



So planen Unternehmen ihre nächste Reaktion auf einen Cyberangriff

In einer Umgebung mit ständig zunehmenden und gezielteren Cyberbedrohungen ist jede Organisation gefährdet. Sophos liefert einen Leitfaden zur proaktiven Planung der Reaktion auf Vorfälle.

Es ist mitten in der Nacht und sie werden von der Nachricht geweckt, dass ihr Unternehmen von Ransomware angegriffen wurde. Reaktionszeit ist wichtig – die Entscheidungen, die sie in den folgenden Sekunden, Minuten und Stunden treffen, haben langfristige operative und regulatorische Konsequenzen, die sich grundlegend auf den Unternehmensbetrieb und damit auch ihren geschäftlichen Ruf auswirken.

Dies ist kein hypothetisches Szenario – es ist eine zunehmend alltägliche Realität für Unternehmen, da Cyberangriffe – einschließlich Ransomware – immer häufiger und komplexer werden. Als Reaktion darauf nutzen viele Organisationen Cybersecurity-as-a-Service (CSaaS), ein Sicherheitsmodell, bei dem externe Spezialisten Unternehmen dringend benötigte Expertise, Abwehrmaßnahmen und Eingriffe auf Abruf bieten. Durch die Auslagerung aller Sicherheitsoperationen oder die Verstärkung bestehender Teams können Unternehmen rund um die Uhr Bedrohungssuche, -erkennung und -reaktion sicherstellen. Ermöglicht wird dies durch Managed Detection and Response (MDR), einem zentralen CSaaS-Angebot.

Aber MDR ist nur die halbe Miete. Unternehmen benötigen außerdem detaillierte Pläne zur Reaktion auf Vorfälle, um von CSaaS-Modellen voll profitieren zu können. Strategische Vorbereitungen ermöglichen schnelles Handeln in Krisenzeiten und optimieren die Zusammenarbeit mit Managed Service Providern (MSPs) und MDR-Partnern. Mit MDR und ganzheitlicher Reaktionsplanung können Unternehmen einen vollwertigen Sicherheitsbetrieb aufbauen, der gegen die immer stärker werdenden Bedrohungen gewappnet ist.

MDR ist der Eckpfeiler der Incident-Response-Planung

Aktive Cyberattacken können für die Verantwortlichen in Unternehmen schnell überwältigend werden. Wenn, bildlich gesprochen, die Sirenen heulen, kann es kompliziert und stressig sein, mehrere Anbieter, Beteiligte und Bereitstellungstools zu verwalten und effektiv zu nutzen. Ohne die Hilfe durch einen Incident-Response-Plan ist es für die Verantwortlichen schwierig, die Schwere eines Angriffs einzuschätzen und alle Rollen und Aufgaben während des gesamten Wiederherstellungsprozesses abzustimmen.

Eine fehlende interne Ausrichtung und Planung verlängert die Reaktionszeit entscheidend, da die Geschäftsführung im Fall der Fälle erst einmal Prozesse klären und feststellen muss, wer in welchem Bereich die Entscheidungsbefugnis hat. Ohne einen Incident-Response-Plan kann es sogar unklar sein, wer im Falle eines Angriffs zu benachrichtigen ist. Im Gegensatz dazu ermöglicht die proaktive Entwicklung von Reaktionsplänen, verschiedene Aktivitätsprotokolle durch Scheinszenarien und Übungen zu evaluieren. Diese Praxis hilft Organisationen, ihre „Reaktionsmuskeln“ für eine Cyberattacke zu stärken und Probleme mit bestehenden Prozessen zu identifizieren.

Ein Incident-Response-Plan gibt den Beteiligten auch die Möglichkeit, eine interne Ausrichtung aufzubauen und sich auf die Integration ausgelagerter MDR-Services vorzubereiten. Angetrieben von einer von Menschen geführten Bedrohungssuche, die in großem Maßstab

durchgeführt wird, stellt MDR sicher, dass Vorfälle schneller entdeckt und damit von vornherein weniger wahrscheinlich sind. Im schlimmsten Fall, wenn Vorfälle auftreten, reduziert die On-Demand-Intervention von MDR-Partnern die Schwere der Auswirkungen. Während des gesamten Incident-Response-Prozesses – von der anfänglichen Erkennung, Eindämmung und Neutralisierung von Bedrohungen bis hin zur Entfernung von Angreifern aus dem Netzwerk – müssen interne Entscheidungsträger, MSPs und MDR-Partner zusammenarbeiten, um die geschäftlichen Auswirkungen abzuwägen und die nächsten Schritte festzulegen. Dies ist das Entscheidende an einem ganzheitlichen Plan zur Reaktion auf Cybervorfälle – er stellt sicher, dass alle Beteiligten ihre Rollen während des gesamten Wiederherstellungszyklus verstehen. Dieser Ansatz ermöglicht auch eine optimierte Beziehung zwischen den Parteien, was letztendlich zu einer schnelleren Neutralisierung von Bedrohungen führt.



5 Schritte für eine gründliche Planung der Reaktion auf Cybervorfälle

Unternehmen sollten nicht bis nach einem Cyberangriff warten, um in eine ganzheitliche Planung der Reaktion auf Vorfälle zu investieren. Angesichts der steigenden Zahl von Ransomware-Angriffen und der Zunahme stark kollaborativer Angriffsmodelle ist jede Organisation ein Ziel. Das Sophos Incident Response Team empfiehlt die folgenden fünf Schritte, um eine solide interne Ausrichtung und optimierte Zusammenarbeit mit externen Experten sicher zu stellen:

1. Bleiben Sie agil. Denken sie daran, dass einige Aspekte ihres Incident-Response-Plans einen flexiblen Ansatz erfordern. Auch wenn eine solide Planung vorhanden ist, sollten sie darauf vorbereitet sein, sich an neue Bedrohungsentwicklungen anzupassen – und ihren Incident-Response-Plan gegebenenfalls auch entsprechend anzupassen.
2. Priorisieren sie die teamübergreifende Zusammenarbeit. Cyberangriffe betreffen alle Aspekte ihres Unternehmens. Stellen sie sicher, dass alle Teams – einschließlich Finanzen, Recht, Marketing und IT – an der Entscheidungsfindung und Risikobewertung beteiligt sind.
3. Sorgen sie für eine gute Hygiene der IT-Umgebung. Eine solide IT-Umgebungshygiene minimiert die Wahrscheinlichkeit von Vorfällen – überprüfen sie daher routinemäßig ihre Sicherheitskontrollen und beheben sie ungepatchte Schwachstellen wie offene RDP-Ports (Remote Desktop Protocol) so schnell wie möglich.
4. Halten sie immer eine physische Kopie ihres Incident-Response-Plans bereit. Wenn ihre Organisation von Ransomware betroffen ist, könnten sich digitale Kopien der Anweisungen unter den verschlüsselten Dateien befinden.
5. Nutzen sie MDR-Spezialisten mit Erfahrung in der Reaktion auf Vorfälle. Selbst erfahrene interne Sicherheitsteams profitieren von MDR-Betriebsteams mit umfassenden Branchenkenntnissen. Diese Anbieter sind mit den spezifischen Bedrohungen, denen sie ausgesetzt sind, bestens vertraut und wissen, wie sie schnell und effektiv reagieren können.

Social Media von Sophos für die Presse

Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf  und 

LinkedIn: <https://www.linkedin.com/groups/9054356/>

Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de