A1 Digital Incident Response

Servicebeschreibung & -bedingung

Version: 1.2
Datum: 01.02.2024

Inhaltsverzeichnis

1 Allgemeines

Diese Servicebeschreibung und -bedingung gilt ab 01.05.2022. Sie erläutert die Leistungen von A1 Digital Deutschland GmbH (im Folgenden: A1 Digital), welche Ihnen im Rahmen der Durchführung eines A1 Digital Incident Response (im Folgenden: IR) 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/de/agb/.

Kunde von A1 Digital Incident Response kann nur ein Unternehmer im Sinne des § 14 des Bürgerlichen Gesetzbuches (BGB) sein.

2 A1 Digital Incident Response Service

Mit dem IR Service gibt A1 Digital dem Kunden die Möglichkeit, im Rahmen eines Cyber-Security Vorfalls jederzeit und kurzfristig Hilfe durch erfahrene ExpertInnen anzufordern.

A1 Digital setzt derzeit die folgenden Subunternehmer ein:

IKARUS Security Software GmbH (IKARUS).

Sollte eine Weitergabe von Teilaufgaben an den globalen Spezialisten Mandiant Corp. (2318 Mill Road Suite 500 Alexandria, VA 22314 United States) erfolgen, erfolgt dies in vorheriger Absprache mit dem Kunden.

A1 Digital behält sich vor das Service in Englisch zu erbringen.

3 Servicebeschreibung

A1 Digital bietet den Incident Response Service rund um die Uhr, 365 Tagen im Jahr mit einer Reaktionszeit von 4 Stunden an, wenn ein Cyber-Security Vorfall vorliegt bzw. begründet vermutet wird. Voraussetzung für das Incident Response Service ist ein erfolgreiches Onboarding.

Bei einem Cyber Security Vorfall führen Spezialisten eine Erstinvestigation durch, gegebenenfalls kommt es auch zu einer tiefergehenden Analyse mittels Spezialsoftware.

Hierfür werden dem Kunden notwendige Ressourcen bereitgestellt, wenn es zu einem Cyber Security Vorfall kommt. Der Kunde hat somit 24/7 Zugriff auf Ressourcen, die normalerweise kurzfristig nicht zu bekommen sind.

3.1 Onboarding

Vor der eigentlichen Serviceerbringung erfolgt ein einmaliges Onboarding mit einem ersten Security Check, in dem A1 Digital zusammen mit dem Kunden die eingesetzten Applikationen und Systeme und das aktuelle Sicherheits- und Risiko-Niveau ermittelt und sämtliche notwendigen Prozesse einrichtet. Mit Abschluss des Onboardings und des ersten Security Check ist der Incident Response Service verfügbar. Bereits in der Onboarding Phase haben die Kunden die Möglichkeit Vorfälle während der Geschäftszeiten von IKARUS (entsprechend der Website: https://www.ikarussecurity.com) zu melden. Die Unterstützung in dieser Phase erfolgt nach dem Best Effort Prinzip.

3.2 Security Check

Zusammen mit dem Onboarding und in einem jährlich stattfindenden Workshop wird die aktuelle Unternehmens-Struktur und Technologieinfrastruktur des Kunden erhoben und ein Überblick über den Reifegrad des Unternehmens in den verschiedensten Bereichen der IT-Security erstellt. Diese Analyse ermöglicht eine schnelle und zielgerichtete Hilfe im Falle eines Security-Vorfalls.

3.3 Security-Vorfall

Es besteht jederzeit die Möglichkeit, den Incident Response Service zu aktivieren und Hilfe bei der Bearbeitung eines Cyber-Security Vorfalls anzufordern. A1 Digital ist berechtigt hierfür Subunternehmer einzusetzen. Die Reaktionszeit beträgt 4 Stunden ab Eingang der Anforderung.

Security-Vorfälle werden dabei nach einem bewährten 3-Phasen-Modell bearbeitet, um den Kunden schnell und effizient unterstützen zu können.

Phase 1

Nachdem sich der Kunde mit dem Incident Response Team in Verbindung gesetzt hat, wird mit der Erstuntersuchung auf der Basis der vorhandenen Threat Intelligence Plattform begonnen. Es werden z.B.: Log Files analysiert und auf bereits branchenbekannte Indicators of Compromise durchsucht. Je mehr aussagekräftige Informationen und Daten zur Verfügung gestellt werden, desto besser kann die Analyse erfolgen.

Phase 2

Sofern die Untersuchungen der Phase 1 kein eindeutiges Bild ergeben hat, werden in der zweiten Phase mittels Analyse-Software detaillierte Erkenntnisse zum Vorfall in Erfahrung gebracht. Aus diesen Erkenntnissen können drei mögliche Handlungsempfehlungen resultieren:

Handlungsempfehlung 1:

Es handelt sich um ein Ereignis, bei dem keine potenziell schadhafte Software festgestellt werden können. Der Vorgang wird abgeschlossen und die zuvor ausgerollte Analyse-Software wird deinstalliert.

Handlungsempfehlung 2:

Es wird potenziell schadhafte Software gefunden, diese kann jedoch beseitigt werden. Mit Beseitigung wird der Vorgang abgeschlossen und die zuvor ausgerollte Analyse-Software wird deinstalliert.

Handlungsempfehlung 3:

Es wird potenziell schadhafte Software gefunden. Die Beseitigung dieser Software ist jedoch mit erhöhten Risiken verbunden und / oder kann nur mit spezialisiertem Wissen erbracht werden. Daher ist die Unterstützung der SpezialistInnen des Unternehmens Mandiant notwendig.

Phase 3

Bei einem Vorfall, für den die Handlungsempfehlung 3 vergeben wurde, erhält der Kunde ein Angebot zur Einbindung zusätzlicher Ressourcen des Unternehmens Mandiant.

3.4 Berichte und Empfehlungen

Berichte zeigen das Ergebnis der Analyse, den finalen Report und Management Summary auf. Maßnahmen weisen auf Empfehlungen sowie nächste Schritte zur Behebung des potenziellen Security Incidents hin.

4 Kontaktaufnahme

Der Kunde erhält nach der Bestellung eine eigene Rufnummer, um 24/7 telefonisch einen Security-Incident melden zu können. Darüber hinaus ist auch ein 24/7 Kontakt via E-Mail möglich.

Zu beachten ist, dass A1 Digital/IKARUS//Mandiant Techniker ausschließlich mit den technischen Ansprechpartnern des Kunden kommunizieren, welche der Kunde während der Pre-Phase bekannt geben muss.

5 Pakete

A1 Digital Incident Response

Das „A1 Digital Incident Response" Paket inkludiert den Security Check und 24/7 SLA mit 4h Reaktionszeit sowie einen 24 Stundenpool.

Arbeitstunden

Sobald die ExpertInnen aktiv werden, fallen Arbeitsstunden an.

Das Paket „ A1 Digital Incident Response" enthält einmalig 24 Arbeitsstunden" und ermöglicht dem Kunden, mit Security Experten 24/7 in Kontakt zu treten, Cyber Security Vorfälle zu melden und auf für den Kunden reservierte Ressourcen zugreifen zu können.

Zusätzlich benötigte Stunden werden nach den tatsächlichen Aufwänden in Stunden dem Kunden verrechnet.

Nicht genutzte Stunden verfallen und werden bei einer Vertragsverlängerung in das nächste Jahr nicht übernommen.

6 Service Level

Der Service ist 24/7 an 365 Tagen im Jahr verfügbar.

Die Reaktionszeit nach Eingang einer Serviceanforderung beträgt 4 Stunden.

Ausgenommen sind Fälle höherer Gewalt.

7 Leistungsabgrenzungen

Im Standardservice nicht enthaltene Leistungen

- Vor Ort Unterstützung: Der Service nur via Fernwartung erbracht.
- Monitoring: Im Service ist kein Monitoring enthalten. Cyber-Security Vorfälle müssen per Telefon oder per E-Mail an die bekannt gegebenen Kontakte gemeldet werden.
- Systemwiederherstellung: Es erfolgt keine Wiederherstellung von Systemen (z.B. aus Back-Ups).

- Konfigurationen: Es erfolgt keine Konfiguration/Änderung etc. von Hard- oder Software von Drittanbietern.
- Ersatzteile: Es erfolgt kein Einbau von Ersatzteilen für Hardware, die an einem Standort des Kunden eingesetzt wird.
- Wartung: Es erfolgt kein Patchen oder Einspielen von Upgrades oder Updates von Software, die beim Kunden installiert ist.
- Garantie: Es wird nicht garantiert, dass befallene Systeme vollständig bereinigt, gerettet oder wiederhergestellt werden können. Insoferne ist A1 Digital für Schäden oder Geschäftsausfälle jeglicher Art, die durch eine Cyber-Security Attacke oder vergleichbare Bedrohungen entstanden sind, nicht verantwortlich.
- Lizenzen: Der Kunde erwirbt im Rahmen des Incident Response Services keine Software. Die eingesetzte Software kann dem Kunden aber separat zum Kauf angeboten werden.

8 Konditionen und Voraussetzungen

Konditionen und Voraussetzungen für den Incident Response Service

- Mitwirkung des Kunden bei der Planung und Organisation der Support Leistungen.
- Der Kunde hat die notwendigen Kontaktdaten übermittelt.
- Der Kunde hat einen Cyber Security Vorfall an per E-Mail oder Telefon gemeldet.
- Der Fernzugriff auf die IT-Systeme des Kunden ist vollumfänglich möglich.
- Alle notwendigen Benutzerkonten, Informationen und Kennwörter sind verfügbar.
- Der Service ist in den Sprachen Deutsch und Englisch verfügbar.
- 3rd Level TechnikerInnen kommunizieren ausschließlich mit dem technischen IT-Personal des Kunden. Sollte der Kunde über kein eigenes technisches IT-Personal verfügen, so gilt der/die technische Hauptverantwortliche als HauptansprechpartnerIn.

9 Kostenpflichtige Zusatzservices

Im Rahmen des 3-Phasen-Modells können zusätzliche Kosten entstehen.

Hierbei handelt es sich um Spesen oder Kosten für Softwarelizenzen und ggf. deren Installation. Für solche zusätzlichen Leistungen erhält der Kunde ein Angebot.

Zusätzliche Arbeitsstunden werden nach geleistetem Aufwand verrechnet.

10 Leistungsänderung

A1 Digital ist berechtigt, das angebotene Service jederzeit durch technologisch weitgehend gleichwertige Lösungen zu ersetzen, sofern das vertraglich zugesagte Service unberührt bleibt.

11 Datenschutzanhang zur Leistungsbeschreibung

Im Rahmen der Erbringung diesen Services agieren wir als Auftragsverarbeiter (AV) für Ihre personenbezogenen Daten.

Die Kategorien von Daten, die erhoben werden und der Betroffenenkreis können daher je nach Produkt variieren.

Produktname/Beschreibung des Geschäftsvorganges	Sub-Auftragsverarbeiter	Land der Verarbeitung
A1 Digital Incident Response	IKARUS Security Software GmbH	Österreich

Welche Daten werden verarbeitet?

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

☐ Login, Passwörter

Wer sind die Betroffenen?

☒ Vertragspartner Kunde nat. Person
☒ Vertragspartner Kunde jur. Person
☒ Vertragspartner Kunde berechtigter Mitarbeiter
☒ User Enterprise Kunde
☒ sonstiger Ansprechpartner des Vertragspartners
☐ Kinder
☐ Schutzbedürftige Personen (krank_behindert)
☒ Vertragspartner Lieferanten
☒ Vertragspartner Lieferanten Mitarbeiter

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 technischorganisatorischen Maßnahmen sicherzustellen. Es ist dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

- Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;

Zugangskontrolle

- Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen,
- Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

Zugriffskontrolle

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

Trennungskontrolle

- Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden,
- z.B. Mandantenfähigkeit, Sandboxing;

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) Technisch nicht möglich.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

- Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, 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, z.B.: Protokollierung, Dokumentenmanagement;

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

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

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management;

Incident-Response-Management;

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);