datensatz **nicht in der zentralen Verwaltung des Unternehmens eingebunden.**[1]

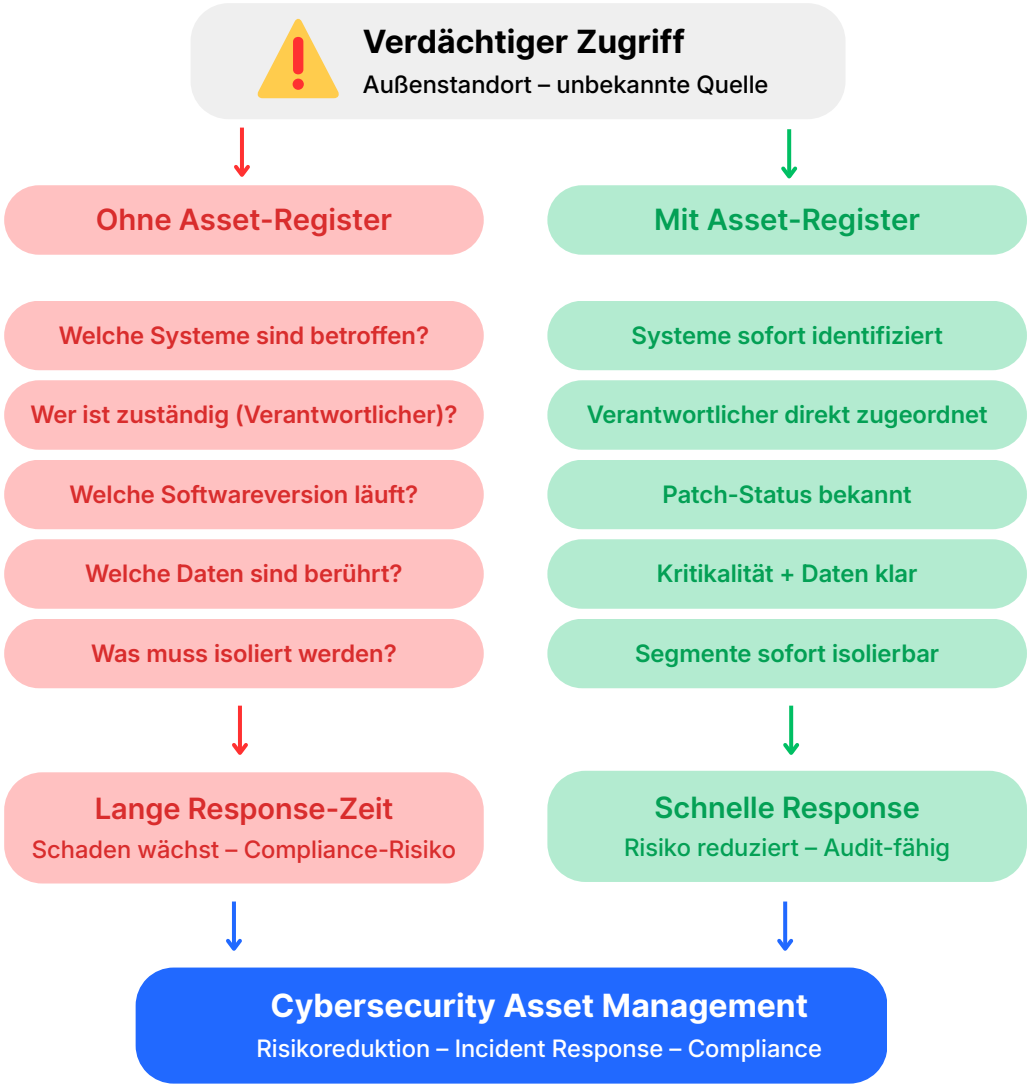
- IBMs „Cost of a Data Breach Report 2025" besagt zudem, dass 40 Prozent der untersuchten Datenpannen Daten in mehreren Umgebungen betreffen und diese Fälle mit durchschnittlich 283 Tagen besonders lange bis zur Identifikation und Eindämmung brauchen.[2]

Ein einfaches Szenario zeigt die Relevanz: Ein verdächtiger Zugriff – etwa über ein externes System oder ein nicht sauber inventarisiertes Cloud-Konto – macht sofort sichtbar, wie entscheidend Transparenz über alle Assets ist.

Ohne zentrale Asset-Sicht fehlen dem Incident-Response-Team klare Antworten auf Fragen wie: Welche Systeme sind betroffen, wer ist zuständig, welche Daten sind berührt und was muss isoliert werden? Das verzögert die Reaktion und erhöht das Risiko. Mit einem belastbaren Asset-Register lassen sich betroffene Systeme dagegen unmittelbar identifizieren, priorisieren und den Verantwortlichen zuordnen.

Die gegenüberstehende Darstellung verdeutlicht, wie Informationen zu Patch-Status, Kritikalität, Segmenten, Identitäten, Schnittstellen und Standorten zentral verfügbar werden – und damit eine schnelle, auditfähige Response ermöglichen.

Cybersecurity Asset Management wird so von einer Randdisziplin der Inventarisierung zu einer Voraussetzung für wirksame Risikoreduktion, handlungsfähige Incident Response und belastbare Compliance.



1.2 Für wen dieser Report ist

Dieser Report richtet sich an **Unternehmen, die ihre Sicherheits- und Compliance-Prozesse auf eine belastbare Asset-Basis** stellen möchten.

Vor allem für folgende Rollen ist dieser Report interessant:

- CISO und IT-Sicherheitsverantwortliche
- IT-Leitung und IT-Operations
- OT- und Produktionsverantwortliche
- Facility-Management-Leitung
- Compliance-, Risiko- und Audit-Verantwortliche
- interne Revision und Governance-Teams

Oft sind grundlegende Security-Standards und regulatorische Anforderungen bereits bekannt, beispielsweise ISO 27001, NIS2 oder branchenspezifische Vorgaben. **Häufig fehlt jedoch ein pragmatischer Ansatz, wie sich ein vollständiges und sicheres Asset-Inventar in der Praxis aufbauen und betreiben lässt.**

Genau hier setzt dieser Report an.

Er verbindet technische, organisatorische und prozessuale Perspektiven und zeigt, wie Unternehmen ein zentrales Asset-Register als Sicherheitsfundament etablieren können.

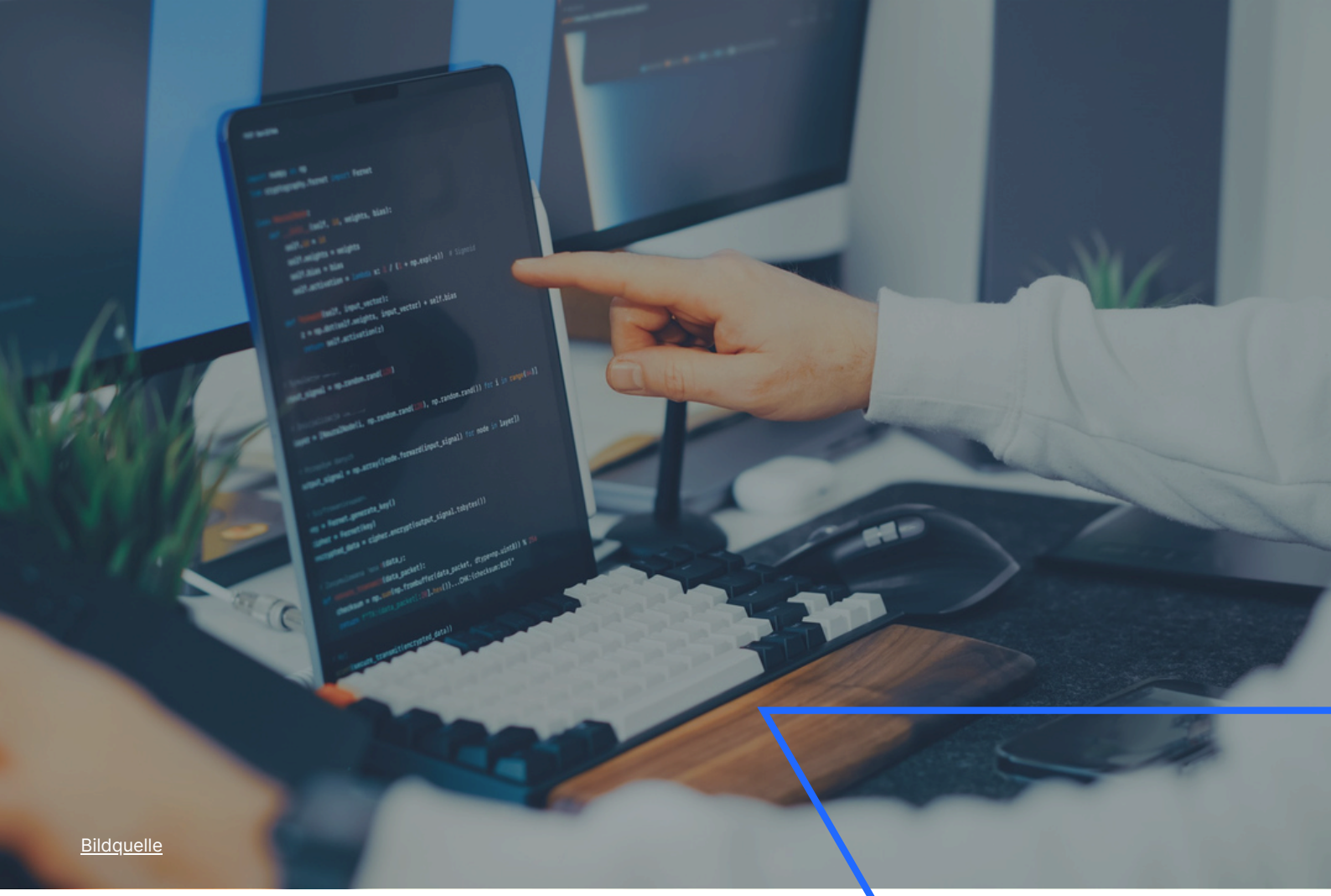
1.3 Ziele & Aufbau des Reports

Der Report zeigt, warum ein unvollständiges Asset-Inventar nicht nur ein Verwaltungsproblem ist, sondern ein direkter **Risikofaktor für Cybersecurity und Compliance.** Er zeigt, warum unbekannte Assets, fehlende Verantwortung und fragmentierte Bestandsdaten Patch-Prozesse, Incident-Response, Auditfähigkeit und Management-Reporting schwächen.

Darauf aufbauend erläutert der Report, welche **Anforderungen sich aus Normen und regulatorischen Rahmenwerken** an ein belastbares Asset-Register ergeben und bietet zusätzlich ein pragmatisches Zielbild für den Aufbau eines sicheren Asset-Registers: mit relevanten Asset-Klassen, Rollen und Verantwortlichkeiten, einem einfachen Reifegradmodell, zentralen Security-Prozessen und KPI-Beispielen.

Im weiteren Verlauf soll daraus ein 90-Tage-Blueprint ableitbar werden, mit dem Unternehmen ihren aktuellen Reifegrad einschätzen und konkrete Verbesserungen priorisieren können.

Bildquelle



Bildquelle

Was ist Cybersecurity Asset Management (CSAM)?

Begriffe & Scope

Was ist Cybersecurity Asset Management (CSAM)?
Begriffe & Scope

Bevor ein Asset-Register aufgebaut werden kann, braucht es ein klares Verständnis auf die Frage: Was genau fällt unter Cybersecurity Asset Management und was unterscheidet es vom klassischen IT Asset Management?

2.1 Definition & Abgrenzung

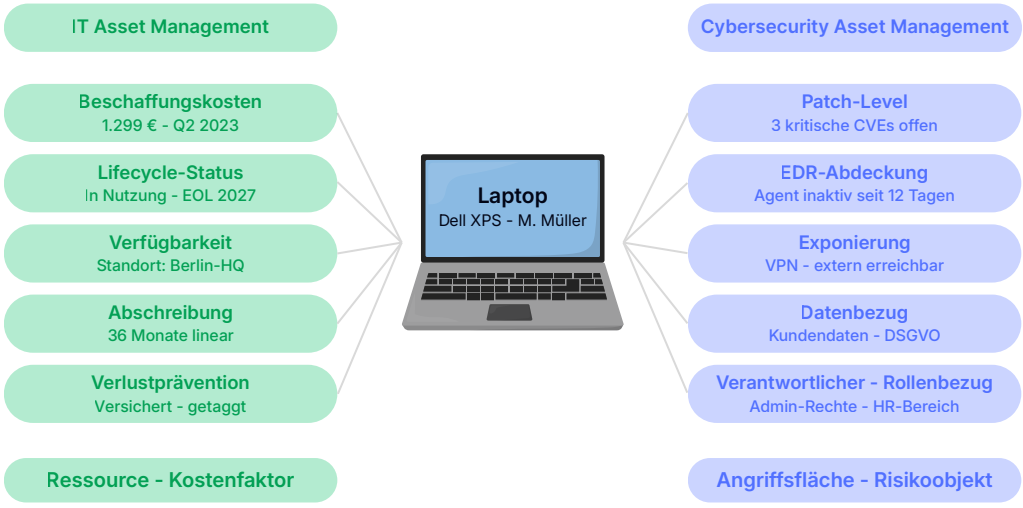
> Cybersecurity Asset Management ist der kontinuierliche Prozess, alle sicherheitsrelevanten Assets eines Unternehmens zu identifizieren, zu erfassen, zu klassifizieren, mit Verantwortlichkeiten zu versehen und mit Sicherheits- sowie Risikoinformationen zu verknüpfen.

Im Unterschied zum klassischen IT Asset Management steht dabei nicht der betriebliche oder kaufmännische Lifecycle im Vordergrund, sondern die Frage, welche Risiken, Abhängigkeiten und Angriffsflächen mit einem Asset verbunden sind.

Während ITAM Assets primär als Betriebs- oder Kostenobjekte betrachtet, erweitert CSAM diese Sicht um Security- und Compliance-Kontext – etwa Patch-Status, Exponierung, Kritikalität, Identitäten, Schwachstellen oder Verantwortlichkeiten.

Dadurch wird aus einem verwalteten Gerät ein steuerbares Sicherheitsobjekt.

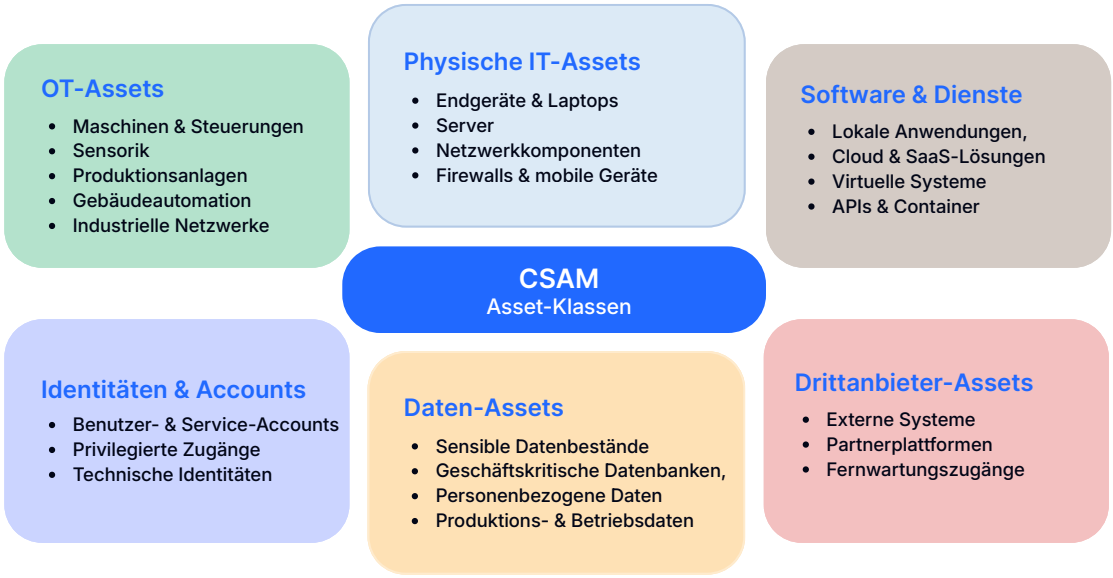
Die folgende Darstellung verdeutlicht diesen Perspektivwechsel anhand eines konkreten Beispiels: Während ein Laptop im ITAM-Kontext primär als verwaltetes Betriebsgerät betrachtet wird, steht im CSAM-Kontext dessen Sicherheits- und Risikoprofil im Mittelpunkt – etwa Verantwortlichkeit, Patch-Status, Exponierung oder vorhandene Security-Kontrollen.



2.2 Welche Asset-Klassen umfasst der Geltungsbereich?

Ein wirksames Cybersecurity Asset Management umfasst deutlich mehr als klassische Endgeräte oder Server. Grundsätzlich sollten alle Items erfasst werden, die Sicherheits-, Compliance- oder Betriebsrisiken verursachen können.

Typische Asset-Klassen im CSAM:



Entscheidend ist dabei nicht nur die reine Existenz eines Assets, sondern dessen Kontext:

- Kritikalität
- Verantwortlichkeit
- Sicherheitsstatus
- Abhängigkeiten
- und Compliance-Relevanz

Nur dadurch wird aus einer Inventarliste ein verlässliches Asset-Register.

2.3 Rollen & Verantwortlichkeiten im CSAM-Setup

Ein zentrales Asset-Register funktioniert nur dann zuverlässig, **wenn die entsprechenden Verantwortlichkeiten eindeutig definiert** sind. Jedes sicherheitsrelevante Asset und Objekt benötigt einen klaren Verantwortlichen – fachlich, technisch oder organisatorisch. Fehlt diese Zuordnung, bleibt die Pflege lückenhaft und Reaktionen auf Änderungen oder Incidents verzögern sich.

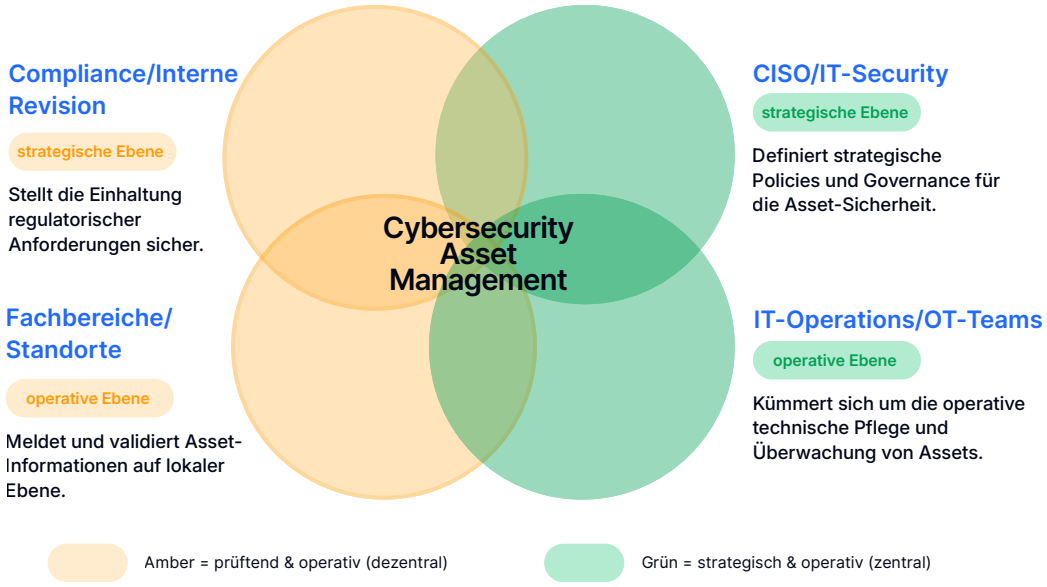
Ein wirksames Cybersecurity Asset Management verteilt Verantwortlichkeiten bewusst auf **strategische, operative und prüfende Ebenen**. Die folgende Abbildung zeigt ein typisches Rollenmodell, in dem diese Ebenen zusammenlaufen.

CSAM verbindet dabei die strategische Rolle von CISO und IT-Sicherheit mit den operativen Aufgaben der IT-/OT-Teams und Fachbereiche sowie der prüfenden Funktion von Compliance und interner Revision in einem gemeinsamen Modell.

Amber markiert dezentrale operative und prüfende Verantwortlichkeiten, Grün zentrale strategische und operative Verantwortlichkeiten.

Was ist Cybersecurity Asset Management (CSAM)?
Begriffe & Scope

Rollenmodell im Cybersecurity Asset Management
CSAM verbindet strategische, operative und prüfende Verantwortlichkeiten in einem gemeinsamen Modell.



2.4 Reifegradmodell für Cybersecurity Asset Management

Moderne Unternehmen befinden sich beim Bereich des Cybersecurity Asset Management in sehr unterschiedlichen Entwicklungsständen. Es lohnt sich deshalb, vor Implementierung von weiterer Software, zunächst einen Blick darauf zu werfen, in welchem Zustand sich die Firma aktuell befindet. **Ein einfaches Reifegradmodell hilft dabei, die eigene Ausgangslage realistisch einzuordnen.**

Level 1 – Fragmentiert
- Asset-Daten liegen in Excel-Dateien oder isolierten Tools
- Keine vollständige Übersicht über IT- und OT-Systeme
- Verantwortung ist unklar oder fehlt
- Daten sind häufig veraltet

Typische Frage:
„Können wir sicher sagen, welche Systeme tatsächlich existieren?“

Level 2 – Konsolidiert
- Erste zentrale Inventare oder CMDB-Strukturen existieren
- Teilweise automatisierte Erfassung
- Grundlegende Security-Daten werden integriert
- Dennoch bestehen Lücken und Medienbrüche

Typische Frage:
„Sind unsere Daten aktuell und vollständig genug für Security-Entscheidungen?“

Level 3 – Gesteuert
- Klare Prozesse und Verantwortlichkeiten sind definiert
- Security-KPIs werden aktiv überwacht
- Asset-Daten unterstützen Patch-, Risiko- und Incident-Prozesse
- Regelmäßige Qualitätskontrollen existieren

Typische Frage:
„Können wir betroffene Assets bei einem Incident innerhalb kurzer Zeit identifizieren?“

Level 4 – Integriert
- Asset-Management ist vollständig in Security- und Compliance-Prozesse eingebunden
- Hohe Datenqualität und kontinuierliche Aktualisierung
- Automatisierte Workflows und Governance-Prozesse
- Auditfähige Nachweise jederzeit verfügbar

Typische Frage:
„Nutzen wir Asset-Daten aktiv zur Steuerung von Risiken und Compliance?“

Bildquelle

Cybersecurity Asset Management

Problemraum & Kontext

Cybersecurity Asset Management: Problemraum & Kontext

In den meisten Unternehmen **mangelt es nicht an Daten – sondern an Konsolidierung**. CMDBs, Discovery-Tools, Cloud-Portale und lokale Listen existieren oft parallel, ohne dass eine konsistente Gesamtsicht entsteht. Gleichzeitig wachsen IT- und OT-Landschaften schneller, als Inventare aktualisiert werden: neue Standorte, kurzfristige Cloud-Ressourcen, externe Dienstleister, nicht verwaltete Endgeräte.

Das Ergebnis sind unklare Zuständigkeiten, wachsende Sicherheitsblindspots und eine Angriffsfläche, die kaum jemand vollständig überblickt. Dieses Kapitel zeigt, wo klassische Ansätze scheitern und welche konkreten Risiken daraus entstehen.

3.1 Wachsende Komplexität von IT- und OT-Landschaften

Die meisten Unternehmen arbeiten heute nicht mehr in einer klar abgegrenzten, zentral steuerbaren IT-Welt. Stattdessen bestehen ihre Umgebungen aus einer **Mischung aus stationärer Büro-IT, Cloud-Diensten, mobilen Endgeräten, SaaS-Plattformen, Identitäten, Netzwerkinfrastruktur, Partnerzugängen sowie – je nach Branche – OT-Komponenten** wie Maschinen, Steuerungen, Sensorik oder Gebäudeautomation. Diese Heterogenität ist in den Branchen Bau, Fertigung, Facility Management und technischen Serviceorganisationen besonders ausgeprägt.

Hinzu kommt die **operative Dynamik**. Neue Baustellen werden eingerichtet, temporäre Netzwerke entstehen, Dienstleister erhalten Zugriff, neue SaaS-Tools werden ohne zentrale Freigabe genutzt, Cloud-Ressourcen werden kurzfristig bereitgestellt, und bestehende Systeme bleiben länger im Einsatz als ursprünglich geplant. Dadurch verschieben sich Asset-Bestände ständig, oft schneller, als zentrale Inventare oder Governance-Prozesse aktualisiert werden.

Das Ergebnis sind unklare Zuständigkeiten und wachsende Sicherheitsblindspots. Ein System existiert zwar technisch, taucht aber nicht in zentralen Registern auf. Ein Gerät ist bekannt, aber keinem aktuellen Owner zugeordnet. Eine Anwendung ist aktiv, aber ihre Kritikalität oder ihr Patch-Status ist nicht sauber dokumentiert. Genau an dieser Stelle beginnt das Kernproblem von Cybersecurity Asset Management.

3.2 Warum klassische Inventare (Excel, CMDB-Inseln, Netzwerk-Tools, Cloud-Portale) nicht mehr reichen

In den meisten Unternehmen existieren bereits zahlreiche Datenquellen – von CMDBs und Discovery-Tools über Cloud- und Endpoint-Plattformen bis hin zu IAM- und Security-Systemen. Das Problem ist meist nicht fehlende Information, sondern fehlende Konsolidierung.

> Klassische Inventare scheitern meist nicht an fehlenden Daten, sondern an mangelnder Aktualität, Konsistenz und fehlendem Sicherheitskontext.

Cybersecurity Asset Management: **Problemraum & Kontext**

Wie in Kapitel 2.1 beschrieben, liegt der Fokus von CSAM auf der risikoorientierten und konsistenten Abbildung sicherheitsrelevanter Assets. Genau daran scheitern viele traditionelle Ansätze in der Praxis, insbesondere wenn Updates manuell erfolgen oder neue

Asset-Typen außerhalb historischer Datenmodelle entstehen.
Besonders deutlich wird das bei CMDB-zentrierten Ansätzen: In statischen oder schema-starren Modellen bleiben cloud-native, kurzfristige, externe oder fachbereichsnahe Assets leicht unsichtbar.

Gleichzeitig fehlen oft direkte Bezüge zu Patch-Status, Schwachstellen, Exponierung, Identitäten, Incident-Historie oder Datenkritikalität. Auch Sicherheitsplattformen liefern meist nur Teilperspektiven auf Assets und müssen daher konsolidiert werden.

> Ein zentrales Asset-Register – **etwa in einer Inventarverwaltungslösung wie Timly** – schafft daraus eine konsistente und operativ nutzbare Sicht für Security, Compliance und Governance.

3.3 Folgen für Sicherheit & Compliance

Angreifer nutzen gezielt Systeme aus, die nicht überwacht, vergessen oder unzureichend abgesichert sind. Besonders kritisch sind dabei:

- veraltete Systeme
- unbekannte Netzwerkgeräte
- nicht dokumentierte Cloud-Dienste
- nicht verwaltete Endgeräte
- OT-Komponenten ohne klare Verantwortlichkeit

Typische Auswirkungen:

Verlängerte Incident-Reaktionszeiten

Bei Sicherheitsvorfällen fehlen häufig schnelle Informationen zu betroffenen Systemen, Verantwortlichkeiten und Abhängigkeiten.

Unvollständige Patch-Abdeckung

Systeme bleiben ungepatcht, weil sie nicht bekannt oder keinem Team eindeutig zugeordnet sind.

Erhöhte Angriffsfläche

Unbekannte oder unverwaltete Assets vergrößern unmittelbar die Angriffsfläche.

Hoher Anteil unbekannter Assets

Unternehmen können häufig nicht zuverlässig nachvollziehen, welche Systeme tatsächlich mit dem Netzwerk verbunden sind.

Audit- und Compliance-Lücken

Nachweise zu Ownership, Sicherheitsmaßnahmen oder Abdeckung müssen häufig manuell zusammengeführt werden.

Die fehlende Transparenz über Assets bleibt damit einer der zentralen strukturellen Risikofaktoren moderner IT- und OT-Umgebungen und wirkt sich direkt auf Angriffserkennung, Reaktionsgeschwindigkeit und Compliance-Fähigkeit aus.

Bildquelle

Normen & regulatorische Anforderungen an das Asset-Register

Normen & regulatorische Anforderungen an das Asset-Register

Regulatorische Anforderungen an das Asset-Management sind für viele Unternehmen längst keine abstrakte Zukunftsfrage mehr. **ISO 27001, NIS2, KRITIS** und weitere Frameworks setzen alle dasselbe voraus: Unternehmen müssen nachvollziehbar wissen, welche Assets sie besitzen, wer dafür verantwortlich ist und in welchem Sicherheitszustand sie sich befinden.

Ein zentrales Asset-Register ist damit keine Kür und kein Bonus, sondern regulatorische Grundlage. Dieses Kapitel zeigt, was die wichtigsten Standards konkret verlangen – und wo sich die Anforderungen überschneiden.

4.1 ISO 27001: Inventar von Informationen und Assets

ISO/IEC 27001 macht deutlich, dass Informationssicherheit ohne Kenntnis der zu schützenden Assets nicht wirksam umgesetzt werden kann. Insbesondere Annex A 5.9 fordert die **systematische Bestandsführung von Informationen und zugehörigen Assets** sowie die Zuordnung klarer Verantwortlichkeiten.

Ein Asset-Register ist damit im ISO-Kontext kein optionales Hilfsmittel, sondern eine **grundlegende Voraussetzung** für Risikobetrachtung, Schutzmaßnahmen und Verantwortlichkeit innerhalb eines ISMS.

Wichtig ist dabei nicht nur das Vorhandensein eines Inventars, sondern dessen Qualität. Annex A 5.9 setzt voraus, dass Inventare **konsistent, aktuell und über den gesamten Asset-Lebenszyklus nachvollziehbar** geführt werden. Für die Praxis bedeutet das: Das Register muss sauber gepflegt, mit Mindestattributen versehen und regelmäßig mit anderen Beständen abgeglichen werden.

Ein belastbares Asset-Register sollte im ISO-Sinn unter anderem beantworten können:

- Welche Assets liegen im Geltungsbereich des ISMS?
- Wer ist für welches Asset verantwortlich?
- Wie werden Kritikalität und Schutzbedarf klassifiziert?
- Wie werden neue, geänderte oder stillgelegte Assets im Register nachgeführt?
- Wie werden Asset-Daten systematisch mit Risiken, Kontrollen und Nachweisen verknüpft?

Typische Auditfragen lauten:

- Wie stellen Sie die Vollständigkeit und Aktualität des Registers sicher?
- Wie wird Verantwortung über den Lebenszyklus hinweg gepflegt?
- Welche Asset-Klassen sind im ISMS-Geltungsbereich enthalten und warum?
- Wie werden Asset-Daten mit Risiko- und Kontrollmaßnahmen verknüpft?

4.2 NIS2: Asset-Management als Basis für Risiko- und Incident-Management

Auch regulatorische Vorgaben wie die europäische NIS2-Richtlinie erhöhen die Anforderungen an Transparenz und Risikosteuerung deutlich. NIS2 schreibt kein konkretes Tool oder Inventarsystem vor. Die Richtlinie fordert jedoch „angemessene technische und organisatorische Maßnahmen“ zur Beherrschung von Cyberrisiken.[3]

In der praktischen Umsetzung setzt dies eine **verlässliche Übersicht über Systeme, Dienste und Verantwortlichkeiten voraus**. Ohne eine konsolidierte Asset-Sicht lassen sich zentrale Anforderungen nur eingeschränkt umsetzen, insbesondere in den Bereichen:

- Risikobewertungen
- Incident Response
- Schwachstellenmanagement
- Business Continuity
- oder Meldepflichten

Besonders relevant ist dabei die Fähigkeit, **betroffene Systeme im Notfall schnell identifizieren** zu können. Unternehmen müssen nachvollziehen können:

- welche Assets betroffen sind
- welche Kritikalität besteht
- welche Standorte involviert sind
- welche Abhängigkeiten existieren

CSAM wird damit zu einem zentralen Treiber regulatorischer Resilienz.

4.3 Weitere Standards & Kundenvorgaben (Überblick)

Neben ISO 27001 und NIS2 existieren **zahlreiche weitere Standards** und Kundenvorgaben, die indirekt ein belastbares Asset-Register voraussetzen.
Dazu gehören unter anderem:

- SOC 2
- TISAX
- branchenspezifische Sicherheitsstandards
- KRITIS-Anforderungen
- Kunden-Audits
- interne Governance-Vorgaben

Auch wenn die Anforderungen unterschiedlich formuliert sind, wiederholt sich in nahezu allen Frameworks dieselbe Grundannahme:

Unternehmen müssen wissen, welche Systeme, Daten und Zugänge sie tatsächlich besitzen und absichern. Ein zentrales, aktuelles Asset-Register wird damit zur gemeinsamen Grundlage für Sicherheit, Compliance und operative Steuerung.

In internationalen Organisationen kommen zusätzlich länderspezifische Anforderungen hinzu – beispielsweise:

- BSI- und KRITIS-Vorgaben in Deutschland
- ANSSI-Rahmenwerke in Frankreich
- INCIBE-orientierte Anforderungen in Spanien

Unternehmen benötigen deshalb zunehmend ein skalierbares, standardisiertes Asset-Management-Modell, das sowohl globale Governance als auch lokale Anforderungen unterstützen kann.

Bildquelle

Blueprint: in 90 Tagen zum sicherheitsorientierten Asset-Register

Blueprint: in 90 Tagen zum sicherheitsorientierten Asset-Register

Ein sicherheitsorientiertes Asset-Register entsteht in der Praxis selten durch ein einzelnes Tool. Entscheidend ist vor allem, dass klar definiert ist, **welche Systeme erfasst werden, woher die Daten kommen, wer verantwortlich ist** und wie das Ganze im Alltag gepflegt wird.

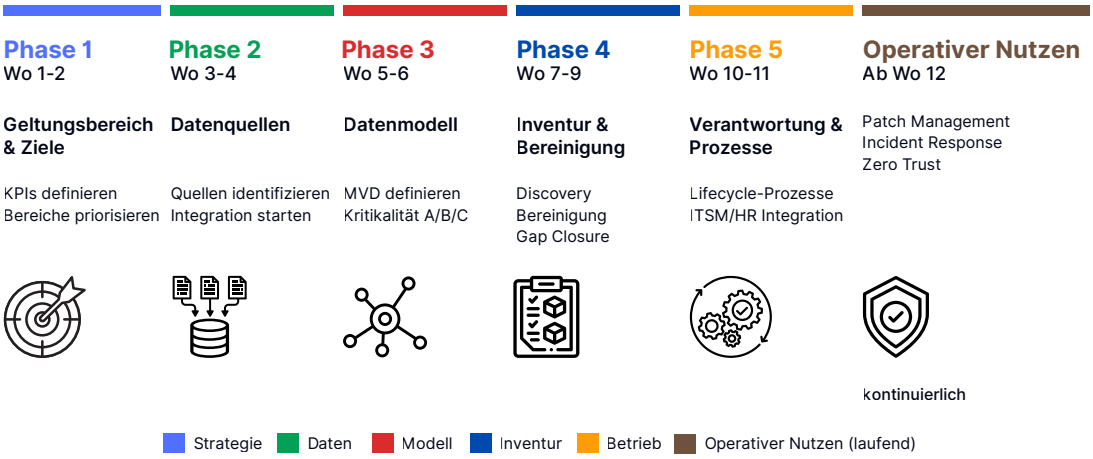
Gerade unbekannte oder nicht verwaltete Assets gehören zu den häufigsten Sicherheitsproblemen, wie unter anderem eine Analyse von Trend Micro zeigt.[4] Deshalb sollte der Aufbau eines Asset-Registers nicht nur als IT-Inventur verstanden werden. Ziel ist vor allem:

- Angriffsflächen besser sichtbar zu machen
- schneller auf Vorfälle reagieren zu können
- Aufwand bei Audits zu reduzieren

Der folgende 90-Tage-Blueprint zeigt einen pragmatischen Einstieg. In den ersten 11 Wochen (Phase 1-5) werden Geltungsbereich, Datenquellen, Datenmodell, Inventur und Prozesse aufgebaut. Ab Woche 12 wird das Register kontinuierlich im operativen Sicherheitsbetrieb genutzt.

Wichtig ist dabei nicht, von Anfang an jedes einzelne Asset vollständig zu dokumentieren. Entscheidend ist ein risikobasierter Einstieg über die sicherheitskritischen Bereiche.

90-Tage-Roadmap: Aufbau eines sicherheitsorientierten Asset-Registers



5.1 Phase 1 – Scope & Ziele festlegen (Woche 1-2)

Viele Projekte scheitern schon am Start, weil ein vollständiges Inventar über alle Systeme, Standorte und Asset-Klassen hinweg angestrebt wird. In der Praxis führt das zu langen Abstimmungen und viel Aufwand, bevor überhaupt ein nutzbares Ergebnis entsteht. Für ein **sicherheitsorientiertes Asset-Register ist deshalb ein risikobasierter Einstieg** sinnvoll.

In den ersten ein bis zwei Wochen sollte der Fokus darauf liegen, einen **klaren Geltungsbereich zu definieren und messbare Ziele** festzulegen. Zuerst sollten die Systeme und Umgebungen erfasst werden, die für Angriffserkennung, Incident Response, Patch-Management und Compliance besonders wichtig sind.

Die folgende Darstellung zeigt typische Startbereiche, die sich dafür in der Praxis bewährt haben.

Blueprint: in 90 Tagen zum sicherheitsorientierten Asset-Register

Typische Startbereiche bei der Asset-Erfassung

Kritische IT-Systeme

Server
Datenbanken

Exponierte Endgeräte

Mobile Geräte
Standortübergreifende Geräte

Privilegierte Accounts

Administratoren
Systemmanager

Zentrale Netzwerkkomponenten

Router
Switches

Produktionsnahe OT-Systeme

Steuerungssysteme
Sensoren

Cloud-Dienste

Sensible Daten
Weitreichende Berechtigungen

> *„Wichtig ist am Anfang nicht Vollständigkeit, sondern Anschlussfähigkeit. Ein einfacher Datensatz mit Owner, Standort und Kritikalität reicht oft aus, um sofort Security-Mehrwert zu erzeugen.“*
>
> **TIMLY CUSTOMER SUCCESS TEAM**

In verteilten Umgebungen – etwa in **Bau, Fertigung oder Facility Management – kann es außerdem sinnvoll sein, mobile oder physisch verteilte Assets früh einzubeziehen.** Gerade dort entstehen häufig Transparenzprobleme und unklare Verantwortlichkeiten. Parallel dazu sollten die Ziele möglichst konkret formuliert werden. Allgemeine Aussagen wie „mehr Transparenz“ reichen dafür nicht aus. **Sinnvoller sind wenige Kennzahlen, mit denen sich Fortschritt und praktischer Nutzen messbar machen lassen.**

Besonders hilfreich sind KPIs, die typische Schwachstellen eines unvollständigen Inventars sichtbar machen:

- unbekannte Assets
- fehlende Verantwortlichkeiten
- unklarer Patch-Status
- langsame Reaktionszeiten bei Sicherheitsvorfällen

Zu Beginn genügt ein **kleines KPI-Set**, das Transparenzlücken und operative Verbesserungen sichtbar macht. Es sollte sowohl die Qualität des Registers als auch den praktischen Nutzen für Sicherheitsprozesse zeigen.

KPI	Warum relevant?	Praktischer Zielwert
Anteil unbekannter Assets	Zeigt blinde Flecken und potenzielle Angriffsfläche	< 5 %
Assets mit zugewiesenem Owner	Voraussetzung für Maßnahmen, Eskalation und Audit-Nachweise	> 90 %
Patch-Transparenz	Zeigt, für wie viele Assets der Patch-Status belastbar bekannt ist	> 95 %
Kritische Assets mit aktueller Klassifizierung	Grundlage für Priorisierung in Security- und Audit-Prozessen	> 90 %
MTTR bei sicherheitsrelevanten Vorfällen	Misst, wie schnell betroffene Assets identifiziert und Maßnahmen eingeleitet werden können	< 4 h (kritische Incidents)

Diese Werte sollten nicht als starre Compliance-Vorgabe verstanden werden. Sie dienen vor allem als **Orientierung für die ersten 90 Tage**. Der eigentliche Nutzen liegt darin, früh sichtbar zu machen, wo die größten Lücken bestehen und ob das Register im Alltag tatsächlich dabei hilft, Sicherheitsprozesse besser zu steuern.

Praxis-Tipp

Ohne klaren Geltungsbereich entsteht schnell ein Register mit vielen Daten, aber wenig Nutzen. Ein risikobasierter Einstieg hilft dabei, die wichtigsten Transparenz- und Sicherheitslücken zuerst zu schließen.

5.2 Phase 2 – Datenquellen identifizieren & konsolidieren (Woche 3-4)

Wenn der Geltungsbereich definiert ist, geht es im nächsten Schritt darum, die wichtigsten **Datenquellen anzubinden und in einer gemeinsamen Sicht** zusammenzuführen. Diese Phase sollte üblicherweise in Woche 3 und 4 abgeschlossen sein.

In den meisten Unternehmen existieren bereits viele Informationen über Assets – allerdings verteilt auf unterschiedliche Systeme wie Active Directory, Cloud-Plattformen, Netzwerk-Tools, OT-Systeme oder lokale Inventarlisten.

Die Herausforderung besteht weniger im Mangel an Daten, sondern darin, diese Bruchstücke zu einer konsistenten Sicht zusammenzuführen.

Für den Einstieg reicht es, zunächst die **Quellen einzubinden, die den größten Mehrwert** für Security und Transparenz liefern. Dazu gehören typischerweise:

- Active Directory oder Identity Provider für Benutzer und Berechtigungen
- Netzwerk-Discovery für aktive Geräte
- Cloud-Plattformen für virtuelle Ressourcen und Dienste
- bestehende Asset- oder Inventarlisten

Diese Werte sollten nicht als starre Compliance-Vorgabe verstanden werden. Sie dienen vor allem als **Orientierung für die ersten 90 Tage**. Der eigentliche Nutzen liegt darin, früh sichtbar zu machen, wo die größten Lücken bestehen und ob das Register im Alltag tatsächlich dabei hilft, Sicherheitsprozesse besser zu steuern.

Praxis-Tipp

Ohne klaren Geltungsbereich entsteht schnell ein Register mit vielen Daten, aber wenig Nutzen. Ein risikobasierter Einstieg hilft dabei, die wichtigsten Transparenz- und Sicherheitslücken zuerst zu schließen.

5.2 Phase 2 – Datenquellen identifizieren & konsolidieren (Woche 3-4)

Wenn der Geltungsbereich definiert ist, geht es im nächsten Schritt darum, die wichtigsten **Datenquellen anzubinden und in einer gemeinsamen Sicht** zusammenzuführen. Diese Phase sollte üblicherweise in Woche 3 und 4 abgeschlossen sein.

In den meisten Unternehmen existieren bereits viele Informationen über Assets – allerdings verteilt auf unterschiedliche Systeme wie Active Directory, Cloud-Plattformen, Netzwerk-Tools, OT-Systeme oder lokale Inventarlisten.

> *Die Herausforderung besteht weniger im Mangel an Daten, sondern darin, diese Bruchstücke zu einer konsistenten Sicht zusammenzuführen.*

Für den Einstieg reicht es, zunächst die **Quellen einzubinden, die den größten Mehrwert** für Security und Transparenz liefern. Dazu gehören typischerweise:

- Active Directory oder Identity Provider für Benutzer und Berechtigungen
- Netzwerk-Discovery für aktive Geräte
- Cloud-Plattformen für virtuelle Ressourcen und Dienste
- bestehende Asset- oder Inventarlisten

5.3 Phase 3 – Datenmodell & Mindestdaten definieren (Woche 5-6)

Sind die wichtigsten Datenquellen zusammengeführt, geht es im nächsten Schritt darum, festzulegen, **welche Informationen pro Asset** tatsächlich benötigt werden. Diese Phase sollte in Woche 5 und 6 abgeschlossen sein. Genau hier werden viele Inventare unnötig komplex, weil zu viele Felder definiert werden, die im Alltag nicht gepflegt werden.

Für ein sicherheitsorientiertes Asset-Register reicht deshalb zunächst ein gemeinsames Mindestdatenmodell: Erfasst werden nur die Informationen, die für Identifikation, Verantwortung, Priorisierung und Sicherheitsmanagement wirklich relevant sind.

Dieses Prinzip lässt sich als **„Minimal Viable Data“** beschreiben – so viele Daten wie nötig, nicht so viele wie möglich.

Mindestdaten pro Asset

Mindestfeld	Warum es wichtig ist
Asset-ID oder eindeutige Bezeichnung	Schafft eine klare Referenz und verhindert Dubletten
Asset-Typ	Unterscheidet z. B. IT, OT, Software, Cloud-Ressource oder Identität
Standort oder logischer Kontext	Zeigt, wo ein Asset eingesetzt wird oder welchem Bereich es zugeordnet ist
Verantwortliche Rolle	Klärt Zuständigkeit für Bewertung, Maßnahmen und Eskalation
Kritikalität	Hilft bei Priorisierung nach Risiko und Business-Auswirkung
Sicherheitsstatus	Macht z. B. Patch-Stand, Prüfstatus oder Auffälligkeiten sichtbar
Lifecycle-Status	Zeigt, ob ein Asset aktiv, in Änderung oder außer Betrieb ist

Diese Felder bilden die gemeinsame Grundlage für unterschiedliche Asset-Typen. **Je nach Umgebung können später weitere Informationen ergänzt werden**, etwa Hersteller, Seriennummer, Firmware-Version, Datenklassifikation oder verknüpfte Schwachstellen.

Zu den wichtigsten Mindestfeldern gehört außerdem eine einfache **Kritikalitätsbewertung**, die hilft, Assets in Sicherheits- und Auditprozessen sinnvoll zu priorisieren.

Für den Einstieg reicht oft ein pragmatisches Modell mit drei Stufen:

Kritikalitätsstufen

Eine solche Einteilung schafft eine gemeinsame Grundlage für Risiko-Bewertungen, Patch-Priorisierung und Incident-Response.

Kritikalität hängt dabei nicht nur vom Asset-Typ ab, sondern von seiner Rolle im Geschäfts- und Sicherheitskontext. Zwei technisch ähnliche Geräte können deshalb unterschiedlich bewertet werden – etwa, wenn eines davon auf sensible Daten zugreift oder einen kritischen Prozess unterstützt.

Praxis-Tipp

Wenige sauber gepflegte Kernfelder sind im Alltag meist wertvoller als ein komplexes Datenmodell, das niemand konsequent nutzt.

5.4 Phase 4 – Initiale Inventur & Bereinigung durchführen (Woche 7-9)

Phase 4 umfasst in der Regel 3 Wochen (Woche 7 bis 9) und ist die arbeitsintensivste Phase. Wenn Datenquellen angebunden und das Mindestdatenmodell definiert sind, beginnt die eigentliche Bestandsaufnahme.

Dabei werden **technische und manuelle Erfassungsmethoden kombiniert – hier kann die Timly Inventur-App** helfen, um möglichst schnell einen nutzbaren Startbestand aufzubauen.

Die folgende Darstellung zeigt typische Erfassungsmethoden, wie sie in dieser Phase zusammenwirken.

Erfassungsmethoden in Phase 4

Automatisches Discovery

IT-ASSETS
Aktive Geräte, Accounts, Cloud-Ressourcen

QUELLEN
Active Discovery, Netzwerk-Scanner, Cloud-APIs

Bereits angebundene Quellen werden direkt genutzt – kein manueller Aufwand

IT-Infrastruktur

Manuelle Erfassung

PHYSISCHE ASSETS
Mobile Assets, Werkzeuge, Ausrüstung

METHODEN
QR-/Barcode-Scan, Listen-Import, Begehungen

Validierung durch Verantwortliche vor Ort sichert Datenqualität

Bau – Fertigung – FM

OT & Legacy

OT-SYSTEME
Maschinen, Steuerungen, Legacy-Anlagen

VORGEHEN
Passive Analyse, SCADA-Bestände, Abstimmung mit Anlagenverantwortlichen

Keine automatische Erkennung – separater Abstimmungsprozess erforderlich

Produktion – OT-Netze

Nach der ersten Erfassung – egal ob über automatisches Discovery, manuelle Erfassung oder separate OT-Prozesse – müssen die Daten **bereinigt und vereinheitlicht** werden. Dazu gehört:

- Dubletten aufzulösen
- fehlende Pflichtfelder wie Owner, Kritikalität oder Standort zu ergänzen
- offensichtliche Lücken zu schließen

Ziel ist dabei kein perfektes Register, sondern ein **arbeitsfähiger Startbestand**, mit dem Sicherheits- und Compliance-Prozesse bereits sinnvoll unterstützt werden können. Verbleibende Lücken lassen sich anschließend schrittweise schließen, sobald das Register im Alltag genutzt wird.

Praxis-Tipp

Die erste Inventur muss nicht vollständig sein – ein Register mit rund 80 % Abdeckung und sauber gepflegten Kerndaten ist oft wertvoller als ein 100-%-Anspruch, der Projekte monatelang verzögert.

5.5 Phase 5 – Verantwortung & Prozesse verankern (Woche 10-11)

In Woche 10 und 11 geht es darum, Verantwortung zu klären und Standardprozesse zu definieren.

Ein zentrales Asset-Register schafft nur dann echten Mehrwert, wenn klar geregelt ist, **wer für ein Asset verantwortlich ist und wann Informationen aktualisiert** werden müssen. Ohne verbindliche Zuständigkeiten werden selbst gut gepflegte Register schnell unvollständig oder veraltet. Deshalb sollten in dieser Phase nicht nur Verantwortliche definiert, sondern auch die wichtigsten Prozesse rund um den Asset-Lifecycle festgelegt werden.

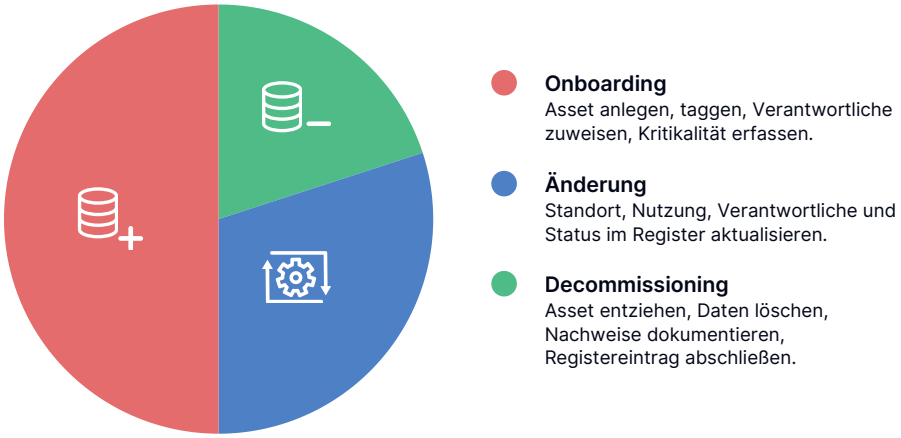
Im Alltag sind drei Situationen entscheidend:

1. **Onboarding**
2. **Änderung**
3. **Decommissioning**

In jeder dieser Phasen muss das Asset-Register sauber gepflegt werden – von der Anlage über Änderungen bis zur Außerbetriebnahme. Die Pflege sollte möglichst direkt in bestehende ITSM-, Beschaffungs- und HR-Prozesse integriert werden, damit Aktualisierungen entlang des Asset-Lifecycles automatisch entstehen.

Die folgende Abbildung zeigt diese drei Prozessmomente:

Asset-Lifecycle: Die drei zentralen Prozessmomente



Praxisbeispiel mit Timly

Damit Asset-Daten langfristig aktuell bleiben, müssen Pflegeprozesse möglichst eng in bestehende Abläufe integriert werden. Mobile Lösungen wie Timly unterstützen dabei insbesondere dezentrale Teams, Wartungsprozesse und standortübergreifende Asset-Verantwortung.

Typische Herausforderungen entstehen durch unklare Zuständigkeiten, fehlende Priorisierung und geringe operative Sichtbarkeit des Nutzens. Deshalb sollte eindeutig definiert sein, welches Ereignis welche Aktualisierung auslöst – und wer dafür verantwortlich ist. Nur klar **definierte Verantwortlichkeiten und Aktualisierungsprozesse sichern die Datenqualität** langfristig.

Praxis-Tipp

Verantwortlichkeit funktioniert nur dann zuverlässig, wenn Asset-Pflege Teil bestehender Prozesse wird. Besonders wirksam ist die Anbindung an ITSM-, Beschaffungs- und HR-Workflows.

5.6 Operativer Nutzen: Sicherheits-Use-Cases (ab Woche 12)

Nach Abschluss der Aufbauphase (Phase 1–5, Woche 1–11) wird das Asset-Register ab Woche 12 kontinuierlich genutzt.

Ein zentrales Asset-Register entfaltet seinen eigentlichen Nutzen erst im operativen Sicherheitsbetrieb. Prozesse wie Patch-Management, Incident-Response oder Zugriffskontrolle funktionieren nur dann effizient, wenn aktuelle und verlässliche Informationen über relevante Assets verfügbar sind.

Ohne diese Grundlage müssen Security-Teams im Ereignisfall Informationen aus unterschiedlichen Systemen und Listen manuell zusammentragen. Mit einem zentral gepflegten Register lassen sich betroffene Systeme schneller identifizieren, priorisieren und nachvollziehbar bearbeiten.

Im Folgenden drei zentrale Use Cases, in denen sich der praktische Mehrwert besonders deutlich zeigt:

Patch-Management

Bei kritischen Schwachstellen beginnt die Arbeit ohne zentrales Asset-Register oft mit einer aufwendigen Suche: Welche Systeme sind betroffen, welche Versionen laufen wo und wer ist verantwortlich? Informationen liegen verteilt in verschiedenen Tools, Listen und Teams.

Mit einem zentralen Asset-Register können **betroffene Systeme direkt gefiltert und priorisiert werden** – etwa nach Software-Version, Standort, Kritikalität oder Owner. Dadurch wird klar, welche Systeme zuerst behandelt werden müssen und wer für die Umsetzung zuständig ist. Patch-Status und Fortschritt bleiben transparent nachvollziehbar.

Incident Response

Bei einem Sicherheitsvorfall – etwa einem verdächtigen Login oder einem Malware-Alarm – ist zunächst unklar, welche Systeme betroffen sind und wie kritisch die Situation ist. Ohne zentrale Datenbasis beginnt häufig eine manuelle Recherche über mehrere Systeme hinweg.

Blueprint: in 90 Tagen zum sicherheitsorientierten Asset-Register

Mit einem Asset-Register steht der notwendige Kontext sofort zur Verfügung: betroffenes System, verantwortlicher Owner, Standort, Kritikalität und mögliche Abhängigkeiten. Dadurch können erste Maßnahmen schneller eingeleitet und Eskalationswege klar gesteuert werden.

Zugriffskontrolle & Zero Trust

Zugriffsentscheidungen basieren in vielen Umgebungen noch auf einfachen Annahmen wie Netzwerkzugehörigkeit oder VPN-Verbindung. Der Kontext des zugreifenden Systems ist dabei oft nicht ausreichend bekannt.

Ein Asset-Register liefert die notwendige Grundlage für kontextbasierte Entscheidungen: **Gerätetyp, Standort, Kritikalität, Patch-Status und Verantwortlichkeit**. Dadurch können Zugriffe differenzierter gesteuert werden – etwa durch Einschränkungen bei unbekannten oder nicht aktuellen Systemen

Praxis-Tipp

Der operative Nutzen eines Asset-Registers zeigt sich nicht in der Datenmenge, sondern in der Geschwindigkeit und Qualität von Entscheidungen. Entscheidend ist, dass im Incident, beim Patch oder bei Zugriffsfragen der notwendige Kontext sofort verfügbar ist.

Bildquelle

Praxisbeispiele aus Bau, Produktion, FM & IT

Praxisbeispiele aus Bau, Produktion, FM & IT

Die vorherigen Kapitel haben gezeigt, wie ein für die Informationssicherheit geeignetes Asset-Register Schritt für Schritt aufgebaut wird. Die folgenden Beispiele zeigen, wie sich diese Struktur im operativen Alltag auswirkt – in Bau, Produktion, IT und Facility Management.

6.1 Mittelständischer Bau- und FM-Dienstleister

Bau- & FM-Dienstleister – 400 MA, 30 Standorte

Mobile Assets, dezentrale Verwaltung über Excel & E-Mail

AUSGANGSLAGE

Verantwortlichkeiten waren unklar, Standorte nicht nachvollziehbar und Audits regelmäßig lückenhaft. Mehrere tausend mobile Assets – Werkzeuge, Prüfgeräte, IT-Equipment – wurden über dezentrale Listen verwaltet, ohne verlässliche Sicht auf Zustand oder Verbleib.

MASSNAHMEN

- QR-basierte Asset-Erfassung direkt vor Ort, standortübergreifend
- Zentrale Zuweisung der Verantwortlichen je Asset
- Integration Identity-Management & Ticketing
- Kritikalitätsmodell A/B/C für Wartungspriorisierung

ERGEBNISSE

Nicht zugeordnete Assets	Incident-Response	Audit-Readiness
~18% → <3%	Tage → <4h	Erstmals vollständig Prüf- und Verantwortlichkeitsnachweise direkt aus dem System

"Der entscheidende Moment ist meist nicht die Einführung selbst, sondern die vollständige Inventur. Danach wird sehr schnell sichtbar, wo keine klaren Zuständigkeiten existieren."

– Timly Customer Success Team

6.2 Fertigungsunternehmen mit OT-Fokus

Fertigungsunternehmen – OT-Fokus, mehrere Werke

Komplexe OT-Umgebungen, parallele Inventarlisten, unbekannte Firmware-Stände

AUSGANGSLAGE

Welche Anlagen wirklich kritisch sind, war nicht dokumentiert – und damit im Störungsfall nicht entscheidbar. Parallele Inventarlisten waren weder aktuell noch konsistent, Firmware-Versionen teilweise unbekannt.

MASSNAHMEN

- Bewusst eingeschränkter Geltungsbereich: nur produktionskritische Anlagen zuerst
- Netzwerk-Discovery als technische Grundgesamtheit
- Manuelle Ergänzung OT-spezifischer Daten (Firmware, Hersteller, Bereich)
- Zuweisung der Verantwortlichen & Kritikalität A/B/C, Anbindung Wartungssystem

ERGEBNISSE

Produktionskritische Assets	Unbekannte Firmware-Stände	Schwachstellenanalyse
>90% **vollständig erfasst**	Hoch → <5%	Erstmals priorisierbar Betroffene Systeme innerhalb kurzer Zeit identifiziert & nach Kritikalität gereiht

"In OT-Umgebungen ist das eigentliche Problem selten die Technik selbst, sondern die fehlende gemeinsame Sicht darauf, welche Systeme wirklich kritisch sind."

– Timly Implementierungsteam

Praxisbeispiele aus Bau, Produktion, FM & IT

6.3 IT-Dienstleister / Managed Service Provider

IT-Dienstleister/Managed Service Provider – 50 Kunden

Heterogene IT-Umgebungen, Assets in Ticketsystemen, Monitoring, Excel verteilt

AUSGANGSLAGE

Im Ernstfall fehlte der konsolidierte Überblick – über Kunden, Systeme und Verantwortlichkeiten hinweg. Assets lagen in verschiedenen Tools verteilt, Reporting erforderte manuelles Zusammenführen pro Kunde.

MASSNAHMEN

- Zentrales Register für interne & kundenbezogene Assets
- Zuordnung zu Kunden & internen Verantwortlichen je Asset
- Automatische Synchronisation via RMM-Tools & Cloud-APIs
- Standardisierte Kundenreports automatisch aus dem Register

ERGEBNISSE

Assets konsistent erfasst	Incident-Identifikation	Reporting
>95% mit Verantwortlichen- & Kundenbezug	Stunden → Minuten	Vollständig automatisiert Regelmäßige Kundenberichte laufen ohne manuellen Aufwand

"Der größte Unterschied entsteht nicht durch mehr Daten, sondern durch weniger Suchaufwand im Ernstfall."

– Timly Customer Success Team

Praxis-Fazit

Die Beispiele zeigen ein wiederkehrendes Muster: Der größte Nutzen entsteht nicht durch perfekte Vollständigkeit, sondern durch eine früh nutzbare Struktur mit klaren Verantwortlichkeiten und konsolidierten Kerndaten. Sobald diese Basis steht, verbessern sich sowohl die operative Sicherheit als auch die Geschwindigkeit im Alltag spürbar.

Bildquelle

Organisatorische Verankerung & Change Management

Organisatorische Verankerung & Change Management

Ein Asset-Register entfaltet seinen Nutzen nicht nur durch die Einführung eines Tools, sondern vor allem durch die **Einbettung in bestehende Verantwortungs- und Prozessstrukturen**. Entscheidend ist die organisatorische Verankerung des Registers in bestehende Betriebs- und Governance-Prozesse.

Damit wird das Register von einer Datenbank zu einer operativen Referenz für Security, IT-Betrieb und Compliance.

7.1 Governance & Rollenmodell

Die strategische Verantwortung für das Asset-Register liegt in der Regel bei der IT-Leitung oder der CISO-Funktion. In dieser Rolle werden Geltungsbereich, Mindestdatenmodell, Kritikalitätslogik sowie die Verbindung zu Risiko- und Compliance-Anforderungen festgelegt.

Entscheidend ist nicht die operative Pflege, sondern die Definition verbindlicher Regeln, nach denen Assets im Unternehmen bewertet und geführt werden.

Die operative Verantwortung liegt dort, wo Änderungen tatsächlich entstehen in:

- IT-Betrieb
- OT-Teams
- Standortorganisationen
- technischen Serviceeinheiten

Diese Gruppen sind dafür verantwortlich, dass Asset-relevante Ereignisse unmittelbar im System abgebildet werden, etwa bei Inbetriebnahme, Standortwechsel, Wartung oder Stilllegung.

In der Praxis entstehen die meisten Inkonsistenzen nicht durch fehlende Zuständigkeit, sondern durch unklare Auslöser: Wer trägt eine Änderung ein, wenn ein Gerät „nur temporär" verlagert wird oder ein Service durch einen externen Dienstleister erfolgt? Ein belastbares Rollenmodell trennt deshalb nicht nur Ebenen, sondern auch Verantwortungsarten.

Die folgende Darstellung zeigt die drei zentralen Verantwortungsebenen im Asset-Register.

Verantwortungsebenen im Asset-Register

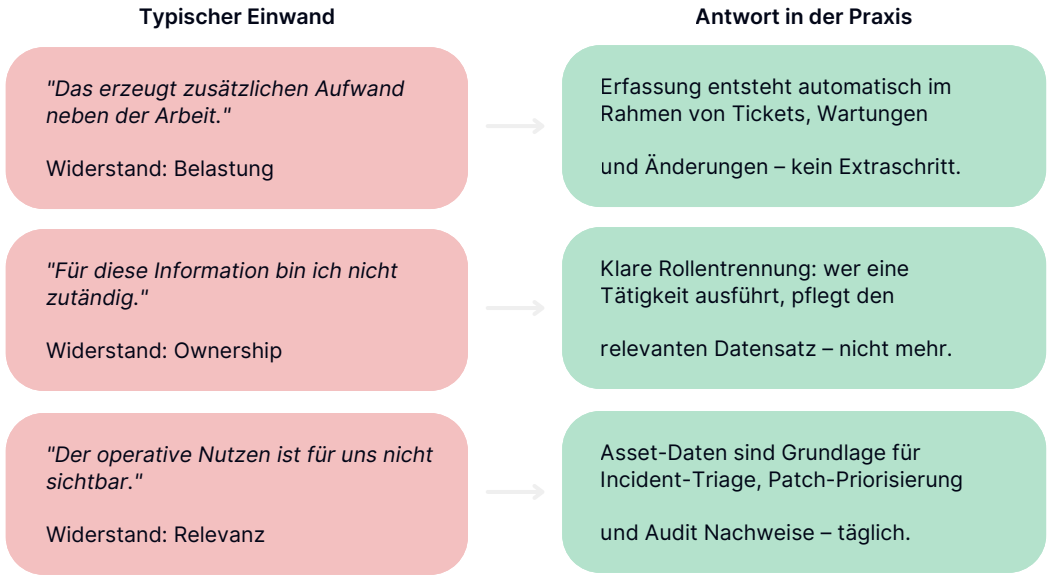
Organisatorische Verankerung & Change Management

7.2 Enablement & Akzeptanz im Alltag

Die Einführung eines Asset-Registers scheitert selten an der Technologie, sondern an der **zusätzlichen Belastung im operativen Alltag**. Typische Rückmeldungen aus der Praxis sind:

- „Das erzeugt zusätzlichen Aufwand im Tagesgeschäft."
- „Für diese Information bin ich nicht zuständig."
- „Der operative Nutzen ist für uns nicht sichtbar."

Akzeptanz entsteht vor allem dann, wenn Asset-Daten direkt im operativen Arbeitskontext gepflegt werden können. Die folgende Darstellung zeigt **drei typische Einwände – und wie sie sich in der Praxis adressieren lassen**.



Wirksam wird das Modell erst, wenn Erfassung und Aktualisierung in bestehende Abläufe integriert sind.

In der Praxis entstehen relevante Asset-Informationen idealerweise direkt im Rahmen bestehender Prozesse – etwa bei Tickets, Wartungen, Change-Requests oder Beschaffungen.

Besonders wirksam sind dabei Prozesse mit möglichst geringer operativer Hürde:

- **Mobile Erfassung und QR-/Barcode-Scanning** vereinfachen Inventur- und Pflegeprozesse im Alltag
- **Wenige verpflichtende Kernattribute** erleichtern den Einstieg und verbessern die Pflegequalität
- **Einordnung im Arbeitskontext:** Asset-Daten unterstützen operative Entscheidungen – etwa bei Incident-Triage, Patch-Priorisierung oder Audit-Nachweisen

> *„Akzeptanz entsteht nicht durch Schulungen, sondern durch Einfachheit. Wenn Teams ein Asset in 10 Sekunden per QR-Scan erfassen können und das Ergebnis sofort im Ticket oder der Wartungsplanung sichtbar ist, wird Pflege zur Gewohnheit – nicht zur Zusatzaufgabe."*
>
> **TIMLY CUSTOMER SUCCESS TEAM**

Organisatorische Verankerung & Change Management

7.3 Integration in bestehende Management-Systeme

Ein Asset-Register entfaltet seinen größten Nutzen, wenn es als zentrale **Referenz zwischen bestehenden Betriebs-, Security- und Compliance-Systemen** fungiert.

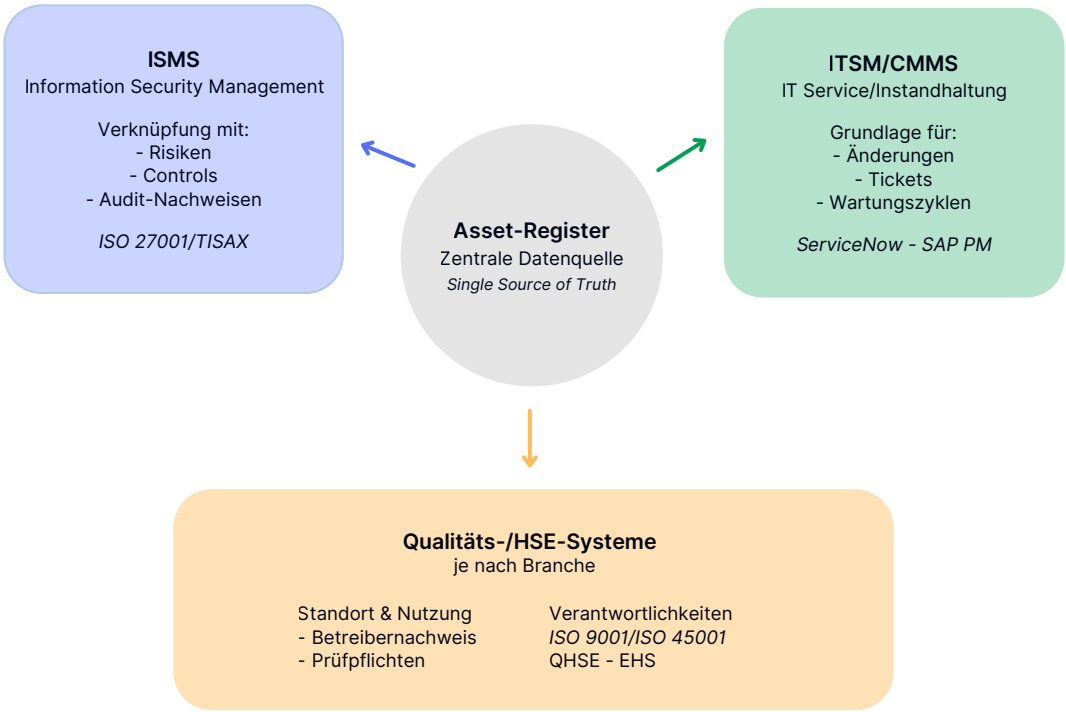
Im Zentrum steht die Integration in drei Systembereiche:

ISMS Verknüpft Assets mit Risiken, Sicherheitsmaßnahmen und Audit-Nachweisen.

ITSM/CMMS
Nutzt das Asset-Register als Grundlage für Change-Requests, Tickets und Wartungszyklen.

Qualitäts-/HSE-Systeme
Stellen je nach Branche die Nachvollziehbarkeit von Standort, Nutzung und Verantwortlichkeiten sicher.

Die folgende Darstellung zeigt, wie das Asset-Register als zentrale Datenquelle zwischen diesen Systemen wirkt.



Wichtig ist eine klare **Zuordnung führender Systeme pro Datenkategorie**. Fehlt diese Zuordnung, entstehen schnell widersprüchliche Datenstände zwischen ITSM, CMMS und Asset-Register.

Entscheidend sind klar definierte Rollen sowie ein eindeutiges Zusammenspiel der Systeme: Das Asset-Register dient als zentrale Referenz, während operative Systeme Änderungen und Lifecycle-Ereignisse liefern.

Typische organisatorische Erfolgsfaktoren im Rollout

- Klare Verantwortlichkeiten entlang des gesamten Asset-Lifecycles (von Onboarding bis Decommissioning)
- Integration in Onboarding-, Change- und Decommissioning-Prozesse
- Reduzierte Einstiegshürden durch minimale Pflichtattribute
- Früh sichtbare operative Nutzen (z. B. schnellere Audits, weniger Rückfragen im Betrieb)

Bildquelle

Kernaussagen & Empfehlungen für Entscheider

Kernaussagen & Empfehlungen für Entscheider

Die folgenden Kernaussagen und Empfehlungen verdichten die zentralen Erkenntnisse dieses Reports und zeigen, welche Maßnahmen Unternehmen jetzt priorisieren sollten, um Cybersecurity Asset Management wirksam und nachhaltig zu etablieren.

8.1 Die fünf wichtigsten Erkenntnisse auf einen Blick

Ein belastbares Asset-Register bildet die operative Grundlage moderner Cybersecurity- und Compliance-Prozesse.

Die folgenden Kernaussagen fassen die wichtigsten Erkenntnisse dieses Reports zusammen:

1. Ohne **konsistente und gepflegte Asset-Daten** bleibt wirksames Cyber-Risikomanagement nur eingeschränkt möglich. Nicht erfasste oder unzureichend verwaltete Systeme zählen zu den häufigsten Ursachen für Sicherheitslücken, verzögerte Incident-Response und unvollständige Patch-Abdeckung.
2. **Regulatorische Anforderungen wie NIS2 oder ISO 27001** setzen nachvollziehbare Asset-Daten, klare Zuständigkeiten und belastbare Nachweise voraus. Isolierte Inventarlisten reichen dafür in dynamischen IT- und OT-Umgebungen nicht mehr aus.
3. Der eigentliche Mehrwert entsteht im **operativen Betrieb**: Ein zentrales Asset-Register verbessert Incident-Response, Patch-Management, Auditfähigkeit und Security-Reporting unmittelbar im Tagesgeschäft.
4. Erfolgreiches CSAM ist deshalb weniger ein Tool-Thema als eine **Kombination aus Governance, integrierten Prozessen und kontinuierlicher Datenpflege**.
5. Besonders wirksam sind **pragmatische Einstiegsmodelle** mit klar priorisierten Asset-Klassen, wenigen Kernprozessen und messbaren Verbesserungen innerhalb der ersten Monate.

8.2 Konkrete Handlungsempfehlungen für die nächsten 6–12 Monate

Der Aufbau eines für die Informationssicherheit geeigneten Asset-Registers sollte nicht als isoliertes IT-Projekt verstanden werden, sondern als schrittweise Weiterentwicklung hin zu einem sicherheitsorientierten Betriebsmodell.

Der folgende Mini-Fahrplan zeigt, welche Maßnahmen sich in der Praxis besonders bewährt haben.

Quick Wins (0–3 Monate)
(entspricht Phase 1–3 des 90-Tage-Blueprints)

- Kritische Asset-Klassen und Scope definieren
- Zentrale Datenquellen konsolidieren
- Mindestdatenmodell und Verantwortung festlegen
- Erste Sicherheits-KPIs etablieren

Operative Stabilisierung (3–6 Monate)
(entspricht Phase 4–5 des 90-Tage-Blueprints)

- Initiale Inventur und Datenbereinigung durchführen
- Asset-Register mit Patch- und Incident-Prozessen verbinden
- Verantwortlichkeiten entlang des Lifecycles verankern
- Datenqualität und Aktualisierung operationalisieren

Strategische Weiterentwicklung (6–12 Monate)
(Weiterentwicklung über den initialen Blueprint hinaus)

- Asset-Register vollständig ins ISMS integrieren
- Audit- und Compliance-Reporting automatisieren
- Zero-Trust- und risikobasierte Steuerung ausbauen
- Reifegradmodell und Governance kontinuierlich weiterentwickeln

Praxis-Tipp

Unternehmen sollten nicht versuchen, sofort ein vollständiges Gesamtinventar aufzubauen. Erfolgreicher sind iterative Modelle mit priorisierten Asset-Klassen und klar integrierten Kernprozessen.

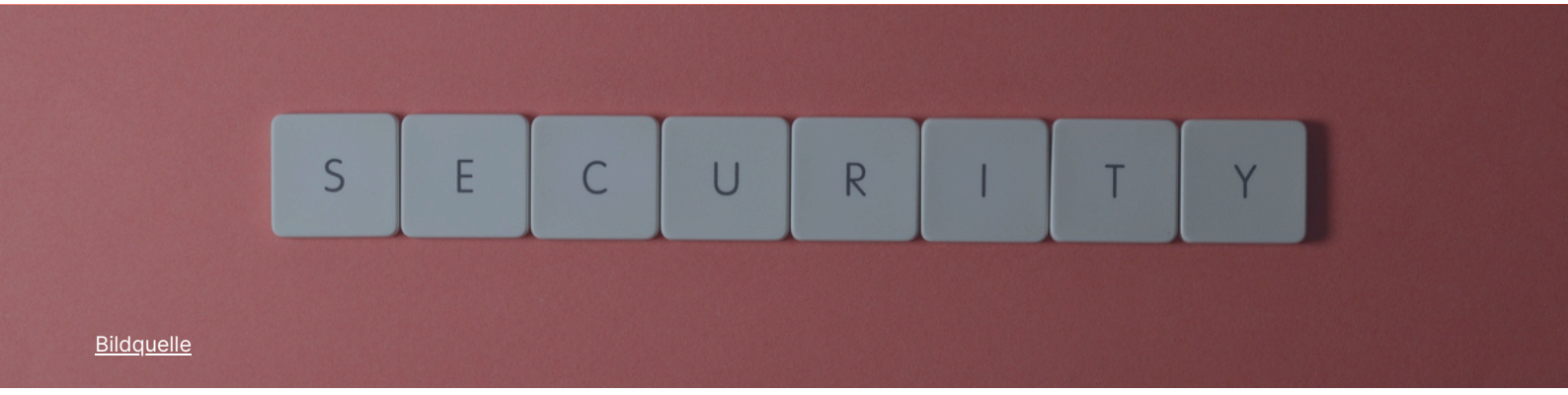
8.3 Ausblick

Cybersecurity Asset Management entwickelt sich zunehmend vom Inventarisierungsprojekt zu einer **zentralen Steuerungsebene für Security, Compliance und operative Resilienz**.

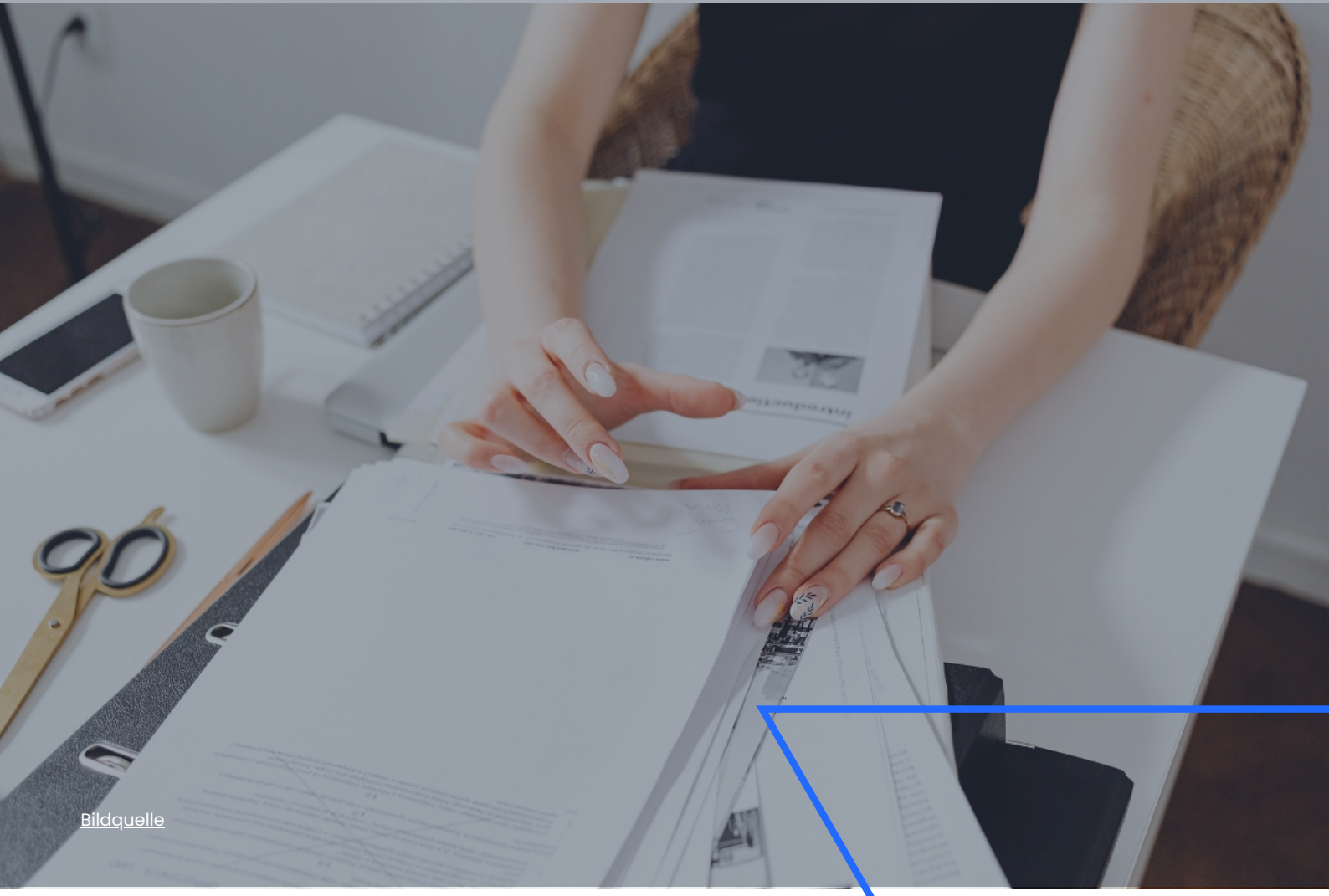
Mit steigenden regulatorischen Anforderungen durch NIS2, ISO 27001, KRITIS oder branchenspezifische Vorgaben wächst der Druck auf Unternehmen, vollständige Transparenz über sicherheitsrelevante Assets nachweisen zu können. Gleichzeitig nehmen hybride IT-/OT-Umgebungen, Cloud-Nutzung, mobile Arbeitsmodelle und externe Zugriffe weiter zu.
Dadurch wird ein belastbares Asset-Register künftig noch stärker zur Grundlage für:

- Risiko- und Compliance-Steuerung
- Zero-Trust-Architekturen
- automatisiertes Vulnerability-Management
- Incident-Response und Resilienz
- Audit- und Nachweisfähigkeit
- integrierte Betriebs- und Wartungsprozesse

Langfristig entwickeln sich moderne CSAM-Ansätze deshalb in Richtung eines **ganzheitlichen Operating Models**, das Security, IT, OT, Instandhaltung, Compliance und ESG-relevante Prozesse miteinander verbindet.



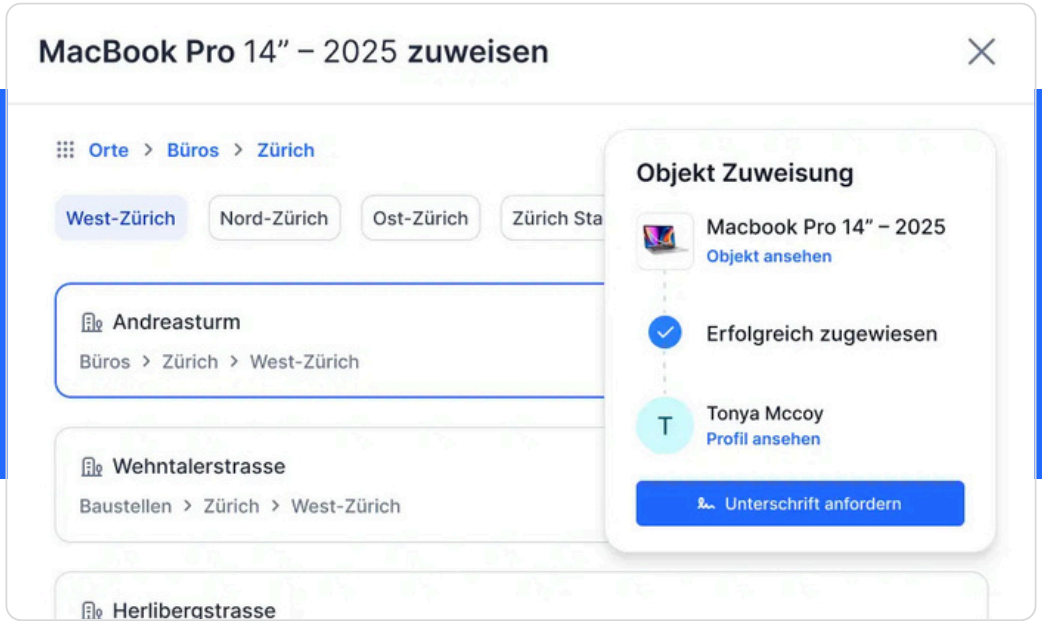
Bildquelle



Bildquelle

Über Timly & Methodik

Timly



Über Timly & Methodik

Timly unterstützt Unternehmen dabei, physische Assets, technische Betriebsmittel und sicherheitsrelevante Ressourcen zentral, mobil und nachvollziehbar zu verwalten. Die Plattform wird insbesondere in Branchen mit **verteilten und dynamischen Asset-Strukturen** eingesetzt – darunter Bau, Industrie, IT, Facility Management, technische Services und industrielle Betriebsumgebungen.

Ein besonderer Fokus liegt auf der Verbindung von physischer Asset-Transparenz mit operativen Prozessen und Security-relevanten Anforderungen. Dazu gehören unter anderem:

- zentrale Verwaltung physischer Assets und Betriebsmittel
- mobile Datenerfassung per Smartphone oder Tablet
- QR- und Barcode-basierte Inventarisierung
- Unterstützung verteilter Standorte und mobiler Teams
- Einbindung von OT-nahen Assets und technischen Anlagen
- Lifecycle- und Wartungsprozesse
- rollenbasierte Verantwortlichkeiten und Nachvollziehbarkeit

Durch die Kombination aus einfacher Erfassung, mobiler Nutzung und zentraler Datenbasis unterstützt Timly Unternehmen dabei, **Transparenzlücken zu reduzieren und Asset-Daten operativ nutzbar** zu machen – sowohl im IT-/OT-Kontext als auch für Sicherheits-, Audit- und Compliance-Anforderungen.

Erfahren Sie in einer kostenlosen Demo, wie sich Asset-Transparenz in verteilten IT- und OT-Umgebungen praktisch umsetzen lässt.

DEMO BUCHEN

9.1 Methodik

Dieser Report basiert auf einer Kombination aus:

- öffentlich verfügbaren Studien und Marktanalysen
- regulatorischen und normativen Anforderungen
- Praxiserfahrungen aus Kundenprojekten
- internen Erkenntnissen aus Workshops, Implementierungen und Nutzerfeedback,
- operativen Beobachtungen aus Branchen mit verteilten Asset-Strukturen

Berücksichtigt wurden unter anderem Erkenntnisse und Anforderungen aus:

- ISO 27001/Annex A
- NIS2-Richtlinie
- Veröffentlichungen von Verizon, IBM und weiteren Cybersecurity-Analysen
- Erfahrungen aus IT-, OT- und Facility-Management-Projekten

Die dargestellten Reifegrade, KPI-Beispiele und Praxisempfehlungen verstehen sich bewusst als pragmatisches Zielbild und nicht als starres Compliance-Modell. Ziel des Reports ist es, Unternehmen einen **praxisnahen Einstieg in den Aufbau eines für die Informationssicherheit geeigneten Asset-Registers** zu ermöglichen – mit Fokus auf Risikoreduktion, operative Umsetzbarkeit und auditfähige Transparenz.

9.2 Quellen

[1] https://www.verizon.com/business/resources/infographics/2025-dbir-infographic.pdf
[2] https://www.ibm.com/reports/data-breach
[3] https://eur-lex.europa.eu/eli/dir/2022/2555/oj
[4] https://www.trendmicro.com/explore/aichangingcyberrisk