IKARUS security software

IKARUS 24/7 incident.response
powered by Mandiant

Servicebeschreibung

Version: 1.2

Datum: 17.09.2021

Inhalt

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna | Phone: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com | Erste Bank Österreich | BIC GIBAATWWXXX | AT142011182122082100 | FN 64708i | Court of Jurisdiction: Vienna | VAT ID: ATU15191405

Allgemeines

IKARUS bietet ein 24/7 Incident Response-Service mit 4 Stunden Reaktionszeit an. Dieses Service garantiert Kunden direkten und schnellen Zugriff auf die IR-Leistungen von IKARUS, wenn im Unternehmen ein Cyber Security Vorfall vorliegt bzw. begründet vermutet wird. IKARUS SpezialistInnen führen eine Erstinvestigation durch, gegebenenfalls kommt es zu einem Software Deployment zur tiefergehenden Analyse. Der letzte Schritt – falls notwendig und vom Kunden gewünscht – ist die Anforderung von globalen Mandiant SpezialistInnen.

IKARUS 24/7 incident.response garantiert im Fall eines Cyber Security Vorfalls unmittelbaren Zugriff auf alle notwendigen Ressourcen – sowohl bei IKARUS, als auch beim Servicepartner Mandiant –, die normalerweise kurzfristig nicht zu bekommen sind. Vorfälle werden nach einem bewährten 3-Phasen-Modell bearbeitet, um Kunden schnell und effizient unterstützen zu können.

Das 24/7 Incident Response („IR“) Service wird durch das Unternehmen IKARUS Security Software GmbH (IKARUS) erbracht. Teilaufgaben können nach Absprache zwischen IKARUS und dem Auftraggeber an den globalen Partner Mandiant Corp. (2318 Mill Road Suite 500 Alexandria, VA 22314 United States) weitervergeben werden. Dieses Dokument beschreibt die Serviceleistungen, die im Kaufpreis pauschal inbegriffen sind, sowie verfügbare zusätzliche Angebote und Leistungen.

Leistungsinhalt des Standardservice

Kunden des Services können sich bei Cyber Security Vorfällen oder einem begründeten Verdacht jederzeit – 24/7 – direkt an IKARUS wenden. Dies gilt auch, wenn das 24/7 IR-Service über einen Partner oder Reseller von IKARUS bestellt wird.

Dem Kunden werden die tatsächlich geleisteten Arbeitsstunden in Rechnung gestellt. Hierfür stehen unterschiedliche Pakete an Stundenpools zur Verfügung. Um Verzögerungen zu vermeiden und damit sich Kunden nicht unter Zeitdruck während eines Sicherheitsvorfalls mit der Bestellung beschäftigen müssen, wird empfohlen, bereits vorab größere Stundenpools zu bestellen. Nähere Informationen dazu erhalten Sie vom IKARUS Vertrieb oder Partner.

IKARUS 24/7 incident.response garantiert allen Kunden eine Reaktionszeit von 4 Stunden ab der Meldung des Vorfalls. Innerhalb dieser 4 Stunden wird das 3-Phasen Modell von IKARUS eingeleitet, das nachfolgend beschrieben wird.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna | Phone: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com | Erste Bank Österreich | BIC GIBAATWWXXX | AT142011182122082100 | FN 64708i | Court of Jurisdiction: Vienna | VAT ID: ATU15191405

Das 3-Phasen IR-Modell von IKARUS

1. Phase: Erstinvestigation

Nach der Kontaktaufnahme mit IKARUS wird innerhalb von 4 Stunden mit der Erstinvestigation auf Basis der IKARUS Threat Intelligence Platform begonnen. Je mehr aussagekräftige Informationen und Daten zur Verfügung gestellt werden, desto besser kann die Analyse in Absprache mit dem Kunden erfolgen.

2. Phase: Software Deployment

In Phase 2 erfolgt zur tiefergehenden Analyse ein Software Deployment von IKARUS. Monitoring, Threat Hunting und Remediation stehen im Vordergrund, es werden detaillierte Erkenntnisse zum Vorfall in Erfahrung gebracht. Aus diesen Erkenntnissen können drei mögliche Handlungsempfehlungen resultieren:

Action Point 1 (AP1):

Es handelt sich um einen Angriff ohne weitere Ereignisse, die als schadhaft zu bezeichnen sind – IKARUS schließt den Case und deinstalliert zuvor von IKARUS ausgerollte Technologien. Zeithorizont des Einsatzes – bis zu max. 1 Woche.

Action Point 2 (AP2):

IKARUS führt eine Bereinigung („Remediation“) der betroffenen Kunden-Systeme durch. Anschließend schließt IKARUS den Case und deinstalliert zuvor von IKARUS ausgerollte Technologien. Zeithorizont des Einsatzes – bis zu max. 1 Woche.

Action Point 3 (AP3):

Die Remediation erreicht Dimensionen, die durch IKARUS Ressourcen allein nicht effizient getragen werden können, und erfordert die zusätzliche Unterstützung der globalen SpezialistInnen von Mandiant. Nach Abstimmung mit dem Kunden wird Phase 3 eingeleitet.

3. Phase: 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 jeweiligen Kundeninfrastruktur, um zusätzliche globale Ressourcen von Mandiant einbinden zu können. IKARUS bleibt auch während der gesamten Phase 3 der erste Ansprechpartner für den Kunden. Zeithorizont des Einsatzes – 1 Woche bis mehrere Wochen.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna | Phone: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com |
Erste Bank Österreich | BIC GIBAATWWXXX | AT142011182122082100 | FN 64708i | Court of Jurisdiction: Vienna | VAT ID: ATU15191405

Kundenonboarding

Unmittelbar nach der erstmaligen Bestellung des IKARUS 24/7 incident.response Services hat der Kunde die Möglichkeit, Cyber Security Vorfälle in einem 8x5 SLA (Service Level Agreement) während der Geschäftszeiten an IKARUS zu melden. Der 8x5 SLA ist für 14 Kalendertage nach Bestellung gültig. Die Geschäftszeiten von IKARUS entnehmen Sie bitte der Website https://www.IKARUSsecurity.com.

Während dieser 14 Kalendertage stimmt IKARUS sämtliche Prozesse darauf ab, dem Kunden den bestellten 24/7 Service zur Verfügung stellen zu können. Dies beinhaltet auch ein vorbeugendes Onboarding beim IR-Partner Mandiant, um eine mögliche Übernahme eines Vorfalls in Phase 3 gewährleisten zu können.

Ab dem 15. Kalendertag nach der Bestellung ist das Onboarding erfolgreich abgeschlossen und dem Kunden steht das IR-Service im 24/7 SLA mit 4 Stunden Reaktionszeit zur Verfügung.

Kontaktaufnahme

Der Kunde erhält nach der Bestellung eine eigene Rufnummer von IKARUS, 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 IKARUS/Mandiant TechnikerInnen ausschließlich mit den technischen AnsprechpartnerInnen des Kunden kommunizieren, die der Kunde bei Bestellung bekannt geben muss.

Optionale kostenpflichtige Zusatzservices

Im Rahmen des 3-Phasen-Modells können dem Kunden zusätzliche Kosten entstehen. Für sämtliche zusätzlichen Kosten erhält der Kunde ein individuelles Angebot vom IKARUS Vertrieb oder ggf. einem IKARUS Partner. Die zusätzlichen Kosten müssen vom Kunden immer vor der Leistungserbringung freigegeben bzw. bestellt werden. IKARUS garantiert volle Kostentransparenz.

Bei den möglichen Zusatzkosten handelt es sich zumeist um zusätzlich notwendige Arbeitsstunden, extra anfallende Spesen oder Kosten für zusätzlich benötigte Softwarelizenzen. Arbeitsstunden werden dem Kunden in Form von Stundenpools, den so genannten „IKARUS get.direct“ Paketen, angeboten.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna | Phone: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com | Erste Bank Österreich | BIC GIBAATWWXXX | AT142011182122082100 | FN 64708i | Court of Jurisdiction: Vienna | VAT ID: ATU15191405

Optional: Stundenpools – IKARUS get.direct

Das Standardservice „IKARUS 24/7 incident.response powered by Mandiant“ zum Basispreis enthält KEINE Arbeitsstunden. Es ermöglicht dem Kunden, mit IKARUS Security ExpertInnen 24/7 in Kontakt zu treten, Cyber Security Vorfälle zu melden und auf für den Kunden reservierte Ressourcen zuzugreifen.

Sobald Phase 1 („Erstinvestigation“) eingeleitet wird, fallen Arbeitsstunden auf Seiten von IKARUS an. Diese müssen in Form von Stundenpools bestellt und entweder zusätzlich zum Standardservice oder in einem Bundle angeboten bzw. verrechnet werden. Ist der Stundenpool aufgebraucht, erhält der Kunde ein Angebot für einen neuen Stundenpool.

Diese notwendigen Stundenpools werden als „IKARUS get.direct“ Pakete angeboten und sind in unterschiedlichen Größen erhältlich. IKARUS empfiehlt, Pakete direkt mit dem IKARUS 24/7 incident.response Service zu bestellen, um bei einem Cyber Security Vorfall keine Zeit mit administrativem Aufwand zu verlieren.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna | Phone: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com | Erste Bank Österreich | BIC GIBAATWWXXX | AT142011182122082100 | FN 64708i | Court of Jurisdiction: Vienna | VAT ID: ATU15191405

Im Standardservice nicht enthaltene Leistungen

- Arbeitsstunden. Das Standardservice enthält keine Arbeitsstunden. Sofern das Standardservice nicht in einem Bundle gemeinsam mit einem inkludierten Stundenpool bestellt wurde, benötigt der Kunde einen Stundenpool („IKARUS get.direct“ Paket), damit IKARUS bei einem Cyber Security Vorfall des Kunden mit Phase 1 beginnen oder weitere Phasen einleiten kann.

- Vor-Ort-Unterstützung. Das Service wird nach Vereinbarung mit dem Kunden via Fernwartung erbracht. Vor Ort Termine werden von IKARUS nach eigenem Ermessen und nur in Ausnahmefällen durchgeführt.

- Monitoring. Im Service ist keine proaktive Überwachung der Kundensysteme durch IKARUS enthalten. Cyber Security Vorfälle müssen vom Kunden an IKARUS per Telefon oder per E-Mail an die bekannt gegebenen Kontakte gemeldet werden.

- Systemwiederherstellung. Es erfolgt keine Wiederherstellung von Kundensystemen (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. IKARUS und dessen Partner können nicht garantieren, dass befallene Kundensysteme vollständig bereinigt, gerettet oder wiederhergestellt werden können.

- Haftung. IKARUS und dessen Partner haften dem Kunden gegenüber nicht für Schäden oder Geschäftsausfälle jeglicher Art, die durch eine Cyber Security Attacke oder vergleichbare Bedrohungen entstanden sind.

- Lizenzen. Der Kunde erwirbt im Rahmen des „IKARUS 24/7 incident.response powered by Mandiant“ Services keine Software. Die eingesetzte Software kann dem Kunden aber separat vom IKARUS Vertrieb oder Partner zum Kauf angeboten werden.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna | Phone: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com |
Erste Bank Österreich | BIC GIBAATWWXXX | AT142011182122082100 | FN 64708i | Court of Jurisdiction: Vienna | VAT ID: ATU15191405

Konditionen und Voraussetzungen für das 24/7 IR-Standardservice

- Mitwirkung des Kunden bei der Planung und Organisation der IKARUS Support Leistungen.
- Der Kunde hat IKARUS seine Kontaktdaten übermittelt.
- Der Kunde hat einen Cyber Security Vorfall an IKARUS per E-Mail oder Telefon gemeldet. Die Kontaktdaten dazu werden dem Kunden von IKARUS vor oder nach der Bestellung des Services 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 TechnikerInnen sind zertifizierte 3rd Level TechnikerInnen u.a. für Softwarelösungen von IKARUS, FireEye und Nozomi. Das Service ist in den Sprachen Deutsch und Englisch verfügbar.
- IKARUS 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 technische Hauptverantwortliche des Kunden als Hauptansprechpartner für IKARUS.
- Das Service läuft – sofern im Kundenvertrag nicht anders geregelt – für 12 Monate und verlängert sich nach Ablauf automatisch um weitere 12 Monate.
- Die Supportstunden aus dem Stundenpool („IKARUS get.direct“) verfallen nach 12 Monaten. Wird allerdings der Kundenvertrag (automatisch oder manuell) um weitere 12 Monate verlängert, so kann der Stundenpool in die nächste Abrechnungsperiode mitgenommen werden. Unter diesen Bedingungen fallen bei der Vertragsverlängerung lediglich die Kosten für das Standardservice an.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna | Phone: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com | Erste Bank Österreich | BIC GIBAATWWXXX | AT142011182122082100 | FN 64708i | Court of Jurisdiction: Vienna | VAT ID: ATU15191405