SOPHOS

bitbone

INCIDENT RESPONSE GUIDE

Wie Sie sich mit einem Incident-Response-Plan effektiv auf Cybersecurity-Angriffe vorbereiten

„Vor allem die Vorbereitung ist der Schlüssel zum Erfolg."

Alexander Graham Bell

bitbone AG
Prymstraße 3 | 97070 Würzburg
T: +49 931 250993-12
M: sales@bitbone.de

www.bitbone.de

Wie verhindern Sie am effektivsten, dass sich ein Cyberangriff zu einer weitreichenden Sicherheitspanne entwickelt? Planen Sie im Vorfeld für den Ernstfall.

Nach einer Sicherheitspanne stellen Unternehmen oft fest, dass ihnen ein effektiver Incident-Response-Plan für Cybersecurity-Vorfälle viel Kosten, Probleme und Betriebsunterbrechungen erspart hätte.

Dieser Guide soll Sie bei der Aufstellung Ihres eigenen Incident-Response-Plans unterstützen, damit Sie im Bedarfsfall bestmöglich auf Vorfälle reagieren können. Diese Empfehlungen basieren auf den realen Erfahrungen der Teams Sophos Managed Threat Response und Sophos Rapid Response, die zehntausende Stunden Erfahrung im Umgang mit Cyberangriffen gesammelt haben.

Incident-Response-Plan für Cybersecurity-Vorfälle

Berücksichtigen Sie bei der Erstellung Ihres Incident-Response-Plans die folgenden 10 Punkte:

Incident-Reponse-Plan in 10 Schritten

1. Wichtigste Stakeholder bestimmen
2. Kritische Ressourcen identifizieren
3. Ernstfall durchspielen
4. Security-Tools bereitstellen
5. Für maximale Transparenz sorgen
6. Zugriffskontrolle implementieren
7. In Analyse-Tools investieren
8. Reaktionsmaßnahmen festlegen
9. Awareness-Trainings durchführen
10. Managed Security Service in Anspruch nehmen

1. Wichtigste Stakeholder bestimmen

Für die ordnungsgemäße Vorbereitung auf einen potenziellen Sicherheitsvorfall ist nicht allein Ihr Sicherheitsteam verantwortlich. Tatsächlich wird sich ein Vorfall wahrscheinlich auf fast jede Abteilung in Ihrem Unternehmen auswirken, insbesondere dann, wenn sich der Vorfall zu einer weitreichenden Sicherheitspanne entwickelt. Um Ihre Reaktionsmaßnahmen effektiv zu koordinieren, müssen Sie zunächst festlegen, wer beteiligt werden soll. Häufig werden Vertreter der Geschäftsleitung, der Sicherheits-, IT-, Rechts- und PR-Abteilungen hinzugezogen.

Die Entscheidung, wen Sie in Ihre Planungaktivitäten einbeziehen wollen, sollten Sie bereits im Vorfeld treffen. Darüber hinaus muss eine Kommunikationsmethode eingerichtet werden, um eine schnelle Reaktion zu gewährleisten. Dabei sollte die Möglichkeit berücksichtigt werden, dass Ihre normalen Kommunikationskanäle (z. B. Unternehmens-E-Mails) von einem Vorfall betroffen sein können.

2. Kritische Ressourcen identifizieren

Um Ihre Schutzstrategie zu erarbeiten und im Ernstfall das Ausmaß und die Folgen eines Angriffs bestimmen zu können, müssen Sie ermitteln, welche Ressourcen für Ihr Unternehmen die höchste Priorität haben. Wenn diese Ressourcen schon im Vorfeld klar definiert sind, kann sich Ihr Incident-Response-Team bei einem Angriff gezielt auf unternehmenskritische Ressourcen konzentrieren und Unterbrechungen des Geschäftsbetriebs auf ein Minimum reduzieren.

3. Ernstfall durchspielen

Auch bei der Reaktion auf Vorfälle gilt „Übung macht den Meister". Natürlich ist es schwierig, den intensiven Druck, dem Ihr Team bei einem Sicherheitsvorfall ausgesetzt sein könnte, eins zu eins nachzuspielen. Trotzdem sorgen Theorieübungen dafür, dass Sie im Ernstfall koordinierter und effektiver reagieren können. Neben Theorieübungen (oft im Rahmen von Red-Team-Übungen) sollten Sie jedoch auch weitreichendere Übungen durchführen, in die verschiedene Stakeholder aus dem gesamten Unternehmen mit einbezogen werden.

Im Rahmen von Theorieübungen sollten die Reaktiosmaßnahmen Ihres Unternehmens auf eine Vielzahl möglicher Incident-Response-Szenarien durchgespielt werden. Jedes dieser Szenarien kann auch Stakeholder umfassen, die über das unmittelbare technische Team hinausgehen. Ihr Unternehmen sollte im Voraus festlegen, wer bei der Erkennung eines Angriffs informiert werden muss, auch wenn der Angriff erfolgreich abgewehrt wurde.

Zu den häufigsten Szenarien bei der Reaktion auf Vorfälle gehören:

- **Ein aktiver Angreifer wird in Ihrem Netzwerk erkannt:** In einem solchen Fall ist entscheidend, dass das Response-Team ermittelt, wie ein Angreifer Ihre Umgebung infiltrieren konnte, welche Tools und Techniken verwendet wurden, welche Ressourcen anvisiert wurden und ob Persistenz etabliert wurde. Diese Informationen helfen, die richtige Vorgehensweise zu bestimmen und den Angriff zu neutralisieren.

  Es mag offensichtlich erscheinen, Angreifer so schnell wie möglich aus der Umgebung zu entfernen. Einige Sicherheitsteams entscheiden sich jedoch dafür, den Angreifer zunächst zu beobachten, um wichtige Informationen über seine Ziele und seine Methoden zu sammeln.

- **Datenpanne:** Wenn eine Datenpanne festgestellt wird, sollte Ihr Team ermitteln können, was und wie exfiltriert wurde. Aus diesen Informationen ergibt sich anschließend die angemessene Reaktion, einschließlich der potenziellen Notwendigkeit zur Einhaltung von gesetzlichen und Compliance-Vorschriften, die ggf. eine Benachrichtigung von Kunden oder die Einbeziehung von Rechts- oder Strafverfolgungsbehörden vorsehen.

- **Ransomware-Angriff:** Wenn kritische Daten und Systeme verschlüsselt wurden, muss Ihr Team nach einem Plan vorgehen, um die betroffenen Ressourcen so schnell wie möglich wiederherzustellen. Dazu sollte ein Prozess zur Wiederherstellung von Systemen aus Back-ups gehören. Um sicherzustellen, dass der Angriff nicht wiederholt wird, sobald Sie wieder online sind, sollte das Team untersuchen, ob der Zugriff des Angreifers auch wirklich gekappt wurde. Darüber hinaus sollte eine unternehmensweite Entscheidung darüber getroffen werden, ob Ihr Unternehmen in Extremsituationen bereit wäre, ein Lösegeld zu zahlen, und wenn ja, in welcher Höhe.

- **Kompromittierung eines Systems mit hoher Priorität:** Sollte ein System mit hoher Priorität kompromittiert werden, ist Ihr Unternehmen möglicherweise nicht in der Lage, seinen Geschäftsbetrieb wie gewohnt aufrechtzuerhalten. Zusätzlich zu allen Schritten, die im Rahmen eines Incident-Response-Plans erforderlich sind, sollte Ihr Unternehmen auch die Erstellung eines Business-Recovery-Plans in Betracht ziehen, damit Unterbrechungen des Geschäftsbetriebs im Ernstfall auf ein Minimum reduziert werden.

4. Security-Tools bereitstellen

Am besten schützen Sie sich vor Vorfällen, imdem Sie bereits im Vorfeld Vorkehrungen treffen. Stellen Sie sicher, dass Ihr Unternehmen über geeigneten Schutz für Endpoints, Netzwerk, Server, Cloud, Mobilgeräte und E-Mails verfügt.

5. Für maximale Transparenz sorgen

Ohne die erforderliche Transparenz über alle Vorgänge während eines Angriffs wird Ihr Unternehmen Schwierigkeiten haben, angemessen zu reagieren. Bevor es zu einem Angriff kommt, sollten IT- und Sicherheitsteams sicherstellen, dass sie über das nötige Handwerkszeug verfügen, um das Ausmaß und die Folgen eines Angriffs bestimmen zu können, einschließlich der Ermittlung von Eintrittspunkten und Persistenzpunkten der Angreifer. Um sich vollständige Transparenz zu verschaffen, müssen Sie auch Protokolldaten sammeln, wobei der Schwerpunkt auf Endpoint- und Netzwerkdaten liegt. Viele Angriffe werden erst nach Tagen oder Wochen entdeckt. Daher sollten Sie Verlaufsdaten unbedingt über mehrere Tage oder Wochen (ggf. sogar Monate) speichern und Back-ups erstellen, um im Bedarfsfall zur Vorfallsanalyse darauf zurückgreifen zu können.

6. Zugriffskontrolle implementieren

Angreifer können schwache Zugriffskontrollen ausnutzen, um die Abwehr Ihres Unternehmens zu unterwandern und Berechtigungen auszuweiten. Stellen Sie daher regelmäßig sicher, dass Sie über wirksame Zugriffskontrollen verfügen. Hierzu gehören unter anderem die Bereitstellung einer mehrstufigen Authentifizierung, die Beschränkung von Administrator-Rechten auf möglichst wenige Konten (nach dem Prinzip „Principle of Least Privilege"), die Änderung von Standard-Passwörtern und die Reduzierung der Anzahl der zu überwachenden Zugriffspunkte.

7. In Analyse-Tools investieren

Neben der Sicherstellung der erforderlichen Transparenz sollte Ihr Unternehmen in Tools investieren, die während einer Untersuchung den erforderlichen Kontext liefern.

Zu den am häufigsten verwendeten Incident Response Tools zählen EDR (Endpoint Detection and Response) oder XDR (Extended Detection and Response), mit denen Sie in Ihrer gesamten Umgebung nach Indicators of Compromise (IOCs) und Indicators of Attack (IOA) suchen können. Mithilfe von EDR-Tools können Analysten ermitteln, welche Ressourcen kompromittiert wurden, wodurch sich wiederum Ausmaß und Folgen eines Angriffs bemessen lassen. Je mehr Daten – von den Endpoints und darüber hinaus – erhoben werden, desto mehr Kontext steht für die Analyse zur Verfügung. Dieser Kontext verschafft Ihrem Team mehr Transparenz, um wichtige Fragen zu beantworten: Welche Ressourcen hatten die Angreifer im Visier, wie haben sie sich Zugang zur Umgebung verschafft und besteht die Möglichkeit, dass sie erneut auf die Umgebung zugreifen?

Neben EDR-Tools können moderne Sicherheitsteams auch eine SOAR(Security Orchestration, Automation, and Response)-Lösung zur Unterstützung von Reaktionsworkflows bereitstellen.

8. Reaktionsmaßnahmen festlegen

Einen Angriff zu erkennen, ist nur ein Teil des Prozesses. Um angemessen auf einen Angriff zu reagieren, müssen Ihre IT- und Sicherheitsteams in der Lage sein, eine Vielzahl von Reaktionsmaßnahmen zum Stoppen und Beseitigen von Angreifern einzuleiten. Zu diesen Reaktionsmaßnahmen zählen u. a.:

- Isolieren betroffener Hosts
- Blockieren schädlicher Dateien, Prozesse und Programme
- Blockieren von Command and Control (C2) und schädlichen Website-Aktivitäten
- Einfrieren kompromittierter Konten und Zugriffssperrung für Angreifer
- Beseitigen von Artefakten und Werkzeugen des Angreifers
- Schließen von Eintrittspunkten und Persistenzbereichen, die von Angreifern (internen und externen) genutzt werden
- Anpassen von Konfigurationen (Bedrohungsrichtlinien, Aktivieren von Endpoint-Security und EDR auf ungeschützten Geräten, Anpassen von Ausschlüssen usw.)
- Wiederherstellen betroffener Ressourcen über Offline-Backups

9. Awareness-Trainings durchführen

Kein noch so gutes Trainingsprogramm bietet hundertprozentigen Schutz gegen fest entschlossene Angreifer. Schulungssprogramme (z. B. Phishing Awareness) tragen jedoch dazu bei, Ihr Risiko zu verringern und die Anzahl der Warnmeldungen zu begrenzen, auf die Ihr Team reagieren muss. Mit Tools zur Angriffssimulation können Sie ohne Sicherheitsrisiko reale Phishing-Angriffe auf Ihre Mitarbeiter starten. Diejenigen, die auf die Angriffe hereinfallen, müssen ein Trainingsprogramm absolvieren, und Sie können gezielt Benutzergruppen identifizieren, die weitere Schulungen benötigen.

10. Managed Security Service in Anspruch nehmen

Viele Unternehmen sind nicht in der Lage, ohne fremde Hilfe angemessen auf Vorfälle zu reagieren. Eine schnelle und effektive Reaktion erfordert erfahrene Sicherheitsexperten. Um sicherzustellen, dass Sie die richtigen Maßnahmen ergreifen, sollten Sie ggf. einen externen Dienstleister wie einen MDR-Provider (Managed Detection and Response) hinzuziehen.

MDR-Provider bieten 24/7 Threat Hunting, Analysen und Reaktion auf Vorfälle als Managed Service. MDR-Services helfen Ihrem Unternehmen nicht nur, auf Vorfälle zu reagieren, bevor sich diese zu weitreichenden Sicherheitspannen entwickeln. Sie senken auch die generelle Wahrscheinlichkeit eines Vorfalls. MDR-Services werden immer beliebter: Laut Prognosen von Gartner[1] werden im Jahr 2025 die Hälfte aller Unternehmen MDR-Services nutzen. Zum Vergleich: 2019 lag der Anteil noch unter 5 %.

DFIR(Data Forensic Incident Response)-Services werden gelegentlich auch nach einem Vorfall weiter genutzt, um Beweise zum Geltendmachen eines Rechts- oder Versicherungsanspruchs zu sammeln.

Zusammenfassung

Bei einem Cybersecurity-Vorfall zählt jede Sekunde. Ein gut vorbereiteter und durchdachter Reaktionsplan, den alle betroffenen Parteien sofort umsetzen können, kann die Folgen eines Angriffs auf Ihr Unternehmen erheblich abmildern.

Wie Sophos helfen kann

Der MDR-Service von Sophos: Managed Threat Response (MTR)

Sophos Managed Threat Response (MTR) bietet 24/7 Managed Detection and Response mit Threat Hunting durch ein Expertenteam, als Fully-Managed-Service. Das Sophos MTR-Team informiert Sie nicht bloß über Angriffe und verdächtiges Verhalten, sondern ergreift für Sie gezielte Maßnahmen, um selbst hochkomplexe Bedrohungen unschädlich zu machen.

Unsere Experten übernehmen für Sie folgende Aufgaben:

- Proaktives Aufspüren und Prüfen von potenziellen Bedrohungen und Vorfällen
- Nutzen aller vorliegenden Informationen, um Ausmaß und Schwere von Bedrohungen zu bestimmen
- Anwenden geeigneter Maßnahmen je nach Risiko-Bewertung der Bedrohung
- Einleiten von Maßnahmen zum Stoppen, Eindämmen und Beseitigen von Bedrohungen
- Bereitstellen konkreter Ratschläge, um die Ursachen wiederholt auftretender Vorfälle zu bekämpfen

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

Sophos Rapid Response

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.

Das Sophos Rapid-Response-Team besteht aus unterschiedlichen Experten, die per Remote-Zugriff auf Vorfälle reagieren, Bedrohungen analysieren und aufspüren:

- Schnelles Priorisieren, Eindämmen und Beseitigen aktiver Bedrohungen
- Stoppen von Angreifern in Ihrer Umgebung, um weitere Schäden zu vermeiden
- 24/7 Überwachung und Reaktion, um Ihren Schutz zu optimieren
- Empfehlung von Präventiv-Maßnahmen in Echtzeit, um die Ursache zu bekämpfen
- Detaillierte Bedrohungs-Übersicht nach dem Vorfall mit Informationen zur Vorgehensweise

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

Sophos Intercept X Advanced with EDR

Sophos Intercept X Advanced with EDR hilft dabei, dass Ihre Threat-Hunting-Aktivitäten und IT Operations in Ihrer gesamten Umgebung reibungslos funktionieren. Mit Sophos EDR kann Ihr Team detaillierte Fragen stellen, um komplexe Bedrohungen, aktive Angreifer und potenzielle IT-Schwachstellen zu identifizieren und anschließend schnell geeignete Gegenmaßnahmen zu ergreifen. So können Sie Angreifer in Ihrem Netzwerk aufspüren, die sich bislang unauffällig verhalten haben, aber nur auf eine gute Gelegenheit warten, um Ransomware zu installieren.

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

* 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

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

SOPHOS

20-10-09 WPDE (DD)