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

Offensity Security Monitoring & Reporting

Servicebeschreibung

Version: 4.0

Datum: 13.12.2019

Inhaltsverzeichnis

1 Allgemeines

Diese Servicebeschreibung gilt ab 13.12.2019. Sie erläutert die Ausprägung aller Anwendungen von Offensity Security Monitoring (kurz „Offensity"), die Ihnen als Kunde von A1 Digital Deutschland GmbH (kurz „A1 Digital") angeboten und bereitgestellt werden. Sofern hier nicht Abweichendes geregelt wird, kommen die Allgemeinen Geschäftsbedingungen für Cloud und Software Solutions der A1 Digital zur Anwendung: https://www.a1.digital/ueber-a1-digital/agb-a1-digital/.

Alle Offensity Anwendungen sind cloudbasierte Services, die ortsunabhängig genutzt werden können. Die Kunden erhalten die notwendigen Zugangsdaten für die Dauer des gewählten Abonnements (monatlich, jährlich).

Kunde für das Service Offensity kann nur ein Unternehmer im Sinne des § 14 des Bürgerlichen Gesetzbuches (BGB) sein.

2 Anwendungen

Offensity hilft Unternehmen dabei, die zur Sicherheit ihrer extern erreichbaren IT-Systeme technische Maßnahmen nach dem Stand der Technik ergreifen wollen, laufend Schwachstellen zu erkennen. Eine einheitliche Erfassung aller identifizierten Risiken sowie lösungsorientierte Reports reduzieren die Reaktionszeit des Kunden und ermöglichen eine Dokumentation und Priorisierung der zu setzenden Maßnahmen.

A1 Digital übernimmt keinerlei Verantwortung dafür, dass alle vorhandenen Schwachstellen erkannt werden. Abhängig von den gewählten Konfigurationen, ist es beispielsweise immer möglich, einzelne Systeme oder Schwachstellen zu übersehen.

Offensity beinhaltet folgende Anwendungen: Domain-basiertes Asset Discovery, Schwachstellen-Scans und Risikobewertung, und Lösungsorientierte Reports. Die durch Offensity erkannten Schwachstellen und Datensätze werden vertraulich behandelt.

2.1 Domain-basiertes Asset Discovery

Auf Basis von Domain-Namen des Kunden (z.B. „example.com") werden dazugehörende, extern erreichbare IT-Systeme erhoben. Dies umfasst beispielsweise DNS- und Mailserver sowie Subdomains.

2.1.1 Domain Control Validation

Die Kunden können bei Aktivierung der Domain aktuell zwischen folgenden drei dem „Stand der Technik" entsprechenden technischen Methoden wählen, mit denen Offensity die Domain-Ownership verifiziert:

- **E-Mail-basierte Domain Control Validation**: Wenn die Bestellung aufgegeben wird, wird eine E-Mail-Adresse aus einer Liste mit akzeptablen Optionen ausgewählt. An diese Adresse wird eine E-Mail gesendet, die einen eindeutigen Validierungscode enthält. Die E-Mail sollte von einer Person empfangen werden, die die Kontrolle über die Domain innehat. Die Liste der zulässigen E-Mail-Adressen für eine bestimmte Domain lautet beispielsweise admin@, administrator@, hostmaster@, postmaster@ oder es handelt sich dabei um eine beliebige

E-Mail-Adresse für Administrator, Registrant, Tech oder Zone, die im WHOIS-Verzeichnis[1] aufscheint.

- **DNS-based Domain Control Validation**: Der Kunde muss einen vordefinierten Textcode als so genannten DNS-Texteintrag in seine DNS-Verwaltungskonsole hochladen.
- **HTTP-based Domain Control Validation**: Der Kunde muss eine Authentifizierungsdatei in den Stammordner seiner Website hochladen.

2.2 Schwachstellen-Scans und Risikobewertung

Die Systeme werden aus dem Internet netzseitig mit Hilfe von Security-Scannern und automatisierten Analysen untersucht, um Informationen oder Hinweise zu erhalten, die ein Angreifer für die Vorbereitung und Durchführung von virtuellen Einbrüchen nutzen kann. Die eingesetzten Werkzeuge überprüfen aktuell bekannte Schwachstellen von Netzwerkkomponenten, Betriebssystemen, Applikationen und Protokollen, soweit sie aus dem Internet nachweisbar sind. Diese werden im Rahmen einer automatisierten Risikoanalyse bewertet. Der Risikostatus wird dokumentiert und kann jederzeit mit vergangenen Ergebnissen verglichen werden. Bei Bekanntwerden neuer Schwachstellen wird – abhängig von technischer Möglichkeit, Umsetzbarkeit, Risikopotenzial und Relevanz – die Kundeninfrastruktur auf Anfälligkeit überprüft.

Der Kunde hat dafür zu sorgen, dass jene Systeme, die für Schwachstellen-Scans verwendet werden, von dynamischen Sicherheitseinschränkungen (wie z.B. Web Application Firewalls, fail2ban, etc.) ausgenommen werden. Eine Ausnahme von statischen Sicherheitsmaßnahmen (wie etwa Packet Filtering Firewall) ist möglich, wird seitens A1 Digital aber nicht empfohlen.

Die Quellsysteme und deren IP-Adressbereiche, die für Schwachstellen-Scans verwendet werden, werden dem Kunden auf Anfrage mitgeteilt.

Von Offensity wird pro Subdomain max. eine dahinterliegende IP-Adresse gescannt.

2.2.1 Permission To Attack

Die Schwachstellen Scans („Security-Scans") können „intrusiv" und „nicht-intrusiv" sein.

- **Intrusive Security-Scans** sind Scans, die technische oder organisatorische Schutzmaßnahmen umgehen können. Diese Scans bedürfen einer rechtlich verbindlichen Zustimmung durch den Kunden

[1] Das WHOIS-Verzeichnis ist eine öffentliche Liste von Domainamen und Kontaktdaten der mit ihnen verknüpften Personen oder Organisationen.

bzw. einen Administrator, dass die aktivierten Subdomains unter jeder Domain (inkl. den dahinterliegenden IP-Adressen) durch Offensity auf Schwachstellen gescannt werden dürfen (sog. „Permission To Attack"). Ohne eine solche Zustimmung können diese Scans illegal sein.

- **Nicht-intrusive Security-Scans** sind Scans, die keine technischen oder organisatorischen Schutzmaßnahmen umgehen, um auf das Vorhandensein von Schwachstellen zu schließen. Dies umfasst etwa das Herausfinden von Software-Versionen. Es ist in der Regel keine Zustimmung des System-Besitzers notwendig.

Nähere Informationen siehe Servicebedingungen 2.3.

2.3 „Deep-Web"-Überwachung

Unfreiwillig veröffentlichte Datensätze dritter Plattformen können zu Sicherheitsproblemen führen, da etwa E-Mail-Adressen und Zugangsdaten von den Nutzern dieser Plattformen in fremde Hände geraten. Offensity überwacht das „Deep Web" (auch „Verstecktes Web"), um veröffentlichte Daten aufzuspüren. Gefundene Datensätze werden auf Basis der Kunden-Domains selektiert und verifiziert, um Kunden über veröffentlichte Datensätze zeitnah zu informieren.

Offensity gleicht Domains und IP-Adressen der Kunden mit öffentlichen und teilöffentlichen Block- und Blacklisten ab, um eine Servicebeeinträchtigung der Kundendienste möglichst frühzeitig zu erkennen. Einträge auf diesen Listen können auch auf Missbrauch oder Kompromittierung der Kundensysteme hinweisen.

2.4 Lösungsorientierte Reports

Die Ergebnisse der laufenden Scans werden in Form eines schriftlichen Reports über das Offensity Reporting Dashboard zur Verfügung gestellt. Es wird eine Kategorisierung der ggf. gefundenen Schwachstellen vorgenommen, die Schwachstelle wird beschrieben, ggf. werden weiterführende Informationen und Hinweise zur Behebung der Schwachstelle dargelegt. Der Bericht wird in englischer Sprache verfasst.

3 Leistungsumfang

Die Leistung von Offensity beinhaltet folgende Lieferobjekte:

- Offensity Security Monitoring inkl. „2.1 Domain-basiertes Asset Discovery", „2.2 Schwachstellen-Scans und Risikobewertung", „2.3 ‚Deep-Web'-Überwachung"
- Zugriff auf das Offensity Dashboard (siehe „2.4 Lösungsorientierte Reports")

4 Zusatzleistungen

Der Kunde hat die Möglichkeit, kostenpflichtige Zusatzleistungen zu Offensity zu bestellen. Zusatzleistungen müssen explizit im Vertrag aufgeführt werden, um in Anspruch genommen werden zu können.

4.1 Collaboration Calls

Mit Collaboration Calls hat der Kunde die Möglichkeit, Security-Beratungsgespräche in Bezug auf erbrachte und zukünftig zu erbringenden Leistungen in Anspruch zu nehmen. Sofern im Vertrag nicht anders geregelt, ist die Dauer auf zwei Stunden am Stück und einmalig pro Monat beschränkt.

Das Gespräch dient zur Besprechung identifizierter Risiken, sowie zur Planung und Abstimmung eventueller zukünftiger Tests. Das Abstimmungstelefonat ist mit einer Vorlaufzeit von zumindest zwei Wochen durch den Kunden aktiv einzufordern. Die Terminfindung geschieht in beiderseitigem Einvernehmen. A1 Digital empfiehlt, die Vereinbarung eines Serientermins. Versäumt der Kunde aus eigenem Verschulden einen Collaboration Call, verfällt der Anspruch für den aktuellen Monat ersatzlos. Kommt der Collaboration Call aus einem anderen Grund nicht zustande, kann er innerhalb eines Monats nachgeholt werden.

A1 Digital bietet einen verschlüsselten Kommunikationskanal für Collaboration Calls an. Möchte der Kunde einen anderen als von A1 Digital vorgeschlagenen Kommunikationskanal nutzen, geschieht dies im Sinne der Vertraulichkeit der Kommunikation auf Verantwortung des Kunden. Ein technischer Ausfall des vom Kunden vorgeschlagenen Kommunikationskanals wird als Verschulden des Kunden gewertet. Collaboration Calls erfolgen ausschließlich über das Internet oder Telefonsysteme (Mobilfunk oder Festnetz).

4.2 Red Teaming

Mit Red Teaming bietet A1 Digital einen monatlichen Pool an Ressourcen (Personentagen), welche für Security Assessments von Systemen und Organisationen genutzt werden können.

4.2.1 Arten von Assessments

Der Kunde hat hierbei die Möglichkeit, innerhalb des vereinbarten Rahmens an Ressourcen, folgende Assessments zu vereinbaren:

a) Security Assessment extern erreichbarer Systeme, die von Offensity kontinuierlich gescannt werden und/oder die durch den Kunden explizit mittels Permission To Attack (siehe **Servicebedingungen Abschnitt 2.3**) freigegeben wurden.
b) Security-Assessment interner Netzwerkinfrastrukturen des Kunden nach expliziter Freigabe.
c) Individuelle Social Engineering Kampagnen (z.B. Phishing-Kampagnen über E-Mail)

Wird nicht zumindest zwei Wochen vor Beginn eines monatlichen Assessments in beiderseitigem Einvernehmen etwas Gegenteiliges vereinbart, wird die unter Punkt a) beschriebene Leistung erbracht. Für alle anderen Assessments, beschrieben in den Punkten b) und c), muss spätestens einen Tag vor Beginn der Durchführung des manuellen Assessments eine schriftliche Permission To Attack erteilt werden (siehe **Servicebedingungen Abschnitt 2.3**). Andernfalls wird die in Punkt a) beschriebene Leistung erbracht.

4.2.2 Interne Netzwerkinfrastruktur

Die unter **Abschnitt 4.2.1** b) beschriebene Leistung erfordert die Installation eines „Jump Hosts" innerhalb des Unternehmensnetzwerks des Kunden. Dies ist eine von A1 Digital bereitzustellende virtuelle Maschine oder Installationsdatei. Die Installation und die Herstellung der Netzwerkkonnektivität ist durch den Kunden zu gewährleisten. Über diesen Jump Host, haben die A1 Digital Assessoren die Möglichkeit, über das Internet auf das zu testende Netzwerksegment zuzugreifen. Der Jump Host kann in Absprache mit dem Kunden überdies dazu verwendet werden, vor der Durchführung der manuellen Assessments automatisierte Prüfungen und Scans der internen Kundeninfrastruktur durchzuführen. Können A1 Digital Assessoren – etwa wegen nicht fristgerechter Installation oder fehlender Netzwerkkonnektivität – nicht auf den Jump Host zugreifen, wird alternativ die in **Abschnitt 4.2.1** a) beschriebene Leistung erbracht.

4.2.3 Authentifizierte Prüfungen

Der Kunde hat im Rahmen der Collaboration Calls (siehe **Abschnitt 4.1**) die Möglichkeit, den A1 Digital Assessoren Zugangsdaten zu Applikationen zur Verfügung zu stellen, um authentifizierte Assessments dieser vornehmen zu lassen.

4.2.4 Zeitraum der Assessments

Der Zeitraum der Assessments wird von A1 Digital festgelegt und mit dem Kunden im Rahmen der Collaboration Calls (siehe **Abschnitt 4.1**) abgestimmt oder auf andere Weise kommuniziert. A1 Digital hat hierbei das Recht, monatliche Ressourcen an zusammenhängenden Tagen zu leisten. Leistet A1 Digital innerhalb eines Monats nicht das vereinbarte Ausmaß an Ressourcen, kann A1 Digital die Tage innerhalb der darauffolgenden zwei Monate leisten. Wurde die Verschiebung verschuldensunabhängig durch den Kunden verursacht oder veranlasst, erhöht sich die Frist auf sechs Monate. Die Leistungsabrechnung erfolgt unabhängig von der Leistungserbringung monatlich.

4.2.5 Sonstiges

Sämtliche Assessments und Prüfungen erfolgen über das Internet. Gegebenenfalls erstellte Berichte, Auswertungen und Aufzeichnungen werden dem Kunden in digitaler Form über einen von A1 Digital festzulegenden Kanal übermittelt.

Sämtliche Assessments und Prüfungen verfolgen einen Time-Box- und Grey-Box-Ansatz. Das bedeutet, dass das Aufdecken von Sicherheitsrisiken Beschränkungen durch Zeit (Time-Box) und Ressourcen sowie Wissen über System-Interna (Grey-Box) unterworfen ist.

Je mehr Zeit, Ressourcen und Wissen einem A1 Digital Assessor zur Verfügung stehen, desto mehr Möglichkeiten hat dieser, Sicherheitsrisiken zu identifizieren.

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: **„Offensity“**

1.2. Folgende Datenarten können regelmäßig Gegenstand der Verarbeitung sein:

(Bitte je nach Produkt/Leistung anpassen)

- ☒ 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:

(Bitte entsprechend Leistungsvereinbarung anpassen)

- ☒ 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		
Google Irland Ltd. (Branch of Google LLC)	Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Irland	Hosting Services	Irland, Frankfurt
Elasticsearch B.V.	Rijnsburgstraat 11, 1059 AT Amsterdam, Niederlande	Hosting Services	Frankfurt

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, Zwei-Faktor-Authentifizierung.

- **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“, Mandantenfähigkeit.

- **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[2] (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.

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

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), 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

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