Sophos Rapid Response

Soforthilfe bei Cyberangriffen

Sophos Rapid Response bietet sofortige Hilfe bei einem Cyberangriff.
Ein Expertenteam erkennt und beseitigt aktive Bedrohungen.
Der Service kann von Sophos-Kunden und Nicht-Kunden genutzt werden.

Bei einem Angriff zählt jede Sekunde

Beim Bekämpfen einer aktiven Bedrohung geht es um Zeit: Wurde der initiale Kompromittierungs-Indikator entdeckt, müssen umgehend Reaktionsmaßnahmen erfolgen, damit die Angreifer ihre Ziele nicht erreichen können.

Mit Sophos Rapid Response holen wir Sie schnell aus der Gefahrenzone. Unsere Experten sind rund um die Uhr für Sie aktiv. Per Remote-Zugriff erkennen und analysieren sie Bedrohungen und reagieren auf Vorfälle. Leistungen:

- Schnelles Erkennen, Eindämmen und Beseitigen aktiver Bedrohungen
- Entfernen von Angreifern aus Ihrer Umgebung, um weitere Schäden zu vermeiden
- 24/7 Monitoring und Reaktion, um Ihren Schutz zu optimieren
- Empfehlung von Präventiv-Maßnahmen in Echtzeit, um die Ursache zu bekämpfen
- Schnelle Bereitstellung von cloudbasierten Technologien in Ihrer gesamten Umgebung
- Analyse ergänzender Daten von Drittanbieter-Technologien
- Bedrohungs-Bericht nach dem Vorfall mit detaillierten Informationen zu unserer Vorgehensweise

Leistungen von Rapid Response

Rapid Response bietet neben der Beseitigung des akuten Cyberangriffs eine Reihe weiterer Vorteile:

	Sophos Rapid Response
Eindämmen und Beseitigen von Bedrohungen, mit Information über ergriffene Maßnahmen	✔
24/7 Threat Hunting, Monitoring und Reaktion	✔
Dedizierter Ansprechpartner bei aktiver Bedrohung und direkter Telefon-Support	✔
Analyse zusätzlicher Daten von Drittanbieter-Technologien	✔
Schnelle Bereitstellung mit Konto-Aktivierung am selben Tag	✔
Bericht nach dem Vorfall mit Details zur Vorgehensweise	✔

Kontakt

- RapidResponse@sophos.com
- +49 611 711 867 66

Highlights

- Blitzschnelle Erkennung und Beseitigung aktiver Bedrohungen
- Incident Response und 24/7 Monitoring für 45 Tage
- Dedizierter Ansprechpartner
- Bedrohungs-Bericht nach dem Vorfall mit Details zu unserer Vorgehensweise
- Transparenter Festpreis ohne versteckte Kosten
- Ggf. bei Ihrer Versicherung erstattungsfähig
- Nach Nutzung von Rapid Response bei Wunsch nahtlose Umstellung auf eine Sophos Managed Threat Response (MTR) Subscription möglich

SOPHOS

Aktive Beseitigung von Bedrohungen

Die Sophos Rapid-Response-Experten sind auf die Beseitigung aktiver Bedrohungen spezialisiert. Egal was bei Ihnen vorliegt – eine Infektion, eine Kompromittierung oder ein unbefugter Zugriff, bei dem versucht wird, Ihre Sicherheitskontrollen auszuhebeln: Wir beseitigen das Problem.

Die Sophos Rapid-Response-Experten gehören zum Team des Sophos MDR-Services, das für Kunden 24/7 proaktiv Bedrohungen aufspürt, analysiert und Reaktionsmaßnahmen ergreift.

Keine versteckten Kosten

Traditionelle Incident Response (IR) Services werden stündlich berechnet, und oft wird die Zeit unterschätzt, die zur vollständigen Beseitigung einer Bedrohung erforderlich ist. Das kann teuer für Sie werden. Schlimmer noch: Traditionelle IR-Services werden hierdurch verleitet, Ihnen möglichst viele Stunden in Rechnung zu stellen.

Sophos Rapid Response basiert auf einem Festpreis-Modell ohne versteckte Kosten und wird nach Anzahl der Benutzer und Server in Ihrer Umgebung berechnet. Außerdem wird unser Service remote bereitgestellt. So können wir sofort ohne jede Verzögerung Reaktionsmaßnahmen einleiten. Es liegt in unserem und in Ihrem Interesse, Sie so schnell wie möglich aus der Gefahrenzone zu holen, da Zeit keine Rolle für den Preis spielt.

Schnelle Bereitstellung

Um eine schnellstmögliche Reaktion zu gewährleisten, verteilen wir im Rahmen des blitzschnellen Sophos-Bereitstellungsprozesses auf allen sichtbaren Endpoints und Servern unmittelbar Sophos Agents.

Anschließend entwickeln wir eine Austauschstrategie, bei der bisherige Produkte durch den Einsatz spezieller „Removal"-Programme ersetzt werden. Unser Remote-Team mit Experten für die Bereitstellung erstellt einen individuellen Maßnahmenplan für Sie, bei dem Automatisierungstools zur Massenbereitstellung im gesamten Netzwerk genutzt werden.

Das Team arbeitet gemeinsam daran, den Integritäts-Status des Sophos Agents im gesamten Netzwerk zu optimieren. Dabei stellen unsere Experten sicher, dass Konfigurationen Best Practices entsprechen, um so die Analyse zu beschleunigen.

Vorgehensweise bei Rapid Response

Nachdem der Einsatz von Rapid Response auf Sophos-Seite genehmigt wurde und der Kunde unseren Service-Vertrag akzeptiert hat, werden wir sofort aktiv. Es gibt bei Rapid Response vier Hauptphasen – Onboarding, Triage, Neutralisierung und Monitoring.

Onboarding

- Erstgespräch zum Klären der Kontaktpräferenzen und ggf. bereits getroffener Reaktionsmaßnahmen
- Bestimmen von Ausmaß und Auswirkungen des Angriffs
- Gemeinsames Festlegen eines Reaktionsplans
- Bereitstellung der Service-Software

Triage

- Bestandsaufnahme der Betriebsumgebung
- Aufspüren bekannter Kompromittierungs-Indikatoren oder Angriffsaktivitäten
- Datenerfassung und Einleitung von Analyse-Aktivitäten
- Gemeinsame Erarbeitung eines Plans zum Ergreifen von Reaktionsmaßnahmen

Neutralisierung

- Blockieren des Angreifer-Zugriffs
- Verhinderung weiterer Schäden an Assets oder Daten
- Unterbindung weiterer Datenexfiltration
- Empfehlung von Präventiv-Maßnahmen in Echtzeit, um die Ursache zu bekämpfen

Monitoring

- Für insgesamt 45 Tage ohne zusätzliche Kosten (entspricht MTR Advanced)
- Kontinuierliches Monitoring, um ein erneutes Auftreten zu erkennen
- Bedrohungs-Bericht nach dem Vorfall

Bedrohungs-Bericht

Sobald wir die aktive Bedrohung gegen Ihr Unternehmen beseitigt haben, erhalten Sie einen Bericht, in dem die von uns ergriffenen Maßnahmen und alle Analyse-Ergebnisse detailliert aufgeführt sind. Außerdem enthalten sind Empfehlungen zu langfristigen Maßnahmen, mit denen Sie ein erneutes Auftreten ähnlicher Bedrohungen in Zukunft verhindern können.

24/7 Monitoring and Response nach dem Vorfall

Sobald wir den aktiven Vorfall behoben und die akute Bedrohung beseitigt haben, stellen wir Sie ohne zusätzliche Kosten auf unseren 24/7 MDR-Service MTR Advanced um, bis zum Ende der 45 Tage, die im Service beinhaltet sind.

Sollte die Bedrohung innerhalb dieser 45 Tage zurückkehren oder eine neue Bedrohung auftreten, ergreifen wir weitere Reaktionsmaßnahmen, ohne dass zusätzliche Kosten für Sie anfallen. Wenn ein Angriff bei Ihnen 45 Tage lang aktiv ist, ergreifen wir 45 Tage lang Abwehrmaßnahmen.

Bei Ihnen findet gerade ein Angriff statt?

Kontaktieren Sie uns bitte auf Englisch über eine der beiden folgenden Optionen:

- per E-Mail an **RapidResponse@sophos.com**
- telefonisch über folgende Rufnummer:
  +49 611 711 867 66 (D/AT/CH)

Die Rufnummern für alle anderen Regionen finden Sie unten.

Die KollegInnen sind 24x7 erreichbar. Falls gerade alle Experten im Gespräch sind, erreichen Sie nach 2 Min. die Voicebox. Bitte hinterlassen Sie Ihren Namen, Ihre Rufnummer und eine kurze Beschreibung des Vorfalls in englischer Sprache. Sie erhalten dann so schnell wie möglich einen Rückruf.

Rufnummern für andere Regionen:

USA/weltweit: +1 4087461064

Frankreich: +33 186539880

UK: +44 1235635329

Australien: +61 272084454

Kanada: +1 7785897255

Weitere Informationen unter
sophos.de/rapidresponse

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

22-05-12 DS-DE (DD)

SOPHOS