Lösungsbroschüre

SOPHOS

Sophos Emergency Incident Response

Umfassende Unterstützung als Komplett-Service – von der Analyse bis zur Wiederherstellung

Soforthilfe bei Cyberangriffen

Wenn Ihr Unternehmen angegriffen wird, zählt jede Sekunde. Im Falle eines Vorfalls benötigen Sie schnelle Maßnahmen, Effizienz sowie interdisziplinäre Sicherheitskenntnisse und Expertise. Zudem benötigen sie Transparenz und Fachwissen über die sich ständig weiterentwickelnde globale Bedrohungslandschaft und die neuesten Taktiken und Techniken der Bedrohungsakteure.

Sophos Emergency Incident Response bietet Soforthilfe bei Cyberangriffen und ergreift schnelle Maßnahmen zum Bewerten, Eindämmen, Analysieren und Bereinigen des Vorfalls. Dank jahrelanger Erfahrung und Expertise in verschiedenen Bereichen können unsere Experten akute Bedrohungen schnell priorisieren, eindämmen und beseitigen, bevor weiterer Schaden entsteht. Sophos nutzt die Erkenntnisse von Tausenden Einsätzen, um empfohlene Verbesserungen und vorbeugende Maßnahmen zu entwickeln, die nicht nur die Ursache des Vorfalls beheben, sondern auch dazu beitragen, Ihre Resilienz gegen zukünftige Angriffe zu erhöhen.

Proaktives Stärken von Abwehr und Sicherheits-Status

Sophos Emergency Incident Response verfolgt einen kollaborativen und interaktiven Ansatz. Dabei wird gemeinsam mit Ihrem Team die Situation schnell beurteilt, die Bedrohung nach Bedarf eingedämmt und beseitigt. Außerdem erhalten Sie direkt umsetzbare Empfehlungen zu Wiederherstellungs-Maßnahmen. Unser Team bietet digitale Forensik, Malware-Analyse, Threat Hunting und Threat Intelligence von den Forschungsteams Sophos X-Ops und Counter Threat Unit, um Bedrohungen zu finden und zu beseitigen. Fachübergreifende Experten (wie Penetrationstester und Bedrohungsforscher) stellen sicher, dass die Risiken umfassend verringert und Schäden repariert werden.

Erkennung und Analyse

Erstkontakt und Analyse

Um eine schnellstmögliche Reaktion zu gewährleisten, konzentriert sich Sophos auf die sofortige Bereitstellung von Agenten auf erkennbaren Assets. Durch diese Remote-Incident-Response-Unterstützung können forensische Daten erfasst werden, um die erste Analyse zu unterstützen, geeignete Eindämmungsmaßnahmen zu entwickeln und den Bedarf an zusätzlichen Technologien zu bestimmen. So sind wir in der Lage, uns während unseres Einsatzes bei Ihnen schnell einen Überblick über die Situation zu verschaffen.

Vorteile für Kunden

- Erweitern Sie Ihr Team um interdisziplinäre Experten für digitale Forensik und Incident Response.
- Minimieren Sie die Auswirkungen eines Vorfalls und das Risiko eines erneuten Auftretens durch umfassendes Wissen zur Bedrohung.
- Erhalten Sie mehr Einblick und detaillierte Informationen, um schnell die richtigen Maßnahmen zu beschließen.

Tiefergehende Analyse

Datenerfassung: Assets, betroffene Services, geschäftliche Auswirkungen und andere Angriffsvektoren werden ermittelt.

Iterative Forensik und Bedrohungsanalyse: Forscher, Threat Hunter, Penetrationstester und Analysten helfen dabei, ein umfassendes Verständnis der Bedrohung zu erlangen.

Wiederherstellungsplanung: Parallel und in Abstimmung mit der Analyse wird mit der Wiederherstellungsplanung begonnen.

Reduzieren der Angriffsfläche: Sophos kann interaktive Einblicke in Bedrohungsakteure bieten, um Kontrollen zu validieren und zusätzliche Wiedereintrittspunkte zur umfassenden Risikominderung zu identifizieren.

Lösegeldverhandlungen: Mit ihrer umfangreichen Erfahrung unterstützen unsere Ransomware-Experten Sie bei Lösegeldverhandlungen und geben Empfehlungen zum sicheren und kosteneffizienten Wiederherstellen von Daten.

Bereinigung

Absicherung und Validierung

Gezielte Härtung der Sicherheit: Das Incident-Response-Team leitet und begleitet die taktische Härtung von Sicherheitskontrollen, um ein erneutes Eindringen des Angreifers zu verhindern.

Eindämmung: Unterbindung der Command-and-Control-Kommunikation des Angreifers.

Entfernen des Angreifers: Um den Angreifer dauerhaft aus einem isolierten Netzwerk zu entfernen, ist eine koordinierte Beseitigung seiner Angriffsmechanismen sowie ein Zurücksetzen kompromittierter Domänen erforderlich.

Wiederherstellung

System- und Datenwiederherstellung: Um beim Wiederaufbau von Systemen, der Datenbereinigung und der Wiederinbetriebnahme von Systemen zu helfen, arbeitet das Sophos Incident Response Team mit verlässlichen Partnern zusammen, die Wiederherstellungs-Services nahtlos und sicher bereitstellen.

Host-Validierung: Mit unserer branchenführenden Agent-Technologie stellen wir sicher, dass wiederhergestellte Hosts produktionsbereit sind.

Follow-up

Optimierung

Basierend auf den umfangreichen Erfahrungen aus tausenden Incident-Response-Einsätzen gibt Sophos Empfehlungen für bessere Reaktionsmaßnahmen und zur Entwicklung und Umsetzung einer Security-Roadmap.

Nach Abschluss des Einsatzes stellen wir Ihnen auf Wunsch einen ausführlichen Bericht zur Verfügung – mit vollständiger Dokumentation der ergriffenen Maßnahmen, Analyseergebnissen und konkreten Empfehlungen zur nachhaltigen Risikominimierung.

Leistungen

- Schnelle Erkennung und Beseitigung aktiver Bedrohungen.
- Schnelle Implementierung von Technologien.
- Erfassung und Analyse digitalforensischer Daten, um Kompromittierungs-Indikatoren zu erkennen und Angreifer-Aktivitäten nachzuverfolgen.
- Threat Hunting zum Identifizieren von Aktivitäten durch Bedrohungsakteure.
- Technische Unterstützung und Beratung bei Vorfällen – remote und vor Ort.
- Akkreditiertes globales Incident Response Team mit Expertise für gängige und außergewöhnliche Cyberbedrohungs-Szenarien.
- Vorfallsspezifische Bedrohungsdaten und Einblicke in aktuelle Methoden von Angreifern.
- Professionelle Lösegeldverhandlung.
- Bericht zum Vorfall mit Details zu den durchgeführten Maßnahmen, Erkenntnissen und Empfehlungen.

Warum Sophos für Incident Response?

Sophos bringt umfangreiche Erfahrung in jedes Cybersecurity-Notfall-Szenario ein. Wir bieten umfassende Incident-Response-Services für Unternehmen und Organisationen unterschiedlichster Größen und Branchen für verschiedenste Arten von Vorfällen – von gezielten Angriffen auf einzelne Systeme bis hin zu großflächigen Sicherheitsvorfällen, die kritische Geschäftsprozesse beeinträchtigen oder lahmlegen.

Unser erfahrenes Incident Response Team vereint Fachwissen aus nationalen, militärischen und organisatorischen Computer Security Incident Response Teams (CSIRTs), Strafverfolgungsbehörden und Geheimdiensten. Die Experten kombinieren praxisnahe Erfahrung, Bedrohungsanalysen unserer X-Ops- und Counter Threat Units, Ergebnisse aus Sicherheitstests und -bewertungen sowie fundierte Sicherheitsanalytik – für schnelle Untersuchungen und eine sichere Wiederherstellung.

Bei Ihnen findet gerade ein Angriff statt?

Kontaktieren Sie unsere Incident-Response-Experten über die untenstehende E-Mail-Adresse oder über die Rufnummer für Ihre Region.

E-Mail: EmergencyIR@sophos.com

Deutschland: +49 61171186766

Österreich: +43 73265575520

Schweiz: +41 445152286

Frankreich: +33 186539880

Italien: +39 02 94752 897

Großbritannien und Nordirland: +44 1235635329

USA: +1 4087461064

Kanada: +1 7785897255

Australien: +61 272084454

Falls kein Incident-Response-Experte erreichbar ist, hinterlassen Sie bitte eine Nachricht, damit wir Sie so schnell wie möglich zurückrufen können.

Weitere Informationen unter

sophos.de/emergency-response

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

2025-06-04 BRDE (MP)

SOPHOS