CyberCompare Whitepaper

Sind Incident Response Retainer ihr Geld wert?

Inhalt

1. Teaser zu Beginn

Dem Themenfeld Incident Response, also der Fähigkeit, nach einem Cyberangriff schnell und effektiv zu reagieren ist vor allem aufgrund der leider populär gewordenen Ransomware-Attacken in den letzten Jahren Relevanz zugekommen. Über sogenannte Retainer können sich Unternehmen Expertise von spezialisierten Security-Anbietern sichern. Im Notfall rückt das Sondereinsatzkommando dann vermeidlich schneller, rund um die Uhr und zu gesicherten Konditionen aus.

Dieses Whitepaper beschreibt die wesentlichen Inhalte und bewertet den Nutzen eines solchen Retainers.

2. Einleitung

Der Markt der Incident Response Anbieter ist groß und wächst kontinuierlich. Das sieht man u.a. an der ständig wachsenden Liste der BSI-zertifizierten sogenannten APT-Response Anbietern mit – Stand Mai 2023 – mittlerweile 40 Unternehmen.

Das Wachstum hat wie immer an freien Märkten v.a. mit der Attraktivität zu tun: hier kann gutes Geld verdient werden, denn quasi jedes Unternehmen ist nach einer Cyberattacke auf externe Expertise angewiesen. Da es in diesen Krisensituationen oft um Existenzen geht und jede Stunde Ausfall signifikante Kosten verursacht, ist der Geldbeutel in Richtung der „Helfer“ natürlich deutlich lockerer und es werden problemlos Stundensätze über 250 EUR bezahlt.

Die technische Expertise in Forensik, das Krisenmanagement und v.a. die Erfahrung sind rar gesäht, so dass v.a. zu Randzeiten die Kapazitäten der Anbieter oft stark ausgelastet sind. Zugleich ist es für jedes Unternehmen attraktiv, wiederkehrende Umsätze in der Bilanz oder gegenüber den Shareholdern auszuweisen, also Subskriptionen (‚Annual Recurring Revenue‘). Aus dieser Situation heraus hat die Branche die Retainer geschaffen bei denen Kunden für eine Jahresgebühr definierte und garantierte Leistungen erhalten. Dabei sollten wir jedoch zum einen das Wort ‚garantiert‘ mit einem Sternchen versehene und im Verlauf noch einmal aufgreifen, zudem wollen wir uns eben im folgenden die Leistungen einmal ganz genau anschauen.

Woher haben wir überhaupt unser Wissen und worauf haben wir unsere Meinungen und Empfehlungen gebildet? Als unabhängige Einkaufsplattform haben wir als Bosch CyberCompare bereits eine Vielzahl an Incident Response Projekten begleiten dürfen. Dabei starten wir gerne bereits in der Konzeptphase. Dort besprechen wir, ob ein Retainer überhaupt erforderlich ist, oder z.B. ein guter Basissupport bereits über die Cyberversicherung abgedeckt ist. Je nach Reifegrad der Gesamt-Security-Strategie kann es zunächst auch vollkommen ausreichend sein, 2-3 Hotline-Rufnummern von Incident Response Anbietern im Notfallkonzept zu haben – idealerweise hat man sich aber bereits vorab kennengerlernt und etwaige Preise vorbesprochen.

3. Was steckt drin?

Zunächst der häufig unterschätze Punkt: das Onboarding Ihres Unternehmens. Hier sehen wir im Vorgehen der Anbieter sehr große Unterschiede, die sich natürlich auch oft im Preismodell widerspiegeln. Oftmals startet der Retainer-Vertrag unmittelbar nach einem einstündigen Call, in dem über alle wesentlichen Aspekte informiert wird (z.B. wir eine Kommunikation im Krisenfall konkret stattfindet). Viele unserer Bosch CyberCompare Kunden fühlen sich damit nicht wohl, da so natürlich keine Bindung zwischen Kunden und Anbieter stattfinden kann. Unsere Empfehlung: investieren Sie hier lieber 2 – 3 Personentage extra oder kombinieren Sie das Onboarding mit einer Übung Ihres Notfallplans. So hat der Anbieter eine faire Chance, Sie und Ihre IT kennenzulernen und wichtige Aspekte zu dokumentieren und ggf. mit Ihnen auch an Verbesserungen von Prävention und Verteidigung zu arbeiten.

Beispiele für wichtige Bestandteile, die Sie typischerweise bei den meisten Anbietern vorfinden:

- Möglichkeit ungenutzte Kontingente in andere Services umzuwandeln (z.B. War Gaming, Penetrationtest, Security Consulting)
- Host & Netzwerk Forensik (Analyse der Betriebssysteme und Netzwerke)
- Detection & Analysis, Malware Analysis & Recovery & Reconstruction (inkl. Entfernen von Malware)
- Post Incident Review (Evaluation des Incident Response Management nach der Bewältigung eines Incident)
- Systeme zur Krisenkommunikation
- Datenverarbeitung in der EU und DSGVO-Konformität

Dagegen 4 Beispiele von Serviceleistungen, die nur bei einigen Anbietern inkludiert sind:

- Gerichtsverwertbare Beweissicherung (Umgang mit Datenträgern unter Dokumentation der Überwachungskette, Gewährleistung einer sicheren Aufbewahrung und Unterstützung überprüfbarer Bit-by-Bit-Kopien von Beweismitteln)
- Krisenkommunikation (intern und extern)
- Übernahme des Projektmanagements
- Rechtsberatung & Datenschutzberatung (wenn, dann über Partner)

Abschließend noch 2 oft nachgefragte Themen, die bei den meisten IR-Anbietern nicht unterstützt werden:

- SLA für Vor-Ort Einsätze (Corona hat gezeigt, dass ein Großteil der Einsätze von Remote zu bewältigen ist. Vor-Ort Einsätze finden natürlich statt, werden aber ungern mit SLA versehen)
- Verhandlungen mit Ransomware-Erpressern (sicherlich erteilen die Profis im Hintergrund Tipps, aber in die Verhandlungen direkt steigt schon aus legalen Gründen kein Anbieter direkt ein)

4. Service Level

Service Level Agreements (SLA) sind ein wesentlicher Vertragsbestandteil v.a. für eine Erstreaktion, nachdem Sie den Anbieter über den kritischen Incident informiert haben. Eine 7x24h Abdeckung sollte bei einem IR Retainer immer inkludiert werden. Eine Erreichbarkeit lediglich zu Geschäftszeiten schränkt aus unserer Sicht den Service zu kritisch ein. Die globale Abdeckung des Anbieters bei international aufgestellten Unternehmen ist in diesem Kontext ein relevantes Kriterium. Dabei sollten Sie aber v.a. die wichtigsten Datacenter im Auge haben und nicht zwangsläufig jedes Werk und Vertriebsstandort direkt mitabdecken wollen. Hier spielt also die Regionalität des Anbieters eine Rolle: bevorzugt man eher einen lokalen Experten, der der Unternehmen ggf. bereits kennt und schnell mit dem Auto vor Ort ist, oder setzt man auf einen globalen Champion, welcher Incident Response als Kerngeschäft betreibt.

Wichtig ist dabei auch die Anzahl der zur Verfügung stehenden IR Analysten. Zahlen kleiner als 5 sollten Sie schon kritisch hinterfragen; gleichzeitig muss das kein K.O.-Kriterium dar-stellen, wenn es sich z.B. um einen sehr guten, lokalen Champion handelt (Tipp: fragen Sie auch, wie viele Retainer/

Kunden parallel von dieser Anzahl an Analysten abgedeckt werden müssen).

Abschließend sollten Sie die gewünschten Sprachen klar definieren, v.a. wenn es um Internationalität geht.

5. Kommerzielle Rahmenbedingungen

Schauen wir auf die wesentlichen Bestandteile eines IR Retainers aus kaufmännischer Sicht:

- Welche Grundkosten pro Jahr und initialen Setupkosten fallen an? Z.B. für Onboarding Workshops oder die Aktivierung des Services? Wie schon erwähnt: starten Sie hier lieber nicht zu knapp – ein zu schlankes Onboarding wirkt sich im Einsatzfall oft negativ aus
- Wie viele Stunden sind pro Jahr bereits inkludiert? Das hängt stark von der Unternehmensgröße und den Anforderungen ab. Erfahrungsgemäß sind 40h pro Jahr oft eine sinnvolle Untergrenze und für den Einstieg ein guter Daumenwert
- Welche Kosten fallen für zusätzliche Stunden in und außerhalb der Geschäftszeiten an?
- Wie ist mit Reisekosten umzugehen?
- Welche Laufzeiten werden angeboten?
- Welcher Teil von ungenutzten Stunden lässt sich für andere Security-Services der Anbieter nutzen?

Tipp: Simulieren Sie die Kosten anhand von für Sie typischen Szenarien über alle angefragten Anbieter hinweg. Also z.B. Gesamtkosten über 3 Jahre mit einem kleinen und einem größeren Vorfall. Nur so erhalten Sie einen realistischen Quervergleich, da die Kostenmodelle der Anbieter sonst zu unterschiedlich sind.

6. Pro und Contra

Die Fähigkeit zur Incident Response benötigt jedes Unternehmen. Aber einen IR Retainer nicht zu besitzen, darf erstmal als nicht-fahrlässig eingestuft werden, also anders, als wenn Sie z.B. keine moderne Endpoint Security nutzen, keinen Notfallplan besitzen, oder keinen Prozess zum Schwachstellenmanagement haben.

Es gibt Pro's und Contra's, welche wir in folgender Tabelle für Sie gegenüberstellen. Dabei

Was spricht für einen Incident Response Retainer Vertrag?	Wie kann man auch ohne IR Retainer „überleben"?
Breite Unterstützung durch Experten im **Krisenfallvon Technik bis Kommunikation**	Das **Notfallkonzept** generell auf dem neusten Stand halten und **interne IR Fähigkeiten** stärken
Gesicherte **Kapazität, kommerzielle Planungssicherheit** und passende **Reaktionszeiten** (z.B. im 7x24-Modell) bei einem **Profi**	Prüfen, ob eine **Basis-Betreuung** bereits in der **Cyber-Police** enthalten ist
In einem „guten" IR-Ansatz **kennt der Anbieter das Unternehmen** bereits in Grundzügen und ist **sehr schnell einsatzbereit**	Gezielt nach **IR-Fähigkeiten** im **aktuellen IT-Dienstleisterportfolio** (z.B. IT-Systemhaus) suchen
In vielen Modellen Möglichkeit der **Umwandlung nicht genutzter Stundenpakete**	Unbedingt eine **IT-Krisenübung** durchführen und/oder einen umfangreichen **PenTest/RedTeaming** mit einem passenden Anbieter
Sinnvolle Verbindung mit weiteren Security-Services möglich. IR-Anbieter als **ganzheitlicher Security-Partner**	**Ansprechpartner** und Telefonnummern im **Notfallkonzept** vermerken

7. Fazit

Wenn Sie bereits eine Cyberversicherung abgeschlossen haben, ist es ratsam, sich zum Einen zu erkundigen, welche Incident Response Services bereits im Vertrag inkludiert sind (auf das Service Level achten) und ob man andernfalls völlig frei bei der Auswahl eines zusätzlichen Partners ist.

Wenn Sie sich mit dem Themenfeld Incident Response auseinandersetzen, sollten Sie parallel auch einmal objektiv auf angrenzende Bereiche schauen und sich selbstkritisch bewerten: wie aktuell, umfassend und dabei doch pragmatisch ist das Notfallkonzept aufgestellt? Wurde dieses Konzept im Idealfall auch schon einmal in einer Krisenübung auf Wirksamkeit geprüft? Und: wie stehen technische Lösungen im Bereich Business Continuity da, wie z.B. das Backupkonzept und Desaster Recovery?

Ob Sie dann einen Retainer abschließen, oder sich über ein gutes Partner-Netzwerk absichern, ist alleine Ihre Entscheidung. Tendenziell lohnt sich aus unserer Bewertung heraus ein IR Retainervertrag in den meisten Fällen, da man sich eben nicht nur die „Absicherung“ einkauft, sondern eben frühzeitig mit dem Thema auseinandersetzt und die Experten des Anbieters schon im Vorfeld mit Ihnen zusammen offene Lücken angehen. Dabei wäre unsere Empfehlung aber immer, im Zweifel mit einem sehr guten Anbieter, aber auch einem sehr kleinen Paket (bezogen auf Stunden und Budget) zu starten. Upgraden können Sie jederzeit.

Abschließend möchten wir aus Gesprächen mit Anbietern heraus noch den Aufruf mitgeben, bei einem relevanten Incident dann auch tatsächlich direkt mit dem IR Anbieter in Kontakt zu treten. Zu oft versuchen Unternehmen die Krisenbewältigung zunächst alleine und kontaktieren den externen Profi erst nach 2 – 5 Tagen. Dabei wird dann nicht nur das Ausfall unnötig verlängert, sondern ggf. auch Spuren und Beweismittel zerstört.

Es sind noch Fragen offen, oder Sie wünschen Beratung zu diesem Thema oder einen konkreten Anbieter- und Angebotsvergleich? Treten Sie gerne mit uns in Kontakt. Bosch CyberCompare unterstützt Sie jederzeit als Ihr Partner. Dabei agieren wir stets Anbieterunabhängig und in Ihrem Interesse.

BOSCH

CyberCompare

Kontaktieren Sie uns!

Gemeinsam steigern Sie Ihre Cybersicherheit von einem transparenten Überblick über Ihre Cyber-Bedürfnisse bis hin zur Auswahl geeigneter Anbieter

Individuum. Pragmatisch. Unabhängig.

Kontaktieren Sie das CyberCompare-Führungsteam

Dr Jannis Stemmann (CEO)

Jannis.Stemmann@bosch.com
Telefon: +49 711 811-44954

Philipp Pelkmann (CTO)

Philipp.Pelkmann@bosch.com
Telefon: +49 711 811-15519

Simeon Mussler (COO)

Simeon.Mussler@bosch.com
Telefon: +49 711 811-19893

Bosch CyberCompare Verbände und Branchenkooperationen

Allianz für Cyber-Sicherheit Partner | Secur|Ty made in Germany | Secur|Ty made in EU | ITSECURITY | TeleTrusT Pioneers in IT security. Bundesverband IT-Sicherheit e.V. | CYBERSECURITY MADE IN EUROPE

Besuchen Sie unsere Website:
www.cybercompare.com