SOPHOS

Vier Insider-Tipps von Incident-Response-Experten

Wie Sie schon im Vorfeld effektiv für den Ernstfall planen

Auf einen kritischen Cybersecurity-Vorfall reagieren zu müssen, setzt viele Sicherheitsteams unter enormen Stress. Sich von der erzeugten Drucksituation komplett zu befreien, ist leider ein Ding der Unmöglichkeit. Doch mit unseren Insider-Tipps von Incident-Response-Experten wird Ihr Sicherheitsteam bei der Verteidigung Ihres Unternehmensnetzwerks schnell wieder die Oberhand gewinnen.

Dieser Guide erläutert die wichtigsten Regeln, die jedes Team bei der Reaktion auf Cybersecurity-Vorfälle beherzigen sollte. Diese basieren auf den realen Erfahrungen der Incident-Response-Experten von Sophos, die bereits auf Tausende von Cybersecurity-Vorfällen reagiert und diese erfolgreich neutralisiert haben.

Tipp 1: Reagieren Sie so schnell wie möglich

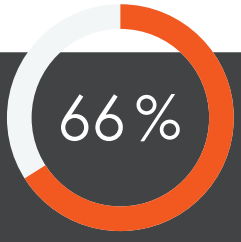
Wenn ein Unternehmen angegriffen wird, zählt jede Sekunde.

Es gibt einige Gründe, warum Teams nicht schnell genug reagieren. Häufig wird die Schwere der Situation verkannt und folglich nicht schnell genug reagiert.

Angreifer schlagen gerne zu den ungünstigsten Zeitpunkten zu: an Feiertagen, an Wochenenden und mitten in der Nacht. Da die meisten Incident-Response-Teams deutlich unterbesetzt sind, kann dies verständlicherweise zu einer „Darum kümmern wir uns morgen"-Mentalität führen. Aber leider kann es morgen zu spät sein, um die Folgen des Angriffs noch abzumildern.

Überforderte Teams neigen außerdem dazu, eher schleppend auf Angriffsindikatoren zu reagieren, da wichtige Signale in der Flut irrelevanter Warnmeldungen untergehen. Selbst wenn zunächst ein Fall geöffnet wird, wird dieser möglicherweise nicht richtig priorisiert, weil es an der nötigen Transparenz mangelt oder zu wenig Kontext vorliegt. Das kostet Zeit, die sich Unternehmen bei der Reaktion auf Vorfälle nicht leisten können.

Selbst wenn das Sicherheitsteam weiß, dass das Netzwerk angegriffen wird und sofort gehandelt werden muss, fehlt es den Verantwortlichen möglicherweise an der notwendigen Erfahrung, um schnell genug über die nächsten Schritte zu entscheiden. Diesen Problemen begegnen Sie am besten, indem Sie im Vorfeld für den Ernstfall planen.



Fast zwei Drittel aller Unternehmen hatte im letzten Jahr Ransomware auf ihren Systeme – und bei 65 % dieser Vorfälle gelang es Angreifern, Daten zu verschlüsseln.[1]

Tipp 2: Geben Sie keine verfrühten Erfolgsmeldungen aus

Bei der Reaktion auf Vorfälle reicht es nicht aus, nur die Symptome zu bekämpfen. Auch die Ursache muss behandelt werden.

Wenn eine Bedrohung entdeckt wird, erfolgt zunächst eine Triage des unmittelbaren Angriffs. Dies könnte bedeuten, eine ausführbare Ransomware oder einen Banking-Trojaner zu bereinigen oder die Exfiltration von Daten zu blockieren. Oft stoppen Teams allerdings nur den ersten Angriff und vergessen, der Ursache auf den Grund zu gehen.

Malware erfolgreich zu entfernen und eine Warnmeldung zu löschen, bedeutet jedoch nicht, dass der Angreifer auch aus der Umgebung eliminiert wurde. Vielleicht handelte es sich sogar nur um einen Testlauf des Angreifers, um die Abwehrmechanismen auszuloten. Wenn der Angreifer weiterhin Zugriff hat, wird er wahrscheinlich erneut und noch vernichtender zuschlagen.

Incident-Response-Teams müssen sicherstellen, dass sie die Grundursache des abgewehrten Erstvorfalls beheben. Hat der Angreifer immer noch Zugriff auf die Umgebung? Ist eine zweite Angriffswelle geplant? Incident-Response-Experten, die bereits Tausende von Angriffen behoben haben, wissen, wann und wo genauere Analysen erforderlich sind. Sie suchen nach allen nur erdenklichen Hinweisen, die Angreifer im Netzwerk hinterlassen und ergreifen entsprechende Gegenmaßnahmen.

So konnten die Incident-Response-Experten von Sophos beispielsweise in einem Fall einen aktiven Angriff stoppen, bei dem die Angreifer ganze dreimal über einen Zeitraum von neun Tagen versuchten, ein Unternehmen mit Ransomware zu attackieren.

Da das Unternehmen noch kein Sophos MDR-Kunde war, wurde zunächst das Sophos Rapid-Response-Team beauftragt.

In der ersten Angriffswelle (die letztlich durch die Endpoint-Protection-Lösung des Unternehmens blockiert wurde) attackierten Angreifer gezielt 700 Computer mit Maze-Ransomware und stellten eine Lösegeldforderung in Höhe von 15 Mio. US-Dollar. Nachdem das Sicherheitsteam des Unternehmens das Ausmaß des Angriffs erkannt hatte, zog es die Experten vom „Sophos Managed Detection and Response (MDR)"-Team hinzu.

Die Incident-Response-Experten von Sophos ermittelten schnell das kompromittierte Administratorkonto, identifizierten und entfernten mehrere Schaddateien und blockierten die Befehle und die Kommunikation der Angreifer mit C2 (Command and Control). Das Sophos MDR-Team war anschließend in der Lage, zwei weitere Angriffswellen abzuwehren. Hätten die Angreifer Erfolg gehabt und hätte das Opfer gezahlt, hätte dies eine der höchsten Lösegeldzahlungen aller Zeiten werden können.

In einem anderen Fall reagierte das Sophos MDR-Team auf eine potenzielle Ransomware-Bedrohung, erkannte aber schnell, dass es keine Hinweise auf Ransomware gab. An diesem Punkt hätten einige Teams den Fall zu den Akten gelegt und sich anderen Aufgaben gewidmet. Das Sophos MDR-Team führte jedoch weitere Analysen durch und kam einem historischen Banking-Trojaner auf die Spur. Zum Glück für den Kunden war diese Bedrohung nicht mehr aktiv. Das Beispiel zeigt jedoch, warum es so wichtig ist, sich nicht nur den ersten Symptomen zu widmen, sondern auch der eigentlichen Ursache auf den Grund zu gehen. Denn gerade diese kann entscheidende Hinweise auf einen groß angelegten Angriff liefern.

Tipp 3: Sorgen Sie für vollständige Transparenz

Nichts macht die Verteidigung eines Unternehmens komplizierter, als während des Angriffs aufgrund mangelnder Transparenz praktisch „blind" zu sein. Es ist wichtig, Zugriff auf hochwertige relevante Daten zu haben, um potenzielle Angriffsindikatoren korrekt identifizieren und der Ursache auf den Grund gehen zu können.

Effektive Teams sammeln relevante Daten, um Signale zu identifizieren. Sie sind in der Lage, die Signale von irrelevanten Informationen zu trennen, und wissen, wie sie diese priorisieren müssen.

Signale erfassen

Bei zu wenig Transparenz über eine Umgebung werden Angriffe schnell übersehen. Im Laufe der Jahre wurden viele Big-Data-Tools auf den Markt gebracht, um diese spezielle Herausforderung zu lösen. Einige verlassen sich auf ereigniszentrierte Daten wie Protokoll-Ereignisse, andere nutzen bedrohungsorientierte Daten und wieder andere verfolgen einen hybriden Ansatz. Das Ziel dabei ist immer das gleiche: Genügend Daten zu sammeln, um aussagekräftige Einblicke für die Analyse und Abwehr von Angriffen zu erhalten, die sonst übersehen würden.

Das Sammeln hochwertiger relevanter Daten aus einer Vielzahl von Quellen gewährleistet vollständige Transparenz über die Tools, Taktiken und Prozesse (TTPs) eines Angreifers. Ansonsten stehen die Chancen schlecht, dass der Angriff in seiner Gesamtheit zuverlässig identifiziert wird.

Irrelevante Daten reduzieren

Aus Angst, dass ihnen im Zweifelsfall nicht alle erforderlichen Daten vorliegen, um sich ein vollständiges Bild von einem Angriff zu machen, sammeln einige Unternehmen (und die Sicherheitstools, auf die sie sich verlassen) einfach alle verfügbaren Daten. Noch mehr Heu auf den Heuhaufen zu werfen, macht es jedoch nicht einfacher, die Nadel im Heuhaufen zu finden. Außerdem erhöhen sich nicht nur die Kosten für die Datenerfassung und -speicherung, sondern es wird auch eine Flut irrelevanter Daten erzeugt, die Sicherheitsteams überfordert. Zudem wird durch eine Vielzahl von False Positives wertvolle Zeit verschwendet.

Kontext berücksichtigen

Es gibt ein Sprichwort unter Threat-Detection-and-Response-Experten: „Inhalte sind der Rolls-Royce, aber Kontext ist der Mercedes." Beide sind für ein effektives Incident-Response-Programm entscheidend. Durch die Anwendung aussagekräftiger Metadaten, die mit Signalen in Zusammenhang stehen, können Analysten feststellen, ob Signale unbedenklich oder schädlich sind.

Eine der wichtigsten Komponenten einer effektiven Bedrohungs-Erkennung und -Reaktion ist die Priorisierung der wichtigsten Signale. Am einfachsten lassen sich die wichtigsten Warnmeldungen mit einer Kombination aus Kontext, von den Sicherheitstools (d. h.Endpoint-Detection-and-Response-Lösungen), künstlicher Intelligenz, Threat Intelligence und der Wissensdatenbank des Bedieners ermitteln.

Der Kontext hilft dabei, den Ursprung eines Signals, die aktuelle Angriffsphase, damit zusammenhängende Ereignisse und die potenziellen Folgen für das Unternehmen zu ermitteln.

Tipp 4: Nehmen Sie Hilfe in Anspruch

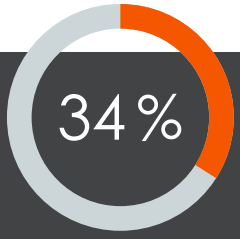
Einen Sicherheitsvorfall effektiv zu bekämpfen, ist keine leichte Aufgabe. Sollte der Ernstfall eintreten, sind Erfahrung und Routine gefragt. IT- und Sicherheitsteams, die unter hohem Druck auf einen Sicherheitsvorfall reagieren müssen, geraten ohne entsprechende Vorbereitung und Spezialkenntnisse schnell an ihre Grenzen – oft mit verheerenden Folgen für das betroffene Unternehmen.

Eines der größten Probleme, mit denen die Cybersecurity-Branche heute konfrontiert ist, ist der Mangel an qualifizierten Mitarbeitern, die in der Lage sind, Vorfälle zu analysieren und auf diese zu reagieren. Laut Angaben von ESG Research2 fehlen 34 % der Unternehmen die entsprechenden Fachkräfte, um bei einem Angriff auf einen Endpoint die Ursache und die Angriffskette zu ermitteln.

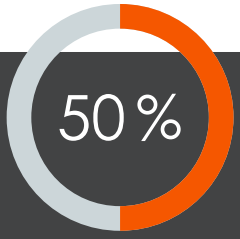
Wie können Unternehmen dem rasanten Anstieg an zunehmend komplexen Bedrohungen Herr werden, ohne massiv in IT-Security-Personal zu investieren? Durch den Einsatz von Managed Security Services. Genauer gesagt: Managed Detection and Response (MDR) Services. MDR-Services sind ausgelagerte Security Operations, die von einem Expertenteam bereitgestellt werden und dabei Aufgaben der IT-Security-Abteilung ihrer Kunden übernehmen. Zu den Serviceleistungen gehören Analysen durch ein Expertenteam, Bedrohungssuche (Threat Hunting), Überwachung in Echtzeit sowie die Reaktion auf Vorfälle, kombiniert mit Technologien zum Erfassen und Analysieren von Bedrohungsdaten. Laut Prognosen von Gartner werden im Jahr 2025 die Hälfte aller Unternehmen MDR-Services nutzen.3 Ein Trend, der aufzeigt, dass immer mehr Unternehmen realisieren, dass sie für den Betrieb eines umfassenden Security-Operations- und Incident-Response-Programms Unterstützung benötigen.

Für Unternehmen, die keinen MDR-Service implementiert haben und auf einen aktiven Angriff reagieren, sind spezielle Incident-Response-Services eine gute Alternative. Incident-Response-Experten werden hinzugezogen, wenn das Sicherheitsteam an seine Grenzen stößt und externe Experten benötigt, um den Angriff zu sichten und sicherzustellen, dass der Angreifer auch wirklich eliminiert wurde.

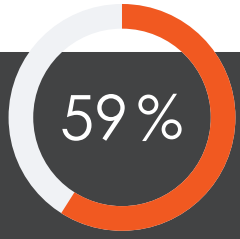
Selbst Unternehmen mit einem Team von erfahrenen Sicherheitsanalysten können von der Zusammenarbeit mit einem Incident-Response-Service profitieren, um Lücken beim Service (z. B. Nächte, Wochenenden, Feiertage) und Fachpersonal zu schließen.



Laut Angaben der Analystenfirma ESG fehlen 34 % aller Unternehmen Fachkräfte, um bei einem Angriff auf einen Endpoint die Ursache und die Angriffskette zu ermitteln.[2]



Im Jahr 2025 werden bereits die Hälfte aller Unternehmen MDR-Services nutzen. Zum Vergleich: 2019 lag der Anteil noch bei unter 5 %.[3]



Bei einer Befragung von 5.600 IT-Entscheidern im Jahr 2022 gaben 59 % an, dass die Komplexität der Angriffe auf ihr Unternehmen im letzten Jahr zugenommen hat.[4]

Wie Sophos helfen kann

Sophos Managed Detection and Response (MDR) Service

Haben Sie Bedenken, dass Ihr Unternehmen nicht gut genug auf schwere Sicherheitsvorfälle vorbereitet ist? In diesem Fall sollten Sie den Sophos Managed Detection and Response (MDR) Service von Sophos in Betracht ziehen.

Unser 24/7 MDR-Service Sophos MDR bietet lückenlose Bedrohungssuche, Detection und Response aus Expertenhand. Das Sophos MDR-Team informiert Sie nicht bloß über Angriffe und verdächtiges Verhalten, sondern ergreift für Sie gezielte Maßnahmen, um selbst hochkomplexe Bedrohungen unschädlich zu machen. Wenn der Ernstfall eintritt, ergreift das Sophos MDR-Team per Remote-Zugriff Maßnahmen zum Stoppen, Eindämmen und Beseitigen der Bedrohung. Darüber hinaus bietet das Team von Security-Operations-Experten konkrete Ratschläge, um die Ursachen wiederholt auftretender Vorfälle zu bekämpfen.

Weitere Informationen finden Sie unter www.sophos.de/mdr

Sophos Rapid Response

Wenn Ihr Unternehmen angegriffen wird und sofortige Unterstützung bei der Reaktion auf Vorfälle benötigt, kann Sophos Ihnen helfen.

Sophos Rapid Response bietet Soforthilfe durch ein Expertenteam beim Erkennen und Beseitigen aktiver Bedrohungen. Das Onboarding beginnt binnen weniger Stunden und die Triage ist in der Regel nach 48 Stunden abgeschlossen. Der Service steht sowohl Sophos-Kunden als auch Nichtkunden zur Verfügung.

Die Experten von Sophos Rapid Response ergreifen per Remote-Zugriff schnelle Maßnahmen zum Priorisieren, Eindämmen und Beseitigen aktiver Bedrohungen. Angreifer werden aus Ihrer Umgebung entfernt, um weiteren Schäden vorzubeugen.

Weitere Informationen finden Sie unter www.sophos.de/rapidresponse

Sophos XDR

Sophos XDR synchronisiert als branchenweit einzige XDR-Lösung native Endpoint-, Server-, Firewall-, E-Mail-, Cloud- und M365-Sicherheit. Verschaffen Sie sich einen ganzheitlichen Überblick über Ihre Unternehmensumgebung – mit umfangreichen Datensätzen und umfassenden Analysen zur Bedrohungserkennung, -analyse und -reaktion sowohl für dedizierte SOC-Teams als auch für IT-Administratoren.

Weitere Informationen und eine kostenlose Testversion finden Sie unter www.sophos.de/xdr

[1] Ransomware-Report 2022 – basiert auf einer unabhängigen Befragung von 5.600 IT-Entscheidern aus 31 Ländern: https://www.sophos.com/de-de/whitepaper/state-of-ransomware
[2] https://www.esg-global.com/blog/soapa-discussion-on-edr-and-xdr-with-jon-oltsik-and-dave-gruber-video-part-1
[3] Gartner, Market Guide for Managed Detection and Response Services, 26. August 2020, Analysten: Toby Bussa, Kelly Kavanagh, Pete Shoard, John Collins, Craig Lawson, Mitchell Schneider
[4] Ransomware-Report 2022 – basiert auf einer unabhängigen Befragung von 5.600 IT-Entscheidern aus 31 Ländern: https://www.sophos.com/de-de/whitepaper/state-of-ransomware

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

© Copyright 2022. Sophos Ltd. Alle Rechte vorbehalten.
Eingetragen in England und Wales, Nr. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, GB
Sophos ist die eingetragene Marke von Sophos Ltd. Alle anderen genannten Produkt- und Firmennamen sind Marken oder eingetragene Marken ihres jeweiligen Inhabers.

22-08-08 WPDE (PC)