A1 Business

A1 Incident Response

Servicebeschreibung

Version: 2.0

Datum: 01.10.2022

A1 Business

Inhaltsverzeichnis

A1 Telekom Austria AG (A1) erbringt das Service „A1 Incident Response" (IR) im Rahmen ihrer technischen und betrieblichen Möglichkeiten nach den Allgemeinen

Geschäftsbedingungen für Solutions von A1 (AGB Solutions) in der jeweils geltenden Fassung, wie im Angebot festgehalten, soweit hier oder im Angebot keine von diesen abweichenden oder ergänzenden Regelungen getroffen werden. Diese Servicebeschreibung gilt für Unternehmen im Sinne von § 1 Konsumentenschutzgesetz in der geltenden Fassung.

Sofern nichts anderes ausdrücklich vereinbart ist, wird das Service als Dienstleistung erbracht, sodass ein besonderes Arbeitsergebnis nicht geschuldet ist; der Kunde trägt die Projekt- und Ergebnisverantwortung. Der Kunde ist verpflichtet, die erbrachten Dienstleistungen unabhängig von der Erreichung eines von ihm etwaig erwarteten Erfolgs nach Aufwand zu den vereinbarten Preisen zu bezahlen.

Die Verfügbarkeit, konkret geschuldeter Leistungsumfang und Leistungsmerkmale sowie

Qualität der einzelnen Dienste ergibt sich aus der Servicebeschreibung. Formlose Erklärungen von Mitarbeitern (auch per E-Mail) sind unwirksam.

1 A1 IR Service

Das IR Service stellt für Unternehmen im Ernstfall eine bedeutsame Maßnahme zur Behebung eines Sicherheitsvorfalls dar, welche rund um die Uhr verfügbar ist.

Durch richtige Reaktionsmaßnahmen, rasche Behandlung und gezielte Analysen kombiniert mit effektiver Abwehr und Bereinigung der kritischen Faktoren sowie schneller Wiederherstellung der Geschäftsservices, trägt das A1 IR Service zur Eindämmung des monetären und reputativen Schadens und Minimierung der Produktionsausfälle in Unternehmen bei.

Mit dem IR Service steht Unternehmen ein 5-Stufen-Plan mit einem bewährten 3-Phasen Modell zur Verfügung und damit wird auf unsere langjährige Erfahrung mit Security Zwischenfällen zurückgegriffen.

2 Partnerschaften

A1 erbringt dieses IR Service in Partnerschaft mit IKARUS Security Software GmbH (IKARUS), sowie Mandiant Corp. (Mandiant), dem globalen Spezialisten für Cyber Security Vorfälle. Teilaufgaben können nach Bestellung vom Kunden und in Absprache zwischen A1 und IKARUS an den Partner Mandiant Corp. (2318 Mill Road Suite 500 Alexandria, VA 22314 United States) weitervergeben werden.

3 Allgemeines

A1 bietet ein 24/7 IR-Service mit 4 Stunden Reaktionszeit beginnend nach dem erfolgreichen Onboarding an. Dieses Service soll Unternehmen die Möglichkeit geben, sich jederzeit direkt an IKARUS zu wenden, wenn im betroffenen Unternehmen ein Cyber Security Vorfall vorliegt bzw. begründet vermutet wird. Spezialisten führen eine Erstinvestigation durch, gegebenenfalls kommt es auch zu einem Software Deployment zur tiefergehenden Analyse.

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

Dieses Dokument beschreibt die Serviceleistungen, die im Preis pauschal inbegriffen sind.

4 Leistungsinhalt des IR-Services

Kunden des IR Services haben die Möglichkeit, sich bei Cyber Security Vorfällen, oder einem begründeten Verdacht darauf, 24/7 direkt an IKARUS zu wenden.

Dem Kunden werden die tatsächlich geleisteten Arbeitsstunden in Rechnung gestellt. Hierfür stehen zusätzlich zu den im jeweiligen IR Paket enthaltenen Stunden, weitere Service Stunden am A1 Marketplace Kundendashboard zur Verfügung. Diese sind pro Stundeneinheit bestellbar.

Die Reaktionszeit beträgt 4 Stunden ab der Meldung des Vorfalls. Innerhalb dieser 4 Stunden wird das 3-Phasen Modell von IKARUS eingeleitet, welches nachfolgend beschrieben wird. A1 unterstützt bei einer etwaigen datenschutzrechtlichen Angelegenheit hinsichtlich einer Meldung an die Datenschutzbehörde.

5 5-Stufen IR-Plan

5.1 Pre-Phasen

5.1.1 Security Check

In einem Kundenworkshop wird die Unternehmens-Struktur und -Technologieinfrastruktur erhoben und ein aufschlussreicher Überblick über den Reifegrad sowie der Resilienz eines Unternehmens in den verschiedensten Bereichen der IT-Security erstellt. Diese Unternehmensbewertung hilft Problemfelder zu identifizieren und Handlungsschritte zu planen. Cyber Sicherheit bedarf adäquater IT-Security Prozesse.

Hiermit ergeben sich Erkenntnisse der Organisation und der IT-Architektur. Außerdem bietet der Workshop dem Kunden Mehrwert und trägt zur Prävention von Cybervorfällen bei. Selbst wenn kein Sicherheitsvorfall passiert, erhält der Kunde eine Zusammenfassung der Empfehlungen zu Erhöhung seiner Sicherheit.

5.1.2 Onboarding

Spätestens vier Wochen nach der offiziellen erstmaligen Beauftragung steht dem Kunden das IKARUS Team im Rahmen eines 24/7 SLA (Service Level Agreement) mit 4h Reaktionszeit zur Verfügung.

Während dieser Transition werden auch sämtliche interne Prozesse bei A1 sowie bei den Partnerschaften eingerichtet, um den Kunden das IR Service entsprechend zur Verfügung zu stellen. Kunden erhalten die Möglichkeit Vorfälle mit einem 8x5 SLA (Service Level Agreement) bei IKARUS während der Geschäftszeiten (entsprechend der Website: https://www.ikarussecurity.com) zu melden. IR Unterstützung erfolgt nach „best effort".

Diese Phase (5.1) dient zur Vorbereitung auf das IR Service, welche innerhalb von 4 Wochen stattfindet.

5.2 3-Phasen IR-Modell

5.2.1 Erstinvestigation

Nachdem sich der Kunde mit dem IKARUS Team in Verbindung gesetzt hat, wird mit der Erstinvestigation begonnen. Es werden z.B.: Log Files analysiert und auf bereits branchenbekannte IOCs (Indicator of Compromise) durchsucht, etc. Je mehr aussagekräftige Informationen und Daten hier zur Verfügung gestellt werden, desto besser kann die Analyse in Absprache mit dem Kunden erfolgen. In Phase 1 wird ein MNDA (Mutual Non-Disclosure Agreement) unterzeichnet.

5.2.2 Tiefenanalyse

Hier erfolgt ein Software Deployment zur tiefergehenden Analyse. Außerdem geht es in dieser Phase um Monitoring, Threat Hunting („Bedrohungssuche") und Remediation (Sanierung bzw. Bereinigung). Es werden detaillierte Erkenntnisse zum Vorfall in Erfahrung gebracht. Auf Basis dieser Erkenntnisse können 3 mögliche Handlungsempfehlungen resultieren:

Action Point 1 (AP1):

Es handelt sich um einen Angriff mit keinen weiteren Ereignissen, die als schadhaft bezeichnet werden können – Case wird geschlossen und Deinstallation der ausgerollten Technologie. Zeithorizont des Engagements – bis zu max. 1 Woche.

Action Point 2 (AP2):

Die Remediation ist vom Umfang und Komplexität her voraussichtlich von IKARUS selbst innerhalb von einer Woche durchführbar. Zeithorizont des Engagements – bis zu max. 1 Woche.

Action Point 3 (AP3):

Die Remediation erreicht Dimensionen, die durch IKARUS Ressourcen allein nicht getragen werden können. Die Situation erfordert zusätzliche, globale Unterstützung von Spezialisten von Mandiant. Es wird nach Abstimmung mit dem Kunden Phase 3 eingeleitet.

5.2.3 Engagement Mandiant

Handelt es sich um einen Cyber Security Vorfall, der von IKARUS als „AP3" klassifiziert wird, erhält der Kunde ein Angebot auf Basis der Kundeninfrastruktur, um zusätzliche, globale Ressourcen von Mandiant einbinden zu können. A1 und IKARUS bleiben auch während der gesamten Phase 3 immer der erste Ansprechpartner für den Kunden. Zeithorizont des Engagements – 1 Woche bis mehrere Wochen.

5.3 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.

6 A1 IR Paket Ausprägungen

6.1 A1 Incident Response Professional

Das „A1 Incident Response Professional" Paket inkludiert den Security Check und 24/7 SLA mit 4h Reaktionszeit sowie einen 24 Stundenpool[1] für die Phase 1 („Erstinvestigation") sowie im Bedarfsfall für die Phase 2 („Tiefenanalyse").

Sind entsprechend dem Cyber Security Vorfall weitere Aufwendungen bzw. IR Phasen notwendig, kommen diese demzufolge mit Punkt 10 (Optional) zur Anwendung.

[1] die den sofortigen Arbeitsbeginn der Expert:innen zu jeder Tages- und Nachtzeit ermöglichen

A1 Business

6.2 A1 Incident Response Enterprise

Das „A1 Incident Response Enterprise" Paket inkludiert den Security Check und 24/7 SLA mit 4h Reaktionszeit sowie einen 24 Stundenpool[1] für die Phase 1 („Erstinvestigation") sowie im Bedarfsfall für die Phase 2 („Tiefenanalyse").

Sind entsprechend dem Cyber Security Vorfall weitere Aufwendungen bzw. IR Phasen notwendig, kommen diese demzufolge mit Punkt 10 (Optional) zur Anwendung.

Zusätzlich beinhaltet „A1 Incident Response Enterprise" das Offensity Security Monitoring Paket „Offensity Professional". Die Leistungen dieses Pakets entnehmen Sie bitte der Servicebeschreibung und den Servicebedingungen von „Offensity Security Monitoring & Reporting".

7 Zeiten der Leistungserfüllung

Der Servicelevel beträgt 24/7[2]
Zeitraum Montag bis Sonntag von 00:00 Uhr bis 24:00 Uhr

8 Reaktionszeit

Die Reaktionszeit beträgt 4 Stunden[2]

9 Kontaktaufnahme

Der Kunde erhält nach der Bestellung eine eigene Rufnummer, um 24/7 telefonisch mit IKARUS in Kontakt treten zu können. Darüber hinaus ist auch ein 24/7 Kontakt via E-Mail möglich.

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

[1] die den sofortigen Arbeitsbeginn der Expert:innen zu jeder Tages- und Nachtzeit ermöglichen
[2] Ausgenommen höherer Gewalt

10 Optional

10.1 Kostenpflichtige Zusatzservices

Im Rahmen des 3-Phasen-Modells können dem Kunden zusätzliche Kosten entstehen. Für sämtliche zusätzlichen Kosten erhält der Kunde ein individuelles Angebot bzw. werden mit dem Kunden abgestimmte und geleistete Aufwände per Ticket System erfasst und verrechnet.

Bei möglichen Zusatzkosten und -aufwände handelt es sich zumeist um zusätzlich notwendige Arbeitsstunden, extra anfallende Spesen bzw. Kosten für zusätzlich benötigte Softwarelizenzen und ggf. deren Ausrollung auf notwendigen Systemen oder angeforderten Service Request betreffend A1 managed Services. Zusätzliche Leistungen sind vom Kunden entweder in Form von weiteren Service Stunden - nach Bedarfseinschätzung durch Ikarus – pro Stundeneinheit zu bestellen, oder werden nach geleistetem Aufwand verrechnet. Darüberhinausgehende Anpassungen werden nach Aufwand verrechnet.

10.2 Zusätzliche Service Stunden

Die Pakete „Incident Response Professional" sowie „Incident Response Enterprise" enthalten einmalig 24 Arbeitsstunden und ermöglichen dem Kunden, mit IKARUS Security Experten 24/7 in Kontakt zu treten, Cyber Security Vorfälle zu melden und auf für den Kunden reservierte IKARUS-Ressourcen zugreifen zu können.

Zusätzlich benötigte Service Stunden können am A1 Marketplace Kundendashboard pro Stundeneinheit bestellt werden[1].

10.3 Einbindung Mandiant

Durch das 3-Phasen-Modell hat der Kunde Zugriff auf reservierte Mandiant-Ressourcen. Sollte dies nötig sein, wird auf Basis der Kunden-Infrastruktur dem Kunden von A1 ein Angebot für die Einbindung von Mandiant übermittelt.

[1] Zusätzlich gebuchte Stunden können nicht wieder reduziert werden. Sollte dennoch im Marketplace der zusätzlich gebuchte Stundenpool reduziert werden besteht kein Anspruch auf Rückerstattung.

11 Vertragsdauer

Der Vertrag wird auf 12 Monate befristet geschlossen. Sofern nicht eine der Parteien, unter Einhaltung einer 3-monatigen Frist vor Ablauf mitteilt, den Vertrag beenden zu wollen, verlängert sich dieser Vertrag jeweils um 12 Monate.

Die Supportstunden aus dem Stundenpool verfallen bei Vertragsbeendigung, Barablöse ausgeschlossen. Bei Vertragsverlängerung wird der nicht verbrauchte Stundenpool, in die nächste Vertragsverlängerung mitgenommen.

12 Verrechnung

Für die Nutzung des Service vereinbaren die Vertragsteile ein Nutzungsentgelt, das einerseits vom gewählten Paket sowie andererseits von den ggf. zusätzlich benötigten Service Stunden abhängt.

Die Abrechnung der IR-Service Pakte und ggf. zusätzlicher Aufwände erfolgt: Jährlich oder monatlich im Voraus bzw. nach Aufwänden.

13 A1 Single Point of Contact (SPOC)

Zusätzlich benötigte Aufwände im Zuge eines Cyber Security Vorfalls können ausschließlich durch vom Kunden genannte autorisierte Mitarbeiter (Pre-Phase definierte Personen) oder bevollmächtigte Personen beim SPOC in Form eines „Service Request" beauftragt werden.

Kontaktaufnahme mit dem SPOC erfolgt per E-Mail oder Webportal.

13.1 Service Request (Serviceauftrag)

Sofern der Kunde ein anderes Service bestellt hat und daher eine spezielle Mitwirkung von A1 erforderlich ist, ist ein Service Request erforderlich.

Service Requests sind nicht im Preis inkludiert und werden ausschließlich gesondert nach Aufwand abgerechnet, zum Beispiel über einen zusätzlichen Stundenpool oder zum jeweils aktuellen Stundensatz gemäß der Liste für Sonstige Dienstleistungen von A1. Zeitfenster

für die Durchführung und eventuell nötige Zeitfenster für Abschaltungen von Systemen werden gemeinsam mit dem Kunden geplant.

13.2 Kontakt A1 SPOC

tech.business-service@a1.net

14 Schnittstelle A1 - Partner

A1 Ticketing System für Einmeldung von Request

15 In IR Paketen nicht enthaltene Leistungen

- Vor-Ort-Unterstützung beim Kunden. Das Service wird nach Vereinbarung mit dem Kunden via Fernwartung erbracht. Vor Ort Termine werden nach eigenem Ermessen und nur in Ausnahmefällen durchgeführt.
- Im Service ist keine proaktive Überwachung der Kundensysteme enthalten. Cyber Security Vorfälle müssen vom Kunden an IKARUS per Telefon oder per Mail an die bekannt gegebenen Kontakte gemeldet werden.
- Es erfolgt keine Wiederherstellung von Kundensystemen (z.B.: aus Back-Ups)[1].
- Er erfolgt keine Konfiguration/Änderung, etc. von Hard- oder Software von Drittanbietern[1].
- Kein Einbau von Ersatzteilen für Hardware, die an einem Standort des Kunden eingesetzt wird.
- Kein Patchen, Einspielen von Upgrades oder Updates von Software, die beim Kunden installiert ist[1].
- A1 und dessen Partner können nicht garantieren, dass befallene Kundensysteme vollständig bereinigt, gerettet oder wiederhergestellt werden können.
- A1 und dessen Partner haften dem Kunden gegenüber nicht für Schäden, Geschäftsausfälle, o.ä. jeglicher Art, die durch eine Cyber Security Attacke oder vergleichbare Bedrohungen entstanden sind.

[1] Ausgenommen hiervon sind A1 managed Service Kunden mit übereinstimmendem Service Vertrag und vorheriger abgestimmter Beauftragung durch den Kunden.

- Der Kunde erwirbt im Rahmen der „Incident Response" Pakete keine Software. Die eingesetzte Software kann dem Kunden aber separat zum Kauf angeboten werden.

16 Konditionen und Voraussetzungen für das 24/7 IR-Service

- Mitwirkung des Kunden in den Pre-Phasen (Security Check sowie Onboarding) sowie bei der Planung und Organisation der Support Leistungen.
- Der Kunde gibt relevante Kontaktdaten und bevollmächtigte Personen sowie Prozesse entsprechend einem ISMS (Information Security Management System) bekannt.
- Cyber Security Vorfälle können an IKARUS per Mail oder Telefon gemeldet werden. Die Kontaktdaten werden dem Kunden vor oder nach der Bestellung des Service übermittelt.
- Der Fernzugriff auf die IT-Systeme des Kunden ist im Bedarfsfall vollumfänglich möglich (aufrechte Internetverbindung mit ausreichender Bandbreite).
- Alle notwendigen Benutzerkonten Informationen und Kennwörter sind verfügbar.
- Die von IKARUS eingesetzten Techniker sind zertifizierte 3rd Level Techniker u.a. für Softwarelösungen von IKARUS, FireEye und Nozomi. Das Service ist in den Sprachen Deutsch und Englisch verfügbar.
- IKARUS 3rd Level Techniker kommunizieren ausschließlich mit technischem IT-Personal des Kunden. Sollte der Kunde über kein eigenes technisches IT-Personal verfügen, so gilt der technische Hauptverantwortliche des Kunden als Hauptansprechpartner für IKARUS.

17 Leistungsänderung

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