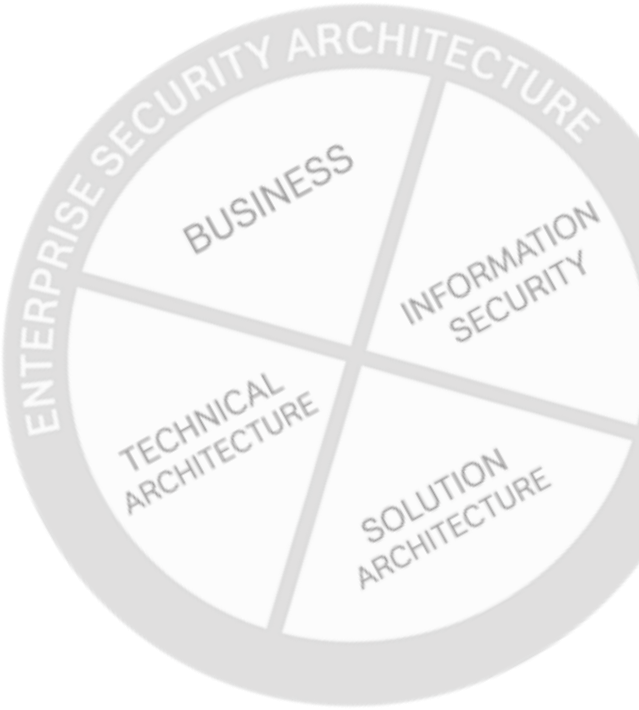
A1 Digital Deutschland GmbH St. Martin Straße 59, 81669 München

A1 Digital Enterprise Security Architecture

Servicebeschreibung & -bedingung



Version: 2.0
Datum: 16.12.2019

Inhaltsverzeichnis

1 Allgemeines

Diese Servicebeschreibung und -bedingung gilt ab 16.12.2019. Sie erläutert die Leistungen von A1 Digital Deutschland GmbH (im Folgenden: A1 Digital), welche Ihnen im Rahmen der Durchführung eines A1 Enterprise Security Architecture Consultings angeboten und bereitgestellt werden.

Sofern hier nicht Abweichendes geregelt wird, kommen die Allgemeinen Geschäftsbedingungen für IoT und Security Solutions von A1 Digital zur Anwendung: https://www.a1.digital/ueber-a1-digital/agb-a1-digital/.

Kunde von A1 Enterprise Security Architecture Consulting kann nur ein Unternehmer im Sinne des § 14 des Bürgerlichen Gesetzbuches (BGB) sein.

2 Servicebeschreibung

A1 Digital berät Unternehmen in den Bereichen Informationssicherheit und Risikomanagement. Je nach Anforderung können entweder nur bestimmte Teilbereiche des Unternehmens oder auch das gesamte Unternehmen analysiert und bewertet werden, Handlungsempfehlungen und Best Practices abgeleitet sowie bei der Behebung von erkannten Problemen unterstützt werden.

Die Beratung durch A1 Digital Enterprise Security Architecture Consulting kann keine absolute Sicherheit für Systeme, Daten oder Prozesse sicherstellen. A1 Digital übernimmt keinerlei Verantwortung dafür, dass vorhandene Schwachstellen erkannt werden. Abhängig von den gewählten Konfigurationen, ist es beispielsweise immer möglich, einzelne Systeme oder Schwachstellen zu übersehen.

Um jedem Unternehmen basierend auf den unternehmerischen Anforderungen die bestmögliche Beratung bieten zu können, wurde das **A1 Digital Enterprise Security Architecture-Modell** entwickelt.

Die Grundlage dieses Modells bildet eine Kombination aus branchenweiten Standards und Frameworks sowie die jahrelange Erfahrung der A1 Digital Security-Experten im IT Security Consulting-Bereich. Daraus wurde ein standardisiertes Beratungsmodell geformt, welches sowohl allgemein als auch Branchen-spezifisch auf die Gegebenheiten des Unternehmens eingeht.

Das ESA-Modell ist in vier Teilbereiche (Sichtweisen) untergliedert:

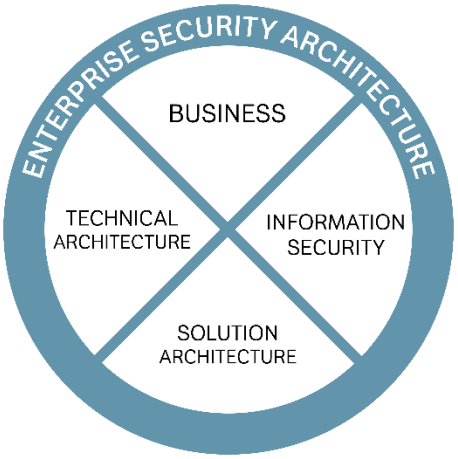
> Business
betrachtet die betriebliche Sichtweise der Risiken

sowie dessen Auswirkungen auf das operative Geschäft

> Information Security

betrachtet die Geschäftsprozesse, regulatorische Vorgaben, Dokumentationen, Sicherheitskonzepte sowie

das Risiko-und Qualitätsmanagement im Unternehmen



> Solution Architecture

betrachtet die strategische Ausrichtung sowie die

Architektur und das Design der IT-Infrastruktur inkl.

aller Systeme und Lösungen

> Technical Architecture

betrachtet die technische Bewertung, Design,

Implementierung und Überprüfung bestimmter IT-

Systeme

2.1 Consulting Services

Basierend auf dem ESA-Modell werden von A1 Digital verschiedenste Consulting-Leistungen in Form von Paketen angeboten. Obwohl diese Pakete grundsätzlich standardisiert sind, kann es je nach Unternehmensgröße und -anforderung sinnvoll sein, Pakete zu kombinieren oder Teilbereiche aus den einzelnen Paketen herauszulösen und zu einem neuen Gesamtpaket zusammenzufassen. Daraus ergibt sich eine für jeden Kunden individuell abgestimmte Consulting-Leistung mit eigener Aufwandsabschätzung.

Aktuell gibt es folgende Consulting Services:

- Risk Evaluation
- Security Checkup
- Datacenter Security Assessment
- Cloud Readiness Assessment
- DDOS Protection
- Data Breach Simulation
- Business Process Assessment
- Incident Response
- Get your certification!

2.1.1 Risk Evaluation

Mittels des Risk Evaluation-Pakets wird das gesamte Unternehmen einer detaillierten Analyse unterzogen. Ziel der Analyse ist es, einen ganzheitlichen Überblick über die im Unternehmen verwendeten Technologien, Architekturen und Prozesse zu bekommen, um dessen Bewertung nach einheitlichen Kriterien durchführen zu können und daraus weitere Handlungsschritte ableiten zu können.

Umfang

Basierend auf den vier Sichtweisen des ESA-Modells gliedert sich die Analyse in folgende Teilbereiche:

- Compliance, Policies & Frameworks
- Infrastructure & Datacenter Security
- Cloud Security
- Identity & Access Management
- Application Security
- Data Protection
- IT Operations

Ablauf

Die Analyse des Unternehmens wird von erfahrenen Security-Experten der A1 Digital in Form von Analyseworkshops durchgeführt. Jeder Security-Experte ist Spezialist in seinem Gebiet und führt die Analyse anhand einer innerhalb A1 Digital einheitlichen Fragemethodik durch. Durch dieses Vorgehen ist sichergestellt, dass sowohl ein standardisierter und vergleichbarer Report erstellt wird als auch die persönliche Erfahrung des Security-Experten in die Bewertung des Unternehmens mit einfließt.

Neben den Security-Experten, welche die Analyseworkshops durchführen, begleitet als interner Projektmanager und Single-Point-of-Contact ein Lead Consultant das Projekt.

Das Risk Evaluation-Paket gliedert sich in die folgenden Arbeitspakete:

- Im **Kickoff** werden die Rahmenbedingungen für das Projekt abgestimmt, die Zuständigkeiten und Verpflichtungen geklärt, Folgetermine festgelegt sowie im Vorfeld benötigte Dokumente spezifiziert.

- Danach werden die zuvor angeforderten **Dokumente** gesichtet sowie der Analyseworkshop vorbereitet.
- Im Zuge der **Analyseworkshops** werden Experten aus allen Teilbereichen Interviews mit den verantwortlichen Personen führen, um Detailinformationen zum jeweiligen Gebiet zu erhalten. Auch werden erste Bewertungen und Einschätzungen abgegeben.
- Danach werden die Unterlagen und erhaltenen Informationen aufbereitet, die **Risikobewertung** durchgeführt, weitere Maßnahmen zu den einzelnen Teilbereichen definiert und ein detaillierter Bericht erstellt.
- Bei der **Präsentation der Ergebnisse** werden alle Erkenntnisse und Maßnahmen der Analyse und der Risikobewertung sowie ein Fahrplan für die Zukunft präsentiert.

2.1.2 Security Checkup

Mittels des A1 Digital Security Checkups werden Unternehmen einer grundlegenden Analyse hinsichtlich ihres Entwicklungsstands in den Themen Informationssicherheit und Risikomanagements unterzogen. Obwohl des geringeren Umfangs im Vergleich zur Risk Evaluation, gibt der Security Checkup einen groben, aber aufschlussreichen Überblick über den Reifegrad eines Unternehmens in den verschiedensten Bereichen der IT-Security. Diese Unternehmensbewertung, durchgeführt von Experten der A1 Digital, hilft Unternehmen, Problemfelder zu identifizieren und Handlungsschritte zu planen.

Umfang

Gleich dem Risk Evaluation-Pakets basiert die Analyse auf den vier Sichtweisen des ESA-Modells und gliedert sich in folgende Teilbereiche:

- Compliance, Policies & Frameworks
- Infrastructure & Datacenter Security
- Cloud Security
- Identity & Access Management
- Application Security
- Data Protection
- IT Operations

Je nach Unternehmensanforderung können mittels des Security Checkups zielgerichtete, interne Audits zur Vorbereitung auf bevorstehende Zertifizierungen durchgeführt werden. Diese Audits werden auf Basis der unternehmensinternen Sicherheitsrichtlinien/Policies sowie internationaler Standards (z.B. ISO 27001, ISO 27018, GDPR, SOC1/SOC2, PCI-DSS, CSA STAR, etc.) durchgeführt und werden im Rahmen der Erstgespräche mit dem Kunden definiert.

Ablauf

Die Analyse des Unternehmens wird von erfahrenen Security-Experten der A1 Digital in Form eines Analyseworkshops durchgeführt. Jeder Security-Experte führt die Analyse anhand einer innerhalb A1 Digital einheitlichen Fragemethodik durch. Durch dieses Vorgehen ist sichergestellt, dass sowohl ein standardisierter als auch vergleichbarer Report erstellt wird.

Der Security Checkup gliedert sich in die folgenden Arbeitspakete:

- Im **Kickoff** werden die Rahmenbedingungen für den Analyseworkshop abgestimmt, die auf Kundenseite benötigten Personen und Stakeholder bekannt gegeben und der Zeitpunkt des Analyseworkshops definiert.
- Im Zuge der **Analyseworkshops** werden Interviews mit den verantwortlichen Personen im Unternehmen geführt und die Bewertungsmatrix ausgefüllt.
- Danach werden die gesammelten Informationen in der Bewertungsmatrix aufbereitet, die **Risikobewertung** durchgeführt und der Ergebnisbericht erstellt.
- Bei der **Präsentation der Ergebnisse** werden alle Erkenntnisse der Analyse und der Risikobewertung präsentiert.

2.1.3 Datacenter Security Assessment

Mittels des Datacenter Security Assessment-Pakets wird die Rechenzentrums-Landschaft eines Unternehmens unter die Lupe genommen. Nach detaillierter Analyse der aktuellen Bedrohungslage in der Unternehmensbranche, der Sicherheitsanforderungen Richtung interner und externer Kunden, der verwendeten Technologien und Lösungen, der internen Prozesse und gelebten Abläufe sowie der Stakeholder des Unternehmens in Bezug auf die gesamte Rechenzentrums-Landschaft wird die Infrastruktur auf Basis von einheitlichen Kriterien bewertet. Aus dieser Bewertung werden Handlungsempfehlungen für die kurz- und langfristige Verbesserung der Rechenzentrums-Landschaft erarbeitet und präsentiert.

Umfang

Basierend auf den vier Sichtweisen des ESA-Modells gliedert sich die Analyse in folgende Teilbereiche:

- Allgemeine Architektur LAN

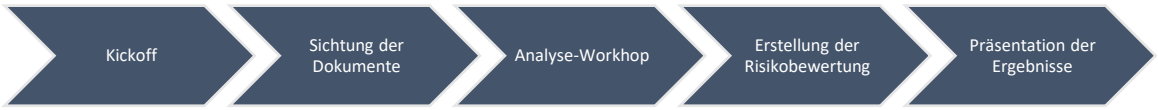
- Allgemeine Architektur WAN
- Verwendete Technologien und Lösungen
- Physische Sicherheit
- Netzwerksegmentierung und Berechtigungskonzept
- Zutrittspunkte von extern für administrativen und produktiven Netzwerkverkehr
- Anbindung und Interkonnektivität der Rechenzentren
- Providerkonzept, externe Dienstleister und Zulieferer

Ablauf

Die Analyse des Rechenzentrums-Landschaft wird von erfahrenen Security-Experten der A1 Digital in Form eines Analyseworkshops unter Verwendung einer einheitlichen Fragemethodik durchgeführt. Durch dieses Vorgehen ist sichergestellt, dass sowohl ein standardisierter und vergleichbarer Report erstellt wird als auch die persönliche Erfahrung des Security-Experten in die Bewertung des Unternehmens mit einfließt.

Neben den Security-Experten, welche den Analyseworkshop durchführen, begleitet als interner Projektmanager und Single-Point-of-Contact ein Lead Consultant das Projekt.

Das Datacenter Security Assessment-Paket gliedert sich in die folgenden Arbeitspakete:



- Im **Kickoff** werden die Rahmenbedingungen für das Projekt abgestimmt, die Zuständigkeiten und Verpflichtungen geklärt, Folgetermine festgelegt sowie im Vorfeld benötigte Dokumente spezifiziert.
- Danach werden die zuvor angeforderten **Dokumente** gesichtet sowie der Analyseworkshop vorbereitet.
- Im Zuge des **Analyseworkshops** werden Interviews mit den verantwortlichen Personen führen, um Detailinformationen zum jeweiligen Gebiet zu erhalten. Auch werden erste Bewertungen und Einschätzungen abgegeben.
- Danach werden die Unterlagen und erhaltenen Informationen aufbereitet, die **Risikobewertung** durchgeführt, weitere Maßnahmen zu den einzelnen Teilbereichen definiert und ein detaillierter Bericht erstellt.

- Bei der **Präsentation der Ergebnisse** werden alle Erkenntnisse und Maßnahmen der Analyse und der Risikobewertung sowie ein Fahrplan für die Zukunft präsentiert.

2.1.4 Cloud Readiness Assessment

Mittels des Cloud Readiness Assessment-Pakets wird der aktuelle Reifegrad eines Unternehmens in Hinblick auf Bestrebungen, die digitale Transformation weiter voranzutreiben und Cloud-Technologien und -Lösungen zu verwenden, gemessen. Im Zuge der Unternehmensanalyse werden spezielle Gesichtspunkte wie Strategie, interne Prozesse, Organisationsstruktur, Unternehmenskultur sowie die aktuell verwendeten Produkte- und Lösungen im Unternehmen betrachtet. Mit dem daraus gewonnenen Einblick in das Unternehmen wird dieses anhand von einheitlichen Kriterien bewertet, der Reifegrad bestimmt und Handlungsempfehlungen ausgesprochen.

Umfang

Basierend auf den vier Sichtweisen des ESA-Modells gliedert sich die Analyse in folgende Teilbereiche:

- Historie des Unternehmens
- Betriebliche Anforderungen und Probleme
- Strategie und geplantes Wachstum
- Unternehmenskultur
- Prozesslandschaft
- Eigenschaften sowie Vor- und Nachteile von Mitbewerbern

Ablauf

Die Risikoanalyse und Reifegradbewertung wird von erfahrenen Security-Experten der A1 Digital in Form eines Analyseworkshops unter Verwendung einer einheitlichen Fragemethodik durchgeführt. Durch dieses Vorgehen ist sichergestellt, dass sowohl ein standardisierter und vergleichbarer Report erstellt wird als auch die persönliche Erfahrung des Security-Experten in die Bewertung des Unternehmens mit einfließt.

Neben den Security-Experten, welche den Analyseworkshop durchführen, begleitet als interner Projektmanager und Single-Point-of-Contact ein Lead Consultant das Projekt.

Das Cloud Readiness Assessment-Paket gliedert sich in die folgenden Arbeitspakete:

- Im **Kickoff** werden die Rahmenbedingungen für das Projekt abgestimmt, die Zuständigkeiten und Verpflichtungen geklärt, Folgetermine festgelegt sowie im Vorfeld benötigte Dokumente spezifiziert.
- Danach werden die zuvor angeforderten **Dokumente** gesichtet sowie der Analyseworkshop vorbereitet.
- Im Zuge des **Analyseworkshops** werden Interviews mit den verantwortlichen Personen geführt, um Detailinformationen zum jeweiligen Gebiet zu erhalten. Auch werden erste Bewertungen und Einschätzungen abgegeben.
- Danach werden die Unterlagen und erhaltenen Informationen aufbereitet, die **Risikoanalyse und Reifegradbewertung** durchgeführt, weitere Maßnahmen zu den einzelnen Teilbereichen definiert und ein detaillierter Bericht erstellt.
- Bei der **Präsentation der Ergebnisse** werden alle Erkenntnisse und Maßnahmen der Analyse, der Risiko- und Reifegradbewertung sowie ein Fahrplan für die Zukunft präsentiert.

2.1.5 DDOS Protection

Mittels des DDOS Protection-Pakets wird das Unternehmen auf die Verwendung von Technologien zur Vermeidung oder Verringerung von Denial-of-Service (DOS) und Distributed-Denial-of-Service (DDOS) Angriffen, sowohl im normalen Projekt-Umfang als auch in Zuge von Ausschreibungen, vorbereitet. Hierfür werden sowohl die Prozesse im Unternehmen als auch die derzeit vorhandene Infrastruktur im Rechenzentrum analysiert um auf dieser Basis mögliche Deployment-Szenarien für DDOS Protection-Lösungen zu erarbeiten, zu bewerten und Handlungsempfehlungen abzugeben. Nach der Implementierung einer DDOS Protection-Lösung wird das Unternehmen im Zuge der Abnahmetests sowie der Einführung bzw. Adaptierung von Unternehmensprozessen unterstützt und beraten.

Umfang

Basierend auf den vier Sichtweisen des ESA-Modells gliedert sich die Beratungsdienstleistung in folgende Teilbereiche:

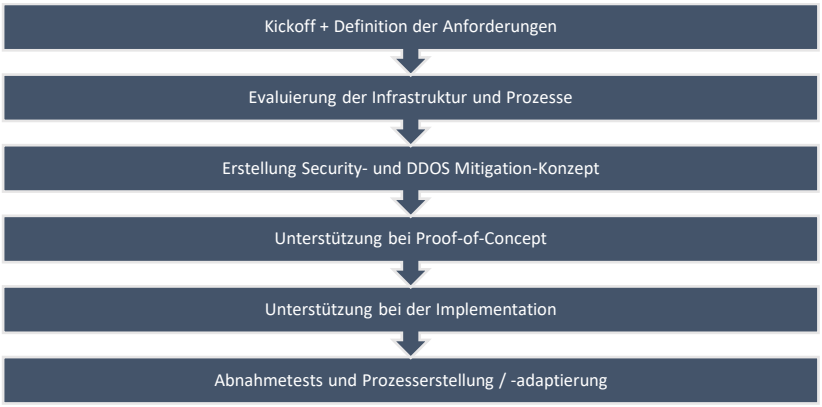
- Evaluierung der aktuellen Rechenzentrums-Infrastruktur
- Evaluierung der aktuellen Prozesse (Incident Response Management)
- Definition der Anforderungen an einen DDOS Mitigation Provider
- Erstellung eines Security- und DDOS Mitigation-Konzepts

- Bewertung möglicher Mitigation Provider
- Durchführen von Proof-of-Concepts
- Unterstützung bei der Angebots- und Implementierungsphase
- Unterstützung bei der Prozesserstellung / -adaptierung
- Durchführung von Abnahmetests

Ablauf

Die Beratungsdienstleistung wird von erfahrenen Security-Experten der A1 Digital durchgeführt. Neben den Security-Experten begleitet als interner Projektmanager und Single-Point-of-Contact ein Lead Consultant das Projekt.

Das DDOS Protection-Paket gliedert sich in die folgenden Arbeitspakete:



- Im **Kickoff** werden die Rahmenbedingungen für das Projekt abgestimmt, die Unternehmensanforderungen im Bereich DDOS eingeholt, die Zuständigkeiten und Verpflichtungen geklärt, Folgetermine festgelegt sowie im Vorfeld benötigte Dokumente spezifiziert.

- Im Zuge der **Evaluierung der Infrastruktur und Prozesse** werden die bestehende Rechenzentrums- und Cloud-Infrastruktur sowie die zugehörigen Unternehmensprozesse und Notfallpläne genauer betrachtet.

- Auf Basis dieser Evaluierung wird ein **Security- und DDOS Mitigation-Konzept** erstellt. Das Konzept betrachtet die Kundenarchitektur in Hinblick auf verschiedene Deployment-Szenarien im DDOS-Bereich. Weitere Inhalte sind ein Implementierungskonzept, eine Schnittstellendefinition der beteiligten Parteien und ein Testplan, welcher im Zuge der Abnahmetests verwendet wird.

- In **Proof-of-Concept** Phase wird gemeinsam mit dem Unternehmen verschiedene Funktionen der teilnehmenden Mitigation Provider, welche

im Vorfeld mittels dem DDOS Mitigation-Konzepts definiert wurden, getestet. Aus diesen Tests werden Rückschlüsse über die Hersteller-Technologie gezogen und in Form einer Check-Liste festgehalten.

- Nach der Beauftragung von Diensten eines oder mehrerer DDOS Mitigation Provider wird das Unternehmen bei der **Implementierung** der Dienste (Auswahl der Deployment-Szenarien, Einbindung in die Unternehmensinfrastruktur, etc.) unterstützt.

- Im Zuge der **Abnahmetests** werden die Dienste nach erfolgreicher Implementation auf Vollständigkeit und Funktionalität überprüft und bewertet. Mittels des zuvor erstellten Testplans werden die Ergebnisse dokumentiert. Neben der technischen Implementierung der Dienste werden auch auf Prozessebene die notwendigen Änderungen oder Adaptionen für den Betrieb der DDOS Mitigation-Lösung durchgeführt.

2.1.6 Data Breach Simulation

Mittels des Data Breach Simulation-Pakets werden die unternehmensinternen Prozesse und Verhaltensregeln hinsichtlich der Datenschutzgrundverordnung (DSGVO) untersucht. Hierfür wird eine Datenschutzverletzung, also eine unerlaubte Offenlegung von (fiktiven) Personal-Daten, simuliert und anschließend dessen Auswirkungen im Unternehmen analysiert, bewertet und präsentiert.

Umfang

Basierend auf den vier Sichtweisen des ESA-Modells gliedert sich die Beratungsdienstleistung in folgende Teilbereiche:

- Analyse der betroffenen Abteilungen und Mitarbeiter hinsichtlich der Einhaltung der Prozesse und Policies
- Analyse der betroffenen Abteilungen und Mitarbeiter hinsichtlich der technischen Kompetenz, einen Sicherheitsvorfall zu klären und die Meldung der Datenschutzverletzung zu initiieren
- Analyse der Prozesse und Policies hinsichtlich Qualität, Vollständigkeit, Konformität und Konsistenz
- Analyse der Prozesse und Policies hinsichtlich der Anforderungen der DSGVO
- Analyse der Kommunikationswege und Kontaktinformationen für externe Stellen

Ablauf

Die Beratungsdienstleistung wird von erfahrenen Security-Experten der A1 Digital durchgeführt. Neben den Security-Experten begleitet als interner Projektmanager und Single-Point-of-Contact ein Lead Consultant das Projekt.

Das Data Breach Simulation-Paket gliedert sich in die folgenden Arbeitspakete:

- Im **Kickoff** werden die Rahmenbedingungen für das Projekt abgestimmt, die Übungsteilnehmer festgelegt, die Zuständigkeiten und Verpflichtungen geklärt, Folgetermine festgelegt sowie im Vorfeld benötigte Dokumente spezifiziert.
- Danach werden die zuvor angeforderten **Dokumente** analysiert. Diese beinhalten die Prozessdokumentation, notwendige Incident Response-Maßnahmen und -Abläufe sowie Kommunikationsschnittstellen zu internen

und externen Stellen. Aus diesen Erkenntnissen wird die Art und er Umfang der Simulation ausgewählt und gemeinsam mit dem Projektansprechpartner vorbereitet.

- **Im Zuge der Simulation** wird der Sicherheitsvorfall den betroffenen Akteuren mitgeteilt, das Verhalten des Unternehmens im Allgemeinen sowie dieser Personen im Speziellen analysiert.
- Nach der Simulation wird der Ablauf und das Vorgehen der Akteure unter den Gesichtspunkten der DSGVO bewertet. Das Ergebnis wird im Anschluss dem Projektteam und den Entscheidungsträgern präsentiert.

2.1.7 Business Process Assessment

Mittels des Business Process Assessment-Paktes werden kritische Geschäftsprozesse im Unternehmen durchleuchtet, analysiert und optimiert. Im Rahmen von Workshops werden mit den unterschiedlichen Prozesseigentümern die Unternehmensanforderungen analysiert und über Probleme und Fehlplanungen in Prozessen diskutiert. Daraus wird ein Änderungsplan erstellt, welcher unterschiedliche Teilbereiche von Prozessen adressiert und im Rahmen eines Prozessoptimierungsprozess ausgeführt werden kann.

Umfang

Basierend auf den vier Sichtweisen des ESA-Modells gliedert sich die Beratungsdienstleistung in folgende Teilbereiche:

- Allgemeiner Workshop mit den Stakeholdern zur Analyse der Unternehmensanforderungen
- Workshops mit den Prozesseigentümern im Bereich
    - Asset Management
    - Patch Management
    - Demand Management
    - User- und Identity Management
    - Incident Management
    - Change Management
    - Problem Management
- Erstellung eines Prozessänderungs- und -Optimierungsplans mit empfohlenen Arbeitsschritten zur Verbesserung verschiedener Prozessbereiche und Arbeitsabläufe

Ablauf

Die Beratungsdienstleistung wird von erfahrenen Security-Experten der A1 Digital durchgeführt. Neben den Security-Experten begleitet als interner Projektmanager und Single-Point-of-Contact ein Lead Consultant das Projekt.

Das Business Process Assessment-Paket gliedert sich in die folgenden Arbeitspakete:

- Im **Kickoff** werden die Rahmenbedingungen für das Projekt abgestimmt, die Zuständigkeiten und Verpflichtungen geklärt, Folgetermine festgelegt sowie im Vorfeld benötigte Dokumente spezifiziert.
- Danach werden die zuvor angeforderten **Dokumente** gesichtet sowie der Analyseworkshop vorbereitet.
- Im Zuge des **Analyseworkshops** werden Interviews mit den verantwortlichen Prozesseigentümern geführt, um Detailinformationen zu den jeweiligen Prozessen und Abläufen zu erhalten. Auch werden erste Bewertungen und Einschätzungen abgegeben.
- Nach der Interview-Phase wird ein **Prozessoptimierungsplan** erarbeitet, welcher die Erkenntnisse aus den Analyseworkshops sowie Vorschläge zur Adaptierung oder Erneuerung verschiedener Unternehmensprozesse beinhaltet. Auf Basis dieses Plans können einzelne Prozesse im Rahmen eines Prozessoptimierungsprozesses angepasst und optimiert werden.
- Abschließend werden die Ergebnisse und Erkenntnisse aus den Workshops sowie der Prozessoptimierungsplan sowohl dem Management als auch den einzelnen Stakeholdern präsentiert und eine Empfehlung zur weiteren Vorgehensweise gegeben.

2.1.8 Incident Response

Mittels des Incident Response-Pakets werden Unternehmen im Bereich der Analyse und der richtigen Verhaltensweise im Zuge eines Sicherheitsvorfalls beraten. Dies umfasst die Adaptierung von Unternehmensprozessen sowie die praktische Durchführung eines Notfall-Planspiels.

Umfang

Basierend auf den vier Sichtweisen des ESA-Modells gliedert sich die Beratungsdienstleistung in folgende Teilbereiche:

- Durchführung eines Analyse-Workshops
- Erhebung und Bewertung der Unternehmensanforderungen
- Bewertung der Risiken und Definition der kritischen Geschäftsabläufe und Prozesse
- Entwicklung von Notfallplänen
- Erstellung und Adaptierung von Incident Response-Prozessen
- Mitarbeiter-Schulungen inkl. Notfall-Planspiele zur Vorbereitung auf Sicherheitsvorfälle

Ablauf

Die Beratungsdienstleistung wird von erfahrenen Security-Experten der A1 Digital durchgeführt. Neben den Security-Experten begleitet als interner Projektmanager und Single-Point-of-Contact ein Lead Consultant das Projekt.

Das Incident Response-Paket gliedert sich in die folgenden Arbeitspakete:

- Im **Kickoff** werden die Rahmenbedingungen für das Projekt abgestimmt, die Zuständigkeiten und Verpflichtungen geklärt, Folgetermine festgelegt sowie im Vorfeld benötigte Dokumente spezifiziert.

- Danach werden die zuvor angeforderten **Dokumente** gesichtet sowie der Analyseworkshop vorbereitet.

- Im Zuge des **Analyseworkshops** werden Interviews mit dem Operations Team, dem internen CERT (sofern vorhanden) sowie den zuständigen Prozesseigentümern geführt, um Detailinformationen zum IT Service Management im Allgemeinen sowie den praktischen Abläufen und Vorgangsweisen im Unternehmen im Speziellen zu erhalten. Auch werden erste Bewertungen und Einschätzungen abgegeben.

- Nach dem Analyseworkshop werden die vorhandenen Incident Response-Prozesse und Geschäftsabläufe bewertet sowie Notfallpläne zu kritischen Prozessen erstellt bzw. sofern vorhanden bewertet und adaptiert.

- Von den Ergebnissen des Analyseworkshops werden **Mitarbeiterschulungen** geplant, in welchen neben der Vermittlung von theoretischem Wissen auch Sicherheitsvorfälle in Form eines Notfall-Planspiels simuliert und durchgegangen werden.

2.1.9 Get your certification!

Unternehmen stehen oft vor der Herausforderung, bestimmte Zertifizierungen zu erlangen, um sowohl externen als auch internen Anforderungen gerecht zu werden. Mittels des „Get your certification!"-Pakets unterstützt A1 Digital ihre Kunden in der Planung und Vorbereitung auf Zertifizierungen wie ISO oder PCI DSS. Erfahrene Auditoren und Experten in den unterschiedlichsten Bereichen der IT-Security erstellen mit dem Kunden Maßnahmenpläne und Arbeitspakete, um bestmöglich auf die Zertifizierungsprüfung vorbereitet zu sein.

Umfang

Basierend auf den vier Sichtweisen des ESA-Modells gliedert sich die Beratungsdienstleistung in folgende Teilbereiche:

- Durchführung von Analyse-Workshops
- Erhebung und Bewertung der Anforderungen der jeweiligen Zertifizierungsstelle
- Erstellung eines Maßnahmenplans unter Betrachtung der Kundenumgebung und -infrastruktur
- Unterstützung in der Durchführung der Maßnahmen:
    - Technische und organisatorische Maßnahmen
    - Durchführung von Mitarbeiterschulungen im Zuge von Prozessänderungen/-adaptionen
- Unterstützung während des Audits / der Zertifizierungsprüfung (sofern möglich und erlaubt)
- Nachbereitung der Audits / der Zertifizierungsprüfung, Definition weiterer Schritte

Mögliche Zertifizierungen (Auszug):

- ISO Domäne (27001, 27018, 9001, etc.)
- PCI DSS
- TISAX

Ablauf

Das „Get your certification!"-Paket gliedert sich in die folgenden Arbeitspakete:

- Im **Kickoff** werden die Rahmenbedingungen für das Projekt abgestimmt, die Zuständigkeiten und Verpflichtungen geklärt sowie Folgetermine festgelegt.

- Im Zuge der **Analyseworkshops** werden Interviews mit den zuständigen Stellen/Abteilungen und Prozesseigentümern geführt, um Detailinformationen zur Infrastruktur und Kundenumgebung im Allgemeinen sowie den praktischen Abläufen und Vorgangsweisen im Unternehmen im Speziellen zu erhalten. Interne Dokumente und Prozesse werden bewertet und den Anforderungen der jeweiligen Zertifizierungsstelle gegenübergestellt.

- Nach dem Analyseworkshops werden **Maßnahmenpläne** erarbeitet und bei der Durchführung dieser Maßnahmen unterstützt. Hier lassen die A1 Digital Experten ihre langjährige Erfahrung als Auditoren diverser Zertifizierungen mit einfließen.

- Sofern es möglich ist, wird sowohl während als auch nach dem **Audit** / der Zertifizierungsprüfung dem Kunden zur Seite gestanden, Schlüsse aus den Ergebnissen des Audits gezogen und weitere Maßnahmen definiert.

3 Servicebedingung

3.1 Nutzungsvoraussetzungen

- Zumindest drei Werktage vor Beginn des Projekts stellt der Kunde A1 Digital den konkreten Scope zur Verfügung.
- Hardware, Zugangsdaten und sonstige Informationen, die für die Erbringung der Leistungen notwendig sind, stehen A1 Digital spätestens am Tag vor Beginn der Dienstleistung zur Verfügung.
- Die Ergebnisse werden in Form eines Berichts als PDF-Format oder PowerPoint an den Kunden übermittelt

3.2 Verantwortlichkeit und Haftung

A1 Digital leistet gegenüber dem Kunden Schadenersatz oder Ersatz vergeblicher Aufwendungen, gleich aus welchem Rechtsgrund (z. B. aus rechtsgeschäftlichen und rechtsgeschäftsähnlichen Schuldverhältnissen, Pflichtverletzung und unerlaubter Handlung), nur in folgendem Umfang:

a) Die Haftung bei grober Fahrlässigkeit, Vorsatz, Arglist und aus Garantie wird hierdurch nicht vertraglich eingeschränkt.

Auch für Schäden aus der schuldhaften Verletzung des Lebens, des Körpers oder der Gesundheit und bei Ansprüchen nach dem Produkthaftungsgesetz gelten die gesetzlichen Regelungen uneingeschränkt.

b) Bei Verletzung einer vertragswesentlichen Pflicht, deren Erfüllung also die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Vertragspartner regelmäßig vertrauen darf (sog. Kardinalpflicht), haftet A1 Digital nur in Höhe des bei Vertragsabschluss typischerweise vorhersehbaren Schadens.

Die Haftung für einfache Fahrlässigkeit ist gegenüber dem Kunden (und auch Körperschaften des öffentlichen Rechts) bei Verletzung einer nicht vertragswesentlichen Pflicht ausgeschlossen.

c) Soweit die Haftung von A1 Digital nach dem Vorstehenden ausgeschlossen oder beschränkt ist, gilt dies auch für die persönliche Haftung der Mitarbeiter, Vertreter und Erfüllungsgehilfen von A1 Digital.

d) Für Schäden, die aus einer vertragswidrigen Verwendung der Leistungen von A1 Digital resultieren, haftet A1 Digital nicht.

Der Kunde hält A1 Digital hinsichtlich sämtlicher von Dritter Seite erhobener Ansprüche, die auf eine Verletzung von Bestimmungen der vorliegenden Vereinbarung durch den Kunden zurückzuführen sind, in vollem Umfang schad- und klaglos.

4 Datenschutz und Datensicherheit

Das Service wird innerhalb Europas betrieben.

Weitere Informationen können unserer Website entnommen werden: https://www.a1.digital/ueber-a1-digital/datenschutz-a1-digital/.

Es gelten die Allgemeinen Geschäftsbedingungen der A1 Digital für Auftragsverarbeitung (AGB AVV). Diese finden Sie auf https://www.a1.digital/at/ueber-a1-digital/agbs/.

5 Datenschutzanhang zur Leistungsbeschreibung

In Rahmen den von uns bereitgestellten Leistungen werden wir Ihre personenbezogenen Daten im Sinne der Art. 28 DSGVO als Auftragsverarbeiter (AV) verarbeiten.

1. Gegenstand des Auftrags

1.1 Der Auftrag des für die Verarbeitung Verantwortlichen an den Auftragsverarbeiter umfasst folgende Produkte oder Leistungen: **„A1 Digital Enterprise Security Architecture"**

1.2 Folgende Datenarten können regelmäßig Gegenstand der Verarbeitung sein:

- ☒ Personen-Stammdaten
- ☐ Personen-Kennungen
- ☐ Besondere personenbezogene Daten
- ☒ Marketing/Sales-Daten mit Personenbezug
- ☒ Personen-Rollen/-Assoziationen
- ☐ Kundeninventar
- ☒ Kundeninteraktionen
- ☐ Verkehrsdaten
- ☐ Bewegungsdaten | Geolocation Data
- ☒ Inhaltsdaten
- ☐ Finanzdaten
- ☐ Login, Passwörter

1.3 Kreis der von der Datenverarbeitung Betroffenen:

- ☐ Kunde des Auftraggebers - natürliche Person
- ☐ Kunde des Auftraggebers - juristische Person
- ☒ User des Enterprise Kunden
- ☒ Mitarbeiter des Auftraggebers
- ☒ Vertragspartner des Auftraggebers
- ☐ Kinder oder Schutzbedürftige Personen

2. Liste der beauftragten Subunternehmer

Name	Firmenadresse	Art der Verarbeitung	Ort der Verarbeitung
Akenes SA (Exoscale)	Boulevard de Grancy 19A	Hosting Services	Schweiz, Deutschland, Österreich, Bulgarien

	1006 – Lausanne Switzerland		
A1 Telekom Austria AG	Lassallestraße 9 A-1020 Wien	Hosting Services	Österreich

3. Technisch-organisatorische Maßnahmen

Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen zur Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen. Sofern in der Leistungsvereinbarung nicht genauer geregelt, obliegt es dem Auftragsverarbeiter, das der jeweiligen Verarbeitung angemessene Schutzniveau insbesondere durch eine Kombination der nachstehend genannten technisch-organisatorischen Maßnahmen sicherzustellen. Es ist dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

A. VERTRAULICHKEIT (ART. 32 ABS. 1 LIT. B DS-GVO)

- **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B. durch Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen.

- **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung durch z.B.(sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.

- **Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch, z.B. Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

- **Trennungskontrolle:** Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. durch Standard-Berechtigungsprofile auf „need to know-Basis".

- **Pseudonymisierung**: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt, und gesondert aufbewahrt.

- **Klassifikationsschema für Daten:** Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

B. DATENINTEGRITÄT[1] (ART. 32 ABS. 1 LIT. B DS-GVO)

[1] Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten.

- **Weitergabekontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch z.B. Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur.

- **Eingabekontrolle**: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch z.B. Dokumentenmanagement.

C. VERFÜGBARKEIT UND BELASTBARKEIT (ART. 32 ABS. 1 LIT. B DS-GVO)

- **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch z.B. Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne.

- **Wiederherstellbarkeit**

D. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (ART. 32 ABS. 1 LIT. D DS-GVO; ART. 25 ABS. 1 DS-GVO)

- **Datenschutz-Management**, einschließlich regelmäßiger Mitarbeiter-Schulungen
- **Incident-Response-Management**
- **Datenschutzfreundliche Voreinstellungen**:
- **Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers