



Offensivity Security Monitoring & Reporting

Servicebedingungen

Version: 4.0

Datum: 13.12.2019





Inhaltsverzeichnis

1. Allgemeines	2
2. Nutzungsvoraussetzungen	3
2.1 Domain Ownership	3
2.2 User-Berechtigungen	3
2.3 Permission To Attack.....	3
2.4 Technische Voraussetzungen	4
3. Leistungen von A1 Digital International GmbH.....	4
3.1 A1 Digital Serviceauskunft	4
4. Serviceverfügbarkeit	4
5. Haftungsausschluss	5
6. Kündigung, Mindestvertragsdauer	6
7. Datenschutz und Datensicherheit	6

1. Allgemeines

Diese Servicebedingungen gelten ab 13.12.2019. Sie erläutern die Nutzung aller Anwendungen von Offensity Security Monitoring (kurz „Offensity“), die Ihnen als Kunde von A1 Digital International 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 Telekom Austria AG zur Anwendung, die sinngemäß auch für die A1 Digital gelten.

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

Kunde für das Service Offensity kann nur ein Unternehmer im Sinne des § 1 des Konsumentenschutzgesetzes (KSchG) sein.



2. Nutzungsvoraussetzungen

2.1 Domain Ownership

Um Offensity nutzen zu können, muss der Kunde entweder selbst Domain Owner sein oder die Zustimmung des Domain Owners einholen und rechtlich verbindlich garantieren, zur Autorisierung der Security Scans befugt zu sein.

2.2 User-Berechtigungen

Für die Bereitstellung von Offensity benötigen wir Vor- und Zuname, Emailadresse sowie Handynummer jener Person/en, auf deren Name/n der Erstzugang und damit die User-Berechtigungen eines Administrators eingerichtet werden sollen. Administratoren haben folgende User-Berechtigungen:

- Zugriff auf sämtliche Reports
- Erhalt von Email-Alerts und SMS-Notifications
- Aktivierung und Deaktivierung weiterer Domains und Subdomains (inkl. der dahinterliegenden IP-Adressen)
- Erteilung einer rechtlich verbindlichen Permission To Attack (siehe „2.3 Permission To Attack“)
- Anlegen weiterer Administratoren

2.3 Permission To Attack

Bevor die in der Servicebeschreibung erläuterten „intrusiven Security-Scans“ durchgeführt werden können muss der Kunde bzw. ein Administrator die rechtlich verbindliche Zustimmung erteilen, dass die zu aktivierenden 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.

Der Kunde bzw. ein Administrator kann das Hinzufügen von weiteren, bzw. das Löschen von bereits aktivierten Domains und Subdomains über das Offensity Dashboard durchführen. Diese fallen automatisch unter die davor bereits erteilte domain-basierte Permission To Attack.

Sollte die Permission To Attack zum Zwecke erweiterter Prüfungen über Domains hinaus erweitert werden müssen (z.B. im Rahmen der in der Servicebeschreibung unter Punkt 4 beschriebenen „Zusatzleistungen“), kann die Permission To Attack schriftlich durch einen Administrator erteilt werden. Dies könnte beispielsweise bei IP-basierten Zielen, internen Netzwerken oder für die Freigabe zu Social Engineering-

Kampagnen notwendig sein, etwa im Zuge von erweiterten Leistungspaketen. Eine erteilte Permission To Attack gilt – sofern durch den Kunden schriftlich kommuniziert – in einem festgelegten Zeitrahmen, alternativ bis zum Ende der Vertragslaufzeit oder bis zum Widerruf.

2.4 Technische Voraussetzungen

Darüber hinaus sind für die Nutzung von Offensity folgende Voraussetzungen seitens des Kunden zu erfüllen, die nicht Produktbestandteile sind:

- Eine aufrechte Internetverbindung
- Internet Browser (Microsoft Edge, Firefox, Chrome)

3. Leistungen von A1 Digital International GmbH

3.1 A1 Digital Serviceauskunft

Dieses Service beinhaltet Auskunft über die Serviceverfügbarkeit und behandelt sämtliche Fragen zu Rechnungen und Datenschutz.

Sie können eine E-Mail an ask.security@a1.digital senden und erhalten Auskunft über folgende Informationen:

- Serviceverfügbarkeit für Ihr Offensity Service
- Information über die erhaltene Rechnung
- Datenschutzanfragen

Hinweis: In diesem Service sind keine technischen Unterstützungsleistungen enthalten.

4. Serviceverfügbarkeit

Hinweis: In diesem Service sind keine technischen Unterstützungsleistungen enthalten.

- Nutzungszeit: Montag bis Freitag, 09:00-17:00 Uhr.
Die Nutzungszeit ist der Zeitraum, in dem die grundsätzliche Leistung dem Kunden zur Nutzung zur Verfügung steht.
- Beobachtungszeitraum: ein Kalenderjahr
- Verfügbarkeit Offensity: 96%
Die Verfügbarkeit ist das in Prozent ausgedrückte Verhältnis zwischen der Zeit, in der eine vereinbarte Leistung vertragskonform nutzbar war, und

dem Beobachtungszeitraum. Ausschließlich kritische Fehler sind verfügbarkeitsrelevant.

$$\text{Verfügbarkeit [\%]} = \frac{(\text{Beobachtungszeitraum} - \text{nicht verfügbare Zeit})}{\text{Beobachtungszeitraum}} \times 100$$

- Wartungsfenster: Die regelmäßige Wartung von Offensivity Services kann eine geplante Serviceunterbrechung erforderlich machen. Daher werden Unterbrechungen, die zur Wartung des Service erforderlich sind, für einen im Voraus definierten Zeitraum, dem so genannten Wartungsfenster, von Offensivity geplant. Darüber hinaus können von A1 Digital außerordentliche Wartungsarbeiten durchgeführt werden, die außerhalb des Wartungsfensters betriebsnotwendig sind. Fremdverzögerungen können zu einer nicht von A1 Digital zu verantwortenden Verlängerung der Wartungsarbeiten führen. Das Wartungsfenster ist Mittwoch 14:00-18:00.

5. Haftungsausschluss

A1 Digital weist darauf hin, dass die Durchführung von Security-Scans und Penetrationstests 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. Dafür ist die Haftung von A1 Digital ausgeschlossen.

Jede identifizierte Subdomain muss durch den Kunden explizit freigeschalten werden, damit sie gescannt wird. Mit dem Freischalten der Subdomain gibt der Kunde verbindlich bekannt, dass er die Befugnis hat, dahinter liegende IP-Adressen attackieren zu lassen. Bei Änderung der DNS-Einträge auf weitere oder andere IP-Adressen ist der Kunde dazu verpflichtet, die Subdomain zu deaktivieren. Bei Nicht-Deaktivierung, darf Offensivity davon ausgehen, dass der Kunde die Befugnis hat, auch die aktualisierten IP-Adressen zu attackieren.

Alle Fragen betreffend Rechte an den 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 haftet nur bei Vorsatz oder grober Fahrlässigkeit. Die Haftung für entgangenen Gewinn, ausgebliebene Einsparungen, Zinsverluste, mittelbare und Folgeschäden, ideelle Schäden, sowie Schäden aus Ansprüchen Dritter, sowie für



verlorengegangene oder veränderte Daten ist ausgeschlossen. Der Kunde hält weiters die A1 Digital hinsichtlich sämtlicher von Dritter Seite erhobener Ansprüche in vollem Umfang schad- und klaglos – ausgenommen sind Schäden, die in vollem Umfang ursächlich aus der Sphäre von A1 Digital stammen.

Sämtliche technischen Prüfungen und 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.

6. Kündigung, Mindestvertragsdauer

Für alle Offensity Produkte existieren Mindestvertragsdauern gegenüber A1 Digital, die Sie als Kunde während des Kaufprozesses wählen können (monatlich, jährlich). Sofern der Vertrag nicht bis spätestens 5 Tage vor Ablauf der Mindestvertragsdauer oder Verlängerungsbindung gekündigt wird, verlängert er sich um das jeweilige periodische Intervall automatisch. Hinsichtlich Vertragskündigung, Änderungen und Umstellungen gelten die Bedingungen von A1 Digital, im Detail: Allgemeinen Geschäftsbedingungen für Cloud und Software Solutions der A1 Digital.

Im Falle der Kündigung eines Abonnements wird der Zugriff auf die Instanz gelöscht.

7. Datenschutz und Datensicherheit

Das Service wird in Rechenzentren innerhalb Europas betrieben.

Weitere Informationen können unserer Website entnommen werden:

<https://www.a1.digital/at/ueber-a1-digital/datenschutzerklärung/>.

Es gelten die Allgemeinen Geschäftsbedingungen der A1 Digital International GmbH für Auftragsverarbeitung (AGB AVV). Diese finden Sie auf

<https://www.a1.digital/at/ueber-a1-digital/agbs/>.