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

A1 Digital Security Assessment

Servicebeschreibung & -bedingungen

Version: 3.0

Datum: 9.12.2019

Inhaltsverzeichnis

1 Allgemeines

Diese Servicebeschreibung und -bedingung gilt ab 9.12.2019. Sie erläutert die Leistungen von A1 Digital Deutschland GmbH (im Folgenden: A1 Digital), welche Ihnen im Rahmen der Durchführung eines A1 Digital Security Assessments angeboten und bereitgestellt werden.

Diese Servicebeschreibung und -bedingungen beinhalten unser gesamtes Portfolio; die konkret vereinbarten Leistungsteile sind je nach Kunde unterschiedlich und ergeben sich aus dem Angebot des Kunden. Die Behebung von identifizierten Fehlern/Schwachstellen ist nicht Teil unserer Leistung.

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 Digital Security Assessments kann nur ein Unternehmer im Sinne des § 14 des Bürgerlichen Gesetzbuches (BGB) sein.

2 Servicebeschreibung

Das Ziel von A1 Digital Security Assessments besteht darin, Schwachstellen in den Informationssicherheitskontrollen eines Unternehmens zu identifizieren. Bei A1 Digital Security Assessments handelt es sich um die Identifikation und Bewertung von Schwachstellen mit technischem Fokus und organisatorischen Aspekten.

A1 Digital Security Assessments können 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.

A1 Digital wird im Angebot, spezifisch für den Kunden, einen Mindesttestumfang empfehlen. Dieser kann – auf Wunsch des Kunden – zugunsten oder zulasten der Qualität des A1 Digital Security Assessments erhöht oder reduziert werden.

2.1 Ablauf

2.1.1 Vorbereitung

In der Vorbereitungsphase wird der Kunde von A1 Digital Assessoren hinsichtlich des Tätigkeitsumfelds analysiert und es werden gemeinsam mit dem Kunden die Zielsetzung und Vorgehensweise diskutiert sowie ein Ansprechpartner während des Projekts festgelegt.

2.1.2 Kick-off Meeting

Im Kick-off-Meeting besprechen die A1 Digital Assessoren gemeinsam mit dem Kunden den Ablauf des A1 Security Assessments. Unter anderem wird hier der zu prüfende Testgegenstand festgelegt und geklärt, wie mit der Erkennung von Gefahrenpotentialen umgegangen werden soll. Außerdem wird Allgemeines zur Durchführung des A1 Digital Security Assessments besprochen, wie Festlegung des Zeitraums und der Sprache des Abschlussberichts.

Der Kunde stellt A1 eine Liste an Zielsystemen schriftlich zur Verfügung und erteilt damit den Auftrag zur Durchführung intrusiver Angriffe („Permission to Attack"). Intrusive Angriffe sind Scans, die technische oder organisatorische Schutzmaßnahmen umgehen können. Diese Scans bedürfen einer expliziten Erlaubnis durch den Besitzer eines Systems, da sie ansonsten illegal sein könnten. Diese „Permission to Attack" ist durch den Kunden mittels schriftlicher Übermittlung der Liste der Zielsysteme vor Durchführung des Tests zu erteilen.

2.1.3 Durchführung

Die Durchführung des A1 Digital Security Assessments wird durch den gewählten Testgegenstand bzw. durch die gewählten Leistungen bestimmt. Die vertraglich vereinbarten Leistungen geben vor, welche Voraussetzungen für die Durchführung des A1 Digital Security Assessments notwendig sind. Nicht beauftragte Leistungen sind nicht Leistungsgegenstand und werden nicht getestet.

2.1.4 Abschlussbericht und Termine

Die Ergebnisse des gesamten A1 Digital Security Assessments werden in einem Abschlussbericht und einer optionalen finalen Präsentation dargestellt. Sollte ein vor Ort Termin notwendig oder gewünscht sein behält sich die A1 Digital die Verrechnung von Reisekosten und Spesen vor. Sämtliche Termine werden mit dem Kunden abgestimmt.

2.2 Technische Security Assessments

Technische Security Assessments liefern eine momentane Aufschlüsselung der Sicherheitslandschaft der geprüften Infrastruktur, der Systeme und Applikationen.

Die im Zuge der Prüfung identifizierten Schwachstellen werden mit entsprechenden Risikobewertungen, empfohlenen Gegenmaßnahmen und detaillierten technischen Beschreibungen in einem Bericht und einer optionalen finalen Präsentation dargestellt. Die Behebung von entdeckten Fehlern/Schwachstellen ist nicht Teil der Leistung.

Anschließend dazu sollten die identifizierten Schwachstellen durch den Kunden behoben und die Maßnahmenempfehlungen der A1 Digital Assessoren umgesetzt werden, wobei eine Regressionsprüfung empfohlen wird. Diese soll sicherstellen, dass alle relevanten Schwachstellen korrekt behoben wurden und dabei keine neuen entstanden sind.

Technische Security Assessments sollten regelmäßig durchgeführt werden, da es sich bei den jeweiligen Prüfungen nur um Momentaufnahmen handelt. Um einen möglichst ganzheitlichen und realistischen Ansatz verfolgen zu können, empfiehlt sich ein Red Teaming-Ansatz, welcher in **Abschnitt 2.2.5** im Detail beschrieben wird.

Es handelt sich dabei um eine mehrschichtige Angriffssimulation, die entwickelt wurde, um zu messen, wie gut die Mitarbeiter und Netzwerke, Anwendungen und physischen Sicherheitskontrollen eines Unternehmens einem Angriff eines echten Gegners standhalten können.

Um ein breites Spektrum an Schwachstellenkategorien abdecken zu können, wird der Penetrationtest in Anlehnung an den Open Web Application Security Project (OWASP) Testing Guide Version 4 durchgeführt.[1] Ziel ist die Identifikation möglichst vieler sicherheitsrelevanter Schwachstellen, welche zum Zeitpunkt der Prüfung auf den getesteten Systemen vorhanden sind.

Die folgenden Abschnitte geben einen Überblick über die Leistungen im Rahmen der Technischen Security Assessments der A1 Digital inkl. Beispielen, wobei, je nach Kundenwunsch, maßgeschneiderte Szenarien und andere Herangehensweisen ausgearbeitet werden können.

2.2.1 Infrastruktur-Tests

Die Infrastruktur eines Unternehmens bietet oft die breiteste Angriffsfläche, weswegen hier eine tiefgreifende Prüfung empfohlen wird. Dabei ist sowohl die externe als auch interne Prüfung von Servern und Clients beinhaltet, aber auch diejenige von kritischen Applikationen.

[1] https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

2.2.1.1 Externe Infrastruktur

Gerade über das Internet erreichbare Infrastruktur hat oft einen kritischen Sicherheitscharakter, da der einfache und oft auch anonyme Zugriff eine niedrige Zugangsbarriere und Hemmschwelle bringt. Klassische Beispiele von externer Infrastruktur sind Mailserver, Fileserver, Firewalls und Webapplikationen, welche jedoch in den meisten Fällen getrennt im Detail untersucht werden.

Information Gathering

Der Kunde stellt der A1 Digital die ihm über seine eigenen Systeme bekannten IP-Adressen und Domain-Namen zur Verfügung.

Es wird versucht, mittels verschiedener Techniken (z.B. whois-, reverse-whois-Abfragen, etc.), weitere Domains und IP-Ranges zu identifizieren. Die Domains werden genutzt, um etwa mittels Certificate Transparency Logs oder Passive DNS, Subdomains und damit weitere IP-Adressen zu enumerieren, um so dem Kunden nicht bekannte Systeme zu präsentieren und diese bei Notwendigkeit nach Rücksprache auch in der Prüfung zu inkludieren.

Asset Discovery und Schwachstellen-Scans

Mittels eines initialen automatisierten Schwachstellen-Scans inklusive Portscan und Service Detection, wird ein Überblick über vorhandene Systeme und Schwachstellen geschaffen.

In weiterer Folge werden identifizierte Schwachstellen – wo notwendig – manuell verifiziert und einer Risikobewertung unterzogen. Der Assessor selektiert auf Basis seiner Erfahrung stichprobenartig potenziell risikoträchtige Systeme, um sie einer genaueren, manuellen Überprüfung zu unterziehen.

Sicherheitsrisiken hinsichtlich (Fehl-)Konfigurationen und Design können nur insoweit erhoben werden, wie sie von außen feststellbar sind.

2.2.1.2 Interne Infrastruktur

Die interne Infrastruktur ist vor allem anfällig für Folgeangriffe nach externen oder Social-Engineering Attacken. Weitere Szenarien sind Angriffe durch eigene Mitarbeiter oder der Befall mit Schadprogrammen. Da sich Angreifer hier im internen Firmennetzwerk bewegen, können die möglichen Folgen erfolgreicher Angriffe kritisch sein. Der Verlust von Kundendaten, Geschäftsgeheimnissen und Denial of Service Angriffe können die kostspielige Folge sein und der Firmenreputation erheblich schaden.

Im Folgenden werden die wichtigsten Komponenten beschrieben, welche in der internen Infrastruktur verwundbar sind, wobei je nach Kundensituation der Fokus auf einzelne Teile gelegt werden kann.

Windows Active Directory

Das Windows Active Directory bildet oft das „IT-Fundament" einer Firma, da Benutzer, Zugriffe und Berechtigungen zentral über dieses System verwaltet werden. Aufgrund der Vielzahl an möglichen Konfigurationen passieren oft Fehler, welche sicherheitsrelevante Auswirkungen haben können.

Ein Szenario für eine Prüfung wäre zum Beispiel die eines Praktikanten, welcher üblicherweise nur über sehr beschränkte Berechtigungen in der Domäne verfügt. Das Ziel dieser Prüfung ist es, die Rechte in der Domain auszuweiten und in weiterer Folge unautorisierten Zugriff auf Daten oder Systeme zu erhalten.

File Shares

Hier werden Dateifreigaben im internen Firmennetzwerk hinsichtlich Zugriffsbeschränkungen evaluiert. Eine Herangehensweise wäre wiederum das Praktikanten-Szenario, in dem ein niedrig privilegierter Benutzer mit Zugriff auf das interne Netzwerk versucht, Zugriff auf alle möglichen Dateifreigaben im internen Netzwerk zu erhalten. Das Ziel ist die Identifizierung sensibler Daten auf Netzwerkfreigaben und die Aufdeckung falsch gesetzter Dateiberechtigungen, welche unautorisierten Zugriff auf diese Daten ermöglichen.

Infrastruktur Server

Im Zuge eines internen Infrastruktur-Tests wird initial ein Port-Scan und ein automatisierter Schwachstellen-Scan durchgeführt, wodurch ein Überblick über die vorhandenen Systeme geschaffen wird. Diese Scans können, wenn gewünscht, mit einer sogenannten „ScanBox" durchgeführt werden. Dabei wird eine virtuelle Maschine (ScanBox) in das interne Firmennetzwerk eingebracht, wobei diese von extern (aus dem Internet) für die Prüfer erreichbar ist. Dies hat den Vorteil, dass bereits vor einem etwaigen internen Test, Schwachstellen aufgedeckt werden können, und der Assessor bereits vorab detaillierte Informationen über den Aufbau des Netzwerks in Erfahrung bringen kann.

In weiterer Folge werden identifizierte Schwachstellen – wo notwendig – manuell verifiziert und einer Risikobewertung unterzogen. Der Assessor selektiert auf Basis seiner Erfahrung stichprobenartig potenziell risikoträchtige Systeme, um sie einer genaueren, manuellen Überprüfung zu unterziehen.

Client Test

Der seitens des Kunden zur Verfügung gestellte „Muster Client" wird durch den Assessor auf installierte und verwundbare Software hin geprüft. Dies umfasst installierte oder dem Benutzer zugängliche und verfügbare Software, Virenschutz, sowie laufende/aktivierte Dienste.

Des Weiteren wird die sichere Konfiguration des Geräts, wie etwa Gruppenrichtlinien, Verschlüsselung, Administrator-Rechte, Netzwerkintegration etc. geprüft.

Application Test
Abhängig von der Client-Technologie werden client-, server- und netzwerkseitige Prüfungen durchgeführt. Je nach Applikation, werden ein oder mehrere Benutzer mit unterschiedlichen Berechtigungen zur Verfügung gestellt.

Des Weiteren werden Prüfungen der gespeicherten Applikations-Daten durchgeführt, sowie entsprechend gesetzte Dateiberechtigungen. Sollte Zugriff auf den Source-Code bestehen, können hier detaillierte Prüfungen durchgeführt werden (mehr Details zu Source Code Analysen sind in **Abschnitt 2.2.3** beschrieben).

2.2.2 Webapplikationen

Webseiten stellen oft ein lohnendes Ziel für Angreifer dar, da diese einfach über Suchmaschinen identifiziert werden können. Moderne Webapplikationen bieten eine Vielzahl an Möglichkeiten, wodurch eine große Angriffsfläche gegeben ist. Die am häufigsten auftretenden Web-Schwachstellen werden in den OWASP Top 10[2] festgehalten.

Sicherheitsprüfungen von Webapplikationen umfassen u.a. eine Prüfung der OWASP Top 10. Die Tests werden an den OWASP Testing Guide (Version 4[3]) angelehnt, um Schwachstellen und fehlerhafte Konfigurationen zu erkennen.

Folgende Punkte werden in einer Sicherheitsprüfung von Webapplikationen typischerweise abgedeckt, wobei der Fokus in enger Abstimmung mit dem Kunden bestimmt wird:

- Manuelle Prüfung der relevanten Punkte des OWASP Testing Guides in der Version 4 mit besonderem Fokus auf die OWASP Top 10.
- Testen von Konfigurations-Schwachstellen wie beispielsweise schwache SSL-Einstellungen oder fehlende Sicherheitsheader.
- (Semi-) Automatisierte Schwachstellenscans.

2.2.3 Source Code Analyse

Die Source Code Analyse bietet eine tiefergreifende Prüfung von Applikationen. Mittels automatisierter Werkzeuge wird der Source Code auf mögliche Schwachstellen durchsucht, welche dann manuell analysiert und verifiziert werden.

Bei kritischen Applikationen wird zusätzlich eine tiefergehende manuelle Vollanalyse empfohlen. Diese ist zeitlich aufwendiger, ermöglicht aber das Auffinden von

[2] https://www.owasp.org/index.php/Top_10-2017_Top_10
[3] https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

komplexen Fehlern und Schwachstellen, welche oft mit automatisierten Source Code Analysen oder externen Penetration Tests nicht identifiziert werden können.

Grundsätzlich kann zwischen folgenden Herangehensweisen unterschieden werden:

1. **Source-Code Quick-Check:** Eignet sich für kleine Module und Plugins (z. B. selbst entwickelte CMS Plugins).

2. **Automatisierte Source-Code Analyse mit manuellem Review der relevanten Punkte:** Eignet sich für komplexere Applikationen mit großem Umfang. Automatisierte Source-Code Scanner dienen dem Tester, um die Schwachstellen initial zu identifizieren – in weiterer Folge wird die Ausnutzbarkeit manuell verifiziert. Dieser Ansatz lässt sich mit Punkt 3) besonders für kritische Funktionen kombinieren.

3. **Tiefgehender manueller Source-Code Review mit teils automatisierten Scans zur Unterstützung:** Eignet sich für kritische Applikationen bzw. Funktionen innerhalb von komplexen Systemen. Der Tester analysiert den Code zu einem großen Teil manuell und kann daher eine tiefergehende Analyse der Software durchführen als in Punkt 2) beschrieben.

2.2.4 Mobile Applikationen

Neue Technologien bergen stets neue Sicherheitsrisiken, und mobile Applikationen stellen hierbei keine Ausnahme dar. Die Sicherheitsaspekte für mobile Anwendungen unterscheiden sich jedoch in einigen wichtigen Punkten von herkömmlicher Desktop-Software.

So gelten etwa moderne mobile Betriebssysteme zumeist als sicherer als traditionelle Desktop-Betriebssysteme. Dennoch können auch hier sicherheitsrelevante Probleme auftreten, wenn die Sicherheitskonzepte bei der Entwicklung mobiler Anwendungen nicht sorgfältig berücksichtigt wurden.

Folgende Aspekte können durch diese Art von Prüfung abgedeckt werden:

- Sichere Datenspeicherung
- Kommunikation zwischen Anwendungen
- Korrekte Verwendung von kryptographischen APIs
- Sichere Netzwerkkommunikation
- Von der App verwendete API-Endpunkte
- Manuelle und/oder automatisierte Quellcode-Analyse

Alle Aspekte der Prüfung sind für Android und iOS verfügbar und sind an die neueste Version des OWASP Mobile Security Testing Guides angelehnt.

2.2.5 Red Teaming

Penetration Tests bieten eine Momentaufnahme der zum Zeitpunkt der Prüfung herrschenden Sicherheitslage eines definierten Scopes.

Im Gegensatz dazu handelt es sich beim Red Teaming um eine umfassende, mehrschichtige Angriffssimulation, um zu messen, wie gut ein Unternehmen einem Angriff eines echten Gegners standhalten kann. Dazu gehören Mitarbeiter und Netzwerke, Anwendungen und physische Sicherheitskontrollen.

Im Zuge dieses Ansatzes können unter anderem Schwachstellen und Risiken in folgenden Bereichen getestet und aufgedeckt werden:

- **Technologie:** Netzwerke, Anwendungen, Router, Switches, Geräte, etc.
- **Personen:** Mitarbeiter, unabhängige Auftragnehmer, Abteilungen, Geschäftspartner, etc.
- **Physische Infrastruktur:** Büros, Lager, Umspannwerke, Rechenzentren, Gebäude, etc.

Das Ziel des Red Teaming-Ansatzes ist es, Wege zu finden, das Unternehmen auf verschiedenste Weisen zu kompromittieren und so die Verteidigung zu unterstützen.

Üblicherweise werden Red Teaming Assessments über einen längeren Zeitraum angesetzt (zum Teil über einen Zeitraum von einem halben Jahr bis ein Jahr).

Durch die große Zeit- und Umfangskomponente kann mittels Red Teaming ein Unternehmen am umfangreichsten geprüft und dadurch geschützt werden. Dieser Ansatz wird bei hoher Sicherheitsnotwendigkeit empfohlen.

2.3 Social Engineering

Die im Folgenden dargestellten Social Engineering-Kampagnen werden in der Regel einmalig in einem gewissen Zeitraum durchgeführt. Ergebnisse, Auswertungen und Empfehlungen für weitere Schritte werden in einem Bericht inklusive Executive Summary präsentiert. Weiters kann eine finale Abschlusspräsentation für das Management angeboten werden.

Im Anschluss sollten gezielte Awareness Trainings durchgeführt werden, wobei diese in der Regel ebenfalls einmalig oder in größeren Intervallen (z.B. jährlich) durchgeführt werden.

Da sich in den meisten Fällen einmalige Prüfungen als nicht sehr wirkungsvoll herausgestellt haben, bietet die A1 Digital kontinuierliche Social Engineering Prüfungen sowie Awareness Trainings an, um ein anhaltendes Bewusstsein im zu prüfenden Unternehmen zu schaffen. Eine detailliertere Beschreibung zu den kontinuierlichen Social Engineering Prüfungen ist in **Abschnitt 2.3.4** zu finden.

Die folgenden Abschnitte geben einen Überblick über das Social Engineering Portfolio der A1 Digital mit Beispielen, wobei, je nach Kundenwunsch, maßgeschneiderte Szenarien und andere Herangehensweisen ausgearbeitet werden können.

2.3.1 Phishing Kampagne

Bei Phishing-Kampagnen wird zwischen zwei Herangehensweisen unterschieden:

- **Breit** aufgestellte Phishing-Kampagnen mit dem Ziel, so viele Daten von so vielen Benutzern wie möglich abgreifen zu können. Darunter fallen klassische Phishing E-Mails, welche ohne oder mit wenig Personalisierung an einen großen Verteilerkreis versendet werden.
- **Gezielte** Phishing-Kampagnen mit dem Ziel, Informationen über einen bestimmten Nutzer oder über einen kleinen Nutzerkreis herauszufinden. Darunter fallen beispielsweise maßgeschneiderte und personalisierte Phishing E-Mails sowie CEO-Fraud Angriffe mit dem Ziel, Überweisungen zu veranlassen.

2.3.1.1 Breit angelegte Phishing Kampagne

Im Folgenden werden einige Beispiele bzw. Szenarien beschrieben, welche typisch für breit angelegte Phishing-Kampagnen sind, wobei diese je nach Kunde von den beschriebenen Szenarien abweichen können.

Mit bösartigen Links zu gefälschten Webseiten

Hierbei werden E-Mails generiert, welche in der Regel einen Link zu einer gefälschten Webseite beinhalten.

Diese Webseite kann beispielsweise eine Kopie der Firmenwebseite darstellen, wobei dem Opfer eine Login-Maske präsentiert wird. Das Ziel ist das Abgreifen von sensiblen Benutzerinformationen wie Windows-Benutzeraccounts sowie zugehörige Passwörter.

Mit bösartigen Anhängen (Malware)
Hierbei werden E-Mails generiert, welche eine bösartige Datei als Anhang beinhalten (beispielsweise eine Malware, welche als Bewerbung getarnt an die HR-Abteilung versendet wird).

Das Ziel ist das Ausführen von Schadcode auf dem Zielrechner, ohne dass die angegriffene Person etwas von dem Angriff mitbekommt. Beispiele wären das Auslesen des Windows-Hostnamens oder das Erstellen eines Screenshots. Eine volle Übernahme des Rechners wäre ebenso denkbar, was das Fernsteuern des Rechners aus der Ferne durch den Angreifer und das Ausbreiten im internen Firmennetzwerk ermöglichen würde.

USB Sticks mit bösartigen Daten (Malware)
Hierbei werden USB-Sticks mit Schadsoftware am Standort ausgestreut (beispielsweise am Unternehmensparkplatz) oder an das Unternehmen versendet. Das Ziel ist wiederum das Ausführen von Schadcode auf den Rechnern, an welche der USB-Stick angesteckt wird. Weiters bestünde die Möglichkeit, statt eines klassischen USB-Sticks ein als USB-Stick getarntes Keyboard zu verwenden, welches beim Anstecken automatisiert Kommandos auf dem Zielrechner ausführt.

2.3.1.2 Gezielt angelegte Phishing-Kampagne
Im Folgenden werden einige Beispiele bzw. Szenarien beschreiben, welche typisch für eine gezielte Phishing-Kampagne sind, wobei diese je nach Kunde von den beschriebenen Szenarien abweichen können.

CEO Fraud
Hierbei ist das Ziel, Überweisungen an vom Angreifer kontrollierte Bankkonten zu veranlassen.

Die typische Vorgehensweise ist dabei, durch Recherche Personen im Unternehmen zu identifizieren, welche Geldüberweisungen veranlassen können. In einem weiteren Schritt wird diese Person direkt via E-Mail oder Telefon kontaktiert, wobei sich der Absender/der Anrufende als Vorgesetzter ausgibt und eine dringliche Überweisung anweist.

Ändern von Gehaltskonten
In diesem Szenario versucht der Angreifer das Gehaltskonto eines Mitarbeiters des Unternehmens auf ein anderes zu ändern. Die typische Vorgehensweise dabei ist, durch Recherche, Personen im Unternehmen zu identifizieren, welche Gehaltskonten ändern können. In weiterer Folge gibt sich der Angreifer als das Opfer aus und

versucht, über gefälschte E-Mails oder Telefonanrufe das Ändern des Gehaltskontos zu veranlassen.

Personalisierte Phishing Mails und OSINT
Hierunter fallen gezielte Phishing E-Mails, welche typischerweise auf Executive-Ebene durchgeführt werden. Im Unterschied zu breiter angelegten Phishing-Kampagnen wird bei gezielten Phishing-Kampagnen die anzugreifende Person einem Open Source Intelligence (OSINT) Check unterzogen, bei dem so viele Informationen aus öffentlichen Quellen über das Opfer gesammelt werden wie möglich. Darunter fallen beispielsweise Wohnort, private E-Mail-Adressen, Kontodaten, Passwörter (beispielsweise aus Data-Breaches) und mehr.

Mithilfe dieser Informationen können maßgeschneiderte Phishing-Angriffe auf Individuen durchgeführt werden, wodurch die Erfolgschancen maßgeblich erhöht werden.

Im Anschluss wäre bei diesem Szenario auch eine gezielte Awareness-Schulung auf Executive-Ebene denkbar.

2.3.2 On-Site Tests

Bei On-Site Tests befinden sich A1 Digital Mitarbeiter vor Ort und versuchen Informationen über das zu prüfende Unternehmen zu erfragen, unerlaubten Zutritt zu erhalten oder das interne Firmennetzwerk zu kompromittieren. Dabei werden komplexe und individuell auf den Kunden zugeschnittene Szenarien entwickelt, um Zutritt zu erlangen. Beispielsweise könnten folgende Ziele eines On-Site Tests definiert werden:

- Physischer Zugang zu Systemen bzw. zur Firmeninfrastruktur
  - Testen der physischen Sicherheit im Gebäude
  - Testen der allgemeinen Awareness von z. B. Security Mitarbeitern oder Mitarbeitern am Empfang
  - Testen von Netzwerkzugängen und etwaigen Sicherheitsmechanismen

- Sensible Firmendaten von Mitarbeitern erfragen
  - Erfragen von Zutrittscodes oder Passwörtern
  - Erfragen von vertraulichen Firmendokumenten (Corporate Espionage)
    - Platzieren von Wanzen im Unternehmen

On-Site Tests sind in den meisten Fällen sehr individuell und in enger Abstimmung mit dem Kunden zu gestalten.

2.3.3 Awareness Trainings

Um den beschriebenen Szenarien entgegenwirken zu können, bieten wir gezielte Awareness-Schulungen an, welche die häufigsten Einfallstore von Social Engineering Angriffen aufzeigen und Gegenmaßnahmen präsentieren. Die Schulungen werden individuell auf die Bedürfnisse des Kunden abgestimmt und beinhalten zumindest folgende Themen:

- Übersicht über aktuelle Bedrohungen
- Passwortsicherheit
- Erkennen von Phishing Mails und Webseiten sowie eine generelle Übersicht, wie man sich sicher im Netz bewegen soll
- E-Mail-Sicherheit
- Physische Sicherheit

2.3.4 Kontinuierliche Social Engineering Prüfungen

Das Schaffen von Sicherheitsbewusstsein (Awareness) von Mitarbeitern in mittleren bis großen Unternehmen gestaltet sich als besonders herausfordernd. Einmalige oder seltene Awareness Schulungen zeigen oft wenig Wirkung.

Deshalb wird empfohlen, Social-Engineering Angriffe und Awareness-Schulungen regelmäßig durchzuführen, um das Sicherheitsbewusstsein der Mitarbeiter aufrecht zu erhalten.

In Abstimmung mit den Kunden werden Prüfungen mehrere Male auf dieselben oder unterschiedliche Mitarbeiter bzw. Zielgruppen durchgeführt. Dabei kann es sich um offensichtliche und stümperhaft durchgeführte Angriffsversuche handeln oder um hoch-professionelle, personalisierte Phishing Mails. On-Site Tests können ebenfalls mehrmals pro Jahr durchgeführt werden, um den Erfolg der abgehaltenen Awareness-Schulungen aufzuzeigen bzw. zu messen.

Unsere Leistungen:

- **Regelmäßige Social Engineering Angriffe**, wobei alles aus unserem Portfolio ein- oder mehrmalig durchgeführt werden kann.
- **Optionale Benachrichtigung der Mitarbeiter**, wenn beispielsweise Phishing-Angriffe via E-Mail erfolgreich durchgeführt wurden. Mitgeliefert wird dabei, welche Daten des Mitarbeiters durch den Angriff kompromittiert wurden und woran der Angriff hätte erkannt werden können.
- **Regelmäßige Awareness Schulungen** mit zahlreichen Praxisbeispielen.

3 Servicebedingungen

3.1 Verfügbarkeit

Die hier beschriebenen Leistungen im Rahmen des A1 Digital Security Assessments werden im Zeitraum zwischen Montag bis Freitag, 06:00-22:00 Uhr durchgeführt.

Hinweis: In diesem Service sind keine technischen Unterstützungsleistungen enthalten.

3.2 Nutzungsvoraussetzungen

- Zumindest drei Werktage vor Beginn des A1 Digital Security Assessments stellt der Kunde A1 Digital den konkreten Scope des A1 Digital Security Assessments (entsprechende IP-Ranges, Domains, Subdomains, Standorte, etc.) zur Verfügung.
- Die Bekanntgabe des konkreten Scopes erlaubt dem Auftragnehmer implizit die Zielsysteme im Rahmen dieses Vertrags anzugreifen („Permission to Attack").
- Um das Service nutzen zu können, muss der Kunde entweder selbst System-Owner sein oder die Zustimmung des/r System-Owner/s einholen und garantieren, zur Autorisierung der Penetration Tests befugt zu sein.
- 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.
- Für die Erbringung eines externen Security Assessments stellt der Kunde sicher, dass vom Assessor angeforderte Freischaltungen (Ausnahmen auf etwaigen IDS/IPS Systemen, Firewalls, etc.) eingerichtet werden. Sollten diese Freischaltungen nicht eingerichtet werden, kann es sein, dass die manuellen und automatisierten Scans unzuverlässige Ergebnisse liefern.
- Für die Erbringung eines internen Security Assessments stellt der Kunde für den Assessor gegebenenfalls einen Firmenrechner bereit sowie benötigte Zugangsdaten. Außerdem stellt der Kunde einen Arbeitsplatz mit einem Bildschirm sowie Zugang zum internen Netzwerk (inkl. der nötigen Freischaltungen) zur Verfügung.
- Für die Erbringung einer Phishing-Kampagne (**siehe Abschnitt 2.3.1**) stellt der Kunde eine Liste an Empfänger-E-Mail-Adressen zur Verfügung, an welche die Kampagne gerichtet werden soll. Sollte vom Kunden gewünscht sein, dass Phishing-Mails mit höchstmöglicher Wahrscheinlichkeit zugestellt werden, ist dieser dafür verantwortlich, dass eine von A1 Digital zu benennende E-Mail-Adresse, welche als Absenderadresse benutzt wird, auf allen E-Mail-Systemen freigeschaltet („Whitelisted") wird. Sollte dies nicht der Fall sein, kann die

Zustellung nicht garantiert werden, da etwaige Schutzmechanismen die Phishing-E-Mails blockieren könnten.

- Die Ergebnisse werden in Form eines Berichts in PDF-Format an den Kunden übermittelt und beinhaltet:
    - Definition des Scopes des A1 Digital Security Assessments
    - Management Summary
    - Risikobeschreibungen, -bewertung und Maßnahmenempfehlungen

3.3 Verantwortlichkeit und Haftung

A1 Digital weist darauf hin, dass die Durchführung eines A1 Digital Security Assessments die Verfügbarkeit und Integrität der Zielsysteme beeinträchtigen kann. Es ist möglich, dass der ordnungsgemäße Betrieb nur durch manuellen Zugriff auf das Zielsystem wiederhergestellt werden kann. Dies bedeutet beispielsweise, dass die Webseite auf dem Zielsystem nicht mehr erreichbar sein könnte, bzw. dass Registrierungen, Anmeldungen oder Bestellungen mit unrichtigen Daten durchgeführt werden könnten. Der Kunde hat allein für alle hierdurch eintretenden nachteiligen Folgen einzustehen.

Jede identifizierte IP-Adresse muss durch den Kunden freigegeben werden, damit sie angegriffen wird. Mit der Übermittlung der Zielsysteme gibt der Kunde verbindlich bekannt, dass er die Befugnis hat, die betreffenden Systeme attackieren zu lassen.

Alle Fragen betreffend Rechte an IP-Adressen oder Domains (z.B. Registrierung, Innehabung, Sperre, Kauf, Miete, Pacht, Sharing, Urheberrechte, Namensrecht, Markenrecht usw.) und allenfalls daraus resultierende Konflikte wird der Kunde im eigenen Bereich abschließend lösen.

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/ueber-a1-digital/agb-a1-digital/.

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 Security Assessment"**

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 1006 – Lausanne	Hosting Services	Schweiz, Deutschland, Österreich, Bulgarien

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

- **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

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