Erstellt von Diana , Daniel, Jens, Christian

Strukturanalyse gemäß BSI IT-Grundschutz für Beste Sicherheit durch AI Gmbh

IT-Sicherheits unternehmen Spezialisiert auf Ai basierter Sicherheitsstrukturen für Server und Unternehmen

25 Angestellte : 2 Geschäftsführer

2 Anwälte für Arbeitsrechts , Informationsrecht, und Cybersicherheit, DSGVO

1 Sicherheitsbeauftragter

1 Marketing Beauftragter

2 Verkäufer

1 Kunden Supporter

3 Auditoren und Schulungspersonal für die Kunden

Alle Anderen sind mindestens System Fachinformatiker mit verschiedenen Spezialisierungen

2 Standorte

Basis Kundenstamm

Eigene kleine Serverfarm um Dienstleistungen bereitzustellen

Einleitung

Zweck und Methodik

Dieses Dokument stellt die Strukturanalyse für das Unternehmen Beste Sicherheit durch AI GmbH dar. Der Zweck dieser Analyse ist die systematische Erfassung, Dokumentation und Aufbereitung der erforderlichen Kenntnisse über den betrachteten Informationsverbund. Dies bildet die unverzichtbare Grundlage für die nachfolgende Implementierung von Informations-Sicherheitsmaßnahmen gemäß dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Die Methodik folgt den Vorgaben und Schritten, wie sie in den Lektionen 3.01 bis 3.07 des BSI Online-Kurses zum IT-Grundschutz dargelegt werden.

Das Hauptziel ist es, ein klares und umfassendes Bild der relevanten Prozesse, Informationen, Anwendungen, IT-Systeme und Infrastrukturen zu gewinnen, um die Schutzvorkehrungen im Rahmen eines Sicherheitskonzepts zielgerichtet und effektiv festlegen zu können.

Kontext des Unternehmens

Unser Unternehmen ist ein IT-Sicherheitsunternehmen, das sich auf die Entwicklung und Bereitstellung von auf künstlicher Intelligenz (KI) basierenden Sicherheitsstrukturen für Server und Unternehmensnetzwerke spezialisiert hat.

Das Unternehmen beschäftigt 25 Mitarbeiter,

darunter zwei Geschäftsführer,

zwei Anwälte mit Spezialisierung auf Arbeitsrecht, Informationsrecht, Cybersicherheit und Datenschutz-Grundverordnung (DSGVO),

einen Sicherheitsbeauftragten,

einen Marketingbeauftragten, zwei Vertriebsmitarbeiter, einen Kundensupportmitarbeiter sowie drei Auditoren und Schulungspersonal für Kunden. Die verbleibenden Mitarbeiter sind System-Fachinformatiker mit verschiedenen technischen Spezialisierungen.

Das Unternehmen operiert von zwei Büro Standorten aus (im Folgenden als Standort

A und Standort B bezeichnet) und betreibt eine eigene kleine Serverfarm (Standort C) zur Bereitstellung seiner Dienstleistungen. Es verfügt über einen etablierten Basis-Kundenstamm.

1. Geltungsbereich des Informationsverbunds (Lektion 3.01)

Definition des Geltungsbereichs

Der Geltungsbereich dieser Strukturanalyse, der sogenannte Informationsverbund, wird hiermit formal definiert. Er umfasst sämtliche organisatorischen, personellen, infrastrukturellen und informationstechnischen Komponenten, die für die Erfüllung des Geschäftszwecks und den Betrieb des Unternehmens beste Sicherheit durch AI relevant sind. Die Definition des Geltungsbereichs ist der erste Schritt, um den Rahmen für die nachfolgenden Analysen klar abzustecken.

- **Geschäftszweck:** Der Kern des Geltungsbereichs ist die Entwicklung, Bereitstellung, Wartung und der Support von KI-basierten Sicherheitslösungen. Dies schließt auch die damit verbundenen Tätigkeiten wie Beratung, Auditierung von Kunden, Umgebungen, Schulungen und Vertriebsaktivitäten ein.

- **Organisatorische Abdeckung:** Der Informationsverbund umfasst alle 25 Mitarbeiter des Unternehmens in ihren jeweiligen Rollen und Verantwortlichkeiten. Dies beinhaltet die Geschäftsführung, die Rechtsabteilung, den Sicherheitsbeauftragten, Marketing, Vertrieb, Kundensupport, Audit/Schulung sowie alle technischen Mitarbeiter (System-Fachinformatiker) in Entwicklung und Betrieb.

- **Physische Standorte:** Eingeschlossen sind beide Bürostandorte sowie der dedizierte Standort der Server Farm (Standort C – spezifische Adresse ist separat zu dokumentieren). Die Berücksichtigung aller relevanten Standorte ist essenziell, wie das Beispiel der RECPLAST GmbH mit ihren verschiedenen Standorten in Bonn und externen Vertriebsbüros zeigt.

- **Technologische Abdeckung:** Alle IT-Systeme (Server, Clients, Netzwerk Komponenten, Peripheriegeräte), Anwendungen Software und Daten (Informationen), die innerhalb der definierten organisatorischen und physischen Grenzen zur Unterstützung der Geschäftsprozesse genutzt, verarbeitet oder gespeichert werden, sind Teil des Informationsverbunds. Dies schließt explizit die Kommunikationsverbindungen zwischen den Standorten sowie die Anbindungen an externe Netze mit ein.

Abgrenzung

Explizit *nicht* Teil des betrachteten Informationsverbunds sind rein private IT-Geräte von Mitarbeitern, sofern deren Nutzung für geschäftliche Zwecke nicht im Rahmen einer genehmigten Bring-Your-Own-Device (BYOD)-Regelung erfolgt und diese Geräte keinen Zugriff auf interne Ressourcen haben.

Ebenfalls ausgeschlossen sind externe Dienstleister oder Cloud-Services, die nicht explizit als Teil der eigenen Dienstleistungserbringung oder kritischen Geschäftsprozessunterstützung identifiziert und in den Geltungsbereich einbezogen wurden (diese wären ggf. separat im Rahmen des Lieferantenmanagements zu betrachten).

Bedeutung der Serverfarm im Geltungsbereich

Die explizite Nennung und Einbeziehung der eigenen Serverfarm (Standort C) in den Geltungsbereich ist von herausragender Bedeutung.[2] Diese Infrastruktur ist das technologische Herzstück des Unternehmens, da hier die Kern-Dienstleistungen – die KI-basierten Sicherheitslösungen – entwickelt, getestet und für Kunden bereitgestellt werden. Folglich werden auf den Systemen an diesem Standort hochsensible und geschäftskritische Informationen verarbeitet und gespeichert, insbesondere die entwickelten KI-Algorithmen und -Modelle (geistiges Eigentum) sowie potenziell Konfigurations- und Betriebsdaten von Kundensystemen. Die physische und logische Trennung der Serverfarm von den regulären Büro Standorten erfordert spezifische und verstärkte Sicherheitsbetrachtungen hinsichtlich Zutrittskontrolle, Umgebungsbedingungen, Netzwerksicherheit (Segmentierung, Firewalls) und dedizierter Administration. Aufgrund ihrer zentralen Rolle und des hohen Werts der dort befindlichen Assets stellt die Serverfarm ein primäres Ziel für Angriffe dar und muss daher in allen nachfolgenden Analyseschritten (Systemerfassung, Raum Dokumentation, Netzplanung, Modellierung) mit besonderer Sorgfalt und Detailtiefe

behandelt werden.

Auswirkung der zwei Bürostandorte

Die Tatsache, dass das Unternehmen von zwei verschiedenen Bürostandorten (Standort A und Standort B) aus operiert, hat ebenfalls wichtige Konsequenzen für die Strukturanalyse. Es ist wahrscheinlich, dass bestimmte Funktionen oder Teams auf die Standorte aufgeteilt sind (z.B. Entwicklung an Standort B, Verwaltung/Vertrieb an Standort A). Dies erfordert zuverlässige und sichere Kommunikationsverbindungen zwischen den Standorten, analog zur Notwendigkeit einer Standleitung oder abgesicherten Verbindung wie im RECPLAST-Beispiel beschrieben.

Die IT-Infrastruktur (Netzwerkkomponenten, Server, Clients) und die implementierten physischen Sicherheitsmaßnahmen können sich zwischen den Standorten unterscheiden und müssen daher standortspezifisch erfasst werden.

Die Strukturanalyse muss die spezifischen Gegebenheiten, die eingesetzten Systeme und die unterstützten Prozesse an *beiden* Standorten detailliert erfassen. Insbesondere bei der Erstellung des Netzwerkplans und der Dokumentation der Räumlichkeiten ist die klare Darstellung beider Standorte und der Verbindungen sowie Abhängigkeiten zwischen ihnen unerlässlich.

2. Zentrale Geschäftsprozesse und Informationen (Lektion 3.03)

Identifikation der Geschäftsprozesse

Die systematische Erfassung der zentralen Geschäftsprozesse ist ein Kernbestandteil der Strukturanalyse, um zu verstehen, welche Aufgaben im Unternehmen durchgeführt werden und welche Informationen dabei eine Rolle spielen.[5] Basierend auf der Unternehmensbeschreibung und den definierten Mitarbeiterrollen lassen sich folgende Hauptgeschäftsprozesse identifizieren. Gemäß der Vorgehensweise in Lektion 3.03 [5] wird jeder Prozess mit einer eindeutigen Kennung, einem Namen, einer Kurzbeschreibung, den Verantwortlichen und den primär benötigten Anwendungen dokumentiert (letzteres wird in Tabelle 2.1 unten zusammengeführt):

- **GP01: Unternehmensführung & Strategie:** Festlegung der Unternehmensziele,

strategische Planung, Managemententscheidungen. (Verantwortlich: Geschäftsführer)

- **GP02: Rechtsberatung & Compliance:** Sicherstellung der Einhaltung rechtlicher Vorgaben (Arbeitsrecht, Informationsrecht, Cybersicherheit, DSGVO), Vertragsprüfung, rechtliche Beratung interner Abteilungen. (Verantwortlich: Anwälte)

- **GP03: Informationssicherheitsmanagement:** Entwicklung, Umsetzung und Überwachung der Informationssicherheitsleitlinie und -maßnahmen, Koordination sicherheitsrelevanter Aktivitäten. (Verantwortlich: Sicherheitsbeauftragter)

- **GP04: Marketing & Öffentlichkeitsarbeit:** Planung und Durchführung von Marketingkampagnen, Pflege der Unternehmenswebseite, Erstellung von Marketingmaterialien, Kommunikation nach außen. (Verantwortlich: Marketing Beauftragter)

- **GP05: Vertrieb & Akquise:** Identifikation potenzieller Kunden, Angebotserstellung, Vertragsverhandlungen, Kundenakquise. (Verantwortlich: Verkäufer)

- **GP06: Kundensupport:** Bearbeitung von Kundenanfragen, technische Unterstützung, Störungsbehebung, Pflege der Wissensdatenbank. (Verantwortlich: Kundensupporter)

- **GP07: Auditierung & Schulung:** Durchführung von Sicherheitsaudits bei Kunden, Erstellung von Auditberichten, Konzeption und Durchführung von Schulungen zu Produkten und Sicherheitsthemen. (Verantwortlich: Auditoren/Schulungspersonal)

- **GP08: Entwicklung KI-Sicherheitslösungen:** Forschung, Design, Implementierung, Test und Wartung der KI-basierten Sicherheitssoftware und -algorithmen. (Verantwortlich: System Fachinformatiker - Spezialisierung

KI/Entwicklung)

- **GP09: Betrieb & Wartung der Serverfarm/Dienste:** Sicherstellung des Betriebs der Serverinfrastruktur (Standort C), Installation, Konfiguration, Wartung und Überwachung der Systeme und Dienste, Backup-Management. (Verantwortlich: System Fachinformatiker - Spezialisierung Betrieb/Infrastruktur)

- **GP10: Interner IT-Support & Administration:** Verwaltung der internen IT-Infrastruktur an den Bürostandorten (Clients, Netzwerk, lokale Server), Benutzerverwaltung, Support für Mitarbeiter. (Verantwortlich: System Fachinformatiker - Spezialisierung Support/Admin)

- **GP11: Personalwesen:** Verwaltung von Mitarbeiterdaten, Gehaltsabrechnung, Recruiting (ggf. durch GF/Recht abgedeckt oder teilweise extern).

- **GP12: Finanzbuchhaltung:** Rechnungsstellung, Forderungsmanagement, Buchführung (ggf. durch GF abgedeckt oder teilweise extern).

Identifikation kritischer Informationen

Parallel zur Prozesserfassung müssen die wesentlichen Informationen identifiziert werden, die in diesen Prozessen benötigt, erzeugt, verarbeitet oder gespeichert werden. Die Kritikalität dieser Informationen ergibt sich aus den Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit sowie aus gesetzlichen (z.B. DSGVO) oder vertraglichen Verpflichtungen. Für Beste Sicherheit durch ai sind insbesondere folgende Informationskategorien relevant:

- **Kundendaten:** Namen, Adressen, Kontaktdaten von Ansprechpartnern, Vertragsdetails, Konfigurationsdaten der eingesetzten Sicherheitslösungen beim Kunden, Auditberichte, Supportanfragen und -protokolle. Diese Daten unterliegen strengen Datenschutzanforderungen (DSGVO).

- **Geistiges Eigentum (IP):** KI-Algorithmen (Trainingsdaten, Modelle, Parameter), Source Code der entwickelten Software, detaillierte Entwicklungsdokumentationen, interne Forschungsberichte und -daten, technische Konzepte, Geschäftsgeheimnisse. Dies stellt den Kernwert des Unternehmens dar.

- **Mitarbeiterdaten:** Personendaten (Namen, Adressen, Sozialversicherungsnummern, Bankverbindungen), Gehaltsinformationen, Arbeitsverträge, Beurteilungen, Zugangsdaten und Berechtigungen. Diese Daten sind ebenfalls durch DSGVO und Arbeitsrecht geschützt.

- **Finanzdaten:** Buchhaltungsunterlagen, Rechnungen (Ein- und Ausgang), Umsatzdaten, Bankdaten, Steuerinformationen.

- **Betriebsdaten:** Konfigurationen von Servern, Netzwerkkomponenten und Sicherheitssystemen, Netzwerkpläne, interne Sicherheitsrichtlinien und -konzepte, System- und Anwendungs-Log Files, Backup-Daten.

- **Rechtsdokumente:** Kundenverträge, Lieferantenverträge, Compliance-Nachweise (z.B. für DSGVO), interne rechtliche Gutachten und Stellungnahmen, Korrespondenz mit Behörden

Tabelle 2.1: Geschäftsprozesse und Kritische Informationen

Prozess-ID	Prozessname	Kurzbeschreibung (Ziel, Abläufe)	Verantwortliche(r)	Kritische Informationen (Beispiele)	Zugehörige Anwendungen (IDs aus Abs. 3)
GP01	Unternehmensführung & Strategie	Festlegung und Verfolgung der Unternehmensziele, strategische Entscheidungen	Geschäftsführer	Finanzdaten, Strategiepapiere, Mitarbeiterdaten (Managementebene)	A01, A02, A07
GP02	Rechtsberatung & Compliance	Sicherstellung rechtlicher Konformität (DSGVO, Cybersec, Arbeitsrecht), Vertragsmanagement	Anwälte	Rechtsdokumente, Mitarbeiterdaten, Kundendaten (im Kontext Compliance), IP (im Kontext Schutz)	A01, A02, A08
GP03	Informationssicherheits Mgmt.	Management der Informationssicherheit im Unternehmen	Sicherheitsbeauftragter	Betriebsdaten (Sicherheitskonzepte, Logs), Compliance-Nachweise	A01, A02, A09
GP04	Marketing & Öffentlichkeitsarbeit	Steigerung der Bekanntheit,	Marketing Beauftragter	Marketingmaterialien,	A01, A02, A05 (CRM-Teil)

		Lead-Generierung		Website-Daten, ggf. Kontaktdaten Interessenten	
GP05	Vertrieb & Akquise	Gewinnung neuer Kunden, Angebotserstellung, Vertragsabschluss	Verkäufer	Kundendaten (potenziell/Bestand), Angebotsdaten, Vertragsentwürfe, Finanzdaten (Preise)	A01, A02, A05
GP06	Kundensupport	Hilfe bei Anfragen und Problemen, Sicherstellung der Kundenzufriedenheit	Kundensupporter	Kundendaten (Bestand), Support-Tickets, Konfigurationsdaten (Kunde), Betriebsdaten (Logs zur Analyse)	A01, A02, A06
GP07	Auditierung & Schulung	Prüfung von Kundenumgebungen, Wissensvermittlung	Auditoren/Schulungspersonal	Kundendaten (Audit Objekte, Berichte), Schulungsmaterialien (IP)	A01, A02, ggf. spezial. Audit-Tools

GP08	Entwicklung KI-Sicherheitslösungen	Erstellung und Pflege der Kernprodukte	System Fach Informatiker (Entwicklung/KI)	Geistiges Eigentum (Code, Algorithmen, Modelle), Entwicklungsdoku, Testdaten	A01, A02, A03, A04
GP09	Betrieb & Wartung Serverfarm	Sicherstellung der Verfügbarkeit und Sicherheit der Dienstleistungsplattform	System Fach Informatiker (Betrieb/Infra)	Betriebsdaten (Konfigs, Logs, Backups), ggf. Kundendaten (Betrieb), IP (eingesetzte Software)	A01, A02, A10, A11
GP10	Interner IT-Support & Admin	Sicherstellung der internen IT-Funktionalität	System Fachinformatiker (Support/Admin)	Betriebsdaten (interne Configs, Logs), Mitarbeiterdaten (Konten)	A01, A02, A06 (intern), A10
GP11	Personalwesen	Verwaltung der Mitarbeiter Belange	GF/Recht/Extern	Mitarbeiterdaten (vollständig)	A01, A02, ggf. A07 (HR-Teil)
GP12	Finanzbuchhaltung	Korrekte Abbildung der Finanzströme	GF/Extern	Finanzdaten (vollständig), Kundendaten (Rechnun	A01, A02, A07

				gsstellung), Mitarbeiterdaten (Gehalt)	

Die Erstellung dieser Tabelle ist fundamental, da sie die direkte Verbindung zwischen den wertschöpfenden Aktivitäten (Prozessen) und den zu schützenden Gütern (Informationen) herstellt.

Sie klärt Verantwortlichkeiten und bildet die Basis für die spätere Schutzbedarfsfeststellung, da der Schutzbedarf von Informationen oft maßgeblich durch den Kontext des Geschäftsprozesses bestimmt wird, in dem sie verwendet werden.

Zudem ist die Zuordnung der benötigten Anwendungen der erste Schritt zur Modellierung der Abhängigkeiten im Informationsverbund.[6]

Hoher Schutzbedarf durch Kernkompetenz und Compliance

Die Natur des Geschäftsmodells von Beste Sicherheit urch Ai – die Entwicklung hochspezialisierter KI-Sicherheitslösungen – und die explizite Nennung interner Rechtsexpertise für Informationsrecht und DSGVO deuten auf einen inhärent hohen Schutzbedarf hin.

Die entwickelten KI-Algorithmen, der Source Code und die zugehörigen Forschungsdaten stellen das zentrale geistige Eigentum und damit den Kernwert des Unternehmens dar.

Eine Kompromittierung dieser Informationen durch Diebstahl oder Manipulation hätte existenzbedrohende Folgen.

Gleichzeitig ist die Verarbeitung von Kundendaten im Rahmen der Sicherheitsdienstleistungen (z.B. Konfigurationsdaten, Audit-Ergebnisse, Support-Anfragen) extrem sensibel und unterliegt strengen gesetzlichen (DSGVO) und potenziell vertraglichen Vertraulichkeit Anforderungen.

Das Vorhandensein spezialisierter Anwälte im Team unterstreicht das Bewusstsein und

die Verpflichtung des Unternehmens zur Einhaltung dieser komplexen rechtlichen Rahmenbedingungen.

Folglich müssen insbesondere die Informationskategorien "Geistiges Eigentum (KI)" und "Kunden Sicherheitsdaten" bei der späteren Schutzbedarfsfeststellung höchste Schutzstufen in Bezug auf Vertraulichkeit und Integrität erhalten.

Die Geschäftsprozesse GP02 (Rechtsberatung & Compliance), GP07 (Auditierung & Schulung), GP08 (Entwicklung KI-Sicherheitslösungen) und GP09 (Betrieb & Wartung Serverfarm) sind aufgrund der dort verarbeiteten Informationen als besonders kritisch einzustufen.

3. Wesentliche Anwendungen (Lektion 3.04)

Identifikation der Anwendungen

Aufbauend auf den identifizierten Geschäftsprozessen werden nun die wesentlichen Software-Anwendungen erfasst, die zur Unterstützung dieser Prozesse eingesetzt werden. Eine Anwendung wird als wesentlich betrachtet, wenn sie für die Erledigung von Fachaufgaben oder die Durchführung von Geschäftsprozessen notwendig ist und aufgrund des Schutzbedarfs der verarbeiteten Informationen ein Mindestmaß an Schutz erfordert.[7] Die Identifikation erfolgt idealerweise durch Gespräche und Workshops mit den Anwendern, den Anwendungs- und Geschäftsprozess Verantwortlichen sowie sachkundigen Mitarbeitern der IT-Abteilung.[7] Für [Name des Unternehmens] sind typischerweise folgende Anwendungskategorien relevant:

- **A01: Standard-Büroanwendungen (Office Suite):** Umfasst Textverarbeitung, Tabellenkalkulation, Präsentationssoftware und E-Mail-Client (z.B. Microsoft 365, LibreOffice). Wird prozessübergreifend genutzt.
- **A02: Kommunikations- und Kollaborationstools:** Instant Messaging (z.B. Slack, Mattermost), Videokonferenzsysteme (z.B. Teams, Zoom, Jitsi), E-Mail-Server-Software (z.B. Exchange, Postfix/Dovecot).
- **A03: Entwicklungsumgebungen & Werkzeuge:** Integrierte Entwicklungsumgebungen (IDEs wie VS Code, PyCharm), Compiler/Interpreter, Versionskontrollsysteme (z.B. Git mit GitLab/GitHub/Bitbucket), Build-Automatisierung (z.B. Jenkins, GitLab CI), Containerisierung Plattformen (z.B. Docker, Podman) und Orchestrierung (z.B. Kubernetes). Primär für GP08.
- **A04: KI/ML-Plattformen & Bibliotheken:** Spezialisierte Frameworks (z.B. Tensor Flow, PyTorch, Scikit-Learning), Datenanalyse- und Visualisierungstools (z.B. Jupyter Notebooks, Pandas, Matplotlib), Software für Data Annotation und Modelltraining. Primär für GP08.

- **A05: CRM-System (Customer Relationship Management):** Software zur Verwaltung von Kundenkontakten, Vertriebsaktivitäten und Kundenhistorie (z.B. Salesforce, SugarCRM, Odoo CRM). Primär für GP05, GP04, GP06.
- **A06: Support-Ticket-System:** Anwendung zur Erfassung, Zuweisung und Nachverfolgung von Kundenanfragen und Supportfällen (z.B. Jira Service Management, Zammad, OTRS). Primär für GP06, teilweise GP10 (intern).
- **A07: ERP/Finanzbuchhaltung Software:** System zur Verwaltung von Geschäftsprozessen wie Buchhaltung, Rechnungsstellung, ggf. Personalwesen (z.B. SAP Business One, DATEV, Odoo ERP). Genutzt in GP12, GP11, GP01, GP05.
- **A08: Rechts-/Compliance-Management-Software:** Ggf. spezialisierte Tools für Vertragsmanagement, DSGVO-Dokumentation (Verarbeitungsverzeichnisse etc.), Compliance-Überwachung. Genutzt in GP02.
- **A09: Interne Sicherheitsanwendungen:** Managementkonsolen für Antivirus/Endpoint Detection and Response (EDR), Security Information and Event Management (SIEM)-System, Vulnerability Scanner, Management-Interfaces von Firewalls und anderen Sicherheitssystemen. Genutzt in GP03, GP09, GP10.
- **A10: Zentrale Verzeichnisdienste & Systemmanagement:** Active Directory oder LDAP zur Benutzer- und Rechteverwaltung, Systemmanagement-Tools (z.B. Ansible, Puppet), Monitoring-Software (z.B. Nagios, Zabbix, Prometheus/Grafana). Genutzt in GP09, GP10.
- **A11: Virtualisierungsmanagement-Software:** Plattform zur Verwaltung der virtualisierten Serverumgebung in der Serverfarm (z.B. VMware vCenter, Proxmox VE Webinterface). Primär für GP09.

Dokumentation der Anwendungen

Die identifizierten wesentlichen Anwendungen werden gemäß den Vorgaben aus Lektion 3.04 [7] tabellarisch erfasst.

Tabelle 3.1: Wesentliche Anwendungen

Anwendungs-ID	Name	Kurzbeschreibung (Funktion, verarbeitete Infos)	Verantwortliche(r)	Hauptbenutzergruppen	Zugehörige Geschäftsprozesse (IDs)
A01	Office Suite	Standard-Bürokommunikation, Dokumentenerstellung (Texte, Tabellen, Präsentationen)	IT-Admin (GP10)	Alle Mitarbeiter	Alle GPs
A02	Kommunikations- und Kollaborationstools	E-Mail, Chat, Videokonferenzen, Datenaustausch	IT-Admin (GP10)	Alle Mitarbeiter	Alle GPs
A03	Entwicklungsumgebungen & Werkzeuge	Softwareentwicklung, Code-Verwaltung, Build, Test (IP: Source Code, Configs)	Leitung Entwicklung (GP08)	Entwicklung (GP08)	GP08
A04	KI/ML-Plattformen & Bibliotheken	Entwicklung, Training, Evaluierung von	Leitung Entwicklung (GP08)	Entwicklung (GP08)	GP08

		KI-Modellen (IP: Algorithmen, Modelle, Daten)			
A05	CRM-System	Verwaltung von Kunden- und Interessentendaten, Vertriebsprozesse (Kundendaten)	Leitung Vertrieb (GP05)	Vertrieb (GP05), Marketing (GP04)	GP04, GP05, GP06
A06	Support-Ticket-System	Bearbeitung von Supportanfragen (Kundendaten, Betriebsdaten Kunde/Intern)	Leitung Support (GP06)	Support (GP06), IT-Admin (GP10)	GP06, GP10
A07	ERP/Finanzbuchhaltung Software	Buchhaltung, Rechnungsstellung, ggf. HR (Finanzdaten, Kundendaten, Mitarbeiterdaten)	GF / Leitung Finanzen	GF (GP01), Buchhaltung (GP12)	GP01, GP05, GP11, GP12
A08	Rechts-/Compliance-Management-Software	Verwaltung von Verträgen, DSGVO-Doku (Rechtsdokumente,	Rechtsabteilung (GP02)	Recht (GP02)	GP02

		Kundendaten, Mitarbeiterdaten)			
A09	Interne Sicherheitsanwendungen	Überwachung und Steuerung der internen IT-Sicherheit (Betriebsdaten: Logs, Konfigs)	SIBE (GP03), IT-Betrieb (GP09)	SIBE (GP03), IT-Betrieb (GP09)	GP03, GP09, GP10
A10	Zentrale Verzeichnisdienste & System Mgmt.	Benutzerverwaltung, Rechtevergabe, Automatisierung (Mitarbeiterdaten, Betriebsdaten: Configs)	IT-Betrieb (GP09/GP10)	IT-Betrieb (GP09), IT-Admin (GP10)	GP09, GP10
A11	Virtualisierungsmanagement-Software	Verwaltung der Serverfarm-Virtualisierung (Betriebsdaten: Configs, Performance)	IT-Betrieb (GP09)	IT-Betrieb (GP09)	GP09

Diese Tabelle ist ein zentrales Element der Strukturanalyse nach BSI. Sie dokumentiert die eingesetzte Software systematisch und schafft die notwendige Verbindung zwischen den Geschäftsprozessen (Abschnitt 2) und der unterstützenden Technologie. Diese Information ist entscheidend für die spätere Modellierung von Abhängigkeiten – um beispielsweise zu verstehen, welcher Geschäftsprozess ausfällt, wenn eine bestimmte Anwendung nicht verfügbar ist – und für die Zuweisung von Schutzbedarf auf Anwendungsebene.

Granularität der Erfassung

Bei der Erfassung wurde auf eine angemessene Granularität geachtet, wie in Lektion 3.04 empfohlen. Standardisierte Werkzeuge wie das Office-Paket wurden zu einer Gruppe ("A01: Office Suite") zusammengefasst, da eine separate Betrachtung von Textverarbeitung und Tabellenkalkulation in diesem Kontext meist keinen Mehrwert bietet und den Aufwand unnötig erhöht. Hingegen wurden spezialisierte und geschäftskritische Systeme wie die KI/ML-Plattformen (A04), das CRM-System (A05) oder die Virtualisierungsmanagement-Software (A11) einzeln erfasst, da sie spezifische Funktionen erfüllen, unterschiedliche Schutzbedarfe haben und eine differenzierte Betrachtung in den nachfolgenden Schritten erfordern.

Kritische Abhängigkeit von Spezialanwendungen

Obwohl Standardanwendungen wie die Office Suite (A01) und Kommunikationswerkzeuge (A02) für den täglichen Betrieb wichtig sind, hängt der Kern des Geschäftsmodells von [Name des Unternehmens] maßgeblich von hochspezialisierten Anwendungen ab.[7] Die Verfügbarkeit, Integrität und Vertraulichkeit der Daten in den KI-Entwicklungs- und Trainingsumgebungen (A03, A04), die im Prozess GP08 genutzt werden, sind direkt an die Innovationsfähigkeit, die Produktqualität und damit den Markterfolg gekoppelt. Ebenso sind das CRM-System (A05) und das Support-System (A06) entscheidend für die professionelle Interaktion mit Kunden und die Erfüllung vertraglicher Pflichten in den Prozessen GP05 und GP06. Die Betriebs- und Management Software für die Serverfarm (A11, A10, A09), genutzt in GP09, ist wiederum kritisch für die zuverlässige Bereitstellung der verkauften Dienstleistungen. Diese Spezialanwendungen müssen daher bei der Schutzbedarfsfeststellung und der Risikoanalyse mit hoher Priorität behandelt werden. Ihre Abhängigkeiten zu den zugrundeliegenden IT-Systemen (Abschnitt 4) [6] und den genutzten Netzkomponenten (Abschnitt 5) [6] müssen im Rahmen der Modellierung (Abschnitt 8) präzise erfasst und bewertet werden.

4. Eingesetzte IT-Systeme (Lektion 3.06)

Identifikation der IT-Systeme

In diesem Schritt werden alle relevanten Hardware-Komponenten des Informationsverbunds erfasst, auf denen die zuvor identifizierten Anwendungen (Abschnitt 3) betrieben werden oder die für den Aufbau und Betrieb der Kommunikationsnetze (Abschnitt 5) erforderlich sind.[6] Dies umfasst physische und virtuelle Server, Netzwerkgeräte, Arbeitsplatzrechner und relevante Peripherie.

- **Server (Standort C - Serverfarm):**
  - S-C-VIRT: Virtualisierungs Hosts (Cluster für Hochverfügbarkeit)
  - S-C-AI: Dedizierte Server für KI-Training/Inferenz (ggf. mit GPU-Beschleunigung)
  - S-C-WEB: Webserver für Kundenportal/Dienste
  - S-C-DB: Datenbankserver
  - S-C-STOR: Storage-Systeme (NAS/SAN) für Datenablage und VM-Storage
  - S-C-BCKP: Backup-Server und -Speicher
  - S-C-MGMT: Management-Server (für Virtualisierung, Monitoring, Deployment etc.)
  - S-C-AD: Domänencontroller (ggf. redundant)

- **Server (Standort A/B - Bürostandorte):**
  - S-A/B-AD: Ggf. lokale (read-only) Domänencontroller
  - S-A/B-FILE: Ggf. lokale Fileserver (falls nicht zentralisiert oder Cloud-basiert)
  - S-A/B-PRINT: Ggf. lokale Printserver

- **Netzwerkkomponenten (Alle Standorte):**
  - N-GW-INET: Router/Firewall für Internetanbindung (redundant?)
  - N-GW-VPN: VPN-Gateway für Standortvernetzung und Fernzugriff
  - N-FW-SEG: Interne Firewalls zur Netzwerksegmentierung (z.B. zwischen Büro- und Servernetz)
  - N-SW-CORE: Core-Switches (redundant?)
  - N-SW-ACCESS-A/B/C: Access-Switches an den Standorten
  - N-WLAN-AP-A/B: WLAN Access Points in den Bürostandorten

- **Arbeitsplatzrechner (Clients - Standort A/B):**
  - C-STD: Standard-Desktops/Laptops für Verwaltung, Marketing, Vertrieb, Support (ca. 15-18 Stück)
  - C-DEV: Leistungsstärkere Desktops/Laptops für Entwickler (ca. 5-7 Stück)
  - C-LEGAL: Desktops/Laptops für Rechtsabteilung (2 Stück)

- **Peripheriegeräte (Standort A/B):**
  - P-PRINT-A/B: Netzwerkdrucker/Multifunktionsgeräte
  - P-SCAN-A/B: Ggf. separate Netzwerkscanner

- **Sonstige Systeme:**
  - O-TK: Ggf. VoIP-Telefonanlage (falls im Netzwerk integriert)
  - O-AI-HW: Ggf. spezialisierte Hardware für KI-Entwicklung/Tests (z.B. Edge Devices)

Dokumentation der IT-Systeme

Die identifizierten IT-Systeme werden gemäß den Vorgaben aus Lektion 3.06 [6] tabellarisch erfasst. Diese Tabelle dient als zentrales Inventar der technischen Infrastruktur.

Tabelle 4.1: IT-Systeme (Auszug)

System-ID	Bezeichnung (Gruppe + Anzahl)	Beschreibung (Typ, Einsatzzweck)	Plattform (Hardware, OS)	Standort (Raum-ID aus Abs. 5)	Status	Administrator(en)	Hauptbenutzergruppen	Relevante Anwendungen (IDs aus Abs. 3)
S-C-VIRT	Virtualisierungs Hosts (3)	Server für Betrieb virtueller Maschinen (VMs) in Serverf	Dell PowerEdge R7x0 / VMware ESXi 7.x	GC-SVR01	Betrieb	IT-Betrieb (GP09)	(Infrastruktur)	A11, (alle auf VMs laufenden)

		arm						
S-C-AI	KI-Trainingsserver (2)	Server mit GPUs für rechenintensives KI-Modelltraining	Supermicro XYZ / Ubuntu Server + NVIDIA	GC-SVR01	Betrieb	IT-Betrieb (GP09), Dev (GP08)	Entwicklung (GP08)	A04
N-GW-INET	Internet Firewall Cluster (2)	Firewall für Absicherung der Internetverbindung	Palo Alto PA-xxxx / PAN-OS	GC-TEC 01	Betrieb	IT-Betrieb (GP09)	(Infrastruktur)	A09
C-STD	Standard Clients (ca. 16)	Laptops/Desktops für Büroarbeiten, Vertrieb, Support, Marketing	Lenovo ThinkPad/ThinkCentre / Win 10/11	GA-Rxx, GB-Rxx	Betrieb	IT-Admin (GP10)	MA Verwaltung, Vertrieb etc.	A01, A02, A05, A06, A07
C-DEV	Entwickler Clients (ca. 6)	Leistungsstarke Laptops/Desktops für Softwareentwicklung	Dell Precision / Linux (Ubuntu)	GB-Rxx	Betrieb	IT-Admin (GP10), Dev (GP08)	Entwicklung (GP08)	A01, A02, A03, A04

P-PRINT-A	Netzwerkdrucker Standort A (1)	Zentraler Drucker/Kopierer/Scanner für Standort A	Kyocera TaskAlfa / -	GA-R05	Betrieb	IT-Admin (GP10)	MA Standort A	(Betriebssystem-Druckdienste)

Die Erstellung dieser Tabelle ist gemäß BSI [6] unerlässlich, um die konkreten Hardware-Assets des Informationsverbunds zu inventarisieren. Die Verknüpfung mit dem Standort (Raum-ID) [4] und den relevanten Anwendungen [6] ist entscheidend für die spätere Analyse von Abhängigkeiten sowie für die Bewertung physischer und technischer Risiken. Die Angaben zu Plattform und Status sind wichtig für das Patch- und Lifecycle-Management. Diese Liste bildet die Grundlage für die spätere Auswahl und Anwendung spezifischer IT-Grundschutz-Bausteine (z.B. SYS.* für Serversysteme, NET.* für Netzwerkkomponenten).

Konsistenz mit dem Netzplan

Es ist von großer Bedeutung, dass die in dieser Tabelle erfassten IT-Systeme, insbesondere die Netzwerkkomponenten und Server mit ihren Bezeichnungen, konsistent mit den Darstellungen im Netzplan (siehe Abschnitt 5) sind.[6] Inkonsistenzen können zu Missverständnissen und Fehlern in späteren Phasen der Sicherheitskonzeption führen.

Heterogenität der IT-Systeme und differenzierte Betrachtung

Die IT-Landschaft von [Name des Unternehmens] ist trotz der überschaubaren Mitarbeiterzahl heterogen. Sie umfasst Standard-Büro-Clients, spezialisierte Entwickler-Workstations, eine Vielzahl unterschiedlicher Servertypen (Virtualisierung, KI, Web, Datenbanken) sowie komplexe Netzwerkinfrastruktur, verteilt auf drei physisch getrennte Standorte.[6] Diese Systeme unterscheiden sich in Hardware, Betriebssystemen, Konfigurationen und vor allem in ihrem Einsatzzweck und ihrer Kritikalität für das Unternehmen. Der Schutzbedarf eines KI-Training Servers (S-C-AI), auf dem wertvolles geistiges Eigentum verarbeitet wird, ist naturgemäß deutlich höher als der eines Standard-Büro-Clients (C-STD). Dies erfordert angepasste Administrationsprozesse und differenzierte Sicherheitsmaßnahmen. Eine sinnvolle

Gruppierung von Systemen (siehe Abschnitt 7) ist daher notwendig, um den Analyseaufwand zu bewältigen. Diese Gruppierung darf jedoch kritische Unterschiede nicht verwischen.[8] Insbesondere die hoch kritischen Systeme wie die KI-Server, die zentralen Virtualisierungs Hosts, die Datenbankserver und die wesentlichen Netzwerkkomponenten (Internet-Firewall, Core-Switches) erfordern auch nach einer Gruppierung oft eine detaillierte Einzelbetrachtung in der Schutzbedarfsfeststellung und Risikoanalyse. Die klare Trennung und Kennzeichnung der Systeme nach ihrem Standort (Standort A, Standort B, Standort C/Serverfarm) ist ebenfalls für die weitere Analyse unerlässlich.

5. Räumlichkeiten und Kommunikationsnetze (Lektion 3.05 & 3.07)

Erfassung der Räumlichkeiten

Gemäß der Methodik des IT-Grundschutzes [4] müssen alle Gebäude und Räume erfasst werden, die im Zusammenhang mit den betrachteten Informationen, Geschäftsprozessen und IT-Systemen von Bedeutung sind. Dies geht über reine Server- oder Technikräume hinaus und umfasst auch normale Büroräume, Besprechungsräume, Archive und ggf. auch die Verlegewege wichtiger Kommunikationsleitungen innerhalb der Gebäude. Werden IT-Systeme wie Server oder Datenträgerarchive in speziellen Schutzschränken untergebracht, sind diese Schränke ebenfalls als relevante Objekte zu erfassen.[4]

- **Standort A (z.B. Verwaltung/Vertrieb):**
  - GA: Gebäude A
  - GA-R01..R10: Büroräume (Einzel-/Mehrpersonen)
  - GA-R11: Besprechungsraum
  - GA-R12: Technikraum/Netzwerkverteiler
  - GA-R13: Archivraum (falls vorhanden)
- **Standort B (z.B. Entwicklung/Support):**
  - GB: Gebäude B
  - GB-R01..R08: Büroräume (Entwickler, Support)
  - GB-R09: Entwickler-Labor/Testumgebung
  - GB-R10: Besprechungsraum
  - GB-R11: Technikraum/Netzwerkverteiler
- **Standort C (Serverfarm):**
  - GC: Gebäude C (ggf. Rechenzentrum eines Dienstleisters oder eigener Bau)
  - GC-SVR01: Serverraum 1
  - GC-SVR02: Ggf. Serverraum 2 (Redundanz/Trennung)
  - GC-TEC01: Technikraum (Netzwerk, Stromversorgung, Kühlung)

- GC-ADM01: Ggf. Büro für Administration vor Ort

Tabelle 5.1: Räumlichkeiten (Auszug)

Raum-ID	Bezeichnung (Gruppe)	Standortadresse/Gebäude)	Beschreibung (Nutzung)	Zugehörige IT-Systeme (IDs aus Abs. 4)
GA-R01	Büro Geschäftsführung	Standort A	Einzelbüro	C-STD (GF)
GA-R12	Technikraum Standort A	Standort A	Netzwerkverteilung, ggf. kl. Server/TK	N-SW-ACCESS-A, S-A/B-AD (falls hier), O-TK
GB-R01	Büro Entwicklung Team 1	Standort B	Mehrpersonenbüro Entwickler	C-DEV (Team 1)
GB-R09	Entwickler-Labor	Standort B	Testaufbauten, Spezialhardware	O-AI-HW
GC-SVR01	Serverraum 1 Serverfarm	Standort C	Haupt Serverraum, Racks 1-10	S-C-VIRT, S-C-AI, S-C-B, S-C-DB, S-C-STOR etc.
GC-TEC01	Technikraum Serverfarm	Standort C	Netzwerkanbindung, USV, Klima	N-GW-INET, N-SW-CORE-C

Die Erfassung der Räumlichkeiten ist die Grundlage für die Bewertung der physischen Sicherheit und der Umgebungsbedingungen (z.B. Brandschutz, Klimatisierung, Zutrittskontrolle), die typischerweise im IT-Grundschutz-Baustein INF.* behandelt werden. Die Zuordnung der IT-Systeme zu den Räumen in dieser Tabelle ist entscheidend, um physische Risiken für spezifische technische Komponenten zu identifizieren (z.B. ein ungesicherter Server in einem allgemein zugänglichen Büroraum). Eine Gruppierung ähnlicher Räume (z.B. alle Standard Büros an Standort A) kann den Detaillierungsgrad in späteren Schritten reduzieren.[4]

Erstellung des Netzplans

Ein aktueller und aussagekräftiger Netzplan ist eine zentrale Anforderung der Strukturanalyse gemäß Lektion 3.05.[3] Er stellt die informationstechnische Infrastruktur und deren Vernetzung grafisch dar.

- **Inhalt:** Der Netzwerkplan muss alle wesentlichen IT-Systeme aus Abschnitt 4 (Server, Clients, Netzwerkkomponenten wie Router, Switches, Firewalls, APs, sowie relevante Peripherie wie Netzwerkdrucker) enthalten.[3]
- **Verbindungen:** Die logischen Verbindungen zwischen diesen Systemen (LAN-Verkabelung, WLAN-Verbindungen) sind darzustellen.[3]
- **Standortdarstellung:** Die drei Standorte (Standort A, Standort B, Standort C/Serverfarm) müssen klar voneinander abgegrenzt und mit ihren jeweiligen internen Netzwerkstrukturen abgebildet werden.
- **Standortvernetzung:** Die Art und Weise, wie die Standorte A und B miteinander verbunden sind (z.B. über eine gesicherte VPN-Verbindung über das Internet oder eine dedizierte Leitung), muss ersichtlich sein.[2]
- **Serverfarm-Anbindung:** Die Anbindung der Server Farm (Standort C) an die Bürostandorte und insbesondere an das Internet muss klar dargestellt werden. Dies beinhaltet die Platzierung von Firewalls und potenziellen demilitarisierten Zonen (DMZs).
- **Externe Verbindungen:** Die Anbindung(en) an das Internet sind zu kennzeichnen, idealerweise mit Angabe des Typs (z.B. Glasfaser, DSL) und der Bandbreite.[3] Eventuelle dedizierte Verbindungen zu externen Partnern oder Kunden sind ebenfalls aufzunehmen.
- **Sicherheitskomponenten und Segmentierung:** Firewalls, VPN-Gateways und andere zentrale Sicherheitskomponenten müssen im Plan deutlich hervorgehoben werden. Wichtig ist auch die Visualisierung der Netzwerksegmentierung, d.h. die logische Trennung verschiedener Netzbereiche (z.B. Servernetz, Client Netz

Standort A, Client Netz Standort B, Entwicklungsnetz, Management Netz, DMZ).

Diagramm 5.2: Netzwerkplan

(Hinweis: Der Netzwerkplan ist ein separates grafisches Dokument, das mit geeigneten Werkzeugen wie z.B. Microsoft Visio, draw.io oder ähnlichem erstellt wird. Er verwendet standardisierte Symbole für verschiedene Gerätetypen und Verbindungen.)

Der Netzplan ist nicht nur eine Bestandsaufnahme, sondern ein wichtiges Analyseinstrument.[3] Er visualisiert die komplexe Topologie des Netzwerks und die Kommunikationsbeziehungen zwischen den Systemen. Er hilft dabei, potenzielle Engpässe (Bottlenecks), einzelne Auswahlpunkte (Single Points of Failure) und logische Angriffspunkte zu identifizieren. Die im Netzplan vorgenommene Gruppierung von Systemen (z.B. Zusammenfassung der Clients eines Standorts zu einem "Client-Netz") dient der Übersichtlichkeit, wie auch im Beispiel der RECPLAST GmbH praktiziert.[3] Der Plan ist eine essenzielle Grundlage für die Konfiguration von Netzwerkkomponenten (insbesondere Firewalls und Switches), die Fehlersuche und die Planung zukünftiger Netzwerkänderungen.

Netzwerksegmentierung als kritischer Faktor

Angesichts der Struktur des Unternehmens mit drei Standorten, einer eigenen Serverfarm für kritische Dienste und der Entwicklung von KI-Sicherheitslösungen ist eine durchdachte Netzwerksegmentierung von entscheidender Bedeutung für die Informationssicherheit. Eine "flache" Netzwerkstruktur, in der alle Systeme ohne wesentliche Trennung miteinander kommunizieren können, würde ein erhebliches Sicherheitsrisiko darstellen. Die Serverfarm (Standort C), die das geistige Eigentum und potenziell sensible Kundendaten beherbergt, muss durch Firewalls und idealerweise durch den Einsatz von DMZs streng vom Internet und auch von den allgemeinen Büro Netzwerken (Standort A und B) isoliert werden. Das Entwicklungsnetzwerk (genutzt in GP08) benötigt möglicherweise ebenfalls eine eigene Segmentierung mit spezifischen Sicherheitskontrollen, um den Quellcode und die Entwicklungsdaten zu schützen. Die Verbindungen zwischen den Baumstandorten [2] sowie die Anbindung der Serverfarm müssen durch starke Verschlüsselung (z.B. IPsec oder SSL-VPNs) abgesichert werden. Der Netzplan [3] muss die implementierte (oder geplante) Segmentierung detailliert und nachvollziehbar abbilden. Die Angemessenheit dieser Segmentierung wird ein zentraler Punkt in der späteren

Risikoanalyse sein. Die genaue Dokumentation der eingesetzten Netzkomponenten (insbesondere Firewalls, Router) in Tabelle 4.1.6 und die Modellierung ihrer Nutzung durch die verschiedenen Anwendungen (siehe Matrix 8.3) [6] sind hierfür unerlässlich.

6. Systematische Erfassung der Zielobjekte

Zusammenfassung der erfassten Objekte

In den vorangegangenen Abschnitten wurden die für die Strukturanalyse relevanten Zielobjekte des Informationsverbunds vom [Name des Unternehmens] systematisch erfasst und dokumentiert. Dies erfolgte gemäß der im BSI IT-Grundschutz beschriebenen Vorgehensweise [1] und umfasst die folgenden Kategorien:

- **Geschäftsprozesse und kritische Informationen:** Identifiziert und beschrieben in Abschnitt 2 (siehe Tabelle 2.1).
- **Wesentliche Anwendungen:** Identifiziert und beschrieben in Abschnitt 3 (siehe Tabelle 3.1).
- **Eingesetzte IT-Systeme:** Identifiziert und beschrieben in Abschnitt 4 (siehe Tabelle 4.1).
- **Räumlichkeiten:** Identifiziert und beschrieben in Abschnitt 5 (siehe Tabelle 5.1).
- **Kommunikationsnetze:** Grafisch dargestellt im Netzplan (siehe Beschreibung und Verweis auf Diagramm 5.2 in Abschnitt 5).

Verweis auf die Details Dokumentation

Die detaillierten Listen, Beschreibungen und Attribute der einzelnen Zielobjekte sind in den jeweiligen Tabellen (Tabelle 2.1, Tabelle 3.1, Tabelle 4.1, Tabelle 5.1) sowie im zugehörigen Netzplan (Diagramm 5.2) enthalten. Diese Dokumente bilden die umfassende Datenbasis für die weiteren Schritte des IT-Grundschutz Prozesses.

7. Gruppierung von Einzelobjekten (Lektion 3.02/3.07)

Anwendung der Gruppierungskriterien

Um die Komplexität des Informationsverbunds für die nachfolgende Schutzbedarfsfeststellung und Risikoanalyse handhabbar zu machen, werden ähnliche Zielobjekte zu Gruppen zusammengefasst. Dies betrifft vor allem IT-Systeme, kann aber auch auf Anwendungen oder Räume angewendet werden.[4] Die Gruppierung erfolgt auf Basis definierter Kriterien [8]:

- Gleicher Typ des Objekts (z.B. alle Laptops eines bestimmten Modells).
- Gleiche oder nahezu gleiche Konfiguration (Hardware, Betriebssystem,

wesentliche Software).
- Gleiche oder nahezu gleiche Einbindung in das Netz (gleiches Subnetz, gleiche Firewall-Regeln).
- Gleiche administrative und infrastrukturelle Rahmenbedingungen (gleicher Administrator, gleicher physischer Schutz).
- Gleiche oder sehr ähnlich genutzte Anwendungen.
- Gleicher Schutzbedarf (dieses Kriterium wird oft erst nach der Schutzbedarfsfeststellung final angewendet, kann aber hier bereits als Annahme einfließen).

Definition von Gruppen

Basierend auf den erfassten Objekten und den Gruppierungskriterien werden folgende Gruppen für [Name des Unternehmens] definiert:

- **G-SYS-Client-Std:** Standard-Arbeitsplatzrechner (Laptops/Desktops, ca. 16 Stück) für Mitarbeiter in Verwaltung, Marketing, Vertrieb, Support an Standorten A und B. Annahme: Ähnliche Hardware (z.B. Lenovo ThinkPad/ThinkCentre), Windows OS, Standard-Office- und Kommunikationssoftware, CRM/Support-Zugriff, mittlerer Schutzbedarf. Zugehörige Objekte: C-STD aus Tabelle 4.1.
- **G-SYS-Client-Dev:** Entwickler-Arbeitsplatzrechner (Laptops/Desktops, ca. 6 Stück) an Standort B. Annahme: Leistungsfähigere Hardware (z.B. Dell Precision), Linux OS, spezielle Entwicklungs- und KI-Tools (A03, A04), Zugriff auf Code-Repositories, höherer Schutzbedarf bzgl. IP-Vertraulichkeit/Integrität. Zugehörige Objekte: C-DEV aus Tabelle 4.1.
- **G-SYS-Client-Legal:** Arbeitsplatzrechner (Laptops/Desktops, 2 Stück) für Rechtsabteilung an Standort A. Annahme: Standard-Hardware, Windows OS, Zugriff auf vertrauliche Rechtsdokumente und Compliance-Daten (A08), hoher Schutzbedarf bzgl. Vertraulichkeit. Zugehörige Objekte: C-LEGAL (muss in Tab 4.1 ergänzt werden).
- **G-SYS-Server-Virt:** Virtualisierung Hosts (Cluster, 3 Stück) in der Serverfarm (Standort C). Annahme: Identische Hardware/Konfiguration, VMware ESXi, kritisch für Verfügbarkeit vieler Dienste, hoher Schutzbedarf. Zugehörige Objekte: S-C-VIRT aus Tabelle 4.1.
- **G-SYS-Server-AI:** KI-Trainings-/Konferenzserver (2 Stück) in der Serverfarm (Standort C). Annahme: Spezialhardware (GPUs), Linux OS, Verarbeitung von IP, sehr hoher Schutzbedarf (Vertraulichkeit, Integrität). Zugehörige Objekte: S-C-AI aus Tabelle 4.1.
- **G-SYS-Net-Firewall-INET:** Internet Firewall Cluster (2 Stück) in der Serverfarm

(Standort C). Annahme: Identische Hardware/OS (Palo Alto), kritisch für Netzwerksicherheit und Verfügbarkeit externer Dienste, sehr hoher Schutzbedarf. Zugehörige Objekte: N-GW-INET aus Tabelle 4.1.

- **G-SYS-Net-Switch-Access-A:** Access-Switches (z.B. 2 Stück) am Standort A. Annahme: Gleicher Typ/Konfiguration, verbinden Clients/Drucker im Büro A, mittlerer Schutzbedarf. Zugehörige Objekte: N-SW-ACCESS-A (aus Tab 4.1).
- **G-RAUM-Büro-StdA:** Standard-Büroräume (ca. 10 Stück) am Standort A. Annahme: Ähnliche Nutzung (Büroarbeit), vergleichbare physische Grundsicherung (Türen, Fenster), Standard-Schutzbedarf für Büroumgebung. Zugehörige Objekte: GA-R01..R10 (ohne GF/Bespr.) aus Tabelle 5.1.[4]
- **G-RAUM-Serverraum:** Serverräume (1-2 Stück) am Standort C. Annahme: Spezielle physische Sicherung (Zutritt, Klima, Strom), beherbergen kritische IT, hoher Schutzbedarf. Zugehörige Objekte: GC-SVR01, GC-SVR02 aus Tabelle 5.1.[4]

Tabelle 7.1: Gruppen von Einzelobjekten (Auszug)

Gruppen-ID	Beschreibung der Gruppe	Zugehörige Objekt-IDs (Beispiele)	Begründung für die Gruppierung (Kriterien nach)
G-SYS-Client-Std	Standard-Arbeitsplätze (Verwaltung, Vertrieb etc.)	C-STD (alle)	Gleicher Typ (Laptop/Desktop), ähnl. Konfig (Win, Office, CRM), ähnl. Netzanbindung, ähnl. Nutzung, ähnl. Schutzbedarf
G-SYS-Client-Dev	Entwickler-Arbeitsplätze	C-DEV (alle)	Gleicher Typ (Laptop/Desktop), ähnl. Config (Linux, IDEs, AI-Tools), usw. Nutzung (IP), höherer Schutzbedarf
G-SYS-Server-Virt	Virtualisierungs Hosts Serverfarm	S-C-VIRT (alle)	Gleicher Typ/Config (HW, ESXi), Cluster, Gl. Standort/Admin, Kritik. Verfügbarkeit, hoher Schutzbedarf
G-RAUM-Büro-StdA	Standard-Büroräume Standort A	GA-R02..R10	Gleicher Typ (Büro), Gl. Standort, ähnl. Nutzung, ähnl. physische Sicherung, Standard-Schutzbedarf
G-RAUM-Serverraum	Serverräume Standort C	GC-SVR01, GC-SVR02	Gleicher Typ (Serverraum), Gl. Standort, spez.

			Nutzung (Krit. IT), spez. Sicherung, hoher Schutzbedarf

Die Gruppierung ist ein wichtiger Schritt zur Effizienzsteigerung im IT-Grundschutz-Prozess.[3] Diese Tabelle dokumentiert die gebildeten Gruppen und die Kriterien, die zur Zusammenfassung geführt haben, nachvollziehbar. Sie erleichtert die spätere Zuweisung von IT-Grundschutz-Bausteinen und Sicherheitsmaßnahmen, da diese oft auf ganze Gruppen ähnlicher Objekte angewendet werden können. Gleichzeitig stellt die Dokumentation sicher, dass die Gruppierung nicht willkürlich, sondern auf Basis der definierten BSI-Kriterien erfolgt.

Balance zwischen Vereinfachung und Genauigkeit bei der Gruppierung

Obwohl Beste Sicherheit durch Ai mit 25 Mitarbeitern relativ klein ist, erfordert die Kombination aus diversifizierten Rollen (Entwicklung, Recht, Vertrieb etc.) und einer komplexen Infrastruktur (KI-Entwicklung, eigene Serverfarm) eine sorgfältige Abwägung bei der Gruppierung. Eine zu grobe Zusammenfassung, wie z.B. die Bildung nur einer einzigen Gruppe für alle Client-Rechner, würde die signifikant unterschiedlichen Anforderungen und Schutzbedarfe der Entwickler-, Rechts- und Standard-Arbeitsplätze ignorieren.[8] Dies könnte dazu führen, dass notwendige spezifische Sicherheitsmaßnahmen für besonders schützenswerte Systeme übersehen werden. Umgekehrt würde eine zu feingliedrige Betrachtung, bei der fast jedes System einzeln behandelt wird, den Vorteil der Komplexitätsreduktion durch Gruppierung zunichtemachen. Die hier vorgeschlagene Definition mehrerer Client-Gruppen (Standard, Entwickler, Legal) und mehrerer Server-Gruppen (Virtualisierung, KI etc.) versucht, diese Balance zu finden. Die Begründung jeder Gruppierung anhand der Kriterien aus [8], insbesondere der genutzten Anwendungen und des (angenommenen) Schutzbedarfs, ist dabei entscheidend und muss im weiteren Prozess ggf. angepasst werden.

8. Modellierung des Informationsverbunds (Lektion 3.06)

Darstellung von Abhängigkeiten

Die Modellierung des Informationsverbunds dient dazu, die komplexen Beziehungen und Abhängigkeiten zwischen den erfassten und gruppierten Ziel Objekten sichtbar zu machen. Dies erfolgt primär durch die Erstellung von Matrizen, wie sie in den Lektionen 3.04, 3.06 und 3.07 des BSI-Online-Kurses beschrieben werden.[4] Diese

Matrizen zeigen auf, wie Geschäftsprozesse von Anwendungen, Anwendungen von IT-Systemen und Netzwerken sowie IT-Systeme von ihrer physischen Umgebung abhängen.

Matrix 8.1: Abhängigkeiten Geschäftsprozesse zu Anwendungen

Diese Matrix stellt dar, welche Geschäftsprozesse (aus Tabelle 2.1) welche wesentlichen Anwendungen (aus Tabelle 3.1, ggf. gruppiert) für ihre Durchführung benötigen. Sie basiert auf den Informationen, die bei der Erfassung der Prozesse und Anwendungen gesammelt wurden.[5]

(Beispielhafte Darstellung - eine vollständige Matrix ist zu erstellen)

	A01 Office	**A02 Komm.**	**A03 Dev Tools**	**A04 AI/ ML**	**A05 CRM**	**A06 Support**	**A07 ERP /Fibu**	**A08 Legal**	**A09 Security**	**A10 Mgmt**	**A11 Virt**
GP01 Führung	X	X					X				
GP02 Recht	X	X						X			
GP05 Vertrieb	X	X			X		X				
GP08 Entwicklung	X	X	X	X							

GP09 Betrieb	X	X							X	X	X

Legende: X = Prozess benötigt Anwendung

Diese Matrix visualisiert die direkten Abhängigkeiten der Geschäftsaktivitäten von der eingesetzten Software. Sie ermöglicht eine schnelle Abschätzung der Auswirkungen, wenn eine bestimmte Anwendung (z.B. das CRM-System A05) ausfällt – in diesem Fall wären primär die Vertriebs- und Marketingprozesse betroffen. Sie hilft auch bei der Priorisierung von Anwendungen für Sicherheitsmaßnahmen, basierend auf der Kritikalität der von ihnen unterstützten Geschäftsprozesse.

Matrix 8.2: Abhängigkeiten Anwendungen zu IT-Systemen/Gruppen

Diese Matrix zeigt, auf welchen IT-Systemen oder Systemgruppen (aus Tabelle 4.1 bzw. 7.1) die wesentlichen Anwendungen (aus Tabelle 3.1) betrieben werden oder welche Systeme sie für ihre Funktion benötigen.[6]

(Beispielhafte Darstellung)

	G-SYS-Client-Std	**G-SYS-Client-Dev**	**G-SYS-Server-Virt**	**G-SYS-Server-AI**	**S-C-WEB**	**S-C-DB**	**S-C-AD**
A01 Office	X	X					
A03 Dev Tools		X					
A04 AI/ML		X		X			
A05 CRM	X		V		V	V	V
A11 Virt Mgmt			M				

Legende: X = Läuft direkt auf System/Gruppe, V = Läuft auf VM gehostet von System/Gruppe, M = Management-Anwendung für System/Gruppe

Diese Darstellung verdeutlicht die technische Grundlage der Anwendungen. Sie macht sichtbar, welche Anwendungen betroffen sind, wenn ein bestimmtes IT-System oder eine Gruppe (z.B. die Virtualisierung Hosts G-SYS-Server-Virt) ausfällt. Dies ist entscheidend für die Planung von Hochverfügbarkeitslösungen, das Kapazitätsmanagement und das Änderungsmanagement.

Matrix 8.3: Abhängigkeiten Anwendungen zu Netzkomponenten/Gruppen

Diese Matrix dokumentiert, welche relevanten Netzwerkkomponenten oder -gruppen (aus Tabelle 4.1 bzw. 7.1, z.B. Firewalls, Router, Core-Switches) für die Kommunikation einer Anwendung notwendig sind. Die Erstellung einer solchen Matrix wird explizit in Lektion 3.06 empfohlen.[6]

(Beispielhafte Darstellung)

	G-SYS-Net-Firewall-INET	**N-GW-VPN**	**N-FW-SEG**	**G-SYS-Net-Switch-Access-A**	**G-SYS-Net-Switch-Access-B**	**N-SW-CORE-C**
A02 Komm.	X	X	X	X	X	X
A04 AI/ML			X		X	X
A05 CRM (Web)	X		X			X

Legende: X = Datenverkehr der Anwendung läuft über diese Komponente / ist von ihr abhängig

Diese Matrix visualisiert die Abhängigkeit der Anwendungsfunktion von der Netzwerkinfrastruktur.[6] Sie ist hilfreich bei der Fehlersuche (z.B. Welche Anwendungen sind betroffen, wenn die interne Firewall NGFW-SEG ausfällt?) und unterstützt die Konfiguration von Firewall-Regeln, Quality of Service (QoS) und Intrusion

Detection/Prevention Systemen.

Matrix 8.4: Abhängigkeiten IT-Systeme/Gruppen zu Räumen/Gruppen

Diese Matrix stellt die physische Verortung der IT-Systeme oder -gruppen (aus Tabelle 4.1 bzw. 7.1) in den erfassten Räumen oder Raumgruppen (aus Tabelle 5.1 bzw. 7.1) dar. Diese Darstellung wird in Lektion 3.07 gefordert.[4]

(Beispielhafte Darstellung)

	G-RAUM-Büro-Std A	**GA-R12 Technik A**	**G-RAUM-Büro-Std B**	**GB-R11 Technik B**	**G-RAUM-Serverraum**	**GC-TEC01 Technik C**
G-SYS-Client-Std	X		X			
G-SYS-Client-Dev			X			
G-SYS-Server-Virt					X	
G-SYS-Net-Firewall-INET						X
N-SW-ACCESS-A		X				

Legende: X = System/Gruppe befindet sich in diesem Raum/dieser Raumgruppe

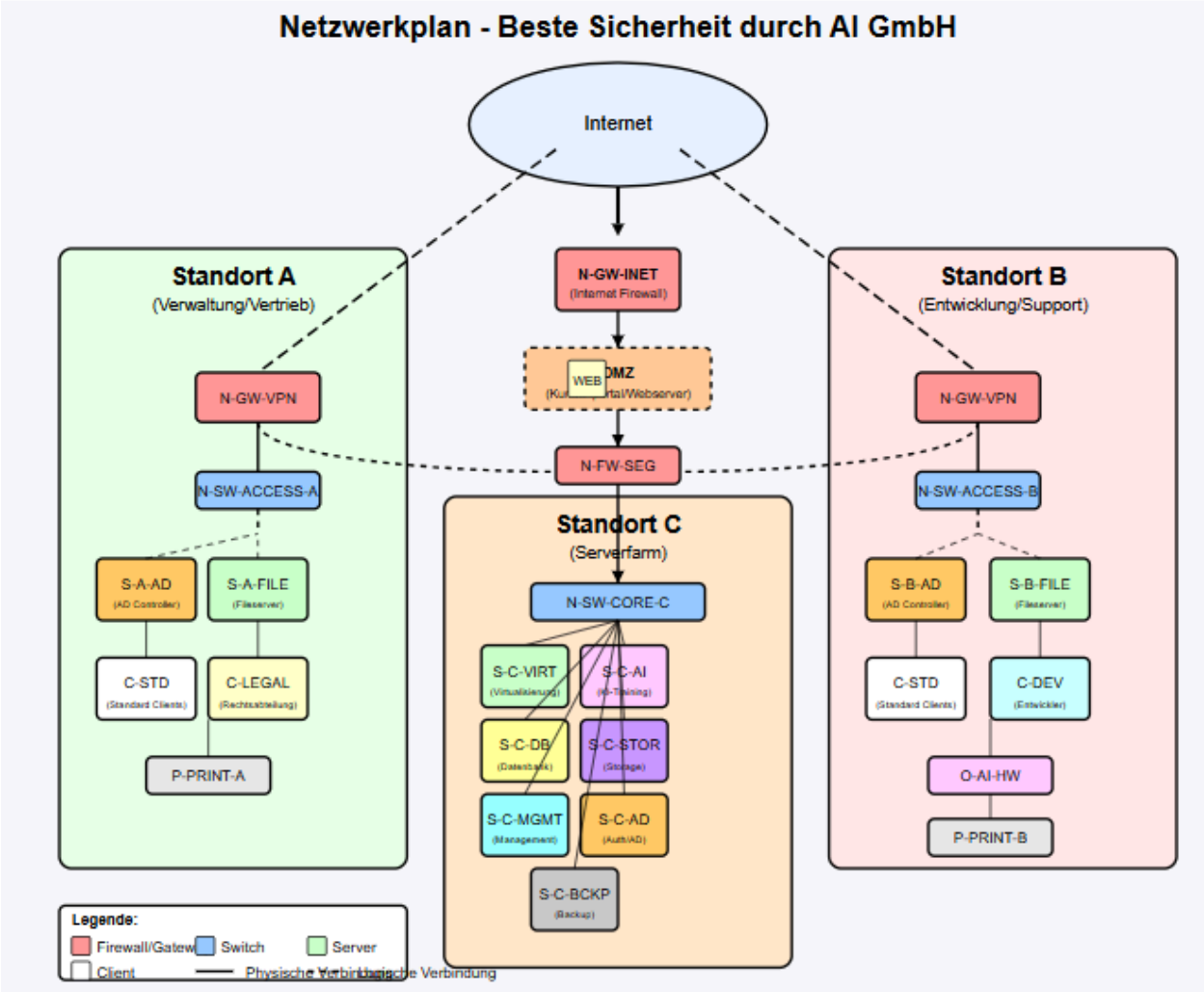
Diese Matrix verknüpft die technischen Assets mit ihrer physischen Umgebung.[4] Sie ist essentiell für die Bewertung von Risiken, die von der Umgebung ausgehen (z.B. Feuer,

Wasser, unbefugter Zutritt, Ausfall der Klimatisierung) und deren potenzielle Auswirkungen auf spezifische IT-Systeme. Sie unterstützt zudem die Planung von Maßnahmen zur physischen Sicherheit wie Zutrittskontrollen oder Umgebungsüberwachung.

Abhängigkeit Ketten als Schlüssel zur Risikobewertung

Die erstellten Matrizen [4] sind mehr als nur eine Dokumentation; sie visualisieren die kritischen Abhängigkeit Ketten im Informationsverbund: Ein Geschäftsprozess (z.B. GP08 Entwicklung) benötigt eine Anwendung (z.B. A04 AI/ML), diese läuft auf einem IT-System (z.B. G-SYS-Server-AI), das wiederum auf Netzwerkkomponenten (z.B. N-SW-CORE-C) angewiesen ist und sich in einem bestimmten Raum (z.B. G-RAUM-Serverraum) befindet. Ein Vorfall an einer Stelle dieser Kette – sei es ein technischer Ausfall eines Servers [6], ein erfolgreicher Cyberangriff auf eine Anwendung [7] oder ein physisches Ereignis wie ein Brand im Serverraum [4] – kann sich kaskadenartig auf alle darüber liegenden Elemente auswirken und letztlich die Fähigkeit zur Durchführung kritischer Geschäftsprozesse [5] beeinträchtigen. Die Modellierung macht diese potenziellen Kaskadeneffekte sichtbar. Besonders kritisch sind dabei die Objekte (Anwendungen, Systeme, Netzkomponenten, Räume), von denen viele andere wichtige Objekte abhängen. Beispiele hierfür sind oft zentrale Authentifizierungssysteme (wie S-C-AD), die Virtualisierungsinfrastruktur (G-SYS-Server-Virt), zentrale Netzwerk-Gateways (G-SYS-Net-Firewall-INETD) oder der Hauptserverraum (G-RAUM-Serverraum C). Die sorgfältige Analyse dieser Abhängigkeit Ketten und die Identifikation solcher kritischen Pfade und potenziellen Single Points of Failure sind eine direkte und unverzichtbare Vorbereitung für die nachfolgenden Schritte der Schutzbedarfsfeststellung und der Risikoanalyse im IT-Grundschutz-Prozess.

Netzwerkplan:



Standorte

- **Standort A (Verwaltung/Vertrieb): Beinhaltet Standard-Clients, Legal-Clients, lokale Server und Netzwerkkomponenten**
- **Standort B (Entwicklung/Support): Umfasst Entwickler-Workstations, Standard-Clients, lokale Server und das Entwicklungs-Labor**
- **Standort C (Serverfarm): Das technologische Herzstück mit den wichtigsten Servern und Sicherheitskomponenten**

Netzwerkinfrastruktur

- **Internet-Anbindung: Zentrale Firewall (N-GW-INET) für die Internetverbindung**
- **VPN-Gateways: Sichere Verbindungen zwischen den Standorten**
- **Netzwerksegmentierung: Interne Firewall (N-FW-SEG) zur Trennung der Netzbereiche**
- **DMZ: Für nach außen erreichbare Dienste wie das Kundenportal**

Serverlandschaft in Standort C

- **Virtualisierungshosts (S-C-VIRT)**
- **KI-Trainingsserver (S-C-AI)**
- **Datenbank- und Storage-Systeme (S-C-DB, S-C-STOR)**
- **Active Directory und Authentifizierung (S-C-AD)**
- **Management- und Backup-Server**

Der Plan zeigt deutlich die mehrschichtige Sicherheitsarchitektur mit entsprechenden Firewalls und die logische Trennung zwischen den verschiedenen Netzwerksegmenten, wie im Dokument beschrieben. Die VPN-Verbindungen zwischen den Standorten sorgen für sichere, standortübergreifende Kommunikation.

Referenzen

1. Lektion 3: Strukturanalyse - BSI, Zugriff am April 14, 2025, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_3_Strukturanalyse/Lektion_3_node.html
2. Lerneinheit 3.1: Das Beispielunternehmen RECPLAST - BSI, Zugriff am April 14, 2025,

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_3_Strukturanalyse/Lektion_3_01/Lektion_3_01_node.html

3. Lerneinheit 3.5: Netzplan erheben - BSI, Zugriff am April 14, 2025, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_3_Strukturanalyse/Lektion_3_05/Lektion_3_05_node.html
4. Lerneinheit 3.7: Räume erheben - BSI, Zugriff am April 14, 2025, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_3_Strukturanalyse/Lektion_3_07/Lektion_3_07_node.html
5. Lerneinheit 3.3: Geschäftsprozesse und Informationen erheben - BSI, Zugriff am April 14, 2025, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_3_Strukturanalyse/Lektion_3_03/Lektion_3_03_node.html
6. Lerneinheit 3.6: IT-Systeme erheben - BSI, Zugriff am April 14, 2025, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_3_Strukturanalyse/Lektion_3_06/Lektion_3_06_node.html
7. Lerneinheit 3.4: Anwendungen erheben - BSI, Zugriff am April 14, 2025, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_3_Strukturanalyse/Lektion_3_04/Lektion_3_04_node.html
8. Lerneinheit 3.2: Objekte gruppieren - BSI, Zugriff am April 14, 2025, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_3_Strukturanalyse/Lektion_3_02/Lektion_3_02_node.html