VDA Verband der Automobilindustrie

Empfehlung

Cybersicherheit in der Lieferkette – IT-Architektur



Vorwort

Die Automobilindustrie befindet sich in einem tiefgreifenden Wandel. Vernetzte Fahrzeuge, softwaregesteuerte Systeme und digitale Wertschöpfungsketten eröffnen neue Chancen, sie eröffnen jedoch zugleich neue Angriffsflächen. Cybersicherheit ist heute nicht mehr nur eine technische Fragestellung, sondern eine strategische Voraussetzung für die Wettbewerbsfähigkeit und Integrität der gesamten automobilen Wertschöpfungskette.

Der vorliegende Leitfaden des Verbandes der Automobilindustrie (VDA) richtet sich an alle Unternehmen, die als Lieferanten, Dienstleister oder Partner in die automobile Lieferkette eingebunden sind. Er formuliert Empfehlungen, bietet praxisnahe Orientierung und stärkt das gemeinsame Verständnis von Cybersicherheit über Unternehmens- und Ländergrenzen hinweg.

Regulatorische Rahmenbedingungen wie NIS 2, EU AI Act, sowie der European Cyber Resilience Act und weitere Regularien setzen Rahmen, sie schaffen Verbindlichkeit, ersetzen aber nicht die Anpassung der Regeln und Maßnahmen auf die Besonderheiten der Branche. Der VDA sieht es als seine Aufgabe, diese Anpassungen zu koordinieren, Best Practices zu definieren und den Austausch zwischen OEM und Lieferanten zu diesem Thema zu fördern.

Cybersicherheit in der Lieferkette ist eine gemeinsame Verantwortung. Sie erfordert Transparenz über Risiken, klar definierte Prozesse zur Schwachstellenbehebung und eine Sicherheitskultur, die von der Entwicklung bis zum Betrieb gelebt wird. Nur wenn alle Glieder der Lieferkette ihren Beitrag leisten, kann das Gesamtsystem als sicher gelten.

Die Empfehlung basiert auf anerkannten Standards wie ISO/IEC 27001, VDA ISA / TISAX und IEC 62443 und ergänzt diese um konkrete architektonische Leitlinien sowie praxisorientierte Maßnahmen. Darüber hinaus werden zusätzliche Themen wie Cloud Security und Künstliche Intelligenz berücksichtigt.

Ein besonderer Dank gilt dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie der Fachgruppe Informationssicherheit des ISACA Germany Chapter e.V. für die Zusammenarbeit und die fachliche Unterstützung bei der Erstellung dieses Dokuments.

Inhaltsverzeichnis

1. Einleitung **4**
1.1 Absicherung der Lieferkette durch TISAX 4
2.1 Erweiterte Anforderungen 5
2. Gegenstand und Geltungsbereich **5**
2.1 Zielsetzung 5
3. Definitionen und Standards **7**
3.1 Fundamentale Sicherheitsprinzipien 7
3.2 Übersicht relevanter Standards 8
3.3 Generisches Architekturmodell 10
4. IT Security **11**
4.1 Identity and Access Management (IAM) 12
4.2 Netzwerksicherheit 15
4.3 Kommunikationssicherheit 20
4.4 Endpoint Security 23
4.5 Datensicherheit 28
4.6 Applikationssicherheit 33
5. Industrial and Operational Technology Security (OT) **36**
5.1 Netzwerksegmentierung und Zonenkonzept 36
5.2 Hartung von OT-Systemen 38
5.3 Physische Sicherheit 39
5.4 Zugangskontrolle in der OT 40
5.5 Schwachstellen- und Patch-Management in der OT 41
5.6 Backup und Wiederherstellung in der OT 42
5.7 Security Monitoring und Incident Response in der OT 44
6. Cloud Security **46**
6.1 Grundlagen 46
6.2 Begriffsdefinitionen / Cloud services (IaaS, PaaS, SaaS) 47
6.3 Shared Responsibility model bei Cloud Services 48
6.4 Bewertung Sicherheitsstandards des Providers 50
6.5 Integration 52
6.6 Betrieb 54
7. Künstliche Intelligenz **60**
7.1 Risiken für KI aufgrund externer Angriffe 62
7.2 Risiken durch Nutzung von KI 70
7.3 Nutzungsszenarien 74
7.4 KI-Governance 79
8. Anhang **81**
Mapping der Anforderungen auf den VDA ISA 2027 Katalog 81
Tabelle mit KPIs 82
Glossar und Begriffsdefinitionen 86

1 Einleitung

Die zunehmende Berichterstattung über Cyberattacken verdeutlicht die stetig wachsende Bedrohung durch kriminelle IT-Angriffe auf Firmennetzwerke. Auch die Automobilindustrie sieht sich mit einer steigenden Anzahl von Vorfällen innerhalb ihrer Lieferketten konfrontiert. Die Folgen solcher Angriffe reichen von Produktions- und Lieferunterbrechungen über den Diebstahl sensibler Unternehmensdaten bis hin zu erheblichen finanziellen Schäden. Besonders besorgniserregend ist die Entwicklung hin zu gezielten Angriffen, die nicht nur auf die Verfügbarkeit und Vertraulichkeit von Daten, sondern zunehmend auch auf deren Integrität abzielen. Dies betrifft insbesondere die Unveränderlichkeit von Produkt-, Software- und Produktionsparametern. Neben der physischen Versorgungskette gewinnt somit auch die Sicherheit in der Software-Lieferkette an Bedeutung, um Störungen kritischer Geschäftsprozesse zu verhindern.
Zusammenfassend gilt, dass die folgenden Haupt-Schutzziele zunehmend gleichberechtigt im Fokus stehen:

- **Vertraulichkeit:** Schutz von Know-how und geistigem Eigentum
- **Verfügbarkeit:** Sicherstellung der Betriebsfähigkeit von IT-Systemen und Produktionsanlagen
- **Integrität:** Verhinderung unautorisierter Änderungen an Software, Produktdaten und Produktionsparametern

1.1 Absicherung der Lieferkette durch TISAX

Um die Resilienz der gesamten Lieferkette gegenüber Cyber-Bedrohungen, insbesondere gegen erpresserische „Ransomware“-Angriffe, zu erhöhen, setzt die Automobilindustrie auf konkrete Maßnahmen.

Ein zentraler Baustein ist der branchenweit etablierte Standard TISAX (Trusted Information Security Assessment Exchange), der auf dem VDA ISA (Information Security Assessment) Katalog basiert.

Der VDA-ISA Katalog definiert Sicherheitsanforderungen in verschiedenen Bereichen der Informationssicherheit und basiert auf international etablierten Standards wie ISO/IEC 27001/27002 (vgl. Kap. 3).

Das TISAX-Modell in Kombination mit dem VDA ISA Katalog ermöglicht eine risikobasierte Bewertung der Informationssicherheit über die gesamte Lieferkette hinweg. Die von den Unternehmen zu implementierenden Schutzmaßnahmen adressieren dabei die oben genannten Schutzziele.

Die Umsetzung von TISAX erfolgt durch eine strukturierte Bewertung der Reifegrade von Informationssicherheitsprozessen. Die TISAX-Teilnehmer bewerten sich gemäß des VDA ISA Katalogs selbst, die Assessments werden von freigegebenen Prüfdienstleistern durchgeführt.

Die Ergebnisse eines TISAX Assessments werden branchenweit anerkannt und sind für viele Unternehmen der Automobilindustrie eine zentrale Voraussetzung, um sensible Informationen sicher auszutauschen.

1.2 Erweiterte Anforderungen

Besonders kritische Lieferanten, beispielsweise Just-in-Sequence (JIS) Lieferanten, unterliegen besonderen Risiken. Die Etablierung zusätzlicher Anforderungen und erweiterten Sicherheitsmaßnahmen kann hier sinnvoll sein, damit diese über eine IT-Sicherheitsarchitektur verfügen, die den aktuellen technologischen Standards entspricht. Dies umfasst ebenfalls die Produktionsanlagen (Operational Technology, OT), die durch Cyberangriffe betroffen sein können (beispielsweise verschlüsselte Anlagen-Steuerungen und Industrie-PC).

Der Nachweis eines erfolgreichen TISAX-Assessments und die Berücksichtigung der relevanten Standards (vgl. Kapitel 3) und Anwendung der Best Practices (vgl. Kap. 4-7) fördert eine gleichartige Sicherheitskultur in der Automobilindustrie und trägt maßgeblich zur Erhöhung der Cyber-Resilienz über das gesamte Lieferantennetzwerk hinweg bei.

Dieses Dokument stellt zudem Vorschläge für Kennzahlen für die Bewertung und somit kontinuierlichen Verbesserung des Reifegrads der eigenen IT-Sicherheits-architektur bereit.

2 Gegenstand und Geltungsbereich

Dieses Dokument beschreibt eine empfohlene Zielarchitektur sowie bewährte Maßnahmen zur Gestaltung der IT-Sicherheit im Rahmen der Zusammenarbeit zwischen Auftraggebern und Auftragnehmern in der Lieferkette. Es dient als Orientierung für Unternehmen, die Komponenten oder Systeme entwickeln und/oder liefern, und unterstützt bei der Ableitung geeigneter Sicherheitsmaßnahmen.

Die dargestellten Inhalte stellen keine verpflichtenden Vorgaben dar, sondern basieren auf etablierten Standards und Best Practices (vgl. Kapitel 3). Sie sollen Unternehmen dabei helfen, eine angemessene und risikoorientierte IT-Sicherheitsarchitektur zu implementieren und kontinuierlich weiterzuentwickeln.

Die Empfehlung richtet sich insbesondere an Unternehmen innerhalb der Automobil-Lieferkette, die unter regulatorische Anforderungen wie die NIS 2 Richtlinie fallen oder vergleichbare Relevanzkriterien erfüllen. Dabei werden sowohl produktionsnahe als auch unterstützende IT-Systeme, Anwendungen und Infrastrukturen betrachtet, die für die sichere Leistungserbringung wesentlich sind.

Die Umsetzung der beschriebenen Maßnahmen liegt in der Verantwortung der jeweiligen Organisation und sollte unter Berücksichtigung individueller Rahmenbedingungen, Risiko-bewertungen sowie geltender gesetzlicher und regulatorischer Anforderungen erfolgen.

2.1 Absicherung der Lieferkette durch TISAX

- Der Aufbau einer gleichartigen, sichere IT-Umgebung innerhalb der gesamten Lieferkette mittels einer resilienten IT-Sicherheitsarchitektur. Diese soll aktuelle und zukünftige Cyber-Bedrohungen proaktiv adressieren und geschäftskritische Prozesse schützen.

- Stärkung der Cyber-Resilienz in der Lieferkette durch Umsetzung angemessener Sicherheitsmaßnahmen.
- Die Verringerung von Betriebsrisiken, um Produktionsausfälle, Datenverluste und wirtschaftliche Schäden zu verhindern.
- Die Anforderungen werden in Form von Kennzahlen messbar gemacht und bieten damit die Möglichkeit einer Selbstbewertung für die jeweiligen Unternehmen. Zudem lassen sich Handlungsbedarfe innerhalb der Unternehmen ableiten und ermöglichen diesen, sich sukzessive in Richtung „Cyber-Exzellenz“ weiterzuentwickeln.

Um den Schutz gegen diese Bedrohungen effektiv zu gestalten, ist es essenziell, die zentralen Gefährdungsszenarien zu kennen. Die nachfolgende Tabelle fasst die wichtigsten Szenarien zusammen, beschreibt kurz die wesentlichen Risiken und nennt die priorisierten Maßnahmen zur Abwehr. Darüber hinaus werden die relevanten Kapitel des Dokuments aufgeführt, so dass bei Bedarf eine vertiefte Auseinandersetzung mit den einzelnen Themen möglich ist.

Gefährdungsszenario	Wichtigste Maßnahmen	Schutzziele	Verweise auf Kapitel
Manipulation der Produktion & industriellen Steuerung	• OT-Netzhärtung • Strenge Zugriffs- und Kommunikationskontrollen • OT-Monitoring	• Verfügbarkeit • Integrität	Kapitel 5: • 5.1 • 5.2 • 5.4 • 5.7
Schadsoftware Ausbreitung zwischen Systemwelten (IT, OT & Cloud)	• Mikrosegmentierung • Least-Privilege-Prinzip • Anomalie-Monitoring	• Vertraulichkeit • Verfügbarkeit • Integrität	Kapitel 4, 5 & 6: • 4.1 • 4.2.1 • 5.1 • 5.4 • 5.7
Standortübergreifende Schadsoftware-Verbreitung	• Netzwerksegmentierung und Zoning • Sichere VPN-Nutzung • Anti-Schadsoftware und EDR	• Vertraulichkeit • Verfügbarkeit	Kapitel 4
Backup-Verschlüsselung durch Schadsoftware	• 3-2-1-1 Backup-Strategie • Verschlüsselung und Zugriffskontrolle • Wiederherstellungstests	• Verfügbarkeit • Integrität	Kapitel 4, 5 & 6: • 4.5.4 • 5.6
Phishing-Angriff (z.B. auf CAD-Daten)	• MFA und starke Authentifizierung • Security-Awareness (Social Engineering) • Zugriffskontrollen	• Vertraulichkeit	Kapitel 4: • 4.1.1 • 4.3.2 • 4.5.2

Einschleusung von Schadsoftware via USB-Geräte & Mobile Devices	• Device Control auf Endpunkten • Einschränkung und Überwachung von USB-Geräten • Zugriffskontrollen	• Verfügbarkeit	Kapitel 4 & 5: • 4.4.2 • 4.5.2 • 4.1 • 5.2
Angriffsszenarien auf KI-Systeme	• Absicherung und Monitoring von KI-Modellen • Mitarbeiterschulung • Einsatz von KI-Detektionssystemen	• Vertraulichkeit • Verfügbarkeit	Kapitel 7

3 Definitionen und Standards

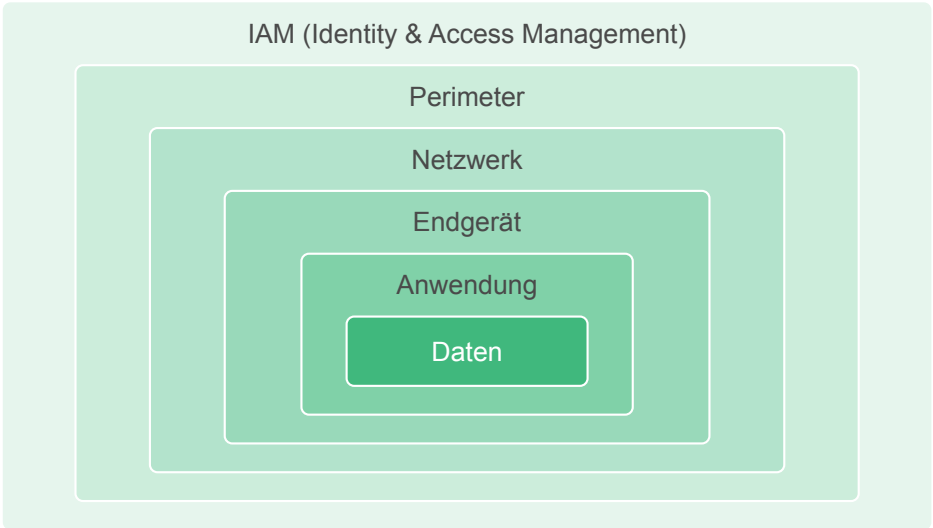
Dieses Kapitel legt die konzeptionelle und normative Grundlage für die folgenden Architekturempfehlungen. Es erläutert die fundamentalen Sicherheitsprinzipien, gibt einen Überblick über die wichtigsten Standards und beschreibt das generische Architekturmodell, das als roter Faden für dieses Dokument dient.

3.1 Fundamentale Sicherheitsprinzipien

3.1.1 Defense-in-Depth

Defense-in-Depth bedeutet, dass man sich nicht auf eine einzige Sicherheitsmaßnahme erlässt. Stattdessen werden mehrere unabhängige Schutzschichten aufgebaut, ähnlich wie bei einer Zwiebel oder einer Burg, die aus mehreren Verteidigungsringen besteht.
Ein Angreifer muss jede Schicht einzeln überwinden. Das macht Angriffe schwieriger, verlangsamt sie und gibt mehr Zeit, um sie zu erkennen und zu stoppen.

Defense-in-Depth Schalenmodell



Zu diesen Schichten gehören:

- Technische Maßnahmen (z. B. Firewalls, Verschlüsselung)
- Administrative Maßnahmen (z. B. Richtlinien, Schulungen)
- Physische Maßnahmen (z. B. Zugangskontrollen)

Fällt eine Schutzschicht aus, greift die nächste. Dadurch entsteht mehr Stabilität und keine einzelne Sicherheitskomponente ist allein entscheidend. Eine besondere Rolle spielt das Identity and Access Management (IAM)[1]. Sie zieht sich durch alle Schichten und steuert, wer worauf zugreifen darf. Deshalb ist eine gute Absicherung des IAM besonders wichtig, es ist eine zentrale Schlüsselkomponente im gesamten Sicherheitskonzept.

3.1.2 Zero-Trust-Architektur

Die Zero-Trust-Architektur unterscheidet sich grundlegend von klassischen Sicherheitsmodellen. Statt einem „inneren“ Netzwerk automatisch zu vertrauen, geht Zero-Trust davon aus, dass kein Zugriff per se vertrauenswürdig ist, egal, ob er von innen oder außen kommt.
Das zentrale Prinzip lautet daher: **„Never trust, always verify“** – niemals vertrauen, immer überprüfen. Jeder Zugriff auf Daten, Anwendungen, Geräte oder Netzwerke muss geprüft werden.

Dies umfasst unter anderem:

- die Überprüfung von Identitäten,
- die Sicherheitsbewertung der Endgeräte,
- die Klassifizierung der angeforderten Daten,
- sowie die Anwendung von Richtlinien nach dem Least-Privilege-Prinzip.

Zero-Trust lässt sich nicht durch ein einziges Produkt oder eine einzelne Maßnahme einführen. Es handelt sich um einen mehrjährigen Transformationsprozess, bei dem viele Bausteine zusammenspielen. Wichtige Elemente, wie sie in diesem Dokument beschrieben sind, etwa Mikrosegmentierung, starke Authentifizierung und umfassendes Monitoring bilden dafür zentrale Bestandteile und unterstützen den Weg hin zu einer echten Zero-Trust-Haltung.

3.2 Übersicht relevanter Standards

Die folgende Übersicht erläutert kurz die für die Automobilindustrie relevantesten Standards, Normen und Gesetze. Die Markierungen **[IT]**, **[OT]**, **[Cloud]** und **[KI]** zeigen den jeweiligen primären Einsatzbereich an. Die hervorgehobenen Standards sind für diese Empfehlung von besonderer Relevanz.

[1] *Im Rahmen des Defense-in-Depth-Ansatzes bildet der Identitätsanteil (Identity and Access Management - IAM) eine zentrale, querschnittliche Sicherheits-Sicherheitsebene, die den kontrollierten Zugriff auf Informationen und Systeme sicherstellt. Identitäten stellen den primären Kontrollpunkt für nahezu alle Zugriffe auf Systeme, Daten und Dienste dar. Ein kompromittiertes oder schwach abgesichertes IAM hebelt nachgelagerte Sicherheitsmaßnahmen effektiv aus. Umgekehrt ermöglicht ein robustes IAM die konsequente Durchsetzung von Least Privilege, Zero-Trust-Prinzipien und die frühzeitige Erkennung von Missbrauch, wodurch das Gesamtrisiko signifikant reduziert und die Wirksamkeit des Defense-in-Depth-Ansatzes maßgeblich gestärkt wird.*

Kernstandards

- **ISO/IEC 27001 [IT] [Cloud] [OT] [KI]:** Der international führende Standard für Informationssicherheits-Managementsysteme (ISMS). Er bietet einen risikobasierten Rahmen für Aufbau, Betrieb und kontinuierliche Verbesserung der Informationssicherheit in einer Organisation und ist die Grundlage für viele andere Zertifizierungen.
- **TISAX (VDA ISA) [IT] [OT]:** Ein etablierter, branchenspezifischer Prüf- und Austauschmechanismus der Automobilindustrie, der auf den Anforderungen des VDA ISA Katalogs basiert. Dieser spiegelt den aktuellen Stand der Technik wider, basiert auf der ISO/IEC 27001 und beinhaltet Risiko-orientiert definierte Sicherheitsmaßnahmen.
- **IEC 62443 [OT]:** Der zentrale internationale Standard für die Cybersicherheit von „Industrial Automation and Control Systems“ (IACS). Er bietet einen umfassenden Rahmen für Betreiber, Integratoren und Hersteller zur Absicherung von Produktionsumgebungen und definiert unter anderem das Zonen- und Conduit-Modell.
- **Center for Internet Security (CIS) Controls & Benchmarks [IT] [OT] [Cloud]:** Eine priorisierte und praxisorientierte Sammlung von technischen Schutzmaßnahmen (Controls) und Konfigurationsanleitungen (Benchmarks). Sie gelten als Goldstandard für Systemhärtung und ergänzen Managementsysteme wie ISO/IEC 27001 auf operativer Ebene.

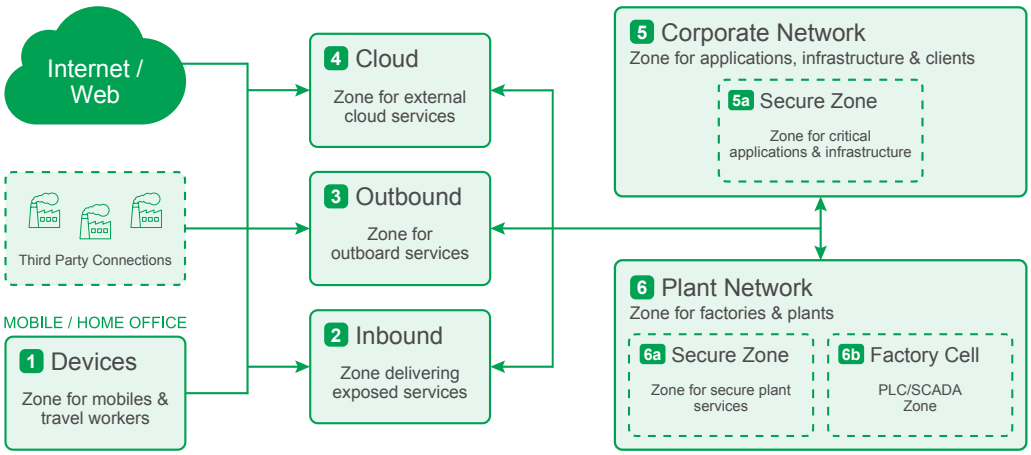
Weitere wichtige Standards und Regularien

- **BSI IT-Grundschutz (BSI 200-Serie) [IT] [OT] [Cloud]:** Der Standard des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Methodik des Sicherheitsmanagements. Er bietet neben einer Vorgehensweise analog zu ISO/IEC 27001 auch umfangreiche Kataloge mit konkreten Maßnahmen für typische IT-Systeme und Szenarien.
- **NIST SP 800 Series [IT] [OT] [Cloud]:** Eine Reihe von Publikationen des US-amerikanischen National Institute of Standards and Technology, die Best Practices für Cybersicherheit abdecken. Besonders relevant sind **SP 800-53** (umfangreicher Maßnahmenkatalog) und **SP 800-82** (Guide to Industrial Control Systems Security).
- **NIS-2-Richtlinie [IT] [OT]:** Eine EU-weite Gesetzgebung zur Erhöhung der Cybersicherheit von „wesentlichen“ und „wichtigen“ Einrichtungen, zu denen viele Unternehmen der Automobilbranche zählen. Sie fordert die Umsetzung von Risikomanagementmaßnahmen und die Meldung von erheblichen Sicherheitsvorfällen.
- **Cyber Resilience Act (CRA) [IT] [OT]:** Ein neues EU-Gesetz, das grundlegende Cybersicherheitsanforderungen für alle Produkte mit digitalen Elementen vorschreibt. Hersteller müssen die Sicherheit über den gesamten Lebenszyklus eines Produkts gewährleisten.
- **Datenschutz-Grundverordnung (DSGVO) [IT] [Cloud] [KI]:** Eine EU-Verordnung, die den Schutz personenbezogener Daten regelt. Sie ist bei allen Maßnahmen relevant, bei denen persönliche Informationen verarbeitet werden.
- **ISO/IEC 27017 [Cloud]:** Ein Leitfaden, der die Maßnahmen der ISO 27002 um spezifische Kontrollen für Cloud-Dienste ergänzt. Er schafft Klarheit über die geteilte Verantwortung zwischen Cloud-Anbieter und Cloud-Kunde.

- **ISO/IEC 27018 [Cloud]:** Ein Verhaltenskodex, der sich speziell auf den Schutz von personenbezogenen Daten (PII) in öffentlichen Cloud-Umgebungen konzentriert.
- **Cloud Security Alliance (CSA) - STAR / CCM [Cloud] [KI]:** Eine führende Organisation, die mit dem „Cloud Controls Matrix“ (CCM) einen umfassenden Kontrollkatalog für Cloud-Sicherheit bietet. Das STAR-Register ermöglicht Transparenz über die Sicherheitsmaßnahmen von Cloud-Anbietern.
- **BSI C_5 (Cloud Computing Compliance Controls Catalogue) [Cloud]:** Ein Anforderungskatalog des BSI, der Mindestanforderungen an die Sicherheit von Cloud-Diensten definiert und oft von deutschen Unternehmen und Behörden gefordert wird.
- **SOC 2 Typ II [Cloud]:** Ein Prüfungsbericht, der von einem unabhängigen Wirtschaftsprüfer erstellt wird und die Wirksamkeit der internen Kontrollen eines Dienstleisters (z.B. Cloud-Anbieter) über einen längeren Zeitraum bescheinigt.
- **ISO/IEC 42001 [KI]:** Der erste internationale Standard für Managementsysteme für Künstliche Intelligenz. Er hilft Organisationen, KI-Systeme verantwortungsvoll zu entwickeln, bereitzustellen und zu nutzen.
- **EU AI Act [KI]:** Die weltweit erste umfassende Regulierung für Künstliche Intelligenz. Sie klassifiziert KI-Systeme nach ihrem Risiko und legt je nach Stufe strenge Anforderungen an Entwicklung, Transparenz und Überwachung fest.
- **MITRE ATT&CK® Framework [IT] [OT] [Cloud]:** Eine global zugängliche Wissensdatenbank über Taktiken und Techniken von Angreifern, basierend auf realen Beobachtungen. Sie ist extrem wertvoll für die Priorisierung von Abwehrmaßnahmen und die Simulation von Angriffen.
- **Stand der Technik von TeleTrusT:** Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) veröffentlicht regelmäßig Dokumente, die den „Stand der Technik“ für bestimmte Sicherheitsbereiche definieren, was insbesondere im Rahmen der DSGVO und anderer Gesetze eine wichtige Orientierung bietet.

3.3 Generisches Architekturmodell

Das folgende „Sechs-Zonen-Modell“ fasst logische Bereiche eines typischen Unternehmensnetzwerks zusammen und dient als Grundlage für die Zuordnung von Schutzmaßnahmen zu den jeweiligen Verantwortungsbereichen.



Die sechs Zonen der Referenz-Sicherheitsarchitektur

- **Zone 1 – Devices (Mobile / Homeoffice):** Beinhaltet alle Endgeräte, die sich außerhalb des Kernnetzwerks befinden. Dies umfasst Laptops von „Road Warriors“, fest eingerichtete Home-Office-Arbeitsplätze und mobile Geräte wie Tablets und Smartphones.
- **Zone 2 – Inbound:** Diese Zone, oft als Demilitarisierte Zone (DMZ) bezeichnet, dient der kontrollierten Bereitstellung von Diensten, die aus dem Internet erreichbar sein müssen. Beispiele sind VPN-Gateways, Reverse Proxies für Webanwendungen oder E-Mail-Server.
- **Zone 3 – Outbound:** Die Gegenrichtung zur Inbound-Zone, kann auch als DMZ für eine kontrollierten Kommunikation „nach außen“ bezeichnet werden, d.h. von internen Systemen zu Zielen im Internet, wie z.B. für den Abruf von Software-Updates, die Nutzung von Threat Intelligence Feeds oder die Synchronisation mit Zeitservern.
- **Zone 4 – Cloud:** Repräsentiert die logische Erweiterung des Unternehmensnetz werks in die Public Cloud. Diese Zone umfasst alle genutzten Dienste, sei es Infra-struktur (IaaS), Plattformen (PaaS) oder Software-as-a-Service (SaaS).
- **Zone 5 – Corporate Network:** Das klassische Büro- und Verwaltungsnetzwerk. Es beherbergt die Clients der Mitarbeiter, die zentrale IT-Infrastruktur (z.B. Active Directory, Fileserver) und kritische Geschäftsanwendungen wie das ERP-System.
- **Zone 6 – Plant Network:** Das Produktionsnetzwerk (OT). Es ist streng vom Corporate Network getrennt und enthält die Anlagen und Maschinensteuerungen. Innerhalb dieser Zone gibt es oft weitere Unterteilungen in sogenannte „Factory Cells“, die einzelne Produktionslinien oder -bereiche umfassen und Systeme wie Speicher-programmierbare Steuerungen (SPSen) oder Bedieneinheiten (SCADA/HMI) beinhalten[2].

Die folgenden Kapitel enthalten eine detaillierte Beschreibung der spezifischen Schutzmaßnahmen für jede dieser Zonen.

4 IT Security

Dieses Kapitel soll die IT Security nicht vollumfänglich abdecken, sondern besonders wichtige Themen im Zusammenhang mit der IT-Sicherheitsarchitektur darstellen:

- Identity and Access Management (IAM)
- Netzwerksicherheit
- Kommunikationssicherheit
- Endpoint Security
- Datensicherheit
- Applikationssicherheit

[2] *Factory Cells beziehen sich auf Netzwerk-Segmente und können sich über mehrere physischen Produktionsanlagen erstrecken. Der Begriff „Zelle“ kann für beides Aspekte verwendet werden, muss hier jedoch im Kontext betrachtet werden.*

Asset Management und Vulnerability Management sind grundlegende Voraussetzungen für eine cyberresiliente Architektur und damit von elementarer sicherheitsarchitektonischer Bedeutung. Ihre organisatorische, prozessuale und methodische Ausgestaltung erfolgt jedoch im Rahmen des Informationssicherheits-Managementsystems (ISMS) und ist damit Bestandteil der TISAX-Anforderungen. Dieses Kapitel betrachtet primär die architektur-relevanten Maßnahmen.

Die Defense-in-Depth-Architektur gemäß Kapitel 3.1.1 durchzieht alle Bereiche mit den vier Phasen: Prävention (Angriffe verhindern), Detektion (Bedrohungen erkennen), Reaktion (auf Vorfälle reagieren) und Kompensation (Schäden begrenzen).

In den folgenden Kapiteln sind Quick Wins pro Maßnahmenblock jeweils hervorgehoben und ermöglichen kurzfristige Sicherheitsverbesserungen mit minimalem Aufwand.

Standard-Maßnahmen bilden das operative Rückgrat, während erweiterte Ausbaustufen Wachstumspfade für größere Organisationen aufzeigen.

4.1 Generisches Architekturmodell

4.1.1 Remove reporting obligations for downstream users

Kurz erklärt und Risiken: Schwache Authentifizierung, vor allem gestohlene Passwörter, ist der häufigste Angriffsvektor. Mehrfaktor-Authentifizierung kombiniert mindestens zwei unabhängige Faktoren (Wissen, Besitz oder Biometrie) und senkt die Wahrscheinlichkeit einer Account-Übernahme deutlich. MFA ist die wirksamste Präventionsmaßnahme für alle Zugriffe, besonders in Zone 1 (Devices) und Zone 4 (Cloud).

Top-Maßnahmen

- Hohe Priorität: Obligatorische MFA für alle administrativen und anderen privilegierten Accounts
- Quick Win: Aktivierung von Authenticator-Apps (Time-based One-Time Passwords - TOTP) für alle Accounts mit administrativen und anderen privilegierten Berechtigungen sowie für Remote-Zugriffe

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Verpflichtende MFA für alle Accounts mit erhöhten Berechtigungen: Administratoren, kritische Geschäftsanwendungen, Remote-Verbindungen
- Authenticator-Apps als kostengünstige Einstiegslösung, Hardware-Token als einen Faktor der MFA für besonders sensitive Bereiche
- Zentrale Authentifizierung über standardisierte Protokolle (OAuth2, OpenID Connect) zur Reduzierung von Komplexität und Verwaltungsaufwand

2. Überwachung und Erkennung

- Kontinuierliches Monitoring von Authentifizierungsversuchen auf Angriffsmuster

- Alarmierung bei ungewöhnlichen Login-Zeiten, Zugriffen aus fremden Regionen oder wiederholten Fehlversuchen
- Anbindung der Authentifizierungsprotokolle an zentrale Auswertung (vgl. Security Monitoring in 4.1-B)

3. Reaktion bei Vorfällen

- Bei Verdacht auf Account-Kompromittierung: Alle Authentifizierungs-mechanismen für den kompromittierten Account sofort ungültig machen („invalidieren“), insbesondere sofortige Beenden aller aktiven Sessions („Session-Invalidierung“) und das Sperren/Widerrufen sämtlicher Credentials, Tokens oder anderer Authentifikatoren, die dem Konto zugeordnet sind.

  (Hinweis: Wenn Verdacht ausschließlich aufgrund zu vieler Anmeldeversuche: Temporäre Sperrung anstatt dauerhafter Sperrung des Accounts)

4. Wiederherstellung und Kontinuität

- Backup-Authentifizierungsmethoden und sichere Registrierungsprozesse („Enrollment“) für neue Geräte und Nutzer implementieren
- Kombination verschiedener MFA-Methoden verhindert Totalausfall. Allerdings erhöht jede zusätzliche Methode den Verwaltungsaufwand, besonders bei kleineren IT-Teams
- Zero-Trust-Identity-Architektur mit kontinuierlicher Verifikation als langfristiges Ziel

Lessons Learned

- MFA nur für externe Zugriffe reicht nicht: Ohne interne MFA wird laterale Bewegung von Angreifern nicht verhindert
- Stufenweise Einführung beginnend mit kritischen Systemen erhöht die Benutzerakzeptanz und ermöglicht Erfahrungssammlung
- Ohne begleitende Schulungen scheitert die Einführung: Benutzerakzeptanz ist ausschlaggebend
- SSO-Integration minimiert die Anzahl erforderlicher Authentifizierungen und reduziert Reibungsverluste

4.1.2 Privileged Access Management (PAM)

Kurz erklärt und Risiken: Privilegierte Konten (Administratoren, Service-Accounts) sind das bevorzugte Ziel von Angreifern. Ihr Missbrauch kann schwerwiegende Auswirkungen in Zone 5 (Corporate) und Zone 6 (Plant Network) haben. PAM implementiert das Prinzip der minimalen Berechtigung (Least Privilege): keine permanenten Administratorrechte, alle Zugriffe nur zeitlich begrenzt (Just-in-Time) und individuell nachvollziehbar.

Top-Maßnahmen

- Hohe Priorität: Just-in-Time-Access für alle Administratorkonten: keine dauerhaften Administratorrechte

- Quick Win: Vorhandene Anmeldungsprotokolle systematisch auf Anomalien bei privilegierten Konten auswerten: ungewöhnliche Uhrzeiten, Mehrfach-Logins, fremde Standorte (manuell oder per einfachem Skript)

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Vollständige Inventarisierung aller privilegierten Accounts im Unternehmen
- Shared Administrative Accounts durch individuelle, eindeutig zuweisbare Benutzerkonten ersetzen. Jede administrative Handlung muss einer natürlichen Person zuordenbar sein. PAM-verwaltete Notfall-Accounts (Break-Glass), bei denen Zugriffe zeitlich begrenzt, automatisch rotiert und individuell protokolliert werden, gelten nicht als „Shared Accounts“ im Sinne dieser Anforderung
- Service Accounts mit dedizierten, starken Credentials und regelmäßiger automatischer Rotation
- Separate Administrationsumgebungen: IT-Umgebungen und OT-Umgebungen (insbesondere bei OT-Umgebungen mit industriellen Steuerungssystemen („SCADA“))

2. Überwachung und Erkennung:

- Protokollierung aller privilegierten Sitzungen als Mindestanforderung. Jede administrative Aktion muss nachvollziehbar und auditierbar sein
- Auswertung je nach Unternehmensgröße: von manueller Stichproben-prüfung bis hin zur Anbindung an ein SIEM-System (Security Information and Event Management)
- Für Unternehmen ohne eigenes Security Operations Center (SOC): Managed-SOC-Dienste als wirtschaftliche Alternative zum Aufbau eigenen Fachpersonals
- Verhaltensbasierte Anomalie-Erkennung (ehem. UBA): Erstellung von Baseline-Profilen für privilegierte Benutzer (Arbeitszeiten, typische Zugriffsmuster, übliche Anwendungen). Alarmierung bei Abweichungen, etwa ungewöhnliche Login-Zeiten, Zugriffe auf fremde Datenbestände oder abnormale Downloadmengen. Die Kalibrierung der Schwellwerte erfordert erfahrungsgemäß mehrere Iterationen
- Zentrale Service-Account-Vault mit automatischer Credential-Rotation als erweiterte Maßnahme

3. Reaktion bei Vorfällen

- Bei Verdacht auf Missbrauch: Sperrung alle privilegierten Zugriffe, einzelne Accounts ebenso wie ganze Benutzergruppen
- Abgestufte Reaktion bei Anomalien: von zusätzlichen Authentifizierungs-anforderungen bis zur temporären Account-Sperrung
- Sperrung muss auch SCADA-Zugriffe und OT-Systeme einschließen, um laterale Bewegung in Produktionsumgebungen zu verhindern

- Bei Account-Kompromittierungen, die sich über Zonengrenzen ausbreiten können: Sperrung betroffener Identitäten. Organisatorische Einbettung im Rahmen des Incident Management

4. Wiederherstellung und Kontinuität

- Zentrale Credential-Verwaltung in verschlüsselten Vaults für Zugriffskontinuität bei Personalwechseln oder Notfällen
- Automatisierte Credential-Rotation reduziert das Risiko durch kompromittierte Passwörter
- Notfallzugänge (Break-Glass-Accounts) eingeplant und getestet

Lessons Learned

- PAM ohne ausreichende Notfallzugänge kann im Ernstfall kritische Systeme unzugänglich machen
- Automatisierte Credential-Rotation schrittweise einführen, beginnend mit Test-/Entwicklungssystemen, um Anwendungsabhängigkeiten zu erkennen
- Fokussierung der Anomalie-Erkennung nur auf technische Metriken ohne geschäftlichen Kontext erzeugt Fehlalarme. Integration von HR-Informationen (Urlaub, Projektwechsel, Rollenwechsel) reduziert Fehlalarme deutlich
- Pilotprojekte mit unkritischen Systemen ermöglichen Erfahrungssammlung ohne Betriebsunterbrechungen
- Integration in bestehende Active-Directory-Infrastrukturen oder Cloud-Identity-Provider vereinfacht die Implementierung

4.2 Netzwerksicherheit

4.2.1 Mikrosegmentierung und Zero-Trust-Architektur

Kurz erklärt und Risiken: Die traditionelle Perimeter-Sicherheit versagt bei bereits eingedrungenen Angreifern. Mikrosegmentierung unterteilt das Netzwerk in granulare Sicherheitszonen, vor allem zur strikten Trennung von Zone 5 (Corporate) und Zone 6 (Plant Network). Jede Verbindung muss explizit verifiziert werden, was das Zero-Trust-Prinzip auf die Netzwerkebene überträgt.

Top-Empfehlungen:

- Hohe Maßnahmen: Netzwerkzonen je Standort definieren: getrennte Bereiche für IT, OT und Sicherheitsinfrastruktur
- Quick Win: Statische VLAN-basierte (VLAN = Virtual Local Area Network) Grundsegmentierung für kritische Systeme, kombiniert mit expliziten Firewall-Regeln zwischen den VLANs (keine unkontrollierte Inter-VLAN-Routierung)

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Trennung kritischer Netzwerksegmente durch VLANs und Firewalls: Produktionsnetze strikt von Office-IT trennen, Gäste- und IoT-Netzwerke isolieren
- Sicherstellen, dass nur vertraute & bekannte Geräte Zugriff zum Netzwerk bekommen. Default-Deny-Richtlinien: alle Verbindungen blockieren, die nicht explizit erlaubt sind
- Umfassende Dokumentation aller Netzwerkflüsse als Grundlage für Segmentierungsrichtlinien
- Vordefinierte Isolationsszenarien für verschiedene Bedrohungstypen, dokumentiert und getestet, sodass im Ernstfall keine manuelle Konfiguration nötig ist

2. Überwachung und Erkennung

- Metadaten-basierte Analyse im Vordergrund: Verbindungspartner, Protokolle, Datenvolumen und Verbindungszeiten auswerten, ohne verschlüsselten Inhalt aufzubrechen
- Signaturbasierte Erkennung und Schwellwert-Alerts auf Basis von Verbindungsmetadaten als solider Grundschutz
- Erweiterte Verhaltensanalysen für Organisationen mit SOC-Kapazität. Erheblichen Tuning-Aufwand und initiale Fehlalarmraten einplanen
- Echtzeit-Dashboard über Netzwerkstatus und aktive Quarantäne-Maßnahmen

3. Reaktion bei Vorfällen

- Reaktion typischerweise auf Host-Ebene: kompromittierte Endgeräte per NAC oder Switch-Port-Deaktivierung isolieren
- Abschaltung ganzer Netzsegmente nur in Extremfällen (z.B. Ransomware-Ausbruch)
- Moderne Angreifer bewegen sich vorwiegend über legitime Protokolle (RDP, SMB, WinRM, PowerShell Remoting). Reine Traffic-Anomalie-erkennung allein reicht nicht aus, sondern muss durch EDR und identitätsbasierte Maßnahmen ergänzt werden
- Mehrstufige Isolationsverfahren: von Switch-Port-Deaktivierung bis zu Standort-Abschottung. Eskalationspfade und Entscheidungsträger vorab definieren
- Für KMU ohne SDN (Software-Defined Networking): Switch-Port per vordefiniertem Skript deaktivieren und Host vom WLAN trennen ist ein praktikabler erster Schritt

4. Wiederherstellung und Kontinuität

- Redundante Netzwerkpfade und alternative Routing-Mechanismen für Geschäftskontinuität bei Isolation einzelner Segmente

- Business-Continuity-Pläne für verschiedene Isolationsszenarien mit alternativen Arbeitsprozessen
- Stufenweise Wiederanbindung isolierter Bereiche nach erfolgreicher Bereinigung. Sauberkeitsprüfung vor Aufhebung der Quarantäne
- SOAR-gestützte Automatisierung (Security Orchestration, Automation and Response) als erweiterte Maßnahme für größere Organisationen

Lessons Learned

- Zu restriktive Segmentierung ohne Geschäftsprozess-Analyse führt zu Betriebsunterbrechungen und Umgehungsversuchen
- Alle Isolationsszenarien regelmäßig testen: Ungetestete Notfallverfahren versagen im Ernstfall
- Parallele Kommunikationskanäle für Notfälle einplanen: Betroffene und Management müssen bei Netzwerk-Isolation rechtzeitig informiert werden
- Regelmäßige Penetrationstests validieren die Wirksamkeit der Segmentierung

4.2.2 Netzwerk-Traffic-Analyse und Monitoring

Kurz erklärt und Risiken: Network Traffic Analysis (NTA) erkennt Bedrohungen, die Perimeter-basierte Maßnahmen umgehen, indem der interne Ost-West-Verkehr innerhalb der Zonen 5 (Corporate Network) und 6 (Plant Network) analysiert wird. NTA ist eine wichtige Komponente im Rahmen des Security Monitorings (vgl. SOC/SIEM in Abschnitt 4.1).

Top-Maßnahmen

- Hohe Priorität: Vollständige Netzwerk-Sichtbarkeit mit Ost-West-Traffic-Monitoring, nicht nur Perimeter-Verkehr
- Quick Win: DNS-basierte Schutzfilter auf Router oder Firewall aktivieren. Blockiert bekannte bösartige Domains und Command-and-Control-Kommunikation mit minimalem Aufwand
- Quick Win: Automatisierte Alarmierung bei kritischen Traffic-Anomalien (z.B. ungewöhnlich hohe Datenvolumen, Verbindungen zu bekannten bösartigen IPs) über vorhandene Firewall- oder Switch-Funktionen

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Network Taps und Switch Port Mirroring für vollständige Erfassung des Netzwerkverkehrs ohne Performance-Beeinträchtigung
- Flow-basierte Analyse zur Erkennung ungewöhnlicher Kommunikations-muster zwischen Netzwerksegmenten
- DNS-Monitoring zur Erkennung von Command-and-Control-Kommunikation über DNS-Tunneling
- Bandbreiten-Monitoring zur Erkennung ungewöhnlicher Datenübertragungen (mögliche Exfiltration)

2. Überwachung und Erkennung

- Baseline-Profile für normale Netzwerkaktivitäten erstellen und Abweichungen automatisch erkennen
- Korrelation von Netzwerkaktivitäten mit Benutzerverhalten
- Nutzung von NTA-Daten für proaktive Bedrohungssuche und Incident-Untersuchungen
- Tuning-Zyklen einplanen: Erkennungsraten optimieren und Fehlalarme systematisch reduzieren

3. Reaktion bei Vorfällen

- Automatisierte Blockierung oder Weiterleitung verdächtiger Verbindungen zur manuellen Analyse
- Integration mit SIEM-System für korrelierte Alarmierung (vgl. Security Monitoring in 4.1)
- Forensische Datenaufbewahrung für detaillierte Incident-Analysen und rechtliche Anforderungen

4. Wiederherstellung und Kontinuität

- Verteilte NTA-Sensoren für Monitoring-Kontinuität bei Ausfall einzelner Komponenten
- Archivierung historischer Traffic-Daten für retrospektive Analysen und Trend-Erkennung
- Backup von NTA-Konfigurationen für schnelle Wiederherstellung nach Systemausfall

Lessons Learned

- Fokussierung nur auf Nord-Süd-Traffic lässt laterale Bewegungen unentdeckt. Ost-West-Monitoring darf nicht fehlen
- Vollständige Netzwerk-Sichtbarkeit inklusive interner Segmente ist Voraussetzung für die Erkennung fortgeschrittener Bedrohungen
- Implementierung mit kritischen Segmenten beginnen und schrittweise ausweiten

4.2.3 Bot-Detection und Rate-Limiting

Kurz erklärt und Risiken: Automatisierte Angriffe (Credential Stuffing, DDoS, Web Scraping) werden durch Bot-Netzwerke durchgeführt und umgehen traditionelle IP-basierte Schutzmaßnahmen. Bot-Detection ist relevant für alle exponierten Architekturbestandteile in Zone 2 (Inbound) und Zone 4 (Cloud/API).

Top-Maßnahmen

- Hohe Priorität: Adaptive Ratenbegrenzung basierend auf Risikobewertung, nicht nur statische Schwellwerte

- Quick Win: IP-Reputation-Listen („Black-Listing“) aktivieren. Die meisten Firewalls und Reverse-Proxies bieten integrierte Feeds bekannter Bot-Netzwerke.

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- IP-basierte Rate-Limits für Requests pro Zeiteinheit und IP-Adresse
- User-Agent-Analyse zur Erkennung bekannter Bot-Signaturen und automatisierter Werkzeuge
- Session-basierte Limits gegen Credential Stuffing (Begrenzung von Login-Versuchen pro Session)
- Geo-Blocking als zusätzliche Filterschicht für Regionen mit hohem Bot-Aufkommen

2. Überwachung und Erkennung

- Verhaltensbasierte Erkennung unnatürlicher Klick-Muster und Navigationsverhalten
- Device Fingerprinting zur Erkennung automatisierter Werkzeuge anhand von Browser- und System-Charakteristika
- Integration externer Bot-Reputation-Datenbanken für proaktive Sperrung

3. Reaktion bei Vorfällen

- Abgestufte Reaktion: von CAPTCHA-Challenges über temporäre Drosselung bis zur IP-Sperrung
- Honeypot-Systeme zur Sammlung von Informationen über Angriffsmuster
- Automatisches Hinzufügen erkannter Bot-IPs zu Sperrlisten

4. Wiederherstellung und Kontinuität

- Whitelist-Mechanismen für legitime automatisierte Zugriffe (APIs, Partner-Systeme)
- Schnelle Entsperrung fälschlicherweise blockierter Benutzer (False-Positive-Handling)
- Lastverteilung zur Vermeidung von Überlast bei Bot-Angriffen

Lessons Learned

- Zu aggressive Ratenbegrenzung blockiert Power-User und API-Clients. Geschäftsauswirkung durch Überblockierung einkalkulieren
- Adaptive Ratenbegrenzung mit Whitelist für bekannte gute Akteure balanciert Sicherheit und Nutzbarkeit
- Bot-Detection-Maßnahmen werden meist auf der WAF implementiert. Verzahnung mit WAF-Konfiguration (vgl. 4.5-B) sicherstellen

4.3 Kommunikationssicherheit

4.3.1 VPN-Sicherheit und Remote-Access

Kurz erklärt und Risiken: Homeoffice und Remote Work verschieben den Perimeter in Zone 1 (Devices). VPN-Infrastrukturen werden damit zum häufigen Angriffsziel. Zero-Trust Network Access (ZTNA) bezeichnet eine Architektur, bei der jeder Zugriff unabhängig vom Netzwerkstandort individuell verifiziert wird. Im Gegensatz zum klassischen VPN, das Zugang zum gesamten Netz gewährt, beschränkt ZTNA den Zugriff auf einzelne Applikationen basierend auf Benutzeridentität und Gerätestatus.

Top-Maßnahmen

- Hohe Priorität: Deaktivierung veralteter VPN-Protokolle (PPTP, L2TP ohne IPSec, SSLV3) gemäß BSI TR-02102. Als aktuelle Standards kommen IKEv2/IPsec oder WireGuard zum Einsatz. Konfigurationshärtung anhand von CIS Benchmarks
- Quick Win: Geo-Blocking aktivieren. Zugriffe aus Regionen ohne Geschäftstätigkeit blockieren (in den meisten Firewalls als Standard-funktion verfügbar)

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Verschlüsselung konfigurieren: Ausschließlich aktuelle Algorithmen (AES-256, SHA-256+). Perfect Forward Secrecy (PFS) aktivieren. Konfiguration gegen BSI TR-02102 oder CIS Benchmarks prüfen
- Split-Tunneling bewusst entscheiden: Vollständiges Tunneling erhöht die Kontrolle, belastet aber die VPN-Infrastruktur. Split-Tunneling kann für vertrauenswürdige Cloud-Dienste akzeptabel sein, wenn DNS-basiertes Routing und Endpoint-Schutz gewährleistet sind. Entscheidung dokumentieren
- Authentifizierung an vorhandenes Identity-Management anbinden: VPN-Anmeldung über bestehenden Verzeichnisdienst (z.B. Active Directory, LDAP) mit obligatorischer MFA. Separate VPN-Zugangsdaten vermeiden
- Für mobile Nutzer und Home-Office: gerätebasierte Vertrauensmodelle statt IP-Allow-Listing. Nur Endgeräte mit gültigem Client-Zertifikat oder bestätigtem Compliance-Status erhalten VPN-Zugang
- Separate VPN-Profile für verschiedene Benutzergruppen (IT-Administration, OT-Wartung, Remote-Mitarbeiter)

2. Überwachung und Erkennung

- Kontinuierliche Analyse von VPN-Logs: simultane Anmeldungen aus verschiedenen Regionen, abnormale Verbindungszeiten
- Verhaltensbasierte Erkennung von Abweichungen normaler Benutzermuster

- Korrelation von VPN-Zugriffen mit bekannten Bedrohungsindikatoren (vgl. Security Monitoring in 4.1)

3. Reaktion bei Vorfällen

- Automatisierte Sperrmechanismen für verdächtige VPN-Verbindungen mit temporärer Account-Deaktivierung
- Massenhafte Deaktivierung aller VPN-Zugänge binnen Minuten als Notfall-Maßnahme
- Forensische Protokollierung aller Aktivitäten für spätere Incident-Analysen

4. Wiederherstellung und Kontinuität

- Redundante VPN-Gateways in verschiedenen Rechenzentren für Ausfallsicherheit
- Out-of-Band-Management für administrative Zugriffe bei Kompromittierung der Haupt-VPN-Infrastruktur
- Ablösung klassischer VPN-Tunnel durch applikationsspezifischen ZTNA-Zugang als langfristiges Ziel

Lessons Learned

- VPN-Endpoint-Sicherheit allein reicht nicht: Kompromittierte Remote-Geräte gefährden das gesamte Netzwerk. Kombination mit Endpoint Compliance Checking nicht vergessen
- Pilotprojekte mit weniger kritischen Benutzergruppen vor unternehmensweiter Ausrollung
- Performance-Monitoring sicherstellen, damit Sicherheitsverbesserungen die Produktivität nicht beeinträchtigen

4.3.2 E-Mail-Sicherheit

Kurz erklärt und Risiken: Phishing-E-Mails sind der häufigste initiale Angriffsvektor, gerade für KMU, die seltener über dedizierte Security-Teams verfügen. Kompromittierte E-Mail-Accounts ermöglichen Datendiebstahl, Ransomware-Infektionen und Business E-Mail Compromise (BEC), bei dem Angreifer sich als Geschäftsführer oder Lieferant ausgeben und Zahlungen umleiten. E-Mail-Sicherheit umfasst technische Filtermaßnahmen ebenso wie die Absicherung der eigenen Domain gegen Missbrauch.

Top-Maßnahmen

- Hohe Priorität: Aktivierung von SPF, DKIM und DMARC auf allen unternehmenseigenen Domains. Verhindert, dass Angreifer E-Mails im Namen des Unternehmens versenden
- Quick Win: SPF-Record in der DNS-Konfiguration veröffentlichen. Rein DNS-basiert, kostenlos, in wenigen Minuten umsetzbar. Damit wird festgelegt, welche Server E-Mails für die Domain versenden dürfen

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- SPF (Sender Policy Framework): Festlegung autorisierter E-Mail-Server in DNS
- DKIM (DomainKeys Identified Mail): Kryptographische Signatur ausgehender E-Mails zur Integritätsprüfung
- DMARC (Domain-based Message Authentication, Reporting and Conformance): Richtlinie für den Umgang mit E-Mails, die SPF/DKIM-Prüfungen nicht bestehen. Schrittweise von „none“ (nur Reporting) über „quarantine“ bis „reject“ hochfahren
- E-Mail-Filterung: Spam- und Malware-Filter auf dem E-Mail-Gateway oder beim Cloud-Provider aktivieren (bei den meisten Anbietern bereits enthalten)
- Anhang-Beschränkungen: Ausführbare Dateien (.exe, .bat, .ps1, .js) in E-Mail-Anhängen blockieren

2. Überwachung und Erkennung

- DMARC-Reporting auswerten: zeigt Missbrauchsversuche der eigenen Domain und fehlerhafte E-Mail-Konfigurationen
- Überwachung eingehender E-Mails auf bekannte Phishing-Indikatoren: gefälschte Absenderdomains, verdächtige Links, manipulierte Anhänge
- Sensibilisierung der Mitarbeiter: regelmäßige Phishing-Awareness-Schulungen und simulierte Phishing-Tests

3. Reaktion bei Vorfällen

- Schnelle Sperrung kompromittierter E-Mail-Accounts und Zurücksetzung der Credentials
- Benachrichtigung aller Mitarbeiter bei identifizierten Phishing-Kampagnen. Klare Meldewege vorab definieren
- Bei Business E-Mail Compromise: sofortige Kontaktaufnahme mit Banken zur Rückabwicklung betrügerischer Überweisungen

4. Wiederherstellung und Kontinuität

- Backup des E-Mail-Archivs für forensische Analysen und Compliance
- Alternative Kommunikationskanäle für den Fall einer großflächigen E-Mail-Kompromittierung (z.B. vorab definierter Messenger-Kanal)
- DMARC-Richtlinie nach Vorfall auf „reject“ hochstufen, falls noch nicht geschehen

Lessons Learned

- SPF/DKIM/DMARC schützen primär die eigene Domain vor Missbrauch. Eingehende Phishing-Mails von fremden Domains erfordern zusätzlich E-Mail-Filterung

- DMARC schrittweise einführen: erst „none“ (Monitoring), dann „quarantine“, dann „reject“. Sofortiges „reject“ kann legitime E-Mails blockieren
- Phishing-Awareness ist keine einmalige Schulung, sondern ein kontinuierlicher Prozess: regelmäßige Tests zeigen, ob die Schulung wirkt
- Business E-Mail Compromise richtet oft mehr finanziellen Schaden an als Ransomware. Zahlungsfreigabe-Prozesse mit Vier-Augen-Prinzip absichern

4.4 Endpoint Security

4.4.1 Endpoint Detection and Response (EDR)

Kurz erklärt und Risiken: EDR ist die notwendige Weiterentwicklung der klassischen Antivirus-Lösung. Traditionelle signaturbasierte Systeme versagen bei modernen Bedrohungen wie dateiloser Malware und Zero-Day-Exploits. EDR analysiert kontinuierlich das Systemverhalten auf Endpunkten und erkennt verdächtige Aktivitäten anhand von Verhaltensmustern. Besonders relevant für heterogene Endpunkte in Zone 1 (Devices), 5 (Corporate Network) und 6 (Plant Network).

Top-Maßnahmen

- Hohe Priorität: Vollständige EDR-Abdeckung inklusive Server und (soweit möglich) OT-Systeme mit zentraler Management-Konsole
- Quick Win: Vorhandene Endpoint-Protection auf höchste Erkennungsstufe konfigurieren und Alerting an zentrale Stelle (SIEM oder Ticket-System, vgl. Security Monitoring in 4.1) anbinden

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Kontinuierliche System-Telemetrie: Prozessausführung, Dateiänderungen, Netzwerkverbindungen, Registry-Änderungen
- Verhaltensbasierte Erkennung von Angriffstechniken (Process Hollowing, DLL Injection, Credential Dumping)
- Automatische Blockierung verdächtiger Aktivitäten in Echtzeit mit forensischer Datenerfassung

2. Überwachung und Erkennung

- Proaktives Threat Hunting anhand von Threat Intelligence und Indicators of Compromise (IoCs)
- Priorisierung von Sicherheitsereignissen nach Schweregrad und Geschäftsauswirkung
- Systemübergreifende Korrelation zur Erkennung koordinierter Angriffe

3. Reaktion bei Vorfällen

- Automatische oder manuelle Isolation kompromittierter Endpunkte

- Remote-Forensik auf isolierten Systemen (Shell-Zugang, Memory Dumps, Disk Images)

4. Wiederherstellung und Kontinuität

- Rollback schädlicher Änderungen auf bekannt saubere Systemzustände
- Image-basierte Wiederherstellung kritischer Systeme
- XDR-Integration mit Netzwerk- und Cloud-Telemetrie als langfristiges Ziel

Lessons Learned

- EDR ohne SIEM-Anbindung führt dazu, dass Alerts in der Masse untergehen. Zentrale Priorisierung ist unerlässlich
- Stufenweiser Rollout ab kritischen Systemen reduziert Betriebsstörungen und ermöglicht Feintuning der Erkennungsregeln
- Performance-Impact vorab testen: EDR-Agenten dürfen Geschäftsprozesse nicht beeinträchtigen

4.4.2 Device Compliance und Management

Kurz erklärt und Risiken: Device Compliance stellt sicher, dass Endgeräte minimale Sicherheitsstandards erfüllen, bevor sie Zugriff auf Unternehmensressourcen erhalten. Nicht-konforme Geräte (veraltete Betriebssysteme, fehlende Patches, deaktivierter Virenschutz) sind ein häufiges Einfallstor für Angriffe. Mobile Device Management (MDM) und Unified Endpoint Management (UEM) automatisieren diese Prüfungen.

Top-Maßnahmen

- Hohe Priorität: Automatisierte Compliance-Prüfung für alle verwalteten Geräte vor Netzwerkzugang
- Quick Win: Bestehende Gruppenrichtlinien verschärfen: Mindestwerte für Patch-Stand, Antivirus-Aktualität und Bildschirmsperre durchsetzen

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Definition von Compliance-Baselines: OS-Patch-Stand, Antivirus-Signaturen, Festplattenverschlüsselung, Firewall-Status
- Automatische Quarantäne nicht-konformer Geräte in separates VLAN mit Selbsthilfe-Portal
- Regelmäßige Inventarisierung aller Endgeräte inkl. BYOD-Geräte

2. Überwachung und Erkennung

- Kontinuierliche Compliance-Überwachung statt einmaliger Prüfung beim Netzwerkzugang
- Dashboards mit Gesamtübersicht über Compliance-Status der Geräteflotte

- Eskalation bei dauerhaft nicht-konformen Geräten

3. Reaktion bei Vorfällen

- Sofortige Sperrung des Netzwerkzugangs bei kritischen Compliance-Verstößen
- Automatische Benachrichtigung des Gerätebesitzers mit Handlungsanweisung

4. Wiederherstellung und Kontinuität

- Selbsthilfe-Workflows für Benutzer zur eigenständigen Behebung einfacher Compliance-Verstöße
- Eskalationspfade für komplexe Fälle (z.B. veraltete Hardware ohne Update-Möglichkeit)

Lessons Learned

- Compliance-Regeln ohne Selbsthilfe-Portal führen zu hohem Support-Aufwand und Frust bei Mitarbeitern
- BYOD-Geräte in die Compliance-Prüfung einbeziehen: Sie sind häufig der schwächste Endpunkt

4.4.3 Endpoint-Isolation und Quarantäne

Kurz erklärt und Risiken: Bei Verdacht auf Kompromittierung muss der betroffene Endpunkt schnell isoliert werden, um laterale Bewegung im Netzwerk zu verhindern. Automatisierte Quarantäne-Mechanismen, meist über die EDR-Lösung gesteuert, blockieren Netzwerkverbindungen und bewahren gleichzeitig forensische Beweise für die spätere Analyse.

Top-Maßnahmen

- Hohe Priorität: Ein-Klick-Isolation für alle verwalteten Endpunkte über die zentrale EDR-/UEM-Konsole
- KMU ohne EDR: Netzwerkkabel ziehen, Host vom WLAN trennen und Switch-Port deaktivieren ist besser als gar keine Isolation. Ein dokumentiertes Verfahren dafür reicht als Startpunkt

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Softwarebasierte Isolation: Blockierung aller Netzwerkverbindungen außer zum Management-Server
- Hardwarebasierte Quarantäne: Switch-Port-Shutdown oder VLAN-Umzuweisung für physische Trennung
- Abgestufte Isolationslevel: von Netzwerk-Quarantäne bis zur kompletten Systemsperrung
- Forensik-Modus: Systemzustand bewahren und Remote-Analyse ermöglichen

2. Überwachung und Erkennung

- Echtzeit-Überwachung isolierter Endpunkte mit Dokumentation aller Aktivitäten
- Automatische Benachrichtigung des Security-Teams bei Isolations-Events
- Status-Dashboard über alle aktuell isolierten Geräte und deren Quarantäne-Status

3. Reaktion bei Vorfällen

- Abgestufte Reaktion je nach Schweregrad und Geschäftsauswirkung
- Massen-Isolation bei wurmartigen Bedrohungen (hunderte Endpunkte gleichzeitig)
- Remote-Forensik auf isolierten Systemen für detaillierte Malware-Analyse

4. Wiederherstellung und Kontinuität

- Alternative Arbeitsplätze bereitstellen, während Primärgeräte isoliert sind
- Automatisierte Bereinigung auf isolierten Endpunkten
- Stufenweise Re-Integration mit Sauberkeits-Prüfung vor Aufhebung der Quarantäne

Lessons Learned

- Vor der Bereinigung immer ein forensisches Image erstellen. Ohne diese Sicherung gehen Beweise verloren
- Eskalationswege und Entscheidungsträger für verschiedene Isolations-Szenarien vorab definieren
- Betroffene Benutzer proaktiv informieren: Isolations-Grund und voraussichtliche Wiederherstellungszeit kommunizieren
- Isolationsmechanismen regelmäßig testen, um Bypass-Möglichkeiten zu erkennen
- Host-basierte Isolation (EDR) und Netzwerk-basierte Isolation (Switch-Port, vgl. 4.2-A) ergänzen sich. Idealerweise beides vorbereiten

4.4.4 Patch-Management

Kurz erklärt und Risiken: Ungepatchte Systeme sind eines der häufigsten Einfallstore für Angriffe. Bekannte Schwachstellen werden oft innerhalb von Tagen nach Veröffentlichung eines Patches aktiv ausgenutzt. Ein systematischer Patch-Prozess stellt sicher, dass Sicherheitsupdates zeitnah, priorisiert und ohne Betriebsunterbrechungen eingespielt werden. Das gilt für alle Systeme von Arbeitsplatzrechnern über Server bis zu Netzwerkkomponenten.

Top-Maßnahmen

- Hohe Priorität: Etablierung eines dokumentierten Patch-Zyklus mit klaren Verantwortlichkeiten und Fristen: mindestens monatlich für Standardsysteme, innerhalb von 72 Stunden für kritische Sicherheitsupdates

- Quick Win: Automatische Updates für Betriebssysteme und Browser auf allen Arbeitsplatzrechnern aktivieren. Sofort umsetzbar, verhindert die häufigsten Angriffsvektoren

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Vollständiges Inventar aller Systeme und Software als Grundlage (was nicht bekannt ist, wird nicht gepatcht)
- Priorisierung nach Risiko: Extern erreichbare Systeme und Systeme mit bekannten aktiv ausgenutzten Schwachstellen zuerst
- Testverfahren für Patches vor Produktiveinsatz, mindestens Stichprobentest auf einem repräsentativen System
- Automatisierung der Patch-Verteilung über vorhandene Werkzeuge (z.B. WSUS, Gruppenrichtlinien, Linux-Paketmanager)
- Sonderbehandlung für OT-Systeme und Produktionsumgebungen: Patches nur in Wartungsfenstern und nach Freigabe durch Hersteller (vgl. Kap. 5)

2. Überwachung und Erkennung

- Dashboard über den Patch-Stand aller Systeme. Abweichungen vom Soll-Stand müssen sofort sichtbar sein
- Automatische Benachrichtigung bei neuen kritischen Schwachstellen (z.B. CERT-Bund-Meldungen, Hersteller-Advisories)
- Regelmäßiger Abgleich mit Schwachstellendatenbanken (CVE)

3. Reaktion bei Vorfällen

- Notfall-Patch-Prozess für kritische Zero-Day-Schwachstellen: beschleunigter Test und Rollout innerhalb von Stunden
- Wenn kein Patch verfügbar: Workarounds dokumentieren und umsetzen (z.B. Dienst deaktivieren, Netzwerkzugang einschränken)
- Rollback-Verfahren für fehlerhafte Patches. Vor dem Einspielen Wiederherstellungspunkt erstellen

4. Wiederherstellung und Kontinuität

- Snapshot oder Backup vor kritischen Patch-Vorgängen
- Dokumentierte Rollback-Prozedur für jede Systemklasse
- Ausnahmeliste für Systeme, die aus technischen Gründen nicht gepatcht werden können, mit dokumentierten Ausgleichsmaßnahmen (Netzwerk-Isolation, verstärktes Monitoring)

Lessons Learned

- Automatische Updates für Endgeräte sind der wirksamste Einzelschutz und sollten standardmäßig aktiviert sein

- OT-Systeme nicht ungeplant patchen. Rücksprache mit dem Hersteller und Wartungsfenster einhalten
- Ein Inventar, das nicht aktuell ist, ist wertlos. Automatisierung der Inventarisierung anstreben
- Patch-Compliance als KPI messen und reporten: was gemessen wird, wird auch gemacht

4.5 Datensicherheit

4.5.1 Datenklassifizierung und -schutz

Kurz erklärt und Risiken: EDR ohne systematische Datenklassifizierung können nachgelagerte Schutzmaßnahmen (Verschlüsselung, DLP, Zugriffsrechte) nicht angemessen dimensioniert werden. Die Klassifizierung bildet die Grundlage, auf der alle weiteren Datensicherheitsmaßnahmen aufbauen, und ist eng mit den IAM- und DLP-Architekturen verzahnt.

Top-Maßnahmen

- Hohe Priorität: Unternehmensweites Klassifizierungsschema definieren und auf alle Datenbestände anwenden
- Quick Win: Bestehende Datenbestände nach einfachem 3-Stufen-Schema (öffentlich / intern / vertraulich / streng vertraulich) kennzeichnen. Für Dateiserver mit vorhandenen Metadaten-/Labeling-Funktionen sofort umsetzbar

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Klassifizierungsschema mit klaren Kriterien und Beispielen für jede Stufe
- Automatische Klassifizierung neuer Dateien anhand von Dateityp, Speicherort und Inhaltserkennung
- Verknüpfung der Klassifizierungsstufe mit konkreten Schutzmaßnahmen (Verschlüsselung, Zugriffsrechte, DLP-Regeln)

2. Überwachung und Erkennung

- Regelmäßige Überprüfung der Klassifizierung auf Aktualität und Konsistenz
- Erkennung falsch klassifizierter oder nicht klassifizierter Datenbestände
- Monitoring von Zugriffen auf hochklassifizierte Daten (Verzahnung mit DAM)

3. Reaktion bei Vorfällen

- Automatische Anwendung verschärfter Schutzmaßnahmen bei Hochstufung der Klassifizierung
- Eskalationsprozess bei Verdacht auf Kompromittierung hochklassifizierter Daten

4. Wiederherstellung und Kontinuität

- Klassifizierungsmetadaten in Backup-Strategie einbeziehen
- Bei Datenwiederherstellung Klassifizierung und zugehörige Schutzmaßnahmen automatisch wiederherstellen

Lessons Learned

- Ein zu komplexes Klassifizierungsschema (>4 Stufen) wird in der Praxis nicht gelebt. Einfach anfangen, später verfeinern
- Klassifizierung ist kein einmaliges Projekt, sondern ein kontinuierlicher Prozess. In den Arbeitsalltag integrieren

4.5.2 Data Loss Prevention (DLP)

Kurz erklärt und Risiken: Unbefugter Transfer oder Diebstahl sensibler („Datenexfiltration“), ob durch externe Angreifer oder Insider, ist eine der größten Bedrohungen für Automobilzulieferer. DLP-Systeme analysieren Datenflüsse an allen Austrittspunkten (E-Mail, Cloud, USB, Web) und blockieren unberechtigte Übertragungen sensibler Informationen wie CAD-Daten, technische Dokumentationen und geistiges Eigentum.

Top-Maßnahmen

- Hohe Priorität: Berücksichtigung von CAD Daten und geistigem Eigentum in der DLP Lösung
- Quick Win: USB-Ports auf Arbeitsplatzrechnern per Gruppenrichtlinie auf Nur-Lesen setzen oder deaktivieren; E-Mail-Anhang-Größenlimits für sensible Dateitypen konfigurieren

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Automatische Erkennung und Klassifizierung sensibler Dateiformate (CAD-Zeichnungen, technische Dokumentationen, Kundendatenbanken)
- Inhaltsbasierte Analyse: Erkennung vertraulicher Informationen anhand von Schlüsselwörtern, Mustern und Datenstrukturen
- Endpoint-DLP für lokale Aktivitäten (USB-Transfers, Screenshots) und Netzwerk-DLP für ausgehende Datenströme
- Integration in E-Mail-Gateways, Web-Proxies und Cloud-Anwendungen

2. Überwachung und Erkennung

- Kontinuierliche Überwachung aller Datenflüsse zur Erkennung verdächtiger Exfiltrationsversuche in Echtzeit
- Erkennung ungewöhnlicher Zugriffsmuster auf sensible Daten (z.B. unübliche Zugriffszeiten, Massendownloads)
- Sofortige Benachrichtigung der Sicherheitsverantwortlichen bei kritischen DLP-Verstößen

3. Reaktion bei Vorfällen

- Automatisches Blockieren, Quarantänieren oder Verschlüsseln bei unberechtigten Datenübertragungen
- Forensische Dokumentation aller Datenflüsse für Incident-Analysen
- Sofortige Sperrung aller Datenexporte bei verdächtigen Aktivitäten
- Korrelation von DLP-Alerts mit SIEM-Ereignissen

4. Wiederherstellung und Kontinuität

- Granulare Ausnahmeregeln und Genehmigungsworkflows für legitime Geschäftsprozesse
- Behandlung von Fehlalarmen zur Minimierung von Produktivitätsverlusten
- Redundante DLP-Instanzen für Ausfallsicherheit

Lessons Learned

- Zu restriktive DLP-Regeln ohne Geschäftsprozess-Analyse führen zu Umgehungsversuchen. Pilotprojekte mit weniger kritischen Datentypen ermöglichen Feintuning
- Benutzerschulungen reduzieren Widerstand und erhöhen Akzeptanz erheblich
- DLP-Regeln regelmäßig überprüfen und anpassen: Erkennungsraten verschlechtern sich ohne kontinuierliches Tuning

4.5.3 Data Access Monitoring

Kurz erklärt und Risiken: Herkömmliche Perimeter-Schutzmaßnahmen und Intrusion Detection Systeme übersehen in der Regel verdächtige Aktivitäten nach erfolgreicher Authentifizierung. Data Access Monitoring (DAM) analysiert kontinuierlich alle Zugriffe auf sensible Daten und erkennt anomale Muster, die auf Insider-Bedrohungen oder Account-Missbrauch hindeuten. Besonders relevant für CAD-Daten und geistiges Eigentum in Zone 4 (Cloud), 5 (Corporate Network) und 6 (Plant Network).

Top-Maßnahmen

- Hohe Priorität: Vollständige Überwachung aller Zugriffe auf CAD-Daten und geistiges Eigentum
- Quick Win: Datei-Zugriffs-Auditing auf kritischen Dateiservern aktivieren (in Windows/Linux als Bordmittel verfügbar) und Logs an zentrales SIEM weiterleiten

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Vollständige Protokollierung aller Dateizugriffe, Datenbankabfragen und Anwendungsinteraktionen mit Zeitstempel und Benutzerkontext
- Definition von Verhaltens-Baselines: normale Arbeitszeiten, typische Dateizugriffe, übliche Datenvolumen pro Benutzer

- Erkennung ungewöhnlicher Zugriffskombinationen und abnormaler Downloadaktivitäten

2. Überwachung und Erkennung

- Echtzeit-Analyse von Zugriffsmustern und Erkennung von Abweichungen gegenüber Baselines
- Verknüpfung von Benutzeraktivitäten mit Systemereignissen und Netzwerkaktivitäten
- Risikobewertung pro Datenzugriff basierend auf Kontext, Sensitivität und Verhaltensindikatoren

3. Reaktion bei Vorfällen

- Abgestufte Reaktion: von zusätzlichen Authentifizierungsanforderungen bis zur temporären Account-Sperrung
- Forensische Dokumentation aller relevanten Aktivitäten
- Notfall-Sperrung kritischer Datenbestände bei akuter Bedrohung
- Verzahnung mit DLP-Systemen zur Verhinderung weiterer Datenexfiltration

4. Wiederherstellung und Kontinuität

- Regelmäßige Anpassung der Baseline-Profile an veränderte Arbeitsweisen zur Reduzierung von Fehlalarmen
- Retrospektive Analyse historischer Zugriffsdaten bei Verdachtsfällen
- Geschäftskritikalität bei Response-Entscheidungen berücksichtigen

Lessons Learned

- Nicht nur große Datenvolumen überwachen: Präzise Angriffe auf hochwertige Einzeldateien bleiben sonst unentdeckt
- Bei der Überwachung von Benutzeraktivitäten die jeweils geltenden Datenschutzvorschriften von Anfang an einbeziehen
- Mit den kritischsten Datenbeständen beginnen und schrittweise ausweiten

4.5.4 Backup und Recovery

Kurz erklärt und Risiken: Moderne Ransomware-Angriffe zielen auch gezielt auf Backup-Systeme ab. Ohne resiliente Datensicherung mit Schutz vor Manipulation ist die Wiederherstellungsfähigkeit nach einem schwerwiegenden Angriff nicht gewährleistet. Unveränderliche Backup-Architekturen nach dem 3-2-1-1-Prinzip (3 Kopien, 2 Medientypen, 1 Offsite, 1 Immutable/Air-Gapped (unveränderlich oder physisch getrennt offline)) sind die letzte Verteidigungslinie.

Top-Maßnahmen

- Hohe Priorität: Unveränderliche Backup-Architektur implementieren. Backups müssen auch bei Administrator-Kompromittierung nicht überschreibbar sein

- Quick Win: Vorhandene Backup-Jobs auf WORM (Write Once, Read Many) bzw. Immutable umstellen, sofern die Backup-Software dies unterstützt; Backup-Integrität durch automatische Wiederherstellungstests validieren

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Unveränderliche Speichertechnologien, die auch bei Admin-Kompromittierung nicht überschrieben werden können
- Offline-Backups physisch vom Netzwerk getrennt (Air-Gap oder Immutable
- Mehrgenerations-Backups: historische Versionen über längere Zeiträume vorhalten
- Verschlüsselung der Backup-Daten im Ruhezustand
- Regelmäßige Disaster-Recovery-Tests von wichtigen Daten, Applikationen und Systemen

2. Überwachung und Erkennung

- Kontinuierliche Integritätsprüfung aller Sicherungsprozesse mit Prüfsummen und Hash-Verifikation
- Erkennung von Verschlüsselungsaktivitäten gegen Backup-Systeme (Ransomware-Frühwarnung)
- Automatische Benachrichtigung bei Backup-Fehlern oder verdächtigen Aktivitäten

3. Reaktion bei Vorfällen

- Meldung an BCM/ITSCM Verantwortliche
- Notfall-Wiederherstellung kritischer Systeme aus sauberen Sicherungen
- Automatisierung der Disaster-Recovery-Prozesse zur Reduktion von RTO und RPO
- Kompromittierte Systeme für forensische Analyse bewahren, bevor überschrieben wird

4. Wiederherstellung und Kontinuität

- Point-in-Time-Wiederherstellung auf Zeitpunkte vor der Kompromittierung
- Granulare Wiederherstellung einzelner Dateien/Datenbanken ohne vollständigen System-Restore
- Betrieb an sekundären Standorten bei Ausfall des Primärstandorts
- Isolierte Wiederherstellungsumgebung zur Vermeidung von Re-Infektion

Lessons Learned

- Vertrauen auf eine einzelne Backup-Technologie ist riskant:
  Ein Angriff kann alle gleichartigen Backups gleichzeitig kompromittieren

- Regelmäßige Recovery-Tests sind Pflicht: Backups, die nie getestet wurden, sind keine Backups
- Backup-Strategie an regulatorische Vorgaben (Aufbewahrungsfristen, DSGVO) anpassen

4.6 Applikationssicherheit

4.6.1 Web Application Firewall (WAF)

Kurz erklärt und Risiken: Web Application Firewalls sind eine wichtige Verteidigungslinie gegen anwendungsspezifische Angriffe wie SQL Injection und Cross-Site Scripting, die herkömmliche Netzwerk-Firewalls nicht erkennen. WAF-Systeme analysieren HTTP/HTTPS-Traffic in Echtzeit und blockieren Angriffe, typischerweise in Zone 2 (Inbound) platziert oder als Edge-Dienst in Zone 4 (Cloud).

Top-Maßnahmen

- Hohe Priorität: Obligatorischer WAF-Schutz für alle extern erreichbaren Web-Services und APIs
- Quick Win: OWASP Core Rule Set auf vorhandener WAF im Monitoring-Modus aktivieren. So werden Angriffsmuster sichtbar, ohne legitimen Traffic zu blockieren. Ohne vorhandene WAF: Cloud-basierte WAF-Dienste ermöglichen Einstieg ohne eigene Infrastruktur

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- OWASP-Top-10-Schutz: Blockierung von Injection-Attacken, Authentifizierungsfehlern und Fehlkonfigurationen
- Eingabevalidierung: Filterung schädlicher Inhalte in HTTP-Parametern, Headers und Body
- Rate Limiting gegen automatisierte Angriffe und DDoS
- Geo-Blocking zur Einschränkung von Zugriffen aus Risikoländern
- API-spezifischer Schutz für REST- und GraphQL-Endpoints

2. Überwachung und Erkennung

- Echtzeit-Analyse aller Web-Requests auf Angriffsmuster
- Erkennung abnormaler Zugriffsmuster und Bot-Aktivitäten
- Verknüpfung von WAF-Alerts mit anderen Sicherheitsereignissen im SIEM
- Integration aktueller Angriffssignaturen und IP-Reputationsdaten

3. Reaktion bei Vorfällen

- Automatische Sperrung erkannter Angreifer für definierte Zeiträume
- Challenge-Response-Mechanismen (z.B. CAPTCHA) zur Bot-Unterscheidung

- Notfall-Schutzmodus für Web-Anwendungen bei schwerwiegen den Angriffen
- Forensische Protokollierung aller Angriffe

4. Wiederherstellung und Kontinuität

- Failover-Mechanismen für WAF-Schutz auch bei Systemausfällen
- Bypass-Modus für Service-Kontinuität bei WAF-Problemen (mit Risikobewertung)
- Behandlung von Fehlalarmen, um Blockierung legitimer Benutzer zu minimieren

Lessons Learned

- WAF immer im Monitoring-Modus starten: Ohne anwendungsspezifisches Tuning sind Fehlalarmraten hoch und blockieren Geschäftsfunktionen
- WAF-Regeln regelmäßig aktualisieren. Veraltete Signaturen schützen nicht gegen aktuelle Angriffstechniken
- WAF-Tests in den Entwicklungsprozess integrieren, damit neue Releases keine WAF-Konflikte erzeugen

4.6.2 Application Rollback und Recovery

Kurz erklärt und Risiken: Nach einer Kompromittierung oder einem fehlgeschlagenen Update muss schnell ein bekanntermaßen sauberer Anwendungszustand wiederhergestellt werden. Versionierte Deployments und Infrastructure as Code (IaC) ermöglichen konsistente, wiederholbare Wiederherstellungen. Ohne erprobte Rollback-Mechanismen verlängern sich Ausfallzeiten erheblich.

Top-Maßnahmen

- Hohe Priorität: Für jede geschäftskritische Anwendung einen dokumentierten und getesteten Rollback-Prozess etablieren
- Quick Win: Deployments versionieren: Bei jedem Release die vorherige Version als Rollback-Ziel vorhalten (z.B. über Deployment-Slots oder Container-Tags)
- KMU ohne Entwicklungspipeline (CI/CD): Vor jedem Update einen Snapshot der VM oder des Servers erstellen und Rollback-Verfahren dokumentieren. Bereits mit Bordmitteln (Hyper-V-Prüfpunkte, VMware-Snapshots, LVM-Snapshots) umsetzbar

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Versionierte Deployments: Jeder Release-Stand wird archiviert und ist jederzeit wiederherstellbar
- Infrastructure as Code (IaC): Infrastruktur und Konfiguration reproduzierbar aus versionierten Definitionen aufbauen

- Getrennte Umgebungen (Staging/Produktion) für sicheres Testen vor dem Rollout

2. Überwachung und Erkennung

- Automatische Gesundheitsprüfung nach jedem Deployment. Bei Fehlerquoten-Anstieg automatisch Rollback auslösen
- Monitoring der Anwendungsverfügbarkeit und Performance-Metriken nach Updates

3. Reaktion bei Vorfällen

- Ein-Klick-Rollback auf die letzte als stabil bekannte Version
- Bei Kompromittierung: Anwendung aus sauberer IaC-Definition und geprüftem Build-Artefakt neu aufbauen
- Zustandssicherung (Datenbank-Snapshots) vor Rollback-Maßnahmen

4. Wiederherstellung und Kontinuität

- Automatisches Failover auf redundante Instanzen während des Rollbacks
- Validierung der Geschäftslogik nach Wiederherstellung
- Dokumentation aller Rollback-Ereignisse für spätere Analyse

Lessons Learned

- Rollback-Prozesse, die nie getestet wurden, funktionieren im Ernstfall nicht. Regelmäßig im Staging üben
- Datenbankmigrationen bei Rollbacks gesondert betrachten: Schema-Änderungen sind oft nicht trivial rückgängig zu machen
- Rollback-Fähigkeit bereits in der Anwendungsarchitektur vorsehen (z.B. abwärtskompatible API-Versionen)

Kennzahlen zur Messung der IT Security Reife

Im Anhang (Kapitel 8, Tabelle 1) dieses Dokuments sind ausgewählte Kennzahlen (Key Performance Indicators, KPIs) aufgeführt, mit denen die Reife der IT Security Architektur gemessen wird.

Die Kennzahlen sind an etablierten Standards und Rahmenwerken ausgerichtet und unterstützen eine nachvollziehbare, kontinuierliche Verbesserung der Informationssicherheit.

Sie ermöglichen eine objektive Bewertung und Berichterstattung des Umsetzungsgrades zentraler Sicherheitsprinzipien (z. B. Zero-Trust), der Wirksamkeit technischer und organisatorischer Maßnahmen.

5 Industrial and Operational Technology Security (OT)

Die Sicherheit der Operational Technology (OT) ist entscheidend für die gesamte IT-Lieferkette. Mit der zunehmenden Digitalisierung und Vernetzung von industriellen Steuerungssystemen, Produktionsanlagen und kritischen Infrastrukturen entstehen neue Möglichkeiten für Effizienz und Automatisierung. Gleichzeitig erhöht sich jedoch die Angriffsfläche für Cyberbedrohungen. OT-Systeme basieren oft auf langlebigen, proprietären Technologien, die nicht für den sicheren Betrieb in einem vernetzten Umfeld entwickelt wurden. Daher sind sie besonders anfällig für Angriffe.

Ein erfolgreicher Cyberangriff auf OT-Infrastrukturen kann schwerwiegende Folgen haben. Er kann Produktionsprozesse stören, physische Schäden verursachen, Menschenleben gefährden und erhebliche wirtschaftliche Verluste nach sich ziehen. Um die Sicherheit von OT-Systemen zu gewährleisten, sind gezielte Maßnahmen erforderlich, die verschiedene Bereiche abdecken.
Hier sind die zentralen Maßnahmen zur Verbesserung der OT-Sicherheit:

- **Netzwerksegmentierung:** Trennung von OT- und IT-Netzwerken zur Einschränkung des Zugriffs auf kritische Systeme.
- **Zugangskontrolle:** Implementierung von Mehrfaktor-Authentifizierung und rollenbasierten Zugriffskontrollen.
- **Überwachung und Erkennung:** Einsatz von SIEM-Systemen und Intrusion Detection Systemen zur Echtzeitanalyse verdächtiger Aktivitäten.
- **Patch-Management:** Regelmäßige Sicherheitsupdates und Testen von Patches in einer sicheren Umgebung.
- **Systemhärtung:** Sichere Konfiguration von Systemen zur Minimierung potenzieller Sicherheitslücken.
- **Einhaltung von Sicherheitsstandards:** Implementierung der ISO/IEC 62443 zur Identifikation und Minderung von Sicherheitsrisiken.
- **Backup & Recovery:** Automatisierte Datensicherung und Testen der Wiederherstellungsverfahren.

Diese Maßnahmen sind in den Kapiteln 5.1 bis 5.7 als ausführliche Empfehlungen detailliert beschrieben. Ihre Umsetzung trägt dazu bei, die Resilienz der OT-Systeme zu stärken und die Sicherheit in der vernetzten Welt zu gewährleisten.

Im Kontext des in Kapitel 4 beschriebenen 6-Zonen-Diagramms gelten die Maßnahmen innerhalb des Produktionsnetzwerkes (6) für jede Linie (6b) und insbesondere die kritischen Komponenten in der Sicherheitszone (6a).

5.1 Übersicht relevanter Standards

Kurz erklärt und Risiken: Die OT-Netzwerksegmentierung ist die architektonische Umsetzung der Trennung zwischen verschiedenen Sicherheitsbereichen. Im Referenzmodell ist dies die fundamentalste Maßnahme zur Härtung der Grenze zwischen dem IT-Netzwerk (Zone 5) und dem Produktionsnetzwerk (Zone 6), wobei die Kommunikation ausschließlich kontrolliert erfolgen darf. Ohne diese strikte Trennung kann ein einzelner Ransomware-Vorfall im IT-Umfeld ungehindert auf die Steuerungssysteme übergreifen und die gesamte Produktion lahmlegen.

Top-Maßnahmen

- Hohe Priorität: Physische oder logische Trennung von IT- und OT-Netzwerken durch eine dedizierte, Firewall-geschützte Zone.
- Quick Win: Erstellung eines Netzwerkplans, der alle bekannten Verbindungen zwischen dem IT- und OT-Netzwerk dokumentiert.

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Implementierung des „Zonen und Conduits“-Modells gemäß IEC 62443 zur weiteren Unterteilung des Produktionsnetzwerks in einzelne Produktionszellen.
- Einsatz von industrietauglichen Firewalls an der IT/OT-Schnittstelle, die OT-spezifische Protokolle verstehen.
- Durchsetzung eines „Implicit-Deny“-Prinzips für den gesamten Datenverkehr, der die Grenze zum Produktionsnetzwerk passiert.

2. Überwachung und Erkennung

- Passive Überwachung des Netzwerkverkehrs innerhalb des Produktionsnetzwerks durch ein spezialisiertes OT-IDS.
- Alarmierung bei jeder neuen, nicht genehmigten Kommunikation zwischen IT- und OT-Netz.
- Protokollierung und regelmäßiges Review aller Firewall-Regeln an den Netzwerk-Übergängen.

3. Reaktion bei Vorfällen

- Einrichtung einer Notfall-Möglichkeit („Not-Aus“) zur schnellen Trennung der IT/OT-Verbindung.
- Isolierung der betroffenen Produktionszelle, um die Ausbreitung auf andere Produktionsbereiche zu verhindern.
- Etablierung klarer Kommunikations- und Eskalationswege zwischen IT-Security- und OT-Betriebs-Teams.

4. Wiederherstellung und Kontinuität

- Sicherung und zentrale Verwaltung der Konfigurationen aller OT-Netzwerkkomponenten.
- Dokumentation aller genehmigten Datenflüsse als Basis für die schnelle und sichere Wiederherstellung.
- Regelmäßige Tests der Netzwerkresilienz und der Isolationsmechanismen.

Lessons Learned

- Eine klare Trennung zwischen IT- und OT-Netzwerken ist anzustreben und bildet die Grundlage jeder wirksamen OT-Sicherheitsstrategie.
- OT-Sicherheitsmaßnahmen müssen die Anlagenverfügbarkeit priorisieren und dürfen den Produktionsprozess nicht beeinträchtigen.

- Flache OT-Netzwerke stellen ein erhebliches Risiko dar und sind durch geeignete Segmentierungsmaßnahmen zu vermeiden.

5.2 Härtung von OT-Systemen

Kurz erklärt und Risiken: Die Härtung von OT-Systemen reduziert die Angriffsfläche der Endpunkte, die sich innerhalb des Produktionsnetzwerks (Zone 6) befinden, indem nicht verwendete Funktionen entfernt oder geblockt werden. Ein ungehärtetes OT-System ist ein leichtes Ziel für Malware, die z.B. über einen unkontrolliert angeschlossenen Wartungs-Laptop eingeschleust wird.

Top-Maßnahmen

- Hohe Priorität: Implementierung von Endpoint Protection (EDR/XDR) oder Application Whitelisting auf allen OT-Systemen.
- Quick Win: Änderung aller bekannten Standardpasswörter und Blockieren der USB-Ports.

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Erstellung von gehärteten „Golden Images“ für Standard-OT-Systeme wie Operator Panels und Engineering Stations.
- Deaktivierung aller nicht betriebsnotwendigen Dienste und Ports auf OT-Endgeräten.

2. Überwachung und Erkennung

- Überwachung der Systemintegrität (File Integrity Monitoring) und Alarmierung bei Konfigurationsänderungen an OT-Geräten.
- Protokollierung aller administrativen Zugriffe und kritischen Änderungen auf OT-Systemen.

3. Reaktion bei Vorfällen

- Isolierung des betroffenen Systems vom Netzwerk in Abstimmung mit der Betriebsleitung.
- Forensische Analyse des Systems zur Identifizierung der Kompromittierungsursache.
- Einspielen eines sauberen, gehärteten Images zur schnellen Wiederherstellung des Betriebs (Golden Images).

4. Wiederherstellung und Kontinuität

- Zentrale und sichere Speicherung aller „Golden Images“ und Konfigurationen für OT-Systeme.
- Dokumentation der Härtungs-Baselines und genehmigter Ausnahmen.
- Regelmäßige Tests der Wiederherstellung eines OT-Systems aus einem gehärteten Image.

Lessons Learned

- Für OT-Systeme sind standardisierte Härtungsleitfäden sowie anerkannte Baselines oder Benchmarks anzuwenden. Nicht benötigte Funktionen und Dienste sind konsequent zu deaktivieren.
- Für das Einspielen von Patches sowie für Wiederherstellungs- und Notfalltests sind ausreichende und regelmäßig geplante Wartungsfenster sicherzustellen.
- Externe Wartungssysteme, insbesondere Dienstleister-Laptops, stellen ein erhöhtes Risiko dar und sind vor der Nutzung in der OT-Umgebung verbindlich abzusichern.

5.3 Physische Sicherheit

Kurz erklärt und Risiken: Im Kontext der Architektur stellt die physische Sicherheit die grundlegende Schutzschicht für das Produktionsnetzwerk (Zone 6) dar. Sie verhindert den unbefugten direkten Zugriff auf Steuerungsanlagen und Netzwerkschränke und schützt so vor Angreifern, die alle Netzwerk-basierten Kontrollen umgehen könnten. Das Risiko ist, dass ein Angreifer durch physischen Zutritt Sabotage betreibt, Malware via USB einschleust oder Menschenleben durch Manipulation von Sicherheitseinrichtungen gefährdet.

Top-Maßnahmen

- Hohe Priorität: Implementierung von angemessenen Zugangskontrollen für alle Produktionsbereiche, Kontroll- und Serverräume.
- Quick Win: Sicherstellen, dass alle Netzwerkschränke und Verteilerkästen in der Produktion sicher verschlossen sind.

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Einsatz eines mehrstufigen Zutrittskonzepts für den Zugang zu sensiblen Anlagenbereichen.
- Physisches Deaktivieren aller ungenutzten Netzwerk-Ports in den Produktionshallen.
- Schutz kritischer Anlagen vor Umwelteinflüssen wie Feuer und Wasser.

2. Überwachung und Erkennung

- Einsatz von Videoüberwachung an kritischen Zugangspunkten zu den OT-Bereichen.
- Protokollierung aller Zutrittsereignisse durch elektronische Schließsysteme.

3. Reaktion bei Vorfällen

- Ein klar definierter Prozess für die Reaktion auf physische Sicherheitsalarme im Produktionsumfeld.
- Analyse der Protokolle zur Identifizierung der beteiligten Personen.
- Überprüfung der betroffenen Systeme auf unautorisierte physische oder logische Änderungen.

4. Wiederherstellung und Kontinuität

- Notfallpläne für den Ausfall der physischen Sicherheitssysteme.
- Regelmäßige Überprüfung und Wartung aller Sicherheitseinrichtungen.
- Schulung der Mitarbeiter bezüglich der Sicherheitsrichtlinien für die Produktionsumgebung.

Lessons Learned

- Technische Schutzmaßnahmen verlieren ihre Wirkung, wenn physischer Zugriff auf OT-Infrastruktur unkontrolliert möglich ist.
- Physische Sicherheit und Cybersicherheit sind in OT-Umgebungen integrale Bestandteile eines gemeinsamen Schutzkonzepts.
- Unkontrollierte oder nicht zurückgebaute Wartungs- und Serviceanschlüsse stellen eine häufige und kritische Schwachstelle dar.

5.4 Zugangskontrolle in der OT

Kurz erklärt und Risiken: Diese Maßnahme ist die entscheidende Kontrolle für alle logischen Zugriffswege in das Produktionsnetzwerk (Zone 6), insbesondere für den kontrollierten Pfad der Fernwartung von extern. Ungesicherte Zugänge mit geteilten Konten oder schwachen Passwörtern sind ein Hauptrisiko. Ein Angreifer, der einen solchen Zugang übernimmt, kann direkt in den Produktionsprozess eingreifen, Steuerungslogik manipulieren, Anlagen abschalten oder Sabotageakte durchführen, was zu direkten, physischen Konsequenzen führen kann.

Top-Maßnahmen

- Hohe Priorität: Absicherung aller Fernwartungszugriffe auf das Produktionsnetzwerk über eine zentrale, kontrollierte Plattform mit MFA.
- Quick Win: Deaktivierung aller permanent aktiven Fernwartungszugänge; diese dürfen nur bei Bedarf und zeitlich begrenzt freigeschaltet werden.

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Einführung von individuellen, nicht geteilten Benutzerkonten für alle Ingenieure und Bediener.
- Durchsetzung von robusten Passwortrichtlinien für OT-Systeme, wo technisch möglich. Mindestlänge 12 bis 16 Zeichen, Empfehlung Passphrasen.
- Implementierung eines Rollen-basierten Zugriffskonzepts (RBAC), das festlegt, wer welche Parameter ändern darf.

2. Überwachung und Erkennung

- Lückenlose Protokollierung aller Anmeldungen, Abmeldungen und kritischen Aktionen an OT-Systemen.
- Überwachung und Aufzeichnung aller Fernwartungssitzungen.
- Alarmierung bei Anmeldeversuchen außerhalb der vereinbarten Wartungsfenster.

3. Reaktion bei Vorfällen

- Möglichkeit zur sofortigen Beendigung einer verdächtigen Fernwartungssitzung.
- Deaktivierung des kompromittierten Benutzerkontos in der OT-Umgebung.
- Analyse der Protokolle und Aufzeichnungen, um die durchgeführten Aktionen nachzuvollziehen.

4. Wiederherstellung und Kontinuität

- Ein klar definierter Prozess für die Notfall-Freischaltung von Zugängen.
- Regelmäßige Überprüfung und Rezertifizierung aller OT-Benutzerkonten und Berechtigungen.
- Sichere Verwaltung von Schlüsseln, Zertifikaten und Passwörtern für OT-Systeme.

Lessons Learned

- Jeder Fernwartungszugang stellt ein potenzielles Risiko für produktive Systeme dar und ist entsprechend zu kontrollieren und abzusichern.
- Die Nutzung geteilter Benutzerkonten ist unzulässig, da sie eine eindeutige Nachvollziehbarkeit und Incident-Aufklärung verhindert.
- Das Prinzip der minimalen Rechtevergabe (Least Privilege) ist auch für Maschinenbediener konsequent umzusetzen.

5.5 Schwachstellen- und Patch-Management in der OT

Kurz erklärt und Risiken: Diese Maßnahme fokussiert sich auf die Assets innerhalb des Produktionsnetzwerks (Zone 6). Anders als im IT-Netz ist sofortiges Patchen hier oft nicht möglich. Unbekannte Schwachstellen stellen ein latentes Risiko dar, da ein Angreifer, der die IT/OT-Grenze überwindet, diese gezielt ausnutzen kann. Die Patch-Verteilung muss daher kontrolliert und in Abstimmung mit dem Betrieb erfolgen, oft über dedizierte Update-Server. Ein effektives Patch-Management beinhaltet das Identifizieren, Bewerten, Testen und Installieren von Updates.

Top-Maßnahmen

- Hohe Priorität: Erstellung und Pflege eines vollständigen Inventars aller OT-Assets inklusive Software- und Firmware-Versionen als Basis für eine risikobasierte Priorierung.
- Quick Win: Abonnieren der Security-Advisories der wichtigsten OT-Hersteller, um proaktiv über neue Schwachstellen informiert zu werden.

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Planung von Patches in enger Abstimmung mit den Betriebs- und Wartungsteams während geplanter Stillstände.
- Testen von Patches in isolierten Umgebungen, definieren Sie Wartungsfenster mit Rollback-Plänen.

- Definition kompensierender Maßnahmen (z.B. verschärfte Netzwerkregeln), wenn ein Patch nicht installiert werden kann.

2. Überwachung und Erkennung

- Durchführung passiver Schwachstellen-Scans, die den Netzwerkverkehr analysieren, ohne die Geräte aktiv zu stören.
- Erkennung von veralteten oder nicht mehr unterstützten (End-of-Life) Komponenten.

3. Reaktion bei Vorfällen

- Ein Notfallprozess für kritische, ausnutzbare Schwachstellen in der OT.
- Priorisierung der Implementierung kompensierender Maßnahmen (virtuelles Patching via IPS), um die Lücke temporär zu schließen.
- Gezielte Überwachung der verwundbaren Systeme auf Anzeichen einer Ausnutzung.

4. Wiederherstellung und Kontinuität

- Testen von Schwachstellenscans und Patches in einer Labor- oder Simulationsumgebung vor der Durchführung bzw. dem Rollout in der Produktion.
- Erstellung von Backups der Systemkonfigurationen vor jeder Patch-Installation.
- Pflege eines validierten Rollback-Plans, um im Fehlerfall schnell zum stabilen Vorzustand zurückzukehren.

Lessons Learned

- Die Verfügbarkeit der Systeme hat Vorrang. Produktive Systeme sollten nur mit getesteten und freigegebenen Patches geändert werden.
- Ein vollständiges und aktuelles Inventar ist Voraussetzung für ein wirksames Schwachstellenmanagement.
- Kann ein System nicht zeitnah gepatcht werden, sind geeignete kompensierende Maßnahmen (z. B. Systemhärtung, Netzwerksegmentierung) umzusetzen. Migrieren Sie, wo möglich, End of Life-Komponenten rechtzeitig.

5.6 Backup und Wiederherstellung in der OT

Kurz erklärt und Risiken: Dieser Prozess sichert die Konfigurationen und Daten der Systeme im Produktionsnetzwerk (Zone 6). Entscheidend ist dabei, dass die Backup-Daten selbst sicher außerhalb des Produktionsnetzwerks, beispielsweise im IT-Netzwerk (Zone 5) oder in der Cloud (Zone 4), aufbewahrt werden. Dies verhindert, dass im Falle einer Kompromittierung der OT die Backups ebenfalls betroffen sind. Regelmäßige und verifizierte Datensicherungen sowie geübte Wiederherstellungsprozesse sind entscheidend, um die Betriebsfähigkeit zu sichern und Datenverlust nach Vorfällen zu minimieren.

Top-Maßnahmen

- Hohe Priorität: Etablierung eines automatisierten Backup-Prozesses für alle kritischen OT-Systeme mit sicherer Ablage außerhalb des Produktionsnetzwerks.
- Quick Win: Identifizierung kritischsten Anlagen und manuelle Sicherung ihrer Konfigurationen auf einem externen, sicheren Speichermedium.

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Definition von Wiederherstellungszielen (RTO/RPO) für alle kritischen Anlagen.
- Anwendung der 3-2-1-1 Backup-Strategie (3 Kopien, 2 Medientypen, 1 Offsite, 1 Immutable/Air-Gapped (unveränderlich oder physisch getrennt offline)) die vor Ransomware geschützt ist.
- Strikte Trennung der Administration der Backup-Umgebung von den regulären OT-Benutzerkonten.

2. Überwachung und Erkennung

- Tägliche Überwachung der Backup-Jobs auf Fehler oder Warnungen.
- Regelmäßige Überprüfung der Integrität und Lesbarkeit der erstellten Backups.
- Alarmierung, wenn für eine kritische Anlage über einen längeren Zeitraum kein erfolgreiches Backup erstellt wurde.

3. Reaktion bei Vorfällen

- Ein klarer Prozess, um im Notfall schnell auf die extern gelagerten Backup-Dateien zugreifen zu können.
- Sicherstellung, dass die Wiederherstellung in einer sauberen, isolierten Umgebung erfolgt.
- Überprüfung der letzten „sauberen“ Backups vor dem bekannten Zeitpunkt eines Vorfalls.

4. Wiederherstellung und Kontinuität

- Pflege detaillierter Wiederherstellungs-Anleitungen (Runbooks) für jede wichtige Anlage.
- Durchführung regelmäßiger, geplanter Wiederherstellungstests.
- Sicherstellung, dass auch die zur Wiederherstellung benötigte Engineering-Software verfügbar ist.
- Warm- oder Cold-Standby für Legacy- oder schwer wiederherstellbare Systeme.

Lessons Learned

- OT-Backups sind regelmäßig auf Wiederherstellbarkeit zu testen; nicht verifizierte Backups erfüllen keinen Schutzzweck.
- Backups von Produktions- und OT-Systemen sind strikt getrennt vom Produktions-netzwerk zu speichern.

5.7 Security Monitoring und Incident Response in der OT

Kurz erklärt und Risiken: Im Architekturmodell ist Monitoring die Fähigkeit, sicherheitsrelevante Ereignisse an den kritischen Übergängen – insbesondere an der IT/OT-Grenze – sowie innerhalb des Produktionsnetzwerks (Zone 6) zu erkennen. Ohne diese Sichtbarkeit agiert der Betrieb im Blindflug, und ein Angreifer könnte unentdeckt vom IT- ins OT-Netzwerk wechseln und dort Schaden anrichten. Das Risiko ist, dass ein Vorfall erst bemerkt wird, wenn es zu einem physischen Schaden oder einem Produktionsausfall kommt.

Top-Maßnahmen

- Hohe Priorität: Implementierung eines passiven OT-Intrusion-Detection-Systems (IDS/NDR) zur Überwachung des Netzwerkverkehrs im Produktionsnetzwerk.
- Quick Win: Etablierung eines klaren Melde- und Eskalationsprozesses für IT- und OT-Mitarbeiter bei Sicherheitsverdachtsfällen.

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Zentrale Sammlung von Logs aus Firewalls, die das OT-Netz schützen, sowie von Systemen innerhalb der OT.
- Definition von Baselines für den „normalen“ Netzwerkverkehr, um Abweichungen erkennen zu können oder Nutzung lernender/Intelligenter Erkennungssysteme.
- Einsatz von EDR auf OT-Systemen, wo dies technisch machbar und vom Hersteller freigegeben ist.

2. Überwachung und Erkennung

- Entwicklung von OT-spezifischen Alarmierungs-Use-Cases (z.B. „Unbekanntes Gerät im OT-Netz“, „SPS-Stopp-Befehl von unautorisierter Quelle“).
- Integration von OT-spezifischen Bedrohungsinformationen.
- Regelmäßiges proaktives „Threat Hunting“ in den OT-Netzwerkdaten.

3. Reaktion bei Vorfällen

- Erstellung eines OT-spezifischen Incident-Response-Plans, der die Betriebsleitung und Anlageningenieure einbezieht.
- Durchführung regelmäßiger Übungen (Table-Top-Simulationen) für OT-Szenarien.
- Klare Anweisungen zur Eindämmung (z.B. Netzwerkisolation) in Abstimmung mit dem Betrieb.

4. Wiederherstellung und Kontinuität

- Nutzung der gesammelten Daten für die forensische Analyse zur Aufklärung des Vorfalls.
- Anpassung der Detektionsregeln basierend auf den „Lessons Learned“ aus dem Vorfall.
- Sicherstellung der Beweismittelsicherung für eventuelle rechtliche Schritte.

Lessons Learned

- Eine wirksame Reaktion auf Sicherheitsvorfälle in der OT erfordert eine enge und klar geregelte Zusammenarbeit zwischen IT-Security-Funktionen und OT-Engineering.
- Sichtbarkeit über Assets, Kommunikation und Zustände im OT-Netzwerk ist eine Grundvoraussetzung für wirksame Schutz- und Abwehrmaßnahmen.
- Incident-Response-Pläne für OT-Umgebungen müssen physische Sicherheitsaspekte sowie die Sicherstellung der Anlagenverfügbarkeit ausdrücklich berücksichtigen.

Zusammenfassende Tabelle: Weiterführende Dokumentation

Kapitel	Relevante Standards/Normen
OT.1 Netzwerksegmentierung	IEC 62443-3-2, IEC 62443-3-3, NIST SP 800-82, BSI-CS 108
OT.2 Härtung von OT-Systemen	IEC 62443-4-2, IEC 62443-3-3, CIS Benchmarks, NIST SP 800-53 (CM)
OT.3 Physische Sicherheit	ISO/IEC 27001 (A.7), IEC 62443-2-1, BSI-Standard 200-2 (INF.2, INF.5)
OT.4 Zugangskontrolle	IEC 62443-3-3 (SR 1.x), NIST SP 800-82, ISO/IEC 27002, BSI IT-Grundschutz (ORP.4)
OT.5 Schwachstellen-Management	IEC 62443-2-3, IEC 62443-4-1, NIST SP 800-40, VDI/VDE 2182
OT.6 Backup und Wiederherstellung	IEC 62443-3-3 (SR 7.3), NIST SP 800-82, ISO/IEC 27001 (A.8.13), BSI 200-4
OT.7 Security Monitoring	IEC 62443-3-3 (SR 2.x, 3.x), NIST Cybersecurity Framework (Detect, Respond), MITRE ATT&CK for ICS

Kennzahlen zur Messung der OT Security Reife

Im Anhang dieses Dokuments (Kapitel 8, Tabelle 1) sind ausgewählte Kennzahlen (Key Performance Indicators, KPIs) aufgeführt, mit denen die Reife der OT Security Architektur bewertet werden kann.

Die Kennzahlen dienen der objektiven Bewertung des Reifegrads von Schutzmaßnahmen in OT Umgebungen, der Segmentierung und Zonen /Zellen Konzepte sowie der Einhaltung sicherheitsrelevanter Maßnahmen.

6 Cloud Security

Im Rahmen des generischen Sechs-Zonen-Modells ist Cloud Security besonders in Zone 4 (Cloud) relevant. Die Anforderungen der IT-Sicherheit aus Kapitel 4 bilden die Basis und müssen auch im Zusammenhang mit Cloud Computing berücksichtigt werden. In diesem Cloud Security Kapitel steht vor allem die Bewertung der Sicherheit in der Cloud im Mittelpunkt, da bei Cloud Computing häufig eine gemeinsame Verantwortung zwischen Cloud-Service-Nutzer und Anbieter besteht. Industriestandards sowie etablierte Sicherheitsstandards spielen dabei eine entscheidende Rolle.

6.1 Grundlagen

Zulieferer in der Automobilindustrie stehen unter wachsendem Druck, ihre IT-Landschaften zu modernisieren, nicht zuletzt durch die zunehmende Verlagerung bestehender On-Premise-Anwendungen in die Cloud. Cloud-Services schaffen die Grundlage für skalierbare Entwicklungsumgebungen, datenbasierte Services und eine engere digitale Zusammenarbeit mit OEMs.

Lieferanten die Multi-Tenant-Cloud-Umgebungen in Produkten und Diensten anbieten, müssen gewährleisten, dass die Daten und Anwendungen der Auftraggeber strikt voneinander getrennt sind. Dies erfordert sowohl logische als auch physische Sicherheitsmaßnahmen, um die Vertraulichkeit, Integrität und Verfügbarkeit der Kundendaten zu gewährleisten. Eine virtuelle Mandantentrennung kann durch den Einsatz von Container-Technologien, virtualisierten Umgebungen oder dedizierten Sicherheitszonen sichergestellt werden. Zusätzlich verhindert eine strikte Zugriffssegmentierung durch Mikrosegmentierung, dass ein kompromittierter Mandant auf andere Mandanten übergreifen kann. Sämtliche gespeicherten Daten müssen mit starken Verschlüsselungsverfahren wie AES-256 gesichert werden, um Missbrauch oder unbefugten Zugriff zu verhindern. Ebenso sollten isolierte Verarbeitungsknoten genutzt werden, um Seitenkanalangriffe oder unbeabsichtigte Datenlecks zu vermeiden.

Die Zugriffskontrolle zwischen lokalen IT-Systemen und Cloud-Umgebungen muss nahtlos integriert sein, um eine einheitliche Sicherheitsrichtlinie zu ermöglichen. Hierzu ist eine zentrale Identitäts- und Zugriffsverwaltung erforderlich, die durch in Identity and Access Management (IAM)-System gesteuert wird. Dies ermöglicht eine sichere Verwaltung von Benutzeridentitäten und deren Berechtigungen über alle Umgebungen hinweg. Single Sign-On (SSO) vereinfacht die Authentifizierung und reduziert Sicherheitsrisiken, während Mehrfaktor-Authentifizierung (MFA) als verpflichtende Maßnahme für alle administrativen und privilegierten Zugänge eingeführt werden müssen. Um sicherzustellen, dass Benutzer nur die minimal erforderlichen Berechtigungen erhalten, wird das Prinzip der geringsten Rechte (Least Privilege Principle) angewendet, ergänzt durch rollenbasierte Zugriffskontrolle (RBAC). Regelmäßige Überprüfungen und Rezertifizierungen der Zugriffsrechte minimieren das Risiko einer Überpreviligierung. Zudem sorgen lückenlose Audit-Logs und die Nutzung von Security Information and Event Management (SIEM)-Systemen für eine effektive Überwachung von Zugriffen und möglichen Sicherheitsvorfällen.
Externe Partner, die Daten des Auftraggebers mit besonderen oder höchsten Schutzanforderungen in ihren eigenen Public-Cloud-Anwendungen verarbeiten, müssen nachweislich über robuste Sicherheitsmaßnahmen verfügen.

Dazu zählen die verpflichtende Zertifizierung nach ISO 27001 sowie ISO 27018 (für Cloud-Service-Provider) und die TISAX Testierung für Unternehmen der Automobilbranche, um ein umfassendes Informationssicherheitsmanagementsystem (ISMS) sicherzustellen. Zusätzlich ist bei der Verarbeitung personenbezogener Daten die DSGVO-Konformität sicherzustellen, einschließlich der Durchführung einer Datenschutz-Folgenabschätzung.

Cloud-Services basieren maßgeblich auf API-Architekturen, daher ist ein besonders kritischer Aspekt die Absicherung dieser API-Schnittstellen. Hierzu gehört die verschlüsselte API-Kommunikation mittels TLS 1.2 oder höher sowie die Nutzung von OAuth 2.0 oder OpenID Connect für eine sichere Authentifizierung. Maßnahmen wie Rate-Limiting und Anomalie Erkennung verhindern Angriffe auf APIs und reduzieren das Risiko einer unbefugten Datenexfiltration. Darüber hinaus müssen alle Cloud-Service-Provider regelmäßige Penetrationstests und Schwachstellenanalysen durchführen sowie Sicherheitslücken durch Bug-Bounty-Programme frühzeitig identifizieren und beheben.

Durch die konsequente Umsetzung von IT-Sicherheitsmaßnahmen (siehe Kapitel 4) und zusätzlichen Cloud Sicherheitsmaßnahmen wird nicht nur eine strikte Mandantentrennung in Cloud-Umgebungen gewährleistet, sondern auch eine sichere und integrierte Zugriffskontrolle geschaffen. Die Sicherung der Lieferkette wird durch Zertifizierungspflichten für externe Partner, API-Sicherheitsmaßnahmen und kontinuierliches Monitoring verstärkt. Dies reduziert das Risiko von Datenlecks, Cyberangriffen und regulatorischen Verstößen und stärkt das Vertrauen in die gesamte Wertschöpfungskette.

Für IT-Verantwortliche ergeben sich daraus konkrete Anforderungen: Neben technischer ntegration rücken Fragen der Informationssicherheit in den Fokus – etwa hinsichtlich Datenhoheit, Zugriffskontrolle, Verschlüsselung, Anbieterzertifizierungen (z. B. ISO 27001, C5, TISAX) und vertraglicher Absicherung. In der gesamten Lieferkette und bei sensiblen Entwicklungs- und Produktionsdaten ist ein sicherer, regelkonformer Cloud-Einsatz unerlässlich.

6.2 Begriffsdefinitionen / Cloud-Services (IaaS, PaaS, SaaS)

Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) stellt skalierbare IT-Infrastrukturressourcen, wie Rechenleistung, Speicher und Netzwerkkomponenten und bedarfsgerecht über eine Cloud-Plattform bereit. Die Verantwortung für Betriebssysteme, Middleware und Anwendungen verbleibt beim Kunden, während der Cloud-Anbieter die physische Infrastruktur sowie deren Verfügbarkeit und Wartung sicherstellt. IaaS ermöglicht eine flexible Skalierung von IT-Ressourcen, optimiert Investitionskosten (CAPEX zu OPEX) und unterstützt eine schnelle Bereitstellung neuer Systeme. Dies macht den Ansatz besonders attraktiv für dynamische Workloads, Test-/Entwicklungsumgebungen und Disaster-Recovery-Szenarien.

Platform as a Service (PaaS)

Platform as a Service (PaaS) bietet eine vollständig verwaltete Plattform für die Entwicklung, das Testen und den Betrieb von Anwendungen, inklusive Laufzeitumgebung, Datenbanken und Middleware.

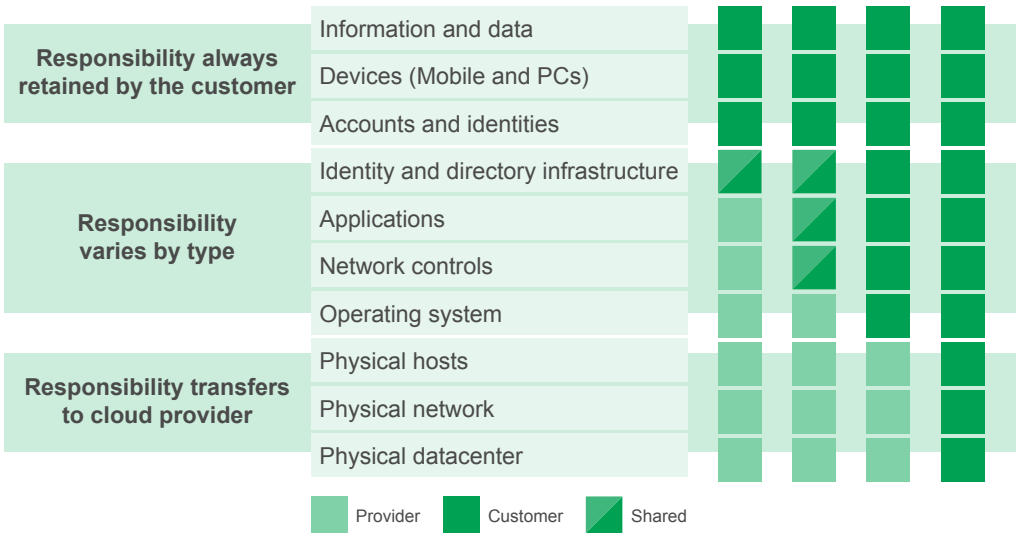
Die Verantwortung für die zugrunde liegende Infrastruktur, Skalierung und Systempflege liegt vollständig beim Anbieter, wodurch sich IT-Teams auf die Entwicklung und Bereitstellung geschäftskritischer Anwendungen fokussieren können. PaaS reduziert den operativen Overhead und beschleunigt Time-to-Market durch automatisierte Prozesse und integrierte DevOps-Werkzeuge. Besonders geeignet ist dieser Ansatz für moderne, Cloud-native Applikationen und Microservices-Architekturen.

Software as a Service (SaaS)

Software as a Service (SaaS) stellt voll funktionsfähige Anwendungen über das Internet bereit, die von Endanwendern direkt genutzt werden können, ohne dass Installation, Wartung oder Infrastrukturmanagement erforderlich sind. Der Anbieter übernimmt sämtliche Aspekte der Betriebsführung – von Verfügbarkeit und Skalierung bis hin zu Sicherheit, Compliance und Updates. Für IT-Verantwortliche bedeutet dies eine deutliche Entlastung im Betrieb und eine konsistente Nutzererfahrung über verschiedene Geräte und Standorte hinweg. SaaS eignet sich insbesondere für standardisierte Geschäftsprozesse wie E-Mail, Kollaboration, CRM oder ERP.

6.3 Shared Responsibility Model bei Cloud-Services

Das Shared Responsibility Model legt fest, welche Sicherheitsaufgaben beim Cloud-Anbieter und welche beim Kunden liegen. Der Anbieter schützt die Infrastruktur, der Kunde ist für eigene Daten, Zugriffe und Konfigurationen verantwortlich. Je nach Service-Modell (IaaS, PaaS, SaaS) verschieben sich diese Verantwortlichkeiten: IaaS verlangt viel Eigenverantwortung vom Kunden, bei PaaS übernimmt der Anbieter mehr Aufgaben, und bei SaaS liegt der Fokus des Kunden auf richtiger Nutzung und Datenschutz.



Top-Maßnahmen

- Hohe Priorität: Sicherheitsstandards des Anbieters überprüfen und Nachweise wie Zertifizierungen (z. B. ISO 27001, C5, SOC 2 Type II) sowie die Einhaltung relevanter Normen und gesetzlicher Anforderungen einfordern.
- Quick Win: Cloud Questionaire auf Basis ISO27001 / C5 mit klar definierten Minimalanforderungen muss vom Cloud Provider befüllt und die umgesetzten Maßnahmen dokumentiert/bestätigt werden

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Verantwortlichkeiten klären: Präzise prüfen, welche Sicherheitsaufgaben beim Cloud-Provider und welche beim eigenen Unternehmen liegen.
- Dokumentation der Verantwortlichkeiten für das gewählte Service-Modell (IaaS, PaaS, SaaS)
- Risikoanalyse durchführen: Die Risiken in Bezug auf Datenhaltung, Datenverarbeitung und Zugriff regelmäßig bewerten und Maßnahmen zur Risikominderung planen.
- Eigene Sicherheitsmaßnahmen umsetzen: Für die eigenen Verantwortungsbereiche (z. B. Zugriffsmanagement, Verschlüsselung, Konfiguration) angemessene Schutzmaßnahmen implementieren

2. Überwachung und Erkennung

- Transparenz und Kommunikation – einen regelmäßigen Austausch mit dem Cloud-Anbieter zu Sicherheitsvorfällen, Updates und Änderungen an Sicherheitspraktiken sicherstellen.
- Eigenen Sicherheitsmaßnahmen regelmäßig überprüfen / auditieren
- Notfalltestszenarien und Durchführung der Tests planen, Ergebnisse dokumentieren und bewerten
- Interne / Externe Penetration Tests durchführen

3. Reaktion bei Vorfällen

- Definition klarer Notfallprozesse, Kommunikationspfade und Verankerung der Cloud Systeme im Notfallhandbuch
- Regelmäßige Simulation von Vorfällen
- Transparenz und Kommunikation: Einen regelmäßigen Austausch mit dem Cloud-Anbieter zu Sicherheitsvorfällen, Updates und Änderungen an Sicherheitspraktiken sicherstellen.

4. Wiederherstellung und Kontinuität

- Pflege detaillierter Wiederherstellungs-Anleitungen (Runbooks) für jeden Cloud-Service.
- Durchführung regelmäßiger, geplanter Wiederherstellungstests.
- Definition einer Exit Strategie

Lessons Learned

- Exit Strategie bei Beendigung des Cloud-Services technisch und kaufmännisch bereits bei der Beauftragung vereinbaren
- Datensicherung außerhalb des Cloud-Services etablieren
- Das Vorhandensein eines ISO27001 Zertifikats bedeutet nicht, dass der genutzte Cloud-Service im Scope abgedeckt ist
- Zuständigkeiten für den Betrieb / Datensicherung / Schwachstellenmanagement / Change Management konkret und verbindlich dokumentieren

6.4 Bewertung Sicherheitsstandards des Providers

Industrie Standards / Normen

Um Sicherheits-, Datenschutz- und Compliance-Risiken wirksam zu minimieren, ist es für IT-Verantwortliche essenziell, dass Cloud Provider anerkannte Standards wie ISO/IEC 27001, C_5, SOC 2 oder ISO/IEC 27018 nachweislich erfüllen. Diese Zertifizierungen dienen als verlässlicher Indikator für ein systematisch umgesetztes Sicherheits- und Risikomanagement.

Verfügt ein Provider über keine entsprechenden Nachweise, liegt die Prüfpflicht beim Kunden. In diesem Fall müsste die IT-Abteilung selbst für eine umfassende technische, organisatorische und rechtliche Bewertung sorgen, etwa durch Vor-Ort-Audits, Penetration Tests oder individuelle Sicherheitsanalysen. Dies verursacht nicht nur zusätzlichen Aufwand, sondern birgt auch operative und regulatorische Risiken.
Der Scope (Geltungsbereich) einer Zertifizierung ist entscheidend für deren Aussagekraft, da sie sich oft nur auf bestimmte Rechenzentren, Dienste oder Unternehmensbereiche bezieht. Daher muss jede Zertifizierung kontextbezogen geprüft werden, um sicherzustellen, dass die jeweils genutzten Cloud-Dienste tatsächlich vom zertifizierten Geltungsbereich abgedeckt sind.

Datenschutz

Beim Einsatz von Cloud-Services ist der Datenschutz ein zentrales Prüfungskriterium, insbesondere wenn personenbezogene oder besonders schützenswerte Daten verarbeitet werden. Unternehmen müssen sicherstellen, dass der Cloud-Anbieter alle Anforderungen der Datenschutz-Grundverordnung (DSGVO) erfüllt – dazu zählen unter anderem ein rechtskonformer Auftragsverarbeitungsvertrag (DPA / AVV), transparente Informationen zur Datenverarbeitung, sowie technische und organisatorische Maßnahmen (TOMs) zum Schutz der Daten. Zudem ist zu prüfen, ob und in welchem Umfang eine Datenübertragung in Drittländer stattfindet und ob hierfür gültige Standardvertragsklauseln (SCC) oder ein angemessener Schutzmechanismus vorliegt. Besonders wichtig ist, dass Verantwortlichkeiten klar geregelt sind und die eingesetzten Dienste tatsächlich innerhalb des zertifizierten Geltungsbereichs (Scope) der Anbieterzertifizierungen liegen.

Regelwerk	Pflicht	Optional	Beschreibung
EU-DSGVO / GDPR	✓		Datenschutz-Grundverordnung der EU – Grundlage für rechtmäßige Verarbeitung personenbezogener Daten.
ISO/IEC 27001	✓		Standard für Informationssicherheitsmanagementsysteme (ISMS).
ISO/IEC 27018		✓	Erweiterung von ISO 27001 für Datenschutz in der Cloud.
ISO/IEC 27017		✓	Empfehlungen für Cloud-spezifische Sicherheitskontrollen.
SOC 2 (Type II)		✓	Auditierung nach Trust Service Criteria – Fokus auf Sicherheit und Verfügbarkeit.

C5 (BSI)		✓	BSI-Katalog für Cloud-Sicherheit – besonders relevant für Deutschland.
Data Processing Agreement	✓		Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO.
Standard Contractual Clauses (CSS)		✓	Standardklauseln für Datenübermittlung in Drittländer.
Binding Corporate Rules (BCR)		✓	Interne Datenschutzregeln für internationale Konzerne.
CSA STAR		✓	Cloud Security Assessment durch die Cloud Security Alliance.
ISO/IEC 22301		✓	Standard für Notfall- und Krisenmanagement (BCM).
TISAX		✓	Informationssicherheitsstandard in der Automobil-industrie.
CSA CCM		✓	Cloud Security Controls (Ziele ist die Standardisierung von Cloud Sicherheitskontrollen / Vergleichbarkeit von Cloud-Providern/-Kunden).

Bewertung der Sicherheits-/Datenschutzstandards des Providers

Geographische und Geopolitische Aspekte

Auch die Cloud-Souveränitätsanforderungen sollten Kunden im Kontext von Cloud Security betrachten, da sie die Kontrolle über Daten, Prozesse und Compliance sicherstellen.

Top-Maßnahmen

- Hohe Priorität: Geographische und geopolitische Souveränität bei der Wahl des Speicherorts beeinflusst, welchen rechtlichen Zugriff Dritte (z. B. Behörden anderer Staaten) auf Daten haben könnten. Daher ist es essenziell, Anbieter und Standorte gezielt auszuwählen.
- Quick Win: Datenlokalisierung – die Kunden sollten wissen, in welchen Ländern und Rechenzentren ihre Daten gespeichert werden. Die Speicherung muss den eigenen Compliance-Anforderungen und gesetzlichen Vorgaben entsprechen, insbesondere bei sensiblen oder personenbezogenen Daten.

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Kontrolle über Verschlüsselung und Schlüsselmanagement: Kunden sollten idealer-weise selbst die Kontrolle über die Verschlüsselung und das Schlüsselmanagement behalten, um unautorisierten Zugriff durch Dritte oder den Cloud-Anbieter zu verhindern.

- Transparenz und Nachvollziehbarkeit: Es muss klar dokumentiert sein, wie und wo Daten verarbeitet werden und wer Zugriff darauf hat. Regelmäßige Audits und Berichte (z. B. SOC 2 Type II) unterstützen die Überprüfung der Einhaltung von Souveränitätsanforderungen.
- Vertragliche und technische Maßnahmen: Es sollten vertragliche Regelungen und technische Maßnahmen getroffen werden, um die Souveränität über die eigenen Daten und Prozesse sicherzustellen und Risiken zu minimieren.

2. Überwachung und Erkennung

- Transparenz und Kommunikation – einen regelmäßigen Austausch mit dem Cloud-Anbieter zu Änderungen im Kontext Compliance, Rechenzentrumsstandorten
- Anforderung des aktuellen SOC 2 Type II Report an und prüfen Sie, ob die im Report beschriebenen Kontrollen und Maßnahmen mit Ihren eigenen Sicherheits-anforderungen übereinstimmen.
- Nutzen Sie den Report als Grundlage für Ihre Risikoanalyse und die Bewertung der gemeinsamen Verantwortlichkeiten. Dokumentieren Sie die Ergebnisse im Rahmen Ihres Auswahl- und Auditprozesses und stellen Sie sicher, dass der Cloudprovider regelmäßige Aktualisierungen des Reports vorlegt.

3. Reaktion bei Vorfällen

- Vertraglich vorab fixieren, dass der Cloudprovider Änderungen im Kontext Rechen-zentrumsstandorten unverzüglich vom Kunden genehmigen lassen muss.
- Vertraglich vorab fixieren, dass Informationssicherheitsvorfälle und daraus resultierende negative Einflüsse auf die Ziele der Informationssicherheit unverzüglich und trans-parent gemeldet werden müssen.

4. Wiederherstellung und Kontinuität

- Pflege detaillierter Wiederherstellungs-Anleitungen (Runbooks) für jeden Cloud Service unter Berücksichtigung geographischer Regularien / vertraglicher Vereinbarungen.

Lessons Learned

- Regelmäßige Überprüfung der Einhaltung der Compliance Anforderungen durch den Kunden ist notwendig, bspw. Jährlicher update des Cloud Questionaires.
- Risikoanalyse und die Bewertung der gemeinsamen Verantwortlichkeiten. Dokumentieren Sie die Ergebnisse im Rahmen Ihres Auswahl- und Auditprozesses und stellen Sie sicher, dass der Cloudprovider regelmäßige Aktualisierungen des Reports vorlegt.
- Definition von Unternehmensstandards für freigegebene Länder für Rechenzentrums-standorte beschleunigt die Entscheidungsprozesse.

6.5 Integration

Neben den in Kapitel 4 dargestellten allgemeinen IT-Sicherheitsmaßnahmen gibt es einige Besonderheiten, die insbesondere im Zusammenhang mit Cloud-Services berücksichtigt werden müssen. Für die sichere Integration eines Cloud-Services in die eigene IT sind u.a. mehrere zentrale Aspekte zu beachten.

- **Identity & Access Management (IAM):** Es muss sichergestellt werden, dass der Zugriff auf Cloud-Ressourcen strikt nach dem Prinzip der minimalen Rechte (Least Privilege) erfolgt. Rollen- und Berechtigungskonzepte sowie eine regelmäßige Überprüfung der vergebenen Zugriffsrechte sind essenziell, um Missbrauch oder unautorisierten Zugriff zu verhindern.
- **Konnektivität:** Die Verbindung zwischen der eigenen Infrastruktur und dem Cloud Service sollte über gesicherte, verschlüsselte Kanäle (z. B. VPN, TLS) erfolgen. Zusätzlich sind Firewalls und Netzwerksegmentierung zu implementieren, um Angriffsflächen zu minimieren.
- **Datenverarbeitung:** Es ist zu prüfen, wo und wie Daten verarbeitet werden. Die Verarbeitung sensibler oder personenbezogener Daten muss im Einklang mit geltenden Datenschutzvorgaben (z. B. DSGVO) erfolgen. Transparenz über die Datenflüsse und Verarbeitungsprozesse ist unerlässlich.
- **Datenhaltung:** Die Speicherung der Daten sollte unter Berücksichtigung von Datenlokalisierung (Geografie, Souveränität) und Compliance-Anforderungen erfolgen. Es ist zu klären, in welchen Ländern und Rechenzentren die Daten abgelegt werden und ob dies mit den eigenen Vorgaben vereinbar ist.
- **Verschlüsselung und Key Management:** Sämtliche Daten, die in der Cloud gespeichert oder übertragen werden, sollten durch starke Verschlüsselungsverfahren geschützt sein. Das Management der Schlüssel (Key Management) sollte idealerweise beim Kunden verbleiben oder durch vertrauenswürdige, auditierte Services erfolgen, um einen unautorisierten Zugriff auf die Daten auszuschließen.
- **Monitoring und Logging:** Alle Aktivitäten in der Cloud sollten kontinuierlich überwacht und protokolliert werden. So lassen sich sicherheitsrelevante Vorfälle schnell erkennen und nachvollziehen. Logs müssen vor Manipulation geschützt, regelmäßig eprüft und datenschutzkonform archiviert werden.

Diese Maßnahmen sind essenziell, um die Sicherheit, Integrität und Vertraulichkeit der eigenen Daten bei der Nutzung von Cloud-Services zu gewährleisten und Compliance-Risiken zu minimieren.

Top-Maßnahmen

- Hohe Priorität: IAM für Cloud-Services vollständig in die IAM Prozesse der on premise Services integrieren.
- Quick Win: Integration der Benutzeridentitäten in den Unternehmensverzeichnisdienst inkl. SSO Realisierung.

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Gesicherte, verschlüsselte Kommunikation
- Netzwerksegmentierung / Einsatz Firewalls
- Prüfung Datenschutzrelevante Aspekte
- Verschlüsselung / Schlüsselmanagement selbst betreiben/weiterentwickeln

2. Überwachung und Erkennung

- Integration des Monitorings und Logging in das zentrale Monitoring und die Logging Infrastruktur des Unternehmens

3. Reaktion bei Vorfällen

- Risikobewertung
- Vorbereitende Maßnahmen umsetzen, damit im Notfall der betroffene Service schnell und unkompliziert deaktiviert werden kann

4. Wiederherstellung und Kontinuität

- Das Management der Schlüssel (Key Management) sowie deren Wiederherstellung / Recovery müssen regelmäßig getestet werden

Lessons Learned

- Schlüsselmanagement sollte beim Kunden verbleiben
- Zentrales Monitoring aller relevanten Services (Cloud + on premise) ist für die Alarmierung und Analyse extrem wichtig

6.6 Betrieb

Beim Betrieb von Cloud-Services müssen Unternehmen sicherstellen, dass neben technischen Sicherheitsmaßnahmen auch organisatorische Prozesse etabliert sind, die den zuverlässigen, transparenten und DSGVO-konformen Einsatz der Dienste gewährleisten. Die folgenden Maßnahmen orientieren sich an den Anforderungen der ISO/IEC 27001:2022 und bilden die Grundlage für ein strukturiertes, risikobasiertes Cloud-Betriebsmodell. Sie helfen dabei, operative Stabilität, regulatorische Sicherheit und strategische Steuerbarkeit sicherzustellen – sowohl gegenüber dem Cloud-Anbieter als auch innerhalb der eigenen Organisation.

- **SLAs (Service Level Agreements):** Definieren verbindlich vereinbarter Leistungskennzahlen wie Verfügbarkeit, Reaktionszeiten und Eskalationsmechanismen. Sie bilden die Grundlage für Servicequalität und müssen regelmäßig überprüft und bei Bedarf angepasst werden.
- **Incident Management:** Ein strukturierter Prozess zur Erkennung, Meldung, Klassifizierung und Behandlung von Sicherheitsvorfällen wie Datenlecks, Systemausfällen oder Angriffen. Dieser Prozess muss klar dokumentiert und mit gesetzlichen Meldepflichten – etwa gemäß DSGVO – abgestimmt sein.
- **Change Management:** Stellt sicher, dass Änderungen an Cloud-Diensten kontrolliert, nachvollziehbar und risikoarm durchgeführt werden. Dazu gehören Freigabeprozesse, Risikobewertung, Kommunikation mit Stakeholdern und ggf. Rollback-Strategien.
- **Service Management / Betrieb:** Umfasst die kontinuierliche Steuerung, Überwachung und Optimierung der eingesetzten Cloud-Dienste im Einklang mit unternehmensinternen ITSM-Prozessen (z. B. nach ITIL). Ziel ist ein stabiler, effizienter und revisionssicherer Betrieb.

- **Vulnerability Management:** Bezieht sich auf die Identifikation, Bewertung und Beseitigung von Schwachstellen innerhalb der Cloud-Infrastruktur. Hierzu zählen regelmäßige Schwachstellenscans, Patch-Management, Penetration Tests sowie der Umgang mit veröffentlichen CVEs.
- **Lieferantenbewertung und -management:** Die ISO/IEC 27001:2022 fordert unter den Kontrollen 5.19 („Supplier relationships“) und 5.22 („Information security for use of cloud services“) ein strukturiertes Management externer Anbieter. Cloud Provider müssen vor Vertragsabschluss risikobasiert bewertet werden – anhand von Sicherheitszertifikaten, Leistungsfähigkeit, Standort, Subdienstleistern und Datenschutzmaßnahmen. Vertragsinhalte wie SLAs, Auditrechte, Exit-Klauseln und technische Anforderungen müssen dokumentiert und im Betrieb regelmäßig geprüft werden. Auch eine kontinuierliche Neubewertung bei Änderungen im Service oder der Risikolage ist verpflichtend.
- **Auditierbarkeit & Nachvollziehbarkeit:** Cloud-Dienste müssen ausreichend dokumentiert, konfiguriert und überwacht sein, um interne sowie externe Audits zu ermöglichen. Dazu gehören u. a. Audit-Logs, Konfigurationshistorien, Zugriffsdokumentation und Nachweise zu Maßnahmenumsetzung.
- **Verfügbarkeits- & Notfallmanagement:** Es müssen Strategien und technische Maßnahmen bestehen, um bei Ausfällen schnell wiederherstellen zu können. Dazu gehören Backup-Konzepte, geografisch redundante Systeme, Disaster-Recovery-Pläne und regelmäßige Tests zur Wirksamkeit.
- **Rollen & Verantwortlichkeiten:** Die Verantwortlichkeiten zwischen Kunde und Cloud-Anbieter müssen klar abgegrenzt sein (Shared Responsibility Model). Intern sind Rollen zur Verwaltung, Absicherung und Überwachung der Cloud-Dienste zu definieren und zu dokumentieren.
- **Green IT / Nachhaltigkeit:** Nachhaltigkeitsaspekte spielen eine wachsende Rolle bei der Auswahl und dem Betrieb von Cloud-Diensten. Zu prüfen sind energieeffiziente Rechenzentren, CO_2-Bilanzen, Anbieter-Transparenzberichte und strategische Klimaziele.
- **Kontinuierliche Verbesserung (ISMS-Zyklus):** Alle Prozesse im Cloud-Betrieb müssen regelmäßig im Rahmen des PDCA-Zyklus (Plan-Do-Check-Act) bewertet und optimiert werden. Das unterstützt eine nachhaltige Sicherheitskultur und stellt die Anpassung an neue Bedrohungslagen sicher.

Top-Maßnahmen

- Hohe Priorität: Service Level Agreements mit konkreter und detaillierte Dokumentation
- Quick Win: Cloud Questionaire auf Basis ISO27001 / C_5 mit klar definierten Minimalanforderungen muss vom Cloud Provider befüllt und die umgesetzten Maßnahmen dokumentiert/bestätigt werden

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Incident / Change / Service Management Prozesse
- Vulnerability und Patcjmanagement Prozesse
- Lieferantenbewertung bei der Auswahl externer Cloud Provider

- Verfügbarkeits- & Notfallmanagement und die Integration der Cloud und Kunden Prozesse
- Rollen & Verantwortlichkeiten
- PDCA / ISMS Zyklus der kontinuierlichen Verbesserung
- Green IT / Nachhaltigkeit

2. Überwachung und Erkennung

- Lieferantenbewertung und -management
- Assessments
- Audits / interne+externe Penetrationtests
- SOC II Reports / Berichte aus Zertifizierungs-/Überwachungsaudits

3. Reaktion bei Vorfällen

- Definition klarer Notfallprozesse, Kommunikationspfade und Verankerung der Cloud Systeme im Notfallhandbuch
- Regelmäßige Simulation von Vorfällen
- Transparenz und Kommunikation: Einen regelmäßigen Austausch mit dem Cloud-Anbieter zu Sicherheitsvorfällen, Updates und Änderungen an Sicherheitspraktiken sicherstellen.

4. Wiederherstellung und Kontinuität

- Pflege detaillierter Wiederherstellungs-Anleitungen (Runbooks) für jeden Cloud-Service.
- Durchführung regelmäßiger, geplanter Wiederherstellungstests.
- Definition einer Exit Strategie

Lessons Learned

- Exit Strategie bei Beendigung des Cloud-Services technisch und kaufmännisch bereits bei der Beauftragung vereinbaren
- Datensicherung außerhalb des Cloud-Services etablieren
- Das Vorhandensein eines ISO27001 Zertifikats bedeutet nicht, dass der genutzte Cloud-Service im Scope abgedeckt ist
- Zuständigkeiten für den Betrieb / Datensicherung / Schwachstellenmanagement / Change-Management konkret und verbindlich dokumentieren

Zusammenfassende Tabelle: Weiterführende Dokumentation

Standards und Frameworks

27001 Annex A (deutsche Control-Bezeichnung)	Cloud-Fokus	BSI C5 IT-Grundschutz
A.5.19 Informationssicherheit in Lieferantenbeziehungen	Steuerung vom CSPs und Subdienstleistern	C5 Governance / Lieferantenmanagement; IT-GS DER.1, ORP.3
A.5.20 Behandlung der Informationssicherheit in Lieferantenvereinbarungen	Sicherheitsanforderungen in Cloud-Verträgen, Auditrechte	C5 Vertragsanforderungen; IT-GS DER.1
A.5.21 Management der Informationssicherheit in der IKT Lieferkette	Subprozessoren und Shared Responsibility	C5 Third-Party Assurance; IT-GS DER.1
A.5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantenleistungen	Subprozessoren und Shared Responsibility	C 5 Third-Party Assurance; IT-GS DER.1
A.5.23 Informationssicherheit bei der Nutzung von Cloud-Diensten	Zentrales Cloud-Control für Nutzung und Governance	C5 Gesamtframework; IT-GS ORP/OPS/CON
A.5.30 IKT Bereitschaft für Business Continuity	Cloud-Resilienz, Multi-Region, Disaster Recovery	C5 BCM; BSI Standard 200-4; OPS.1.1.2
A.8.2 Privilegierte Zugriffsrechte	Admin-Zugriffe und PAM in Cloud	C5 IAM; IT-GS ORP.4
A.5.17 Authentifizierungs-informationen	Schutz von Credentials, API Keys, MFA	C5 Authentisierung; IT-GS ORP.4
A.8.20 Netzwerksicherheit	VPC/VNet Segmentierung und Netzschutz	C5 Netzsicherheit; IT-GS SYS.1.1
A.8.9 Konfigurationsmanagement	Cloud Hardening und Baselines	C5 Systemhärtung; IT-GS CON.8
A.8.15 Protokollierung	Audit-Logs und SIEM Integration	C5 Logging; IT-GS OPS.1.1.5
A.8.16 Überwachungsaktivitäten	Cloud Monitoring und Threat Detection	C5 Monitoring; IT-GS DER.1
A.8.24 Einsatz von Kryptographie	Verschlüsselung und Key Management	C5 Kryptografie; TR-02102; CON.1

A.8.10 Löschen von Informationen	Sichere Datenlöschung und Tenant Exit	C5 Datenlöschung; IT-GS CON.6
A.8.12 Verhinderung von Datenabfluss	Schutz vor Datenexfiltration	C5 Datenschutzmaßnahmen; IT-GS CON.3
A.8.13 Datensicherung	Backup, Restore und Immutable Backups	C5 Datensicherung; IT-GS OPS.1.1.2
A.8.28 Sichere Programmierung	Secure Development für Cloud Apps	C5 sichere Entwicklung; IT-GS APP.4
A.8.29 Sicherheitsprüfungen in Entwicklung und Abnahme	Security Testing und DevSecOps	C5 Sicherheitsprüfungen; IT-GS APP.4
A.8.31 Trennung von Entwicklungs-, Test- und Produktionsumgebungen	Trennung von Cloud-Umgebungen	C5 Mandantentrennung; IT-GS APP.4

Zusammenfassende Tabelle: Weiterführende Dokumentation

Regulatorische Bezüge

27001 Annex A (deutsche Control-Bezeichnung)	NIST	CSA CCM	Regulatorische Bezüge (EU/DE)
A.5.19 Informationssicherheit in Lieferantenbeziehungen	SP 800-161; SP 800-53 SR	STA, GRM	NIS2 Lieferkette; DSGVO Art. 28
A.5.20 Behandlung der Informationssicherheit in Lieferantenvereinbarungen	SP 800-53 SA-9, SR-3	STA, IPY, GRM	DSGVO Art. 28, Art. 32
A.5.21 Management der Informationssicherheit in der IKT Lieferkette	SP 800-161; SP 800-53 SR-5	STA, TVM	NIS2 Art. 21
A.5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantenleistungen	SP 800-161; SP 800-53 SR-5	GRM, LOG	NIS2; DSGVO Rechenschaftspflicht
A.5.23 Informationssicherheit bei der Nutzung von Cloud-Diensten	SP 800-144; SP 800-210	CCM gesamt	DSGVO Art. 28/32; NIS2
A.5.30 IKT Bereitschaft für Business Continuity	SP 800-34	BCR	NIS2 Resilienzpflichten
A.8.2 Privilegierte Zugriffsrechte	SP 800-63B; SP 800-53 AC-2/6	IAM	DSGVO Art. 32

A.5.17 Authentifizierungs-informationen	SP 800-63B	IAM, EKM	DSGVO Art. 32
A.8.20 Netzwerksicherheit	SP 800-207; SP 800-53 SC-7	IVS, NSI	NIS2 Art. 21
A.8.9 Konfigurationsmanagement	SP 800-128; SP 800-53 CM	CCC, TVM	BSI C5; NIS2
A.8.15 Protokollierung	SP 800-92	LOG	NIS2
A.8.16 Überwachungsaktivitäten	SP 800-137	LOG, SEF	NIS2
A.8.24 Einsatz von Kryptographie	SP 800-57; SP 800-175B	EKM, DSI	DSGVO Art. 32
A.8.10 Löschen von Informationen	SP 800-88	DSI	DSGVO Art. 17
A.8.12 Verhinderung von Datenabfluss	SP 800-53 SI	DSP, DSI	DSGVO Art. 32
A.8.13 Datensicherung	SP 800-34	BCR	NIS2
A.8.28 Sichere Programmierung	SP 800-218	AIS, TVM	CRA / AI Act
A.8.29 Sicherheitsprüfungen in Entwicklung und Abnahme	SP 800-218; SP 800-53 SA-11	AIS, TVM	CRA
A.8.31 Trennung von Entwicklungs-, Test- und Produktionsumgebungen	SP 800-53 CM-2	AIS, IVS	DSGVO Art. 25

Kennzahlen zur Messung der Cloud Security Reife

Im Anhang (Kapitel 8, Tabelle 1) dieses Dokuments sind ausgewählte Kennzahlen (Key Performance Indicators, KPIs) aufgeführt, mit denen die Reife der Cloud Security Architektur gemessen wird.

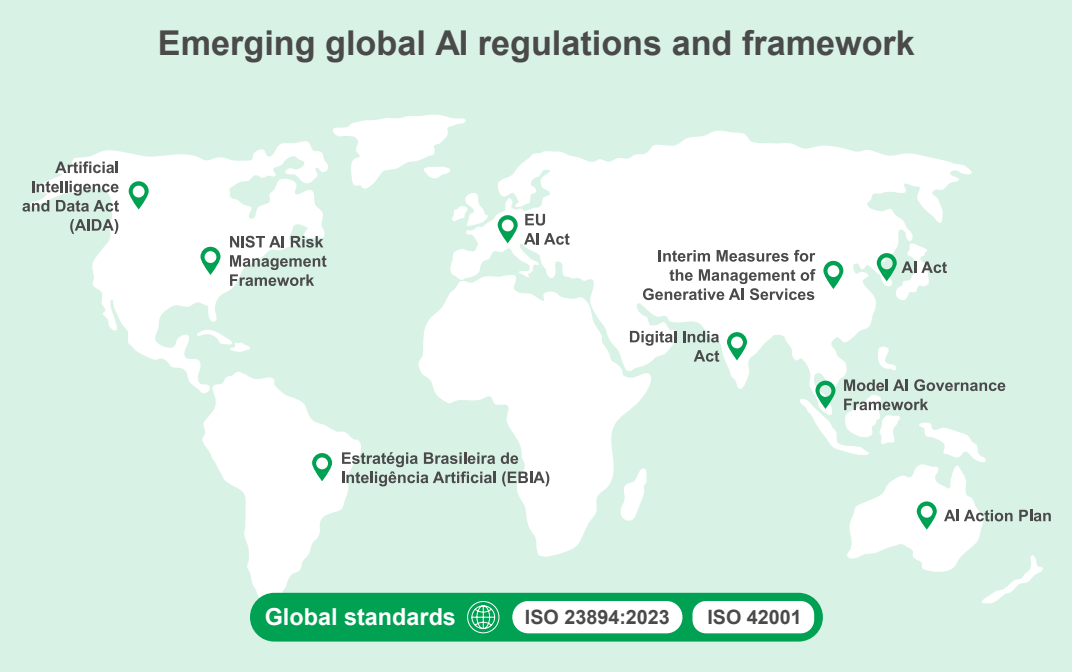
Die Kennzahlen sind an anerkannten Cloud Security Standards und Frameworks wie **ISO/IEC 27017**, **ISO/IEC 27018**, **ISO/IEC 27001** sowie der **Cloud Security Alliance Cloud Controls Matrix (CSA CCM)** ausgerichtet.

Sie unterstützen die objektive Bewertung des Sicherheitsniveaus von Cloud Infrastrukturen und Services, insbesondere im Hinblick auf Shared Responsibility Modelle, Identitäts und Zugriffskontrollen, Mandantentrennung sowie Compliance Anforderungen.

7 Künstliche Intelligenz

Künstliche Intelligenz (KI) ist längst zum integralen Bestandteil der automobilen Lieferkette geworden und beeinflusst sowohl Unternehmensprozesse als auch die Produktentwicklung maßgeblich. Mit dem zunehmenden Einsatz von KI-Systemen ergeben sich jedoch auch neue Risiken und Herausforderungen für die Cybersicherheit, die weit über klassische IT- und OT-Schutzmaßnahmen hinausgehen. Da Angreifer verstärkt KI für gezielte Angriffe einsetzen und KI-gestützte Systeme neue potenzielle Schwachstellen eröffnen, wird die Absicherung von KI-Lösungen für moderne Cybersecurity-Architekturen zunehmend wichtiger.

Die Umsetzung von Responsible-AI-Prinzipien wie Sicherheit, Nachvollziehbarkeit, Transparenz und Robustheit schafft dabei eine wichtige Grundlage, um Informationssicherheit und Cyberrisiken entlang der automobilen Wertschöpfungskette zu minimieren und regulatorische Anforderungen sowie Auditierbarkeit wie den EU AI Act und die ISO/IEC 42001 zu erfüllen.



Weiterführende Quellen:

- OECD AI Principles
- EEE Ethically Aligned Design
- European Commission’s Ethics Guidelines for Trustworthy AI
- Anforderungen, Prüfkriterien und Prüfmethodologien des BSI zu Künstlicher Intelligenz

Für eine strukturierte Betrachtung der Cyber- und Informationssicherheit im Kontext von KI empfehlen sich folgende zentrale Handlungsfelder, die in den nachfolgenden Unterkapiteln näher beleuchtet werden:

1. Risiken für KI aufgrund externer Angriffe

2. Risiken durch Nutzung von KI

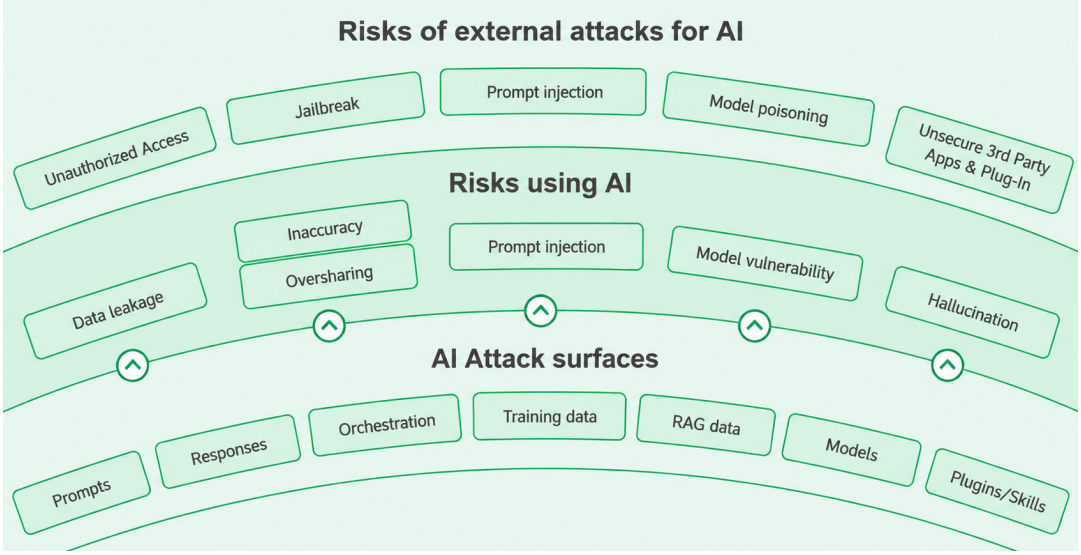
3. Nutzungsszenarien

- Einsatz generativer KI durch Mitarbeitende im Arbeitsalltag
- Anwendung und Einbindung von KI-Applikationen in Geschäftsprozesse
- Integration von KI-Modellen in Produkte und während der Produktentwicklung

4. KI Governance

Die folgende Darstellung zeigt die Risiken in ihrem Kontext und orientiert sich an den OWASP Top 10 KI-Bedrohungen.

Grundsätzlich gelten für ein KI-System die gleichen Sicherheitsanforderungen, die in den vorherigen Kapiteln IT, OT und Cloud adressiert wurden als Grundlage.



Mögliche Angriffsziele auf ein KI System können sein:

- **Prompts:** Durch Prompt Injection können Angreifer die KI manipulieren, um schädliche Aktionen auszuführen oder sensible Daten preiszugeben.
- **Responses:** Manipulierte Antworten können zur Verbreitung von Falschinformationen oder zur Schädigung des Rufes des Systems führen.
- **Orchestration:** Angriffe auf die Orchestrierung können den Ablauf von KI-Prozessen stören oder unbefugten Zugriff ermöglichen.
- **Training Data:** Model Poisoning durch bösartige Trainingsdaten kann zu fehlerhaftem oder schädlichem Verhalten der KI führen.
- **RAG Data:** Manipulation der externen Datenquellen (Retrieval-Augmented Generation) kann zu falschen oder irreführenden Antworten führen.

- **AI Models:** Unbefugter Zugriff auf KI-Modelle ermöglicht es Angreifern, diese zu kopieren, zu verändern oder zu zerstören.
- **Plugins bzw. 3rd Party Apps:** Schwachstellen in Plugins oder Drittanbieteranwendungen können als Einfallstor für Angriffe auf das gesamte KI-System dienen.

Bei der Gestaltung von KI-basierten Architekturen sollte die „Rule of Two“ angewendet werden.

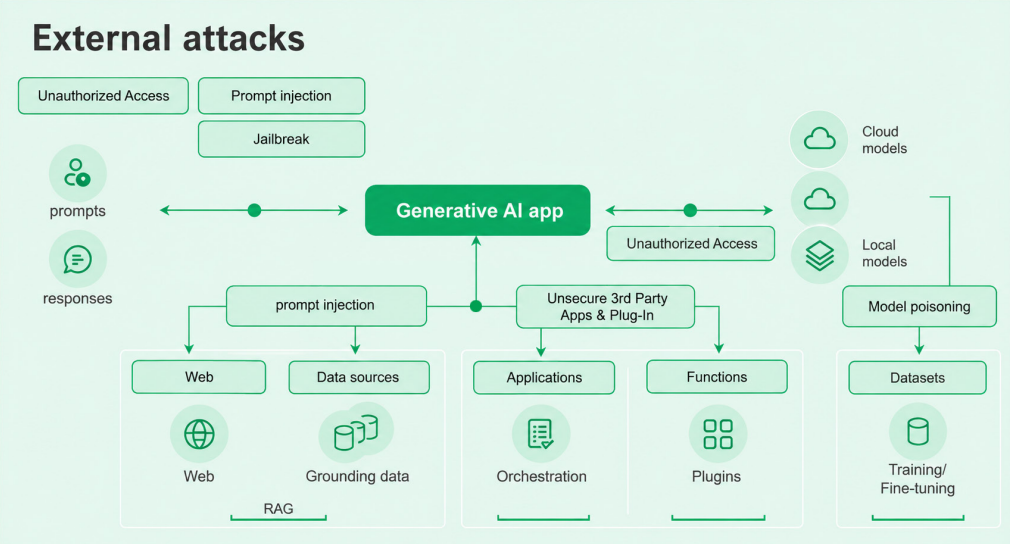
Diese besagt, dass Agenten innerhalb einer Sitzung höchstens zwei der folgenden drei Eigenschaften erfüllen dürfen:

- Ein Agent kann mit nicht vertrauenswürdigen Eingaben umgehen
- Ein Agent kann Zugriff auf sensible Systeme oder private Daten haben
- Ein Agent kann seinen Zustand verändern oder extern kommunizieren

Es ist weiterhin möglich, dass zur Ausführung einer Anfrage alle drei Eigenschaften erforderlich sind. Wenn ein Agent alle drei benötigt, ohne eine neue Sitzung zu starten (d. h. mit einem frischen Kontextfenster), dann sollte es ihm nicht erlaubt sein, autonom zu operieren, und er benötigt zumindest eine Aufsicht – etwa durch eine Human-in-the-Loop-Freigabe oder ein anderes zuverlässiges Validierungsverfahren.

7.1 Risiken für KI aufgrund externer Angriffe

Externe Angriffe auf KI-Systeme können u.a. zu Datenverlust, Manipulation, Desinformation und kompromittierter Sicherheit führen.



7.1.1 Prompt Injection

Kurz erklärt und Risiken: Prompt Injection ist eine Art „Hacking“ für KI-Systeme. Angreifer versuchen, die KI durch manipulierte Eingaben (Prompts) dazu zu bringen, Dinge zu tun, die sie nicht tun sollte – beispielsweise sensible Daten preiszugeben oder schädliche Aktionen auszuführen. Das Risiko besteht darin, dass ein Angreifer das KI-System für seine Zwecke missbrauchen kann. Es gibt direkte Angriffe, bei denen der schädliche Prompt direkt eingegeben wird, und indirekte Angriffe, bei denen die KI durch manipulierte Datenquellen beeinflusst wird.

Top-Maßnahmen

- Hohe Priorität: Eingabevalidierung und Bereinigung von Benutzereingaben, um schädliche Zeichen oder Befehle zu erkennen und ggf. zu entfernen.
- Quick Win: Beschränkung von KI-Funktionen für Benutzer, um zu verhindern, dass sie Aktionen ausführt, die Schaden anrichten könnten.

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Eingabevalidierung und Bereinigung von Benutzereingaben, um schädliche Zeichen oder Befehle zu entfernen.
- Beschränkung von KI-Funktionen, um zu verhindern, dass sie Aktionen ausführt, die Schaden anrichten könnten.
- Zum Schutz vor indirekten Prompt Injections: Validierung externer Datenquellen und Überprüfung der Datenintegrität

2. Überwachung und Erkennung

- Überwachung:
  - Echtzeitüberwachung, um verdächtige Muster oder Anomalien zu erkennen.
  - Einrichtung automatischer Benachrichtigungen, um auf verdächtige Aktivitäten aufmerksam zu werden.
- Protokollierung:
  - Protokollierung der Eingaben, Ausgaben und Aktionen der KI, um eine nachträgliche Analyse zu ermöglichen.

3. Reaktion bei Vorfällen

- Automatisierte Benachrichtigungen an das Sicherheitsteam bei Erkennung eines potenziellen Angriffs.
- Das betroffene KI-System oder die betroffene Komponente sofort isolieren, um eine weitere Ausbreitung des Angriffs zu verhindern.
- Die Quelle der schädlichen Eingabe identifizieren.
- Den Zugriff auf das System für Benutzer sperren, bis die Situation unter Kontrolle ist.

- Eine detaillierte Analyse der Prompt Injection durchführen, um die Art des Angriffs, die verwendeten Techniken und die potenziellen Auswirkungen zu verstehen.
- Orchestrierung von Sicherheitsmaßnahmen:
  – SOAR-Plattformen: Verwendung von Security Orchestration, Automation and Response (SOAR)-Plattformen, um Sicherheitsmaßnahmen zu orchestrieren und automatisierte Reaktionen auf Angriffe zu ermöglichen.

4. Wiederherstellung und Kontinuität

- Regelmäßige Datensicherungen, um im Falle eines Angriffs die Modelle und Daten wiederherstellen zu können.
- Einrichtung eines redundanten KI-Systems, um den Betrieb im Falle eines Angriffs aufrechtzuerhalten.

Lessons Learned

- Eingabevalidierung ist entscheidend, aber nicht ausreichend: Auch wenn die Bereinigung von Eingaben wichtig ist, kann sie nicht alle Angriffe verhindern. Ein umfassenderer Ansatz ist erforderlich.
- Berechtigungen einschränken, um das Schadenspotenzial zu begrenzen: Weniger Berechtigungen bedeuten weniger Möglichkeiten für Angreifer, Schaden anzurichten.
- Überwachung und Protokollierung sind unerlässlich, um Angriffe zu erkennen: Ohne Überwachung bleiben Angriffe oft unbemerkt, bis es zu spät ist.

7.1.2 Jailbreak

Kurz erklärt und Risiken: Jailbreaking ist ein Versuch, aus den Sicherheitsbegrenzungen und Sicherheitsvorkehrungen des KI-Systems auszubrechen. Angreifer versuchen, Sicherheitsvorkehrungen zu umgehen, um Antworten zu erhalten, die normalerweise blockiert würden – z.B. die Generierung von schädlichen, beleidigenden oder illegalen Inhalten. Jailbreaking wird oft durch Prompt Injection erreicht. Das Risiko besteht darin, dass die KI für unethische oder illegale Zwecke missbraucht wird und das Unternehmen dadurch Schaden erleidet (Reputationsverlust, rechtliche Konsequenzen).

Top-Maßnahmen

- Hohe Priorität: Verhaltensüberwachung und Anomalieerkennung, um ungewöhnliche Muster oder Inhalte in den Ausgaben des Modells zu erkennen, die auf einen erfolgreichen Jailbreak hindeuten könnten.
- Quick Win: Nutzung von vorhandenen Build-In Funktionalitäten zur kontinuierlichen Aktualisierung von Sicherheitsrichtlinien, die sich basierend auf dem Kontext der Konversation und dem bisherigen Verhalten des Benutzers anpassen (meist durch KI-Provider bereitgestellt).

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Ausschließliche Nutzung von Modellen, die mit einer Jailbreaks Resilience ausgestattet oder trainiert sind (u.a. über dafür ausgelegte Leaderboards/ Benchmarks ermittelbar)
- Kontinuierlich aktualisierte Sicherheitsrichtlinien: Implementierung von Sicherheitsrichtlinien, die sich dynamisch anpassen, basierend auf dem Kontext der Konversation und dem bisherigen Verhalten des Benutzers.

2. Überwachung und Erkennung

- Verhaltensüberwachung und Anomalieerkennung: Überwachung des Verhaltens des Modells über die reine Eingabevalidierung hinaus, insbesondere die Analyse der Ausgaben des Modells auf ungewöhnliche Muster oder Inhalte, die auf einen erfolgreichen Jailbreak hindeuten könnten.
- Automatisierung der Erkennung von Jailbreaks
- Einsatz von sog. „Canary-Tokens“, die speziell darauf ausgelegt sind, Jailbreak-Versuche zu erkennen. U.a. sollte ein Alarm ausgelöst,
  - wenn die KI aufgefordert wird, ein bestimmtes Wort oder eine bestimmte Phrase zu verwenden, die normalerweise vermieden wird.
  - wenn die KI eine bestimmte logische Bedingung erfüllt, die normalerweise nicht erfüllt werden sollte.
- „Red Teaming“ speziell auf Jailbreaks (ein „Red Team“ simuliert Angriffe auf die Systeme); Durchführung von Red-Teaming-Übungen, bei denen Sicherheitsexperten versuchen, das Modell mit Jailbreak-Techniken anzugreifen.

3. Reaktion bei Vorfällen

- Maßnahmen, siehe Prompt Injection

4. Wiederherstellung und Kontinuität

- Maßnahmen, siehe Kapitel 7.1.1 Prompt Injection

Lessons Learned

- Die Analyse der Ausgaben der KI ist wichtig, um Jailbreak-Versuche zu erkennen, die durch die Eingabevalidierung allein nicht erkannt werden.
- Die Automatisierung der Erkennung von Jailbreak-Versuchen ermöglicht eine schnellere Reaktion.

7.1.3 Unauthorized Access

Kurz erklärt und Risiken: Unbefugter Zugriff ermöglicht es Angreifern, in KI-Systeme einzudringen und diese zu kontrollieren. Das Risiko besteht darin, dass sensible Daten kompromittiert oder gestohlen werden, die KI für böswillige Zwecke missbraucht wird oder der Betrieb des Unternehmens gestört wird.

Top-Maßnahmen

- Hohe Priorität: (Starke) Authentifizierung – Verwendung von starken Authentifizierungsmethoden (z.B. Mehrfaktor-Authentifizierung) bei der Nutzung von KI, um unbefugten Zugriff zu verhindern.
- Quick Win: Verhinderung von „Anonymous“-Anmeldungen, um die Nachverfolgung und Verantwortlichkeit zu gewährleisten.

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Zero-Trust-Architektur (siehe auch BSI: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/ANSSI-BSI-joint-releases/LLM-based_Systems_Zero_Trust.pdf?__blob=publicationFile&v=3): Annahme, dass kein Benutzer oder Gerät automatisch vertrauenswürdig ist und jeder Zugriff einzeln autorisiert werden muss.
- (Starke) Authentisierung:
  - Verwendung von Authentisierungsmethoden bei der Nutzung von KI; Verhinderung von „Anonymous“ Anmeldungen.
  - Verwendung von Mehrfaktor-Authentifizierung (MFA) bei KI mit erhöhtem oder hohem Risiko.
- Autorisierung:
  - Least Privilege-Prinzip: Gewährung der minimal erforderlichen Berechtigungen, um Aufgaben zu erfüllen.
  - Implementierung rollenbasierter Zugriffskontrollen (RBAC) mit dem Least-Privilege-Prinzip.
  - Segmentierung: Segmentiere die KI-Systeme, um den Zugriff auf sensible Daten und Funktionen zu beschränken.

2. Überwachung und Erkennung

- Überwachung und Protokollierung: Detaillierte Protokollierung aller relevanten Aktivitäten, um verdächtige Ereignisse zu erkennen und nachzuvollziehen. Dies umfasst Anmeldeversuche, Zugriffe auf Daten, Änderungen an Konfigurationen und andere sicherheitsrelevante Ereignisse.
- Regelmäßige Sicherheitsüberprüfungen: Schwachstellen hinsichtlich des Zugriffs auf KI-Systeme identifizieren und beheben, bevor sie ausgenutzt werden können. Dies umfasst insbesondere Berechtigungsüberprüfungen.
- Modellvalidierung und -überwachung: Die Überwachung von KI-Systemen auf verdächtige Aktivitäten, wie z. B. Datenverletzungen oder ungewöhnliches Modellverhalten, ist wichtig, um die Integrität der KI-Modelle und der damit verarbeiteten Daten zu gewährleisten.

3. Reaktion bei Vorfällen

- Maßnahmen, siehe Prompt Injection (Kapitel 7.1.1.)

4. Wiederherstellung und Kontinuität

- Maßnahmen, siehe Prompt Injection (Kapitel 7.1.1.)

Lessons Learned

- Grundlegende Schutzmaßnahmen zum unbefugten Zugriff auf KI-Systeme sind wichtig, um das Risiko hinsichtlich Datenverlusts, Missbrauch der KI für böswillige Zwecke und Störungen des Betriebs zu minimieren.
- Überwachung und Erkennung sind unerlässlich, um verdächtige Aktivitäten im Kontext „Access Management“ frühzeitig zu erkennen und auf unbefugten Zugriff zu reagieren.

7.1.4 Model Poisoning

Kurz erklärt und Risiken: Model Poisoning ist das Einbringen schädlicher Daten in den KI-Trainingsprozess. Dies kann dazu führen, dass die KI fehlerhaft arbeitet oder sogar schädliches Verhalten zeigt. Das Risiko besteht darin, dass die KI falsche Entscheidungen trifft, sensible Daten kompromittiert oder für böswillige Zwecke missbraucht wird. Anders als in der klassischen Softwareentwicklung ist eine Manipulation im Entwicklungsprozess eines KI-Modells schwerer zu entdecken und die Auswirkung für das finale Produkt unmittelbar.

Top-Maßnahmen

- Hohe Priorität: Eingeschränkter Datenzugriff (nur autorisiertes Personal) auf Trainingsdaten und das KI-Modell
- Quick Win: Versionskontrolle für das KI-Modell

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Eingeschränkter Datenzugriff: Beschränkung des Zugriffs auf die Trainingsdaten und den Modellentwicklungsprozess auf autorisiertes Personal.
- Datenvalidierung und -bereinigung: Kontrollen der Trainingsdaten, um sicherzustellen, dass keine bösartigen oder manipulierten Daten in das Modell gelangen. (siehe auch als Beispiel: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/kuenstliche-intelligenz_node.html#doc451100bodyText17)
- Versionskontrolle: Verwenden eines Versionskontrollsystems, um Änderungen in Datensätzen zu verfolgen und Manipulationen zu erkennen.
- Zugriff auf die Trainingsdaten und den Modellentwicklungsprozess nur mittels MFA (Multi-Faktor-Authentifizierung).
- Einsatz von robusten Trainingsmethoden/-verfahren, wie Median- und Trimmed-Mean-Aggregation, Ensemble Learning und Adversarial Training.

2. Überwachung und Erkennung

- Anomalieerkennung: Überwachung der Trainingsdaten und des Modellverhaltens, um ungewöhnliche Muster oder Anomalien zu identifizieren, die auf einen Angriff hindeuten könnten.
- Nachverfolgung von Datenursprüngen und -transformationen mit Tools (z.B. von der OWASP).

3. Reaktion bei Vorfällen

- Isolierung des betroffenen Modells: Das kompromittierte Modell sollte sofort isoliert werden, um weiteren Schaden zu verhindern. Dies kann bedeuten, dass das Modell offline genommen oder von produktiven Systemen getrennt wird.
- Forensische Untersuchung: Eine detaillierte Untersuchung des Angriffs ist unerlässlich, um die Ursache, den Umfang und die Art der Manipulation zu verstehen. Dies umfasst die Analyse der Trainingsdaten, des Modellverhaltens und der Systemprotokolle.
- Benachrichtigung relevanter Parteien: Interne Stakeholder (z. B. Sicherheitsteam, Datenwissenschaftler, Management) und gegebenenfalls externe Parteien (z. B. Aufsichtsbehörden, Kunden) sollten über den Vorfall informiert werden. Dies ermöglichten eine koordinierte Reaktion und Transparenz.

4. Wiederherstellung und Kontinuität

- Die infizierten Trainingsdaten müssen bereinigt oder entfernt werden. Anschließend kann das Modell mit sauberen Daten neu trainiert oder aus einem Backup wiederhergestellt werden.
- Die Integrität der Daten und des Modells ist zu gewährleisten, bevor sie wieder in Betrieb genommen werden.

Lessons Learned

- Prävention ist entscheidend: Schutzmaßnahmen wie eingeschränkter Datenzugriff, Datenvalidierung, Versionskontrolle und Trainingsverfahren verhindern Model-Poisoning.
- Überwachung und Erkennung sind notwendig: Kontinuierliche Überwachung von Trainingsdaten und Modellverhalten erkennt Anomalien.
- Schnelle Reaktion minimiert Schaden: Im Falle eines Angriffs sind Isolierung, Untersuchung, Benachrichtigung und Bereinigung/Wiederherstellung entscheidend.

7.1.5 Unsecure 3rd Party Apps & Plug-ins

Kurz erklärt und Risiken: Model Drittanbieter-Apps und Plug-ins (Hinweis: KI-Integrationsarchitekturen basierend auf A2A und MCP sind hier nicht berücksichtigt) können Schwachstellen in KI-Systeme einschleusen, da sie oft Zugriff auf sensible Daten haben. Angreifer können diese Schwachstellen ausnutzen, um unbefugten Zugriff zu erlangen, Daten zu stehlen, KI-Systeme zu manipulieren oder zu kompromittieren. Dies stellt ein erhebliches Sicherheitsrisiko dar.

Top-Maßnahmen

- Hohe Priorität: Regelmäßige Sicherheitsüberprüfungen und Audits von Drittanbieter-Apps und Plug-ins, um Schwachstellen zu identifizieren und zu beheben.
- Quick Win: Verwendung von Whitelisting, um nur vertrauenswürdige Drittanbieter-Apps und Plug-ins zuzulassen.

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Beschränkung der Berechtigungen, die Drittanbieter-Apps und Plug-ins für den Zugriff auf KI-Systeme und Daten haben.
- Verwendung von Whitelisting, um nur vertrauenswürdige Drittanbieter--Apps und Plug-ins zuzulassen.
- Regelmäßige Aktualisierung von Drittanbieter-Apps und Plug-ins, um Sicherheitslücken zu beheben.
- Verwendung von Sandboxing-Technologien, um Drittanbieter-Apps und Plug-ins in einer isolierten Umgebung auszuführen.

2. Überwachung und Erkennung

- Überwachung der Aktivitäten von Drittanbieter-Apps und Plug-ins, um verdächtiges Verhalten (u.a. ungewöhnliche Zugriffsversuche, Manipulation von Informationen im KI-Modell oder Manipulation des Eingabeprompts) zu erkennen.
- Einsatz von Threat Intelligence: Nutzung von Threat Intelligence, um Informationen über bekannte Schwachstellen und Angriffe im Zusammenhang mit Drittanbieter-Apps und Plug-ins zu erhalten.
- Regelmäßige Sicherheitsüberprüfungen und Audits von Drittanbieter-Apps und Plug-ins, um Schwachstellen zu identifizieren und zu beheben.

3. Reaktion bei Vorfällen

- Isolierung betroffener Systeme: Dies verhindert die Ausbreitung des Angriffs auf andere Teile des KI-Systems oder des Netzwerks.
- Durchführung einer gründlichen Untersuchung: Dies erfordert die Zusammenarbeit mit dem Drittanbieter, um Ursache, betroffene Daten und Risiken der Sicherheitsverletzung zu ermitteln. Die Überprüfung von Systemprotokollen und Netzwerkverkehr hilft, weitere Anzeichen einer Kompromittierung zu finden.

4. Wiederherstellung und Kontinuität

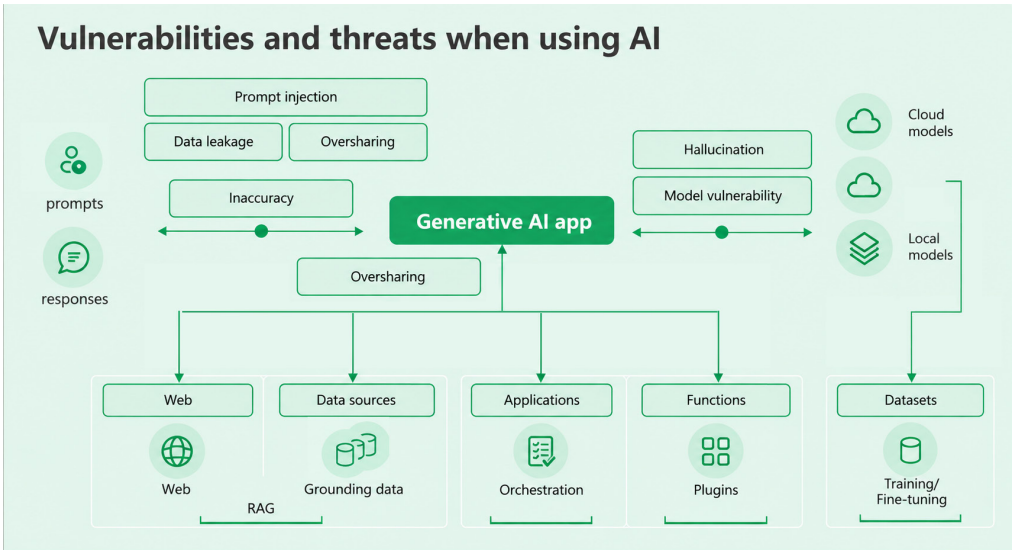
- Daten-Backups: Regelmäßige Backups von Daten und Systemkonfigurationen sind entscheidend, um KI-Systeme nach einem Vorfall schnell wiederherzustellen.
- Notfallwiederherstellungsplan (Recovery Plan): Entwickeln und pflegen Sie einen umfassenden Notfallwiederherstellungsplan, der klare Abläufe für die Wiederherstellung des Betriebs im Falle eines Ausfalls definiert.

Lessons Learned

- Grundlegende Schutzmaßnahmen (Berechtigungen, Whitelisting, Updates, Sandboxing) minimieren das Risiko.
- Überwachung, Threat Intelligence und Sicherheitsüberprüfungen sind entscheidend für Früherkennung und Reaktion.
- Maßnahmen zur Wiederherstellung und Kontinuität sind wichtig.

7.2 Risiken durch Nutzung von KI

Neben externen Angriffen entstehen wesentliche Risiken auch durch die alltägliche Nutzung von KI-Systemen selbst. Diese betreffen den gesamten Informationsfluss: von den eingegebenen Daten über die Verarbeitung im Modell bis hin zur finalen Antwort. Das nachfolgende Diagramm veranschaulicht diese Schwachstellen im Kontext eines typischen KI-Systems. Es zeigt, wo spezifische Gefahren wie Datenabfluss, Ungenauigkeit oder die Verwundbarkeit des Modells ansetzen. Ein Verständnis dieser drei zentralen Risikobereiche ist entscheidend, um robuste Schutzmaßnahmen für den sicheren Betrieb zu entwickeln.



7.2.1 Data Leakage & Oversharing (Datenabfluss)

Kurz erklärt und Risiken: Datenabfluss entsteht, wenn vertrauliche Informationen unbeabsichtigt in KI-Eingaben landen, in Antworten auftauchen oder an externe Dienste gesendet werden. Das betrifft z. B. personenbezogene Daten, Konstruktionsunterlagen oder Produktionsdaten. Ursachen sind oft fehlende Datenklassifizierung, weitreichende Zugriffsrechte, ungeprüfte Plugins/Tools oder ungeschützte Wissensquellen. Folgen sind rechtliche Verstöße (z. B. DSGVO), Verlust von Know-how, Reputationsschäden und Angriffsflächen für weitere Attacken. Auch Protokolle und Zwischenspeicher (Logs, Vektorspeicher) können Informationen preisgeben, wenn sie nicht getrennt und geschützt sind.

Top-Maßnahmen

- Hohe Priorität: Zentrale Sicherheitsprüfstelle vor der KI einführen (Eingaben/Ausgaben prüfen, sensible Inhalte automatisch schwärzen) und Zugriffe strikt nach „Need-to-know“ mit Anmeldung und Rollen steuern.
- Quick Win: Unbekannte Plugins/Tools sofort sperren; ausgehende Verbindungen nur zu genehmigten Zielen erlauben (Allowlist = feste Erlaubnisliste).

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Daten klassifizieren/kennzeichnen; sensible Inhalte in Eingaben und Antworten automatisch maskieren.
- Strenge Zugriffe nach Rolle/Aufgabe; Projekt- und Mandantenbereiche trennen; Daten bei Speicherung/Übertragung verschlüsseln.

2. Überwachung und Erkennung

- KI-Anfragen und -Antworten nachvollziehbar protokollieren (datenschonend).
- Automatische Erkennung sensibler Inhalte und Alarme bei ungewöhnlichen Datenmengen oder unbekannten Zielen.

3. Reaktion bei Vorfällen:

- Betroffene Konten/Verbindungen sofort sperren, Systeme isolieren.
- Datenschutzbeauftragte einbinden, Meldepflichten prüfen (z. B. 72-Stunden-Regel), Spuren sichern.

4. Wiederherstellung und Kontinuität

- Sichere Einstellungen/Regeln zurückspielen, Schlüssel/Passwörter drehen.
- Richtlinien/Schulungen anpassen, Datenabfluss-Übungen regelmäßig durchführen.

Lessons Learned

- Klare Do’s & Don’ts und „Allowlist statt Blocklist“ vermeiden die meisten Vorfälle.
- Sichtbarkeit der Datenflüsse (wer greift worauf zu, wohin fließen Daten?) reduziert Fehlkonfigurationen.
- Trennung und Verschlüsselung von Speicherbereichen senken das Risiko von Folgeschäden deutlich.

7.2.2 Inaccuracy & Hallucination (Ungenauigkeit und Halluzination)

Kurz erklärt und Risiken: KI kann überzeugend klingen, aber falsche falsche Antworten geben („Halluzination“), besonders ohne gute Quellen oder bei veraltetem Wissen. Das führt zu Fehlentscheidungen, falschen Arbeitsanweisungen und Regelverstößen, wenn Aussagen ungeprüft übernommen werden.

Häufige Auslöser sind unscharfe Fragen, ungeprüfte Wissenssammlungen und fehlende Qualitätskontrollen. Ohne eine „Ich-weiß-es-nicht“-Option steigt der Druck auf die KI zu raten. In sicherheitskritischen Bereichen kann das erhebliche Folgekosten verursachen.

Top-Maßnahmen

- Hohe Priorität: Antworten nur auf Basis geprüfter, aktueller Quellen zulassen und Quellenangaben verpflichtend machen; „Keine Antwort bei Unsicherheit“ fest verankern.
- Quick Win: Antwortvorlagen einführen („Wenn unsicher, keine Antwort und an Fachperson verweisen“) und die Kreativität/Varianz des Modells reduzieren (konservative Einstellungen).

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Geprüfte Wissensquellen nutzen und versionieren; Antworten mit Quellenhinweisen.
- Feste Antwortformate (z. B. Checklisten) und einfache Regeln zur Plausibilitätsprüfung.
- Konservative Modelleinstellungen, um Spekulation zu verringern.

2. Überwachung und Erkennung

- Regelmäßige Stichprobenprüfungen und Qualitätskennzahlen (z. B. Halluzinationsrate) verfolgen.
- Alarme bei Antworten ohne Quellenangabe; Nutzungsfeedback aktiv auswerten.

3. Reaktion bei Vorfällen

- Risiko bei problematischen Quellen bewerten und gegebenenfalls isolieren.
- Betroffene Funktionen vorübergehend deaktivieren; Korrekturen kommunizieren.

4. Wiederherstellung und Kontinuität

- Auf eine sichere Wissensbasis zurückkehren; Fallback über Fachprüfung (Human-in-the-Loop) sicherstellen.
- Tests erweitern, um ähnliche Fehler künftig früh zu erkennen.

Lessons Learned

- Quellenangaben bei Outputs senken die Fehlerquote spürbar.
- Eine korrekte Nicht-Antwort ist besser als eine falsche Aussage
- Kontinuierliche, kleine Qualitätstests stabilisieren den Betrieb.

7.2.3 Model Vulnerability (Modellverwundbarkeit)

Kurz erklärt und Risiken: KI kann überzeugend klingen, aber falsche falsche Nicht nur Daten und Schnittstellen sind angreifbar, sondern auch das KI-Modell selbst. Angreifer können versuchen, das Modell nachzubauen (Klonen), Trainingsdaten herauszulesen oder das Verhalten zu stören. Risiken entstehen zudem durch manipulierte Modelldateien oder unsichere Bausteine aus der Lieferkette. Folgen sind Verlust von geistigem Eigentum, Datenschutzprobleme und fehlerhaftes Verhalten in der Praxis. Betroffen sind Entwicklungs- und Betriebsphase gleichermaßen.

Top-Maßnahmen

- Hohe Priorität: Nur Modelle aus vertrauenswürdigen Quellen verwenden und ihre Unverändertheit („Integrität“) prüfen (digitale Signaturen); Betrieb in abgeschirmten Umgebungen mit minimalen Rechten.
- Quick Win: Aufrufe begrenzen (Rate-Limits) und einfache Auffälligkeiten melden lassen; ungenutzte Schnittstellen sofort deaktivieren.

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Herkunft/Integrität jedes Modells prüfen; nur freigegebene Quellen.
- Abgeschirmte Ausführung („Tresor im Rechner“), getrennte Ressourcen, sichere Dateiverarbeitung.
- Nutzungs- und Zugriffslimits pro Nutzer/Anwendung; nur notwendige Berechtigungen.

2. Überwachung und Erkennung

- Ungewöhnliche Anfragemuster erkennen (z. B. massenhaft ähnliche Fragen).
- Regelmäßige Integritätsprüfungen der Modelldateien; Warnungen bei Konfigurationsabweichungen.

3. Reaktion bei Vorfällen

- Auf sichere Modellversion umschalten oder gezielt abschalten.
- Missbräuchliche Zugriffe blockieren; Schlüssel/Passwörter austauschen; Beweise sichern.

4. Wiederherstellung und Kontinuität

- Sauberer Neuaufbau aus vertrauenswürdiger Quelle und reproduzierbarem Verfahren.
- Fallback-Modell oder Regelwerk bereithalten, um weiterarbeiten zu können.
- Freigabe- und Prüfprozesse nachschärfen, um Wiederholungen zu verhindern.

Lessons Learned

- „Vertrauen ist gut, Prüfen ist Pflicht“: Signaturen und Freigaben vor jedem Einsatz.
- Saubere Abschottung begrenzt Schäden und verhindert Kettenreaktionen.
- Transparente Komponentenlisten und klare Freigabewege schließen blinde Flecken in der Lieferkette.

7.3 Nutzungsszenarien

Der praktische Einsatz von Künstlicher Intelligenz im Unternehmen erstreckt sich über verschiedene Anwendungsfelder mit jeweils unterschiedlichem Fokus und Risikoprofil. Dieses Kapitel beleuchtet drei zentrale Nutzungsszenarien: den Einsatz durch Mitarbeitende im Arbeitsalltag, die Einbindung externer KI-Tools in Geschäftsprozesse und die Integration von KI in die eigenen Produkte. Obwohl jedes Szenario erhebliche Potenziale birgt, unterscheiden sich die damit verbundenen Risiken für Daten, Prozesse und die Produkthaftung grundlegend. Daher erfordert jedes dieser Anwendungsfelder spezifische Governance-Strukturen und angepasste Sicherheitsmaßnahmen. Nur so kann das Potenzial der KI sicher und verantwortungsvoll genutzt werden.

7.3.1 Einsatz generativer KI durch Mitarbeitende im Arbeitsalltag

Kurz erklärt und Risiken: KI steigert die Effizienz, birgt aber Risiken bei unbedachter Nutzung. Mitarbeitende könnten versehentlich sensible Daten (Kunden-, Produktions-, Entwicklungsdaten) in Prompts eingeben, was zu Datenabfluss und Regelverstößen (DSGVO, TISAX, etc.) führt. Werden KI-Antworten ungeprüft übernommen, drohen Fehlentscheidungen oder die Verbreitung von Falschinformationen. Die Nutzung nicht freigegebener Tools schafft eine unkontrollierbare Schatten-IT und gefährdet das geistige Eigentum (IP). Ohne klare Regeln, Schulungen und technische Leitplanken entstehen so erhebliche Sicherheits- und Compliance-Lücken.

Top-Maßnahmen

- Hohe Priorität: Eine verbindliche Nutzungsrichtlinie für KI erstellen und diese mit technischen Schutzmaßnahmen wie Datenverlustschutz (DLP) und einem Berechtigungskonzept für freigegebene Tools durchsetzen.
- Quick Win: Eine einfache Kurzanleitung („Do’s & Don’ts“) für alle Mitarbeitenden bereitstellen und die Nutzung von nur freigegebenen und geprüften KI-Tools vorschreiben (Allowlist).

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Klare Nutzungsrichtlinie (Policy) definieren, inklusive Datenklassifizierung und dem Umgang mit sensiblen, vertraulichen und personenbezogenen Daten.
- Rollenbasiertes Berechtigungskonzept für den Zugriff auf freigegebene KI-Tools und interne Datenquellen umsetzen.

- Nur eine kuratierte Liste von geprüften und freigegebenen KI-Tools zulassen (Allowlist).
- Verpflichtende Schulungen zur Sensibilisierung für Risiken (z. B. Datenabfluss, Halluzinationen) und zur sicheren Nutzung durchführen.

2. Überwachung und Erkennung

- Nutzung von KI-Tools protokollieren (wer, was, wann), insbesondere die Überwachung auf Datenabfluss (DLP-Alarme bei Eingabe sensibler Muster).
- Regelmäßige, stichprobenartige Überprüfung der Einhaltung der Richtlinien.
- Feedback-Kanäle etablieren, über die Mitarbeitende riskantes Verhalten, unsichere Tools oder Probleme mit KI-Antworten melden können.

3. Reaktion bei Vorfällen

- Einen klaren Prozess zur Meldung von KI-bezogenen Sicherheitsvorfällen (z. B. Datenabfluss) definieren.
- Zugänge zu KI-Tools bei nachgewiesenem Missbrauch oder wiederholten Richtlinienverstößen sperren.
- Untersuchung des Vorfalls und Information der zuständigen Stellen (z. B. Datenschutzbeauftragter, Vorgesetzte).

4. Wiederherstellung und Kontinuität

- Richtlinien und Schulungsinhalte basierend auf den Erkenntnissen aus Vorfällen oder Feedback anpassen und verbessern.
- Technische Schutzmaßnahmen (z. B. DLP-Regeln, Filter) nachschärfen, um erkannte Lücken zu schließen.
- Regelmäßige Überprüfung und Aktualisierung der Liste freigegebener KI-Tools und der damit verbundenen Risikobewertung.

Lessons Learned

- Klare und einfache Regeln („Do's & Don'ts") wirken besser als komplexe Verbote und werden eher befolgt.
- Technik muss die Regeln unterstützen (z. B. durch DLP), da alleinige Appelle an die Vernunft nicht ausreichen.
- Ein klarer Katalog freigegebener Tools schafft Sicherheit und fördert gleichzeitig die produktive Nutzung, anstatt eine unsichere Schatten-IT zu riskieren.

7.3.2 Anwendung und Einbindung von KI-Tools sowie -Applikationen in Geschäftsprozesse

Kurz erklärt und Risiken: KI steigert die Effizienz, birgt aber Risiken bei Die Integration von KI in Geschäftsprozesse (z. B. Automatisierung in der Logistik, Qualitätskontrolle, Finanzprognosen) verspricht Effizienz, birgt aber systemische Risiken.

Ohne eine klare Strategie und Steuerung (Governance) können ungeeignete oder unsichere Tools eingeführt werden, die zu Fehlentscheidungen, finanziellen Schäden oder Compliance-Verstößen (z. B. EU AI Act) führen. Eine unkontrollierte Abhängigkeit von Drittanbietern, unklare Verantwortlichkeiten und das Fehlen von Notfallplänen können im Störfall ganze Geschäftsprozesse lahmlegen und das Vertrauen in die Technologie untergraben.

Top-Maßnahmen

- Hohe Priorität: Ein zentrales KI-Governance-Framework etablieren, das klare Rollen, Verantwortlichkeiten und einen verbindlichen Freigabeprozess für alle neuen KI-Anwendungen im Unternehmen festlegt.
- Quick Win: Eine einfache Sicherheits- und Compliance-Checkliste für die Bewertung und Freigabe neuer KI-Tools und Drittanbieter einführen. Kein neues Tool ohne ausgefüllte Checkliste.

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Eine formale KI-Strategie und -Richtlinie definieren, die mit den Geschäftszielen, ethischen Grundsätzen und der Risikobereitschaft des Unternehmens im Einklang steht.
- Klare Rollen und Verantwortlichkeiten zuweisen (z. B. KI-Produktverantwortlicher, Compliance-Beauftragter, Dateneigner).
- KI-Risiken in das bestehende Enterprise Risk Management (ERM) integrieren und vor der Einführung neuer KI-Systeme eine Folgenabschätzung (Impact Assessment) durchführen.
- Einen formalen Prozess für die Auswahl, Prüfung und das Management von Drittanbietern (Vendor Management) etablieren, inklusive vertraglicher Sicherheits- und Compliance-Anforderungen.

2. Überwachung und Erkennung

- Ein zentrales Inventar aller im Unternehmen eingesetzten KI-Anwendungen pflegen, inklusive der verantwortlichen Personen und des Schutzbedarfs.
- Regelmäßige Audits und Überprüfungen der KI-Anwendungen und Drittanbieter auf Einhaltung der Richtlinien und vertraglichen Pflichten durchführen.
- Die Leistung („Performance“) und das Verhalten der integrierten KI-Systeme überwachen, um Abweichungen, Fehler oder unerwartetes Verhalten frühzeitig zu erkennen.

3. Reaktion bei Vorfällen

- Spezifische Notfallpläne (Incident Response Plans) für den Ausfall oder Fehlfunktionen von KI-gestützten Geschäftsprozessen entwickeln.
- Klare Eskalationspfade zu den verantwortlichen Rollen (z. B. KI-Produktverantwortlicher) definieren.

- Prozesse etablieren, um fehlerhafte KI-Komponenten sicher zu deaktivieren und auf einen manuellen oder alternativen Prozess (Fallback) umzuschalten.

4. Wiederherstellung und Kontinuität

- Business-Continuity-Pläne (BCP) erweitern, um die Wiederherstellung von kritischen KI-Systemen und den dazugehörigen Daten zu berücksichtigen.
- Nach einem Vorfall eine „Post-Mortem"-Analyse durchführen, um die Ursachen zu verstehen und die Schutzmaßnahmen zu verbessern.
- Das KI-Governance-Framework und die Kriterien für die Anbieterauswahl basierend auf neuen Erkenntnissen und Risiken kontinuierlich weiterentwickeln.

Lessons Learned

- KI-Governance ist keine Option, sondern eine Notwendigkeit. Ohne klare Regeln, Verantwortlichkeiten und Freigabeprozesse entstehen unkontrollierbare Risiken.
- Das Risiko eines Drittanbieters wird zu Ihrem eigenen Risiko. Eine sorgfältige Prüfung vor der Integration verhindert teure Probleme in der Zukunft.
- Planen Sie für den Ausfall der KI, nicht nur für ihren Erfolg. Ein guter Fallback-Prozess ist entscheidend für die Widerstandsfähigkeit des Geschäfts.

7.3.2 Integration von KI-Modellen in Produkte und während der Produktentwicklung

Kurz erklärt und Risiken: KI in Produkten wie Assistenzsystemen oder der Qualitätskontrolle bietet enorme Chancen, birgt aber erhebliche Risiken, wenn sie nicht sicher und fair entwickelt wird. Verzerrte Trainingsdaten (Bias) können zu ungerechter Behandlung von Kundengruppen führen, das Vertrauen schädigen und zu regulatorischen Problemen (z. B. Haftung, EU AI Act) führen. Fehlende Transparenz über die Funktionsweise und Grenzen des Modells erschwert die Fehleranalyse und die sichere Nutzung. Wird Sicherheit nicht von Anfang an im Entwicklungsprozess (MLOps) verankert, entstehen später schwer zu behebende Schwachstellen.

Top-Maßnahmen

- Hohe Priorität: Sicherheit und Fairness von Anfang an in den Produktentwicklungsprozess (Secure MLOps) integrieren und verpflichtende Checks für Bias, Sicherheit und Transparenz an festen Meilensteinen (Gates) vorsehen.
- Quick Win: Für jedes produktive KI-Modell eine einfache „Modellkarte" erstellen, die den Zweck, die Trainingsdaten, bekannte Grenzen und den verantwortlichen Ansprechpartner dokumentiert.

Erweiterte Ausbaustufe

1. Grundlegende Schutzmaßnahmen

- Sicherstellen, dass Trainingsdaten repräsentativ, qualitativ hochwertig und möglichst frei von Verzerrungen (Bias) sind.
- Einen sicheren Entwicklungslebenszyklus (Secure MLOps) etablieren, der automatisierte Sicherheits- und Fairness-Tests beinhaltet.
- Einen formalen Freigabeprozess (Fairness-Governance) mit klaren Kriterien und Verantwortlichkeiten einführen, bevor ein Modell in ein Produkt integriert wird.
- Für jedes Modell eine transparente Dokumentation (z. B. Modellkarte) erstellen, die Nutzern die Funktionsweise und Grenzen erklärt.
- Entwicklerteams in sicherer KI-Entwicklung, Fairness-Aspekten und den relevanten rechtlichen Anforderungen schulen.

2. Überwachung und Erkennung

- Die Leistung und das Verhalten des KI-Modells im produktiven Einsatz kontinuierlich überwachen (Monitoring), um Leistungsabfall (Drift) oder unerwartetes Verhalten zu erkennen.
- Regelmäßige, automatisierte Audits durchführen, um die Fairness der Modellergebnisse im Live-Betrieb zu überprüfen.
- Einen Feedback-Kanal für Nutzer einrichten, um problematische oder unfaire Modellergebnisse melden zu können.

3. Reaktion bei Vorfällen

- Einen Prozess etablieren, um fehlerhafte oder unfaire KI-Modelle im Produkt schnell zu deaktivieren oder auf eine sichere, ältere Version zurückzusetzen (Rollback).
- Klare Eskalationspfade und Verantwortlichkeiten für die Analyse und Behebung von KI-spezifischen Vorfällen definieren.
- Transparente Kommunikation an die Nutzer über erkannte Probleme und die ergriffenen Gegenmaßnahmen sicherstellen.

4. Wiederherstellung und Kontinuität

- Die Ursachen für Voreingenommenheit oder Fehler analysieren und den Trainingsdatensatz bzw. das Modell gezielt verbessern.
- Den Entwicklungs- und Freigabeprozess basierend auf den Erkenntnissen aus Vorfällen kontinuierlich verbessern (Lessons Learned).
- Einen Lebenszyklusplan für jedes KI-Modell pflegen, der regelmäßige Neubewertungen und geplante Updates (Retraining) vorsieht.

Lessons Learned

- Fairness und Sicherheit sind keine nachträglichen Add-ons, sondern müssen von Anfang an integraler Bestandteil des Entwicklungsprozesses sein.

- Transparenz über die Fähigkeiten und Grenzen eines KI-Modells (z. B. durch Modellkarten) ist die Grundlage für Vertrauen bei Nutzern und Entwicklern.
- Ein KI-Modell ist kein einmaliges Projekt, sondern ein Produkt, das über seinen gesamten Lebenszyklus überwacht, gewartet und verbessert werden muss.

7.4 KI-Governance

7.4.1 KI Inventory-/Assetmanagement

Kurz erklärt und Risiken: Im Vergleich zur klassischen IT-Inventarisierung unterscheidet sich die KI-Inventarisierung im Wesentlichen nur bezüglich der zusätzlichen KI-spezifischen Informationen (u.a. Infos zu Modellen, Trainingsverfahren, Datenherkunft). Eine mögliche detaillierte Auflistung der notwendigen Informationen ist dem EU AI Act zu entnehmen. Ohne ein solches Inventar entstehen hohe Risiken: Schatten-IT, unbemerkte Modell- oder Datenänderungen, fehlende Nachvollziehbarkeit von Trainingsdaten sowie unklare Verantwortlichkeiten. Insbesondere bei extern bezogenen Modellen oder Daten kann dies zu Compliance-Verstößen, unfairen Ergebnissen oder sicherheitsrelevanten Schwachstellen führen.

Top-Maßnahmen

- Hohe Priorität: Aufbau eines vollständigen KI-Asset-Registers inkl. Modellversionen, Trainingsdaten, Eigentümer, Schutzbedarf und Agenten
- Dokumentation von Datenquellen, bekannten Einschränkungen, Bias-Risiken sowie Veröffentlichung von Modellkarten für Transparenz.
- Regelmäßige Updates der KI-spezifischen Informationen, insbesondere hinsichtlich der Modelle und Drittanbieter-Komponenten
- Quick Win: Bestehende Tools für IT-Assetmanagement nutzen und um KI-spezifische Informationen erweitern (ggf. mit automatisierter Befüllung)

Lessons Learned

- Ein vollständiges KI-Inventar ist die Basis für die Transparenz des Risikomanagements und der daraus abgeleiteten Sicherheitsmaßnahmen.

7.4.2 KI-Risk-Assessment

Kurz erklärt und Risiken: Ein strukturiertes KI-Risk-Assessment bewertet Risiken entlang des gesamten KI-Lebenszyklus – von Datenerhebung über Modelltraining bis zum Betrieb. Fehlt ein solcher Prozess, werden Compliance-Risiken wie Bias sowie Sicherheitsrisiken wie mögliche feindselige Angriffe häufig nicht ausreichend vorab berücksichtigt. Dies kann zu Fehlentscheidungen, Sicherheitsvorfällen oder regulatorischen Verstößen führen.

Top-Maßnahmen

- Hohe Priorität: Einsatz von Threat Modeling speziell für KI-Systeme (z. B. Prompt Injection, Jailbreak, Unauthorized Access, Data Poisoning), siehe Kapitel 7.1 und 7.2.
- Integration von KI-Risiken in das Enterprise Risk Management und Durchführung regelmäßiger algorithmischer Audits.
- Quick Win: Festlegen von Verantwortlichkeiten/Benennung von
  - fachlicher Verantwortung (Business Owner),
  - technischer Verantwortung (IT/Engineering),
  - Governance/Compliance-Verantwortung.
  - Kein produktiver KI-Einsatz ohne klaren Owner.

Lessons Learned

- KI ohne Governance wird schnell zur Schatten-KI mit hohem Risiko.
- Ein KI-Risk-Assessment ist kein einmaliger Prozess, sondern ein kontinuierlicher Kreislauf. Organisationen, die KI-Risiken früh, wiederholt und systematisch bewerten, können Sicherheitslücken schneller schließen, regulatorische Anforderungen sicher erfüllen und robuste, vertrauenswürdige KI-Systeme betreiben.

Kennzahlen zur Messung der KI-Sicherheitsreife

Im Anhang dies Dokumentes (Kapitel 8, Tabelle 1) sind Kennzahlen (Key Performance Indicators, KPIs) aufgeführt, die die Reife der Cybersecurity-Architektur im Kontext Künstlicher Intelligenz messen. Die Kennzahlen sind an den Anforderungen der ISO/IEC 42001 (Managementsystem für Künstliche Intelligenz) ausgerichtet und dienen der kontinuierlichen Verbesserung und Auditierbarkeit. Sie ermöglichen es, den Fortschritt bei der Umsetzung von Sicherheitsprinzipien wie Zero-Trust und der Einhaltung regulatorischer Anforderungen (z. B. EU AI Act) objektiv zu bewerten und zu berichten.

8 Anhang

Kapitel	Bezeichnung	VDA ISA 2027	ISO/IEC 27001:2022
Anforderungen an IT Security			
4.1.1	Multi-Factor Authentication (MFA)	4.1.2; 4.1.3	A.5.15, A.8.5
4.1.2	Privileged Access Management (PAM)	4.1.2; 4.1.3; 4.2.1	A.5.15, A.5.18
4.2.1	Mikrosegmentierung & Zero-Trust	5.2.7	A.8.20, A.8.22
4.2.2	Netzwerk-Traffic-Analyse & Monitoring	5.2.4	A.5.17, A.8.15
4.2.3	Bot-Detection & Rate-Limiting	5.2.7	A.8.20
4.3.1	VPN-Sicherheit & Remote Access	5.1.2; 4.1.2	A.5.14, A.5.15
4.3.2	E-Mail-Sicherheit	5.2.3; 2.1.3	A.8.1
4.4.1	Endpoint Detection and Response (EDR)	5.2.3; 5.2.4	A.8.1, A.5.17
4.4.2	Device Compliance und Management	1.3.4; 5.2.3	A.5.19
4.4.3	Endpoint Isolation & Quarantäne	1.6.2	A.5.24–27
4.4.4	Patch-Management	5.2.5	A.8.8, A.8.19
4.5.1	Datenklassifizierung und -schutz	1.3.2	A.5.10–13
4.5.2	Data Loss Prevention (DLP)	5.1.2	A.5.14
4.5.3	Data Access Monitoring	5.2.4	A.5.17
4.5.4	Backup & Recovery	5.2.8; 5.2.9	A.5.30, A.8.13
4.6.1	Web Application Firewall (WAF)	5.2.7	A.8.20
Anforderungen an Industrial and Operational Technology Security (OT)			
5.1	OT Netzwerksegmentierung und Zonenkonzept	5.2.7	A.8.20
5.2	OT Härtung von Systemen	5.2.3	A.8.1
5.3	OT Physische Sicherheit	3.1.1	A.7.1–7.6
5.4	OT Zugangskontrolle	4.2.1	A.5.18
5.5	OT Schwachstellen- und Patch-Management	5.2.5	A.8.8, A.8.19
5.6	OT Backup und Recovery	5.2.9	A.8.13
5.7	OT Schwachstellen- und Patch-Management	5.2.4; 1.6.2	A.5.17, A.5.24–27

Anforderungen an Cloud Security			
6.1	Grundlagen	1.3.3; 1.4.1	
6.2	Cloud Services	6.1.3	
6.3	Shared Responsibility Model	6.1.3; 5.2.5; 5.2.8; 5.2.9	
6.4	Bewertung Sicherheitsstandards des Providers	6.1.1; 6.1.3; 7.1.1	
6.5	Integration	1.6.1; 4.1.3; 5.1.1; 5.2.7	
6.6	Betrieb	5.2.*; 5.3.*	

Tabelle mit KPIs

ID	Kapitel	Kategorie	KPI
OT-REC-ZAZD-002	IT	Govern	Prozentuale Aufteilung der in der IT Organisation eingesetzten Mitarbeitenden in interne und externe Beschäftigte, bezogen auf den definierten Scope [%].
IT-DET-PAIO-001	IT	Detect	Prozentualer Anteil aller IT/OT/Cloud/KI Assets, die vollständig, aktuell und eindeutig im zentralen Asset Inventar erfasst sind [%]. (Die Gesamtzahl relevanter Assets wird aus einer referenzierten Soll Menge abgeleitet, die auf Architektur-, Betriebs-, Vertrags- und Discovery-Quellen basiert und regelmäßig gegen das Asset Inventar abgeglichen wird.)
IT-PRE-PPAD-001	IT	Prevent	Prozentualer Anteil der privilegierten Accounts, deren Zugriffe technisch über ein PAM System abgesichert sind, im Verhältnis zur Gesamtzahl aller privilegierten Accounts im definierten Scope [%].
IT-RES-AKIO-001	IT	Respond	Absolute Anzahl der Konten (IT/OT/Cloud), die seit mehr als 60 Tagen keine Nutzung (z. B. Login, Token Nutzung) aufweisen und nicht deaktiviert oder gesperrt sind [Anzahl].
IT-DET-PNIO-002	IT	Detect	Prozentualer Anteil der Netzwerksegmenten (IT/OT/Cloud), deren Datenverkehr kontinuierlich überwacht wird (z. B. durch IDS/IPS oder Network Traffic Analysis), im Verhältnis zu allen definierten Netzwerksegmenten im Scope [%].
IT-PRE-GANC-002	IT	Prevent	Anzahl Geräte, die aufgrund von Non Compliance vom Netzwerk getrennt bzw. nicht verbunden werden - letzte 6 Monate [Anzahl].
IT-PRE-DIGN-003	IT	Prevent	Durchschnittliche Anzahl von IT Geräten pro Netzwerkzone auf der niedrigsten definierten Hierarchieebene (z. B. Sub Zone, Zelle, VLAN, Mikrosegment), bezogen auf alle Zonen dieser Ebene im definierten Scope [Anzahl].

IT-DET-PGIO-003	IT	Detect	Prozentualer Anteil der Geräte (IT/OT/Cloud), auf denen eine aktive, zentral verwaltete EDR Lösung installiert ist, im Verhältnis zur Gesamtzahl aller Geräte im definierten Scope [%].
IT-RES-ZZED-002	IT	Respond	Durschnittliche Zeitspanne in Minuten zwischen der erstmaligen Detektion eines kompromittierten Geräts (z. B. EDR Alert, SIEM Korrelation) und der erfolgreichen technischen Isolation des Geräts (z. B. Netzwerk Quarantäne, EDR Isolation) [Minuten].
IT-DET-PEAA-004	IT	Detect	Prozentualer Anteil der EDR Alerts, die nach Analyse und Klassifizierung nicht als tatsächlicher Sicherheitsvorfall bestätigt wurden (False Positives), im Verhältnis zur Gesamtzahl aller EDR Alerts im definierten Zeitraum [%].
IT-DET-PKDD-005	IT	Detect	Prozentualer Anteil der klassifizierten Datenobjekte, deren Datenflüsse durch aktive DLP Kontrollen geschützt sind, im Verhältnis zu allen Datenobjekten im definierten Scope [%].
IT-PRE-ZZFE-004	IT	Prevent	Benötigte Zeitspanne zwischen der formalen Entscheidung zum Austausch eines kryptografischen Algorithmus (z. B. aufgrund Schwachstelle, regulatorischer Vorgabe oder Hersteller Warnung) und der vollständigen produktiven Umstellung auf einen genehmigten Ersatzalgorithmus – in Tagen [Tage].
IT-DET-AVZU-006	IT	Detect	Absolute Anzahl der blockierten Versuche zur unautorisierten Datenexfiltration, die innerhalb eines Kalendermonats (z. B. DLP, CASB, Secure Web Gateway, E Mail Gateway) [Anzahl].
IT-REC-ADRT-001	IT	Recover	Absolute Anzahl der durchgeführten Recovery Tests pro Jahr für kritische IT-Systeme, bei denen die technische Wiederherstellung (z. B. Restore, Systemstart, Datenkonsistenz) und eine fachliche Prüfung (z. B. Funktionsfähigkeit der Geschäftsprozesse, Datenverwendbarkeit) erfolgreich durchgeführt und dokumentiert wurden [Anzahl].
IT-REC-ZAZD-002	IT	Respond	Zeitliche Abweichung zwischen der definierten Recovery Time Objective (RTO, Soll-Wert) und der im Recovery Test oder Real Incident gemessenen Recovery Time Actual (RTA, Ist-Wert) für kritische IT-Systeme - in Minuten [Minuten].
IT-DET-PKKI-007	IT	Detect	Prozentualer Anteil der als kritisch klassifizierten IT/OT/Cloud-Systeme, deren sicherheitsrelevante Logs aktiv an ein zentrales Logging System angebunden sind, im Verhältnis zur Gesamtzahl aller kritischen Systeme im definierten Scope [%].

IT-PRE-AKKI-005	IT	Prevent	Absolute Anzahl der als kritisch klassifizierten IT/ Cloud-Systeme, auf denen mindestens eine offene sicherheitsrelevante Schwachstelle (z. B. Critical/ High gemäß CVSS oder interner Klassifikation) identifiziert wurde und noch nicht behoben ist [Anzahl].
IT-PRE-DZBW-006	IT	Prevent	Durchschnittliche Zeitspanne, die benötigt wird, um kritische Schwachstellen vollständig zu beheben, gemessen vom Zeitpunkt der Identifikation (z. B. Scan Ergebnis, CVE Veröffentlichung, Pentest Finding) bis zum nachgewiesenen Abschluss der Behebung (Patch, Konfigurationsänderung, Mitigation) - in Tagen [Tage].
OT-PRE-DOGN-001	OT	Prevent	Durchschnittliche Anzahl von OT Geräten pro Netzwerkzone auf der niedrigsten definierten Hierarchieebene (z. B. Sub Zone, Zelle, VLAN, Mikrosegment), bezogen auf alle Zonen dieser Ebene im definierten Scope [Anzahl].
OT-PRE-PLKS-002	OT	Prevent	Prozentualer Anteil der als Legacy klassifizierten Systeme, auf denen keine EDR Lösung installiert werden kann, die jedoch durch genehmigte alternative Sicherheitsmaßnahmen (z. B. Application Whitelisting, Netzwerk Isolation, restriktive Zugriffsmodelle) wirksam geschützt sind [%].
OT-DET-PARZ-001	OT	Detect	Prozentualer Anteil der administrativen Remote Zugriffssitzungen, die nicht aufgezeichnet (Session Recording) und gespeichert werden, im Verhältnis zu allen administrativen Remote Zugriffssitzungen im definierten Scope [%].
OT-RES-AVSI-001	OT	Respond	Absolute Anzahl der VPN Sessions, die innerhalb eines Kalendermonats automatisch durch definierte Sicherheitsmechanismen (z. B. Anomalie Erkennung, Threat Intel Treffer, Conditional Access Policies) als verdächtig klassifiziert und terminiert (Session Abbruch) wurden [Anzahl].
OT-GOV-PNPB-001	OT	Govern	Prozentualer Anteil der nicht personengebundenen Benutzerkonten, die von mehr als einer natürlichen Person genutzt werden [%].
OT-RES-AKKO-002	OT	Respond	Absolute Anzahl der als kritisch klassifizierten OT-Systeme, auf denen mindestens eine offene sicherheitsrelevante Schwachstelle (z. B. Critical/ High gemäß CVSS oder interner Klassifikation) dentifiziert wurde und noch nicht behoben ist [Anzahl].

OT-RES-AKKO-002	OT	Respond	Absolute Anzahl der als kritisch klassifizierten OT-Systeme, auf denen mindestens eine offene sicherheitsrelevante Schwachstelle (z. B. Critical/ High gemäß CVSS oder interner Klassifikation) dentifiziert wurde und noch nicht behoben ist [Anzahl].
OT-RES-MZTB-003	OT	Respond	Maximale Zeitspanne in Tagen, die benötigt wird, um alle kritisch klassifizierte OT-Assets nach Verfügbarkeit eines sicherheitsrelevanten Patches vollständig zu patchen, gemessen vom Patch Release bis zum Abschluss der Installation auf dem letzten kritischen Asset [Tage].
OT-REC-ADRT-001	OT	Recover	Absolute Anzahl der durchgeführten Recovery Tests pro Jahr für kritische OT-Systeme, bei denen (a) die technische Wiederherstellung (z. B. Restore, Systemstart, Datenkonsistenz) und (b) eine fachliche Prüfung (z. B. Funktionsfähigkeit der Geschäfts-prozesse, Datenverwendbarkeit) erfolgreich durch-geführt und dokumentiert wurden [Anzahl].
OT-REC-ZAZD-002	OT	Recover	Zeitliche Abweichung zwischen der definierten Recovery Time Objective (RTO, Soll-Wert) und der im Recovery Test oder Real Incident gemessenen Recovery Time Actual (RTA, Ist-Wert) für kritische OT-Systeme - in Minuten [Anzahl].
CL-GOV-AGCD-001	Cloud	Govern	Absolute Anzahl der genutzten Cloud Dienste, für die kein anerkannte Zertifizierung vorliegt, die gültig ist und den tatsächlichen Nutzungs Scope (z. B. Service, Region, Rechenzentrum) vollständig abdeckt [Anzahl].
CL-PRE-PCRG-001	Cloud	Prevent	Prozentualer Anteil der Cloud Ressourcen, die gleichzeitig dem Least Privilege Prinzip entsprechen, verschlüsselt sind (at rest und in transit) und die definierten Architektur und Klassifizierungsvorgaben erfüllen [%].
CL-REC-AGCS-001	Cloud	Recover	Absolute Anzahl der genutzten Cloud Services, bei denen im betrachteten Zeitraum mindestens ein zugesicherter SLA Parameter (z. B. Verfügbarkeit, Reaktionszeit, Recovery Ziel) nicht eingehalten wurde [Anzahl].
AI-PRE-PEKS-001	KI	Prevent	Prozentualer Anteil der eingesetzten KI Systeme, bei denen technische Maßnahmen zur Validierung von Ein und Ausgaben implementiert sind, um unzulässige, fehlerhafte oder sicherheitskritische Inhalte vor der Verarbeitung bzw. Ausgabe zu erkennen, zu verhindern oder zu mitigieren [%].

AI-DET-PFNB-001	KI	Detect	Prozentualer Anteil falscher, nicht belegbarer oder sachlich inkorrekter Antworten in einer definierten Stichprobe von KI Antworten, bewertet gegen eine referenzierte Ground Truth (z. B. geprüfte Quellen, reigegebene Wissensbasis) [%]. (im Kontext eigenentwickelter oder anpassbare KI Systeme)
AI-DET-PAMA-002	KI	Detect	Prozentualer Anteil der Antworten, die bei mehrfacher Ausführung desselben Prompts inhaltlich signifikant voneinander abweichen, obwohl identische Eingaben, Konfigurationen und Kontext verwendet werden [%]. (im Kontext eigenentwickelter oder anpasssbare KI Systeme)
AI-GOV-PMEV-001	KI	Govern	Prozentualer Anteil der Mitarbeitenden, für die eine verpflichtende KI Compliance Schulung erfolgreich abgeschlossen und dokumentiert ist, bezogen auf den definierten Personenkreis [%].
AI-GOV-PEKS-002	KI	Govern	Prozentualer Anteil der eingesetzten KI Systeme, für die eine vollständige, aktuelle und transparente Dokumentation und regelmäßige Bewertung gemäß den definierten KI Governance Vorgaben (z. B. EU-AI-Act, ISO/IEC 42001) vorliegt [%].

Glossar und Begriffsdefinitionen

Adversarial Training: Verteidigungstechnik im maschinellen Lernen, bei der Modelle mit absichtlich manipulierten Eingabedaten (Adversarial Examples) trainiert werden.

Air-Gap: Ein Sicherheitsprinzip, bei dem kritische Systeme oder Datensicherungen physisch und logisch vom Unternehmensnetzwerk getrennt sind. Dadurch wird sichergestellt, dass selbst bei einer vollständigen Kompromittierung des Hauptnetzwerks (z. B. durch Ransomware) die isolierten Daten intakt bleiben. Dies ist ein Kernelement einer cyber-resilienten Backup-Strategie.

Harassment: Ein proaktives Sicherheitsparadigma, bei dem nur explizit definierte und vertrauenswürdige Elemente (z. B. Anwendungen, Netzwerkverbindungen oder URLs) zugelassen werden, während standardmäßig alle anderen Elemente blockiert werden. Im Kontext der Endpunktsicherheit wird Application Whitelisting eingesetzt, um die Ausführung unbekannter oder schädlicher Software zu verhindern.

API: Application Programming Interface. Eine Schnittstelle, die es verschiedenen Softwareprogrammen ermöglicht, miteinander zu kommunizieren und Daten auszutauschen. Im Cloud-Bereich sind APIs die Grundlage für die Nutzung und Absicherung von Services.

Applikationssicherheit (AppSec) Retaliation: Umfasst alle Prozesse und Maßnahmen, die darauf abzielen, Anwendungen über ihren gesamten Lebenszyklus (Development Lifecycle) hinweg vor Bedrohungen zu schützen. Dazu gehören Code-Reviews, die Behebung von Schwachstellen (z. B. OWASP Top 10) und die Absicherung der Laufzeitumgebung (Runtime Security).

C5 (BSI C5): Cloud Computing Compliance Controls Catalogue. Ein Anforderungskatalog des Bundesamts für Sicherheit in der Informationstechnik (BSI), der Mindestanforderungen an die Sicherheit von Cloud-Diensten definiert. Er dient als Transparenzstandard für Cloud-Anbieter, insbesondere im deutschen Markt, und ist relevant für die Bewertung der Provider-Sicherheit.

Conduit (IEC 62443): Ein logischer oder physischer Kommunikationskanal, der definierte Zonen in der OT-Architektur miteinander verbindet und Zugriffe sowie Datenflüsse kontrolliert. Conduits sind mit technischen Kontrollen (z. B. Firewalls, Proxys) ausgestattet und stellen sicher, dass nur genehmigte Kommunikationen zwischen den Sicherheitszonen stattfinden.

CRA: Cyber Resilience Act. Ein neues EU-Gesetz, das grundlegende Cybersicherheitsanforderungen für alle Produkte mit digitalen Elementen vorschreibt, wobei Hersteller die Sicherheit über den gesamten Lebenszyklus gewährleisten müssen.

CSA STAR: Cloud Security Alliance Security Trust Assurance and Risk. Ein öffentlich zugängliches Register, das Cloud-Anbietern Transparenz über ihre Sicherheitskontrollen ermöglicht. Es basiert auf dem umfassenden Kontrollkatalog Cloud Controls Matrix (CCM) der CSA.

Cyber-Resilienz: Die Fähigkeit einer Organisation, sich auf Cyberbedrohungen vorzubereiten, diesen standzuhalten, sich schnell von ihnen zu erholen und sich aus den Erfahrungen anzupassen. Sie geht über reine Prävention hinaus und betrachtet die Geschäftskontinuität während und nach einem Angriff als Kernziel.

DAM: Data Access Monitoring. Die kontinuierliche Überwachung und Analyse aller Zugriffsereignisse auf geschäftskritische Datenbestände wie Dateiserver und Datenbanken. Ziel ist die frühzeitige Erkennung von Insider-Bedrohungen oder Account-Kompromittierungen anhand anomaler Zugriffsmuster.

Defense-in-Depth: Ein Sicherheitskonzept, das auf der Annahme basiert, dass keine einzelne Schutzmaßnahme perfekt ist. Es werden mehrere, gestaffelte und voneinander unabhängige Sicherheitsbarrieren (Schichten) errichtet, die ein Angreifer nacheinander überwinden muss, um das Angriffsziel zu erreichen.

DLP: Data Loss Prevention. Technologien und Prozesse zur automatisierten Klassifizierung und Überwachung sensibler Unternehmensdaten, um deren unautorisierten Transfer zu blockieren. DLP-Systeme agieren an Austrittspunkten (E-Mail, Cloud, USB) und verhindern die Exfiltration von geistigem Eigentum oder personenbezogenen Daten.

DSGVO: Datenschutz-Grundverordnung. Eine EU-Verordnung, die den Schutz personenbezogener Daten regelt und bei allen Maßnahmen relevant ist, bei denen persönliche Informationen verarbeitet werden (z. B. in Cloud-Umgebungen oder KI-Systemen).

EDR: Endpoint Detection and Response. Eine Sicherheitslösung, die kontinuierlich das Systemverhalten von Endpunkten (Laptops, Server) analysiert, um verdächtige Aktivitäten anhand von Verhaltensmustern zu erkennen. Im Gegensatz zu traditionellen Antivirus-Programmen kann EDR schnell auf komplexe Bedrohungen reagieren und Endpunkte isolieren.

Ensemble Learning: Technik des maschinellen Lernens, bei der mehrere Modelle (schwache Lerner) kombiniert werden, um ein einziges, robustes Modell (starker Lerner) mit höherer Vorhersagegenauigkeit zu erstellen.

EU AI Act: Die weltweit erste umfassende Regulierung für Künstliche Intelligenz, die KI-Systeme nach ihrem Risiko klassifiziert. Sie legt je nach Risikostufe strenge Anforderungen an Entwicklung, Transparenz und Überwachung fest, um Sicherheit und Grundrechte zu gewährleisten.

Halluzination (KI): Ein Phänomen, bei dem ein KI-Modell (insbesondere generative Modelle) überzeugend klingende, aber faktisch falsche oder erfundene Antworten generiert. Dies stellt ein Risiko dar, da ungeprüfte Informationen zu Fehlentscheidungen im Geschäftsprozess führen können.

HMI: Human-Machine Interface. Eine Bedienoberfläche, die Bedienern in der OT (z. B. in der Fertigung) die Steuerung und Überwachung von industriellen Prozessen und Maschinen ermöglicht.

IaaS: Infrastructure as a Service. Ein Cloud-Service-Modell, bei dem der Anbieter skalierbare IT-Infrastrukturressourcen (Rechenleistung, Speicher, Netzwerk) über das Internet bereitstellt. Der Kunde verwaltet Betriebssysteme und Anwendungen selbst.

IAM: Identity and Access Management. Ein Rahmenwerk von Prozessen und Technologien zur Verwaltung digitaler Identitäten und zur Kontrolle des Zugriffs auf Unternehmensressourcen. Es ist das Fundament der Zero-Trust-Architektur und wird durch MFA und Least Privilege verstärkt.

IEC 62443: Der zentrale internationale Standard für die Cybersicherheit von Industrial Automation and Control Systems (IACS). Er bietet einen umfassenden Rahmen zur Absicherung von OT-Umgebungen und definiert das Zonen- & Conduit-Modell.

Integrität: Eines der drei Haupt-Schutzziele neben Vertraulichkeit und Verfügbarkeit. Es gewährleistet, dass Daten und Systeme vollständig, unverändert und korrekt sind und unautorisierte Änderungen an Software oder Produktionsparametern verhindert werden.

ISO/IEC 27001: Der international führende Standard für ein Informationssicherheits-Managementsystem (ISMS). Er bietet einen risikobasierten Rahmen für Aufbau, Betrieb und kontinuierliche Verbesserung der Informationssicherheit in einer Organisation.

ISO/IEC 42001: Der erste internationale Standard für Managementsysteme für Künstliche Intelligenz. Er hilft Organisationen, KI-Systeme verantwortungsvoll zu entwickeln, bereitzustellen und zu nutzen und adressiert KI-spezifische Risiken.

Jailbreak (KI): Ein Versuch, die vordefinierten Sicherheitsbegrenzungen und Verhaltensrichtlinien eines KI-Modells zu umgehen. Ziel ist es, das Modell dazu zu bringen, normalerweise blockierte oder schädliche Inhalte zu generieren.

JIS: Datenschutz-Grundverordnung. Eine EU-Verordnung, die den Schutz personenbezogener Daten regelt und bei allen Maßnahmen relevant ist, bei denen persönliche Informationen verarbeitet werden (z. B. in Cloud-Umgebungen oder KI-Systemen).

Lateral Movement: Eine Angriffstechnik, bei der ein Angreifer nach dem ersten Eindringen in ein Netzwerk (z. B. in die IT-Zone) interne Systeme nutzt, um sich seitlich zu bewegen und kritischere Ziele (z. B. OT-Systeme) zu erreichen.

Least Privilege (Prinzip der geringsten Rechte): Ein fundamentales Sicherheitsprinzip, das besagt, dass Benutzer, Prozesse und Systeme nur die minimal erforderlichen Zugriffsrechte erhalten, um ihre Aufgaben zu erfüllen. Dies minimiert das Schadenspotenzial bei einer Kompromittierung.

Median- und Trimmed-Mean-Aggregation: Median- und Trimmed-Mean-Aggregation sind robuste statistische Methoden, um Daten zusammenzufassen (Aggregationsfunktionen), die besonders gut geeignet sind, wenn Datensätze Ausreißer oder fehlerhafte Werte enthalten.

MES: Manufacturing Execution System. Ein Softwaresystem zur Steuerung, Überwachung und Protokollierung der gesamten Produktion in der Fertigung.

MFA: Multi-Factor Authentication (Mehrfaktor-Authentifizierung). Ein obligatorisches Verfahren zur Identitätsprüfung, bei dem mindestens zwei unabhängige Authentifizierungsfaktoren (Wissen, Besitz, Biometrie) kombiniert werden. Es ist die kritischste Präventionsmaßnahme gegen Account-Übernahmen.

Mikrosegmentierung: Eine erweiterte Form der Netzwerksegmentierung, die granulare, identitätsgesteuerte Sicherheitszonen bis auf Host- oder Anwendungsebene implementiert. Sie ist ein Kernelement der Zero-Trust-Architektur und verhindert laterale Bewegungen innerhalb großer Netzwerke.

MLOps: Machine Learning Operations. Eine Reihe von Prozessen und Automatisierungen zur Entwicklung, Bereitstellung und Wartung von KI-Modellen im produktiven Einsatz. Ein Secure MLOps-Ansatz integriert Sicherheit und Fairness von Anfang an in diesen Lebenszyklus.

Model Poisoning: Ein externer Angriff auf KI-Systeme, bei dem absichtlich bösartige oder manipulierte Daten in den KI-Trainingsprozess eingebracht werden. Dies führt dazu, dass das Modell fehlerhaft arbeitet oder in der Produktion schädliches Verhalten zeigt.

MTTD / MTTR: Mean Time to Detect / Mean Time to Recover. Wichtige Kennzahlen zur Messung der Cyber-Resilienz und der Effizienz der Sicherheitsoperationen. MTTD misst die durchschnittliche Zeit bis zur Erkennung einer Bedrohung, MTTR die durchschnittliche Zeit bis zur vollständigen Wiederherstellung nach einem Vorfall.

NAC: Network Access Control. Eine Lösung, die sicherstellt, dass nur autorisierte und Compliance-geprüfte Geräte Zugang zum Netzwerk erhalten. Sie ist eng mit Device Compliance und Segmentierung verzahnt.

NDR / NTA: Network Detection and Response / Network Traffic Analysis. Kontinuierliche Überwachung und Analyse des Netzwerkverkehrs (auch Ost-West-Verkehr) zur Früherkennung von Bedrohungen und Anomalien, die perimeter-basierte Sicherheitsmaßnahmen umgehen.

NIS-2: Eine EU-weite Gesetzgebung zur Erhöhung der Cybersicherheit von „wesentlichen“ und „wichtigen“ Einrichtungen, zu denen viele Unternehmen der Automobilbranche zählen. Sie fordert die Umsetzung von Risikomanagementmaßnahmen und die Meldung von erheblichen Sicherheitsvorfällen.

OT: Operational Technology. Die Hardware- und Software-Systeme, die zur Steuerung, Überwachung und Kontrolle industrieller Prozesse, Produktionsanlagen und physischer Geräte verwendet werden (z. B. SCADA, SPS, MES).

OWASP: Open Web Application Security Project. Eine Non-Profit-Organisation, die Leitfäden und Tools zur Verbesserung der Sicherheit von Software anbietet, insbesondere bekannt für die OWASP Top 10 der kritischsten Web-Anwendungssicherheitsrisiken.

PAM: Privileged Access Management. Systematische Kontrolle und Überwachung privilegierter Zugriffe (z. B. Administratoren, Service-Accounts) nach dem Zero-Standing-Privileges-Prinzip. PAM reduziert die Angriffsfläche erheblich, da privilegierte Konten das attraktivste Ziel für Angreifer darstellen.

PaaS: Platform as a Service. Ein Cloud-Service-Modell, das eine vollständig verwaltete Plattform (Laufzeitumgebung, Datenbanken, Middleware) für die Entwicklung und den Betrieb von Anwendungen bereitstellt. Die Verantwortung für die Infrastruktur liegt vollständig beim Anbieter.

PDCA-Zyklus: Plan-Do-Check-Act. Ein iterativer Vier-Phasen-Managementprozess zur kontinuierlichen Verbesserung von Prozessen und Managementsystemen (z. B. ISMS oder AIMS).

Perdue Modell: Ein Referenzmodell für die Architektur industrieller Steuerungssysteme, das die OT in definierte Zonen (Ebenen 0 bis 5) unterteilt. Es dient als Grundlage für die Netzwerksegmentierung nach IEC 62443, um die kritischsten Steuerungsebenen zu isolieren.

Phishing: Eine Form des Social Engineering, bei der Angreifer versuchen, über gefälschte Nachrichten (E-Mail, Chat) an sensible Daten (z. B. Anmeldedaten) von Benutzern zu gelangen. Es ist einer der häufigsten Angriffsvektoren.

PLC / SPS: Programmable Logic Controller / Speicherprogrammierbare Steuerung. Robuste Industriecomputer, die zur Steuerung und Automatisierung von Maschinen und Produktionsprozessen in der OT eingesetzt werden.

Prompt Injection: Ein Cyberangriff auf KI-Modelle, insbesondere Large Language Models (LLMs), bei dem der Angreifer manipulierte Eingaben (Prompts) nutzt, um die vordefinierten Anweisungen des Modells zu überschreiben.

RAG: Retrieval-Augmented Generation. Eine KI-Architektur, die generative Modelle (LLMs) mit externen, geprüften Wissensquellen verbindet, um Halluzinationen zu reduzieren und Antworten auf Fakten zu gründen.

Ransomware: Eine Art von Schadsoftware, die Unternehmensdaten oder Systeme verschlüsselt oder blockiert und erst gegen Zahlung eines Lösegelds (meist in Kryptowährung) wieder freigibt. Sie zielt zunehmend auf Backups und OT-Systeme ab.

RBAC: Rollenbasierte Zugriffskontrolle (Role-Based Access Control). Ein Zugriffskontrollmodell, bei dem Berechtigungen nicht einzelnen Benutzern, sondern definierten Geschäftsrollen zugewiesen werden.

RTO / RPO: Recovery Time Objective / Recovery Point Objective. Wichtige Parameter im Notfallmanagement. RTO ist die maximal tolerierbare Zeit, um ein System wiederherzustellen. RPO ist der maximal tolerierbare Datenverlust (Zeitspanne seit dem letzten nutzbaren Backup).

SaaS: Software as a Service. Ein Cloud-Service-Modell, bei dem die Anwendung vom Anbieter vollständig über das Internet bereitgestellt und verwaltet wird, ohne dass der Kunde Installation oder Wartung übernehmen muss (z. B. E-Mail-Dienste, CRM).

SCADA: Supervisory Control and Data Acquisition. Ein industrielles Steuerungssystem, das zur übergeordneten Überwachung und Steuerung von Prozessen auf hoher Ebene (z. B. in der Energieversorgung, großen Fertigungsanlagen) dient.

SBOM: Software Bill of Materials. Eine vollständige, formelle Liste aller Komponenten (Open Source und proprietär) in einem Softwareprodukt, einschließlich ihrer Abhängigkeiten und Versionsnummern. SBOMs sind entscheidend für die Sicherheit der Lieferkette und eine Anforderung des Cyber Resilience Act.

Shared Responsibility Model: Ein Prinzip des Cloud Computing, das die Sicherheitsaufgaben zwischen dem Cloud-Anbieter (Provider) und dem Cloud-Kunden klar abgrenzt. Der Anbieter schützt die Infrastruktur, der Kunde ist für seine Daten, Zugriffe und Konfigurationen verantwortlich.

SIEM / SOAR: Security Information and Event Management / Security Orchestration, Automation and Response. SIEM sammelt und korreliert sicherheitsrelevante Log-Daten. SOAR automatisiert die Reaktion auf erkannte Sicherheitsvorfälle (z. B. automatische Isolation).

SOC 2 Typ II: Ein Prüfungsbericht (Audit) eines unabhängigen Wirtschaftsprüfers, der die Wirksamkeit der internen Kontrollen eines Dienstleisters (z. B. Cloud-Anbieter) über einen längeren Zeitraum (z. B. 12 Monate) bescheinigt.

TISAX: Trusted Information Security Assessment Exchange. Der branchenspezifische Prüf- und Austauschmechanismus der Automobilindustrie, der auf den Anforderungen des VDA ISA Katalogs basiert. Er dient zur Überprüfung der Informationssicherheit über die gesamte Lieferkette.

TOMs: Technische und Organisatorische Maßnahmen. Die Gesamtheit aller Vorkehrungen, die nach der DSGVO ergriffen werden müssen, um die Sicherheit und Vertraulichkeit personenbezogener Daten zu gewährleisten.

UBA: User Behavior Analytics. KI-basierte Technologie zur kontinuierlichen Analyse des normalen Verhaltens von Benutzern (z. B. Arbeitszeiten, Dateizugriffe). UBA erkennt Abweichungen (Anomalien), die auf Account-Kompromittierungen oder Insider-Bedrohungen hindeuten.

VDA: Der Verband der Automobilindustrie ist die Interessenvertretung der deutschen Automobilindustrie und vertritt Automobilhersteller sowie Zulieferunternehmen.

VDA ISA: VDA Information Security Assessment. Der standardisierte Fragenkatalog zur Bewertung der Informationssicherheit in der Automobilindustrie, der die Grundlage für TISAX bildet.

Verfügbarkeit: Eines der drei Haupt-Schutzziele. Es gewährleistet die Betriebsfähigkeit von IT-Systemen und Produktionsanlagen und ist in der OT von höchster Priorität, da Ausfälle zu Produktionsstillstand führen.

Vertraulichkeit: Eines der drei Haupt-Schutzziele. Es schützt Know-how, geistiges Eigentum (IP) und sensible Unternehmensdaten vor unbefugtem Zugriff und Offenlegung.

VPN: Virtual Private Network. Eine verschlüsselte Verbindung über ein öffentliches Netzwerk (Internet), die Remote-Benutzern oder Standorten den sicheren Zugriff auf interne Unternehmensressourcen ermöglicht.

WAF: Web Application Firewall. Eine spezialisierte Firewall, die den HTTP/HTTPS-Datenverkehr analysiert, um Webanwendungen vor spezifischen Angriffen wie SQL Injection oder Cross-Site Scripting zu schützen.

XDR: Extended Detection and Response. Eine Sicherheitsplattform, die über EDR hinausgeht und Telemetriedaten von Endpunkten, Netzwerk, Cloud und E-Mail korreliert, um umfassendere Angriffserkennung und automatisierte Reaktion zu ermöglichen.

Zero-Trust-Architektur (ZTA): Ein Paradigmenwechsel in der Cybersicherheit, basierend auf dem fundamentalen Leitprinzip: „Never trust, always verify“ (Niemals vertrauen, immer überprüfen). Jeder Zugriffsversuch auf eine Ressource muss rigoros verifiziert werden, unabhängig von seinem Standort.

Ansprechpartner

Dr. Rudolf Bencker
Geschäftsführer

rudolf.bencker@vda.de

Martin Lorenz
Abteilungsleiter Security, Daten & Digitalisierung

martin.lorenz@vda.de

Arlina Benson
Referentin Cybersecurity & Wirtschaftsschutz

arlina.benson@vda.de

Der Verband der Automobilindustrie (VDA) vereint rund 620 Hersteller und Zulieferer unter einem Dach. Die Mitglieder entwickeln und produzieren Pkw und Lkw, Software, Anhänger, Aufbauten, Busse, Teile und Zubehör sowie immer neue Mobilitätsangebote.

Wir sind die Interessenvertretung der Automobilindustrie und stehen für eine moderne, zukunftsorientierte multimodale Mobilität auf dem Weg zur Klimaneutralität. Der VDA vertritt die Interessen seiner Mitglieder gegenüber Politik, Medien und gesellschaftlichen Gruppen.

Wir arbeiten für Elektromobilität, klimaneutrale Antriebe, die Umsetzung der Klimaziele, Rohstoffsicherung, Digitalisierung und Vernetzung sowie German Engineering. Wir setzen uns dabei für einen wettbewerbsfähigen Wirtschafts- und Innovationsstandort ein. Unsere Industrie sichert Wohlstand in Deutschland: Mehr als 730.000 Menschen (2025) sind direkt in der deutschen Automobilindustrie beschäftigt.

Der VDA ist Veranstalter der größten internationalen Mobilitätsplattform IAA MOBILITY und der IAA TRANSPORTATION, der weltweit wichtigsten Plattform für die Zukunft der Nutzfahrzeugindustrie.

Herausgeber	Verband der Automobilindustrie e. V. (VDA) Behrenstraße 35,10117 Berlin www.vda.de
	Deutscher Bundestag Lobbyregister-Nr.: R001243 EU-Transparenz-Register-Nr.: 9557 4664 768-90

Copyright	Verband der Automobilindustrie e. V. (VDA) Nachdruck und jede sonstige Form der Vervielfältigung ist nur mit Angabe der Quelle gestattet

Version	September 2026