Sophos Compromise Assessment

Erkennen Sie Cyberbedrohungen, bevor Ihr Geschäft Schaden nimmt

Cyberbedrohungen schlummern oft unerkannt in IT-Umgebungen. Wenn Unternehmen sie erkennen, ist oft schon großer Schaden entstanden. Sophos Compromise Assessment bietet eine schnelle, effektive Methode, um aktuelle oder frühere Angriffsaktivitäten in Ihrer Umgebung zu erkennen, sodass Sie schnell handeln können – bevor Ihr Geschäft geschädigt wird.

Erkennnen Sie verborgene Angriffsaktivitäten

Beim von unserem Expertenteam durchgeführten Sophos Compromise Assessment erkennen wir blitzschnell, ob ein Angreifer Ihre Abwehr durchbrochen hat. Wir bewerten das Risiko für Ihr Unternehmen und geben eine genaue Empfehlung, welche Maßnahmen zur Beseitigung der Bedrohung ergriffen werden sollten.

Dank der umfassenden Erfahrung im Umgang mit modernen, komplexen Bedrohungen können unsere Experten sogenannte Indicators of Compromise (IoCs) erkennen, indem sie eine gezielte Analyse potenziell kompromittierter Assets durchführen. Das Ergebnis ist eine schnelle, genaue Bewertung, die Ihrem Unternehmen hilft, Risiken zu adressieren, Compliance zu wahren und den Betrieb aufrecht zu erhalten.

Sophos Compromise Assessment: Ablauf

Unser Experten-Team kommuniziert in jeder Phase des Assessments direkt mit Ihrem Unternehmen, um Sie über die Art der Bedrohung, das Risiko und die Maßnahmen zu informieren, die ergriffen werden müssen, um den Vorfall zu beheben und die Ursache zu bekämpfen.

1. **Erstes Koordinierungsgespräch** – Zu Beginn des Assessments werden Informationen über die potenzielle Bedrohung ausgetauscht, die wichtigsten Ansprechpartner bestimmt sowie der Bereitstellungsumfang und der Analyseprozess festgelegt.
2. **Bereitstellung von Analysetools** – Es erfolgt eine geführte Installation unserer cloudbasierten Sophos-Plattform. So können Daten auf ausgewählten Geräten sofort erfasst werden und unsere Experten können eine genaue Bewertung des Integritätsstatus vornehmen.
3. **Bedrohungsanalyse und Risikobewertung** – Wird eine aktive Bedrohung gefunden, setzen unsere Experten sofort ein Gespräch mit Ihren wichtigsten Ansprechpartnern an, um das Risiko eines weitreichenden Sicherheitsvorfalls und dringend erforderliche Maßnahmen zu besprechen.
4. **Abschlussgespräch und schriftlicher Bericht** – Sie erhalten eine technische Dokumentation und eine nicht-technische Zusammenfassung. Darin beschrieben sind die Angriffsaktivitäten, das Risiko sowie Empfehlungen zum Beseitigen der Bedrohung und zum Bekämpfen der Ursache.

Alle vier Phasen des Assessments sind in der Regel innerhalb von 7 Tagen nach dem ersten Koordinierungsgespräch abgeschlossen.

Highlights

- Ermitteln Sie schnell, ob ein Angreifer unerkannt in Ihrer Umgebung aktiv ist
- Bewerten Sie das potenzielle Risiko eines weitreichenden Sicherheitsvorfalls
- Kommunizieren Sie in allen Phasen der Analyse direkt mit einem Team von Bedrohungsexperten
- Erhalten Sie eine umfassende Analyse zu Angriffsaktivitäten, eine Risikobewertung sowie Empfehlungen zum Beseitigen der Bedrohung und zum Bekämpfen der Ursache
- Unterstützen Sie Maßnahmen zu Risikomanagement und Compliance sowie Due-Diligence-Maßnahmen im Zusammenhang mit Fusionen und Übernahmen

SOPHOS

Schnelle, gründliche Analyse

Beim Sophos Compromise Assessment erfolgt eine Analyse und Bestimmung verschiedenster Angriffsaktivitäten, darunter:

- Verdächtige Netzwerkaktivitäten
- Laterale Bewegungen
- Anomale und schädliche Dateien
- Automatisierte Malware-Ausführung
- Unbefugte Zugriffe
- Rechteausweitung
- Umgehung der Abwehr
- Diebstahl von Zugangsdaten
- Datenexfiltration
- Nicht verifizierte Skripte

Nach dem Assessment

Bestätigt unser Expertenteam, dass ein Angreifer Ihre Abwehr durchbrochen und Ihre Daten und Ihr Unternehmen kompromittiert hat, gibt es eine Option zum priorisierten Onboarding bei unserem Notfall-Service Sophos Rapid Response. Dieser ergreift Sofortmaßnahmen zum Priorisieren, Eindämmen und Beseitigen der aktiven Bedrohung in Ihrer gesamten IT-Umgebung. Ein hochspezialisiertes Team eliminiert den Angreifer schnell aus Ihrer Umgebung und empfiehlt Echtzeit-Präventiv-Maßnahmen zum Bekämpfen der Ursache.

Werden keine Anzeichen für einen Angriff oder eine konkrete Bedrohung gefunden, können Sie Ihr Unternehmen in Zukunft mit unserem Service Sophos Managed Detection and Response (MDR) schützen. Die Experten unseres MDR-Services sind 24/7 für Sie aktiv, spüren Bedrohungen auf und prüfen potenzielle Vorfälle. Das Team ergreift Maßnahmen, um Bedrohungen zu stoppen, einzudämmen und zu beseitigen, und gibt konkrete Ratschläge, um die Ursache von Vorfällen zu bekämpfen und die Durchsetzung von Sicherheitsvorgaben zu verbessern.

Bei Ihnen findet gerade ein Angriff statt?

Erhalten Sie sofortige Hilfe von Sophos Rapid Response

Bei Ihnen findet gerade ein Angriff statt?

Kontaktieren Sie unseren 24/7 Notfall-Service Sophos Rapid Response. Sophos Rapid Response steht sowohl Sophos-Kunden als auch Nichtkunden zur Verfügung.

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

- per E-Mail an **RapidResponse@sophos.com**
- telefonisch über folgende Nummer: **+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.

Australien: +61 272084454

Frankreich: +33 186539880

Italien: +39 02 947 52897

Kanada: +1 7785897255

Niederlande: +31 162708600

Österreich: +43 73265575520

Schweden:+46 858400610

Schweiz: +41 445152286

Spanien: +34 913758065

USA: +1 4087461064

Vereinigtes Königreich: +44 1235635329

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

2023-06-27 DS-DE (PC)

SOPHOS