Mehr als ein Security-Operations-Center:

Cyber-Threat-Hunting-Teams

Die heutige Komplexität und Vielzahl von Bedrohungen und Angriffen erfordert aktiveres Handeln als noch vor Kurzem. Aufbau und Führung von spezialisierten Cyber-Threat-Hunting-Teams ermöglichen mehr Flexibilität und detailliertere Bedrohungsanalysen.

Von Mathias Fuchs, Innsbruck (AT)

Sicherheitsvorfälle nehmen immer größere Ausmaße an und ihre Aufklärung erfordert den Einsatz von immer mehr Ressourcen – Experten sind gefragter denn je. In den letzten Jahren hat sich die Aufarbeitung und Bereinigung von erkannten, aber auch bisher noch unbekannten Sicherheitsvorfällen deutlich professionalisiert und weiterentwickelt. Aus diesem Grund hat sich die klassische Forensik nicht nur zu einer flexibleren Incident-Response, sondern zu einem regelrechten „Cyber-Threat-Hunting" gewandelt [1,2]: Die Teams, die an einem solchen Fall arbeiten, werden immer größer und müssen entsprechend geführt werden. Hier sind Managementfähigkeiten erforderlich, um den wachsenden Anforderungen bei Aufklärung, Behebung und Nachverfolgung der Vorfälle, aber auch den Erwartungen der Stakeholder gerecht zu werden.

Klassisch gestaltete sich die Aufklärung von Sicherheitsvorfällen so, dass bei jedem potenziell infizierten Host-System eine gezielte forensische Untersuchung durchgeführt wurde. So wäre es notwendig, bei zehn infizierten Host-Systemen zehnmal die gleiche und getrennt voneinander erfolgende Überprüfung einzuleiten. Wenn diese Untersuchungen aufgrund von Zeitdruck durch einen Angriff auch noch parallel durchzuführen wären, müssten also zehn forensische Analysten in nahezu gleicher Zeit Systeme und Daten unter die Lupe nehmen. Das bedeutet einen großen Koordinierungsaufwand und stellt gleichzeitig einen Kostenfaktor da, den sich nicht alle Organisationen leisten können und wollen.

Heute müssen Hunderttausende verschiedener Endpunkte (stationäre PCs, mobile Smartphones, Laptops und Tablets) gewartet und im Zweifelsfall auf Angriffsspuren überprüft werden. Und die Digitalisierung vieler Bereiche des Arbeitsalltags, die bislang noch offline waren, lässt erwarten, dass die Zahl der Schwachstellen in jeder Organisation noch deutlich steigen wird. Die zuvor beschriebene Arbeitsmethode kann also nicht zum Erfolg führen – und dennoch ist sie weiterhin Teil des Alltags in vielen Unternehmen.

Gleichzeitig entwickelt sich die Bedrohungslage exponentiell: Cyberkriminelle werden immer geschickter darin, in Organisationen ganz gezielt Opfer ausfindig zu machen – Mitarbeiter werden über individuelles Phishing dazu verleitet, Schadcode herunterzuladen. Dieser verbirgt sich in Links, die per E-Mails oder SMS zu infizierten Webseiten führen, oder Dateien, in denen sich Makros verbergen – und neuerdings wird sogar in Bild- oder Videodaten versteckte Malware über Social-Media genutzt, um die Geräte der Opfer zu infizieren.

Darauf müssen sich auch die Spezialisten der Abwehr einstellen: Heute muss es darum gehen, ein schnelles und vor allem agiles Cyber-Threat-Hunting-Team zusammenzustellen, um Angriffe auf das eigene Netzwerk aktiv zu verfolgen. Die wichtigste Regel für diese Art der Zusammenarbeit ist das Sammeln und Analysieren von so vielen Informationen wie möglich bei so geringem Ressourceneinsatz wie nötig. Grundvoraussetzung für die erfolgreiche Arbeit ist auf der einen Seite das Können der Analysten, auf der anderen Seite eine effiziente Teamstruktur sowie die Kommunikationsfähigkeiten und Führungserfahrung des Teamleiters.

Abgrenzung zum SOC

Cyber-Threat-Hunting-Teams sind eine Weiterentwicklung der bisherigen Forensik- und Incident-Response-Teams, die in der Regel autark voneinander selbstständig agieren oder deren Anleitung durch interne Fachkräfte erfolgt. Dieses Modell hält den aktuellen Anforderungen der Cybersicherheit nicht mehr stand.

Stattdessen bedarf es eines kompletten Teams, bestehend aus Teamleiter, Cyber-Threat-Hunting-Analysten, Threat-Intelligence-Analysten, Malware-Reverse-Engineers und optional auch noch Spezialisten aus dem Bereich Krisenkommunikation (intern wie extern). Besonders die Threat-Intelligence, also intelligente Bedrohungsanalyse, und

damit einhergehend der Aufbau von Security-Operations-Centers (SOCs) hat hier für eine deutliche Professionalisierung gesorgt (vgl. [3]).

Im Gegensatz zu einem SOC agiert ein Cyber-Threat-Hunting-Team jedoch flexibler und sucht aktiv nach Eindringlingen: Die Mitarbeiter eines SOC agieren erst nach einer Alarmierung durch entsprechende Frühwarnsysteme – während Hunting-Teams im wahrsten Sinne des Wortes auf die Jagd gehen, übernehmen die Mitarbeiter des SOC die Verteidigung.

Managementaufgaben

Cyber-Threat-Hunting-Teams begegnen erheblichen Anforderungen im Projekt-, Kunden- und Medienmanagement. Projektmanagement bedeutet hier die Anleitung der unterschiedlichen Stakeholder in einem Threat-Hunting-Projekt: Besondere Bedeutung kommt dabei der Kommunikation zu, denn sowohl die unterschiedlichen Mitarbeiter des Teams als auch der Auftraggeber müssen kontinuierlich mit Informationen versorgt werden.

Wird nun ein Sicherheitsvorfall detektiert, steht die betroffene Organisation unter enormem Druck, der noch einmal verstärkt wird, wenn die Medien bereits darüber berichten. Zumeist wird dann relativ schnell auf den Vorfall reagiert, ohne sich über die möglichen Folgen bewusst zu sein. Eine akkurate Planung und Ausführung der Aktionen nach dem Vorfall – sowohl intern als auch extern – müssen zeitlich gut aufeinander abgestimmt werden. Daher muss in einem solchen Fall ein vorab erstellter Incident-Response-Plan greifen. Zu viel Kommunikation, die darüber hinaus nicht abgestimmt ist, kann nicht zuletzt dazu führen, dass Angreifer ungewollt weitere wertvolle Informationen erhalten, die sie dann wiederum zur Verstärkung ihrer Bemühungen einsetzen.

Kundenmanagement

Für ein Cyber-Threat-Hunting-Team und besonders dessen Teamleiter ist es zudem enorm wichtig, gleich zu Beginn die Erwartungen des Auftraggebers auf ein realistisches Maß zu senken. Darüber hinaus sollten alle Stakeholder im Unternehmen darüber aufgeklärt werden, wie die Aufarbeitung und Analyse des Sicherheitsvorfalls

Rollen im Cyber-Threat-Hunting-Team

Der Teamleiter

_____ leitet und führt das Team
_____ trifft die Entscheidung, wie viele Ressourcen er benötigt und welche
_____ hält den Kontakt zum Auftraggeber (Erwartungsmanagement, Beruhigung der Geschäftsleitung im Ernstfall)
_____ isoliert das Team vom Druck und Einfluss des Auftraggebers und verhindert, dass dieser die Kontrolle über die Aufklärung übernimmt und in die falsche Richtung leitet
_____ sorgt für Budget-Disziplin
_____ beschafft Grundlageninformationen und stellt diese den Analysten auf einer geeigneten Plattform zur Verfügung

Cyber-Threat-Hunting-Analyst

_____ führt Analysen über die Infrastruktur hinweg durch (dies umfasst host- und netzwerkbasierte Maßnahmen)
_____ übernimmt Triage und Malware-Analyse
_____ nimmt Malware-Funde auf und trägt alle Ergebnisse und Analysen in ein Reporting ein
_____ versorgt Malware-Reverse-Engineers mit Informationen
_____ versorgt Intelligence-Analysten mit Informationen

Intelligence-Analyst

_____ verwaltet und nutzt Analysen in einer Datenbank (also die gesamten Erkenntnisse, die dem Team vorliegen, nicht nur für den aktuellen Fall erforderliche)
_____ teilt Intelligence-Informationen aus diesen Analysen mit anderen Team-Mitgliedern
_____ analysiert Artefakte, die von den Cyber-Threat-Hunting-Analysten und Malware-Reverse-Engineers gefunden wurden
_____ analysiert Angriffe, Angreifer sowie deren Hintergrund und hält die Ergebnisse in einem Report fest

Malware-Reverse-Engineer

_____ untersucht Malware, die von den Cyber-Threat-Hunting-Analysten gefunden wurde
_____ erstellt und teilt „Indicators of Compromise“, um die Malware zukünftig zu erkennen
_____ analysiert die Funktionalität der Malware
_____ fasst Malwarefamilien mithilfe der Intelligence-Analysten zusammen

Medienmanagement / Krisenkommunikation (optional, aber sinnvoll)

_____ unterstützt Teamleiter und Auftraggeber bei der Kommunikation mit den Medien
_____ sammelt und analysiert Medienberichte über den aktuellen Fall und die Hintergründe der Angreifer und ihrer Organisationsform

erfolgen und auf welche Weise die Ergebnisse am Ende aufbereitet und präsentiert werden.

Den Auftraggeber bereits zu Beginn von den Fähigkeiten und dem Vorgehen des Teams zu überzeugen, ist ein zumeist unterschätzter Erfolgsfaktor: Wird das Team von Anfang an mit allen der Organisation zur Verfügung stehenden Mitteln bei der Aufklärung unterstützt, ist die Wahrscheinlichkeit groß, dass man am Ende auch ein Ergebnis vorstellen kann, das dem Unternehmen in Zukunft hilft, Sicherheitsvorfälle zu beschränken.

Beispiel-Szenario

Nachdem auf der Webseite des Internet Storm Centers des SANS Instituts ein Angriff auf ein Unternehmen durch eine Schwachstelle in einem Java-Web-Application-Server beschrieben wurde, prüft der beauftragte Analyst zunächst, ob diese Art von Server im Unternehmen vorhanden ist und ob diese Schwachstelle bereits überall erfolgreich gepatcht wurde.

Wird er fündig, schaut er sich beispielsweise die Prozesslisten der Server an und legt die Datensätze übereinander. Bei einem Webserver findet er eine Anomalie: Ein auffälliger unbekannter Prozess läuft. Sofort sichert der Analyst die potenzielle Schadsoftware direkt aus dem Arbeitsspeicher und stellt sie dem Malware-Spezialisten zur Verfügung. Dieser stellt fest, dass die Malware die Funktionalität eines RDP-Proxys direkt in das Netz des Unternehmens bietet. Nach Rücksprache mit dem Intelligence-Analysten fällt auf, dass ähnliche Malware bereits in vergangenen Angriffen verwendet wurde.

Der Intelligence-Analyst stellt daraufhin dem Incident-Response-Team weitere mögliche Vorgehensweisen dieser speziellen Angreifergruppe vor. Dieses durchsucht nun das ganze Netz nach weiteren Spuren der Angreifergruppe: Auf einigen Servern finden sich Anzeichen in den Event-Logs, dass diese mittels RDP vom kompromittierten Server kontaktiert wurden. Es zeigt sich, dass für die Verbindung ein lokaler administrativer Account genutzt wurde, der auf allen Servern im Unternehmen mit einem Standardpasswort angelegt ist.

Nach der Erstellung einer umfassenden Timeline der Schritte des Angreifers ist sich das Team ziemlich sicher, alle Einfallstore entdeckt zu haben. Es zeigt sich, dass der Angriff noch rechtzeitig bemerkt wurde – der Angreifer kann dann mit wenig Aufwand vorerst aus dem Netz entfernt werden. Der hier beschriebene Vorgang sollte mit Unterstützung eines Cyber-Threat-Hunting-Teams weniger als drei Stunden dauern.

Das Team sollte beispielsweise Zugriff auf alle relevanten Daten erhalten, die für die Analyse wichtig sein könnten. Darüber hinaus ist der Zugang zu allen Systemen erforderlich, die für den so genannten Remediation-Plan zur Behebung des Vorfalls, zum Schließen der Einfallstore und zur Bereinigung infizierter Bereiche wichtig sind. Die rechtlichen und unternehmenseigenen Richtlinien sollten dem Team bekannt gemacht werden, sofern nicht bereits von diesem adressiert.

Ein enger Austausch mit dem in der Organisation eingesetzten Sicherheitsverantwortlichen ist eine weitere Grundbedingung für das Gelingen des Projekts. Als letzter Punkt ist natürlich auch die Budget-Verhandlung ein wichtiges Thema, das bereits vorab geklärt werden sollte.

Medienmanagement

Sollte es bei einem Sicherheitsvorfall bereits Medienberichte geben, kommt es darauf an, die Informationshoheit über den Fall zurückzugewinnen. Dabei ist es wichtig, zunächst alle Informationen zu sichten und der Ursprungsquelle auf den Grund zu gehen. Die Frage ist: Wurden bereits alle verfügbaren Informationen veröffentlicht oder werden noch Informationen zurückgehalten, um nach Reaktion der Organisation die Berichterstattung ausweiten zu können? Jeder Bericht erhöht den Druck auf das Cyber-Threat-Hunting-Team und die betroffene Organisation – umso stärker, wenn die Medien mehr Informationen haben als die Ermittler selbst.

Leider sind die wenigsten Unternehmen auf solche Szenarien vorbereitet und müssen sich erst noch in Krisenkommunikation üben. Aus diesem Grund ist es für Cyber-Threat-Hunting-Teams sinnvoll, hierzu eigene Ressourcen an Bord zu holen – und sei es nur durch einen externen Berater, der aber die nötige Erfahrung im Umgang mit kritischen Pressenachfragen hat.

Generell gilt es, durch eine klare und von Anfang an gesteuerte Informationspolitik die Hoheit über eventuell durchgesickerte Informationen zurückzugewinnen und nur dann weitere Informationen zu veröffentlichen, wenn dies mit allen Stakeholdern eng abgestimmt ist und es das Team bei der Aufklärung unterstützt – beispielsweise bei der Fahndung nach den Urhebern des Angriffs. Allerdings sollte man hier vorsichtig agieren, um etwaige voreilige Verdächtigungen zu verhindern, die sich im Laufe der Nachverfolgung als falsch erweisen könnten.

Fazit

Cyber-Threat-Hunting-Teams sind die Zukunft der Forensik und des Incident-Response-Managements. Wichtig sind klare Rollendefinition und Aufgabenverteilungen innerhalb des Teams (vgl. Kasten auf S. 59). Der

Teamleiter hat dabei eine wichtige Management-Aufgabe: Er muss den Kontakt zum Auftraggeber halten und innerhalb des Teams die Informationshoheit bewahren, um die Arbeit der Cyber-Threat-Hunting- und Intelligence-Analysten sowie der Malware-Reverse-Engineers sowie (optional) des Krisenkommunikators zu erleichtern.

Diese Management-Rolle benötigt eine Reihe von Fähigkeiten, die weniger in der technischen Expertise als vielmehr im klassischen Projektmanagement anzusiedeln sind. Ohne tiefgreifende Kenntnisse in den Bereichen Informationssicherheit, Forensik und Incident-Response ist die Übernahme dieser Funktion allerdings auch nicht möglich.

Spezialisten aus diesen Bereichen sollten sich daher entsprechend ihrer Erfahrung und Fähigkeiten weiterbilden, um den wachsenden Anforderungen gerecht zu werden, mit denen sie bei der Aufarbeitung von Sicherheitsvorfällen jetzt und in Zukunft konfrontiert werden. ■

Dipl.-Ing. Mathias Fuchs ist Head of Cyberdefence bei der InfoGuard AG und SANS-Trainer.

Literatur

[1] Timothy Proffitt, Creating and Managing an Incident Response Team for a Large Company, SANS Institute InfoSec Reading Room, 2007, www.sans.org/reading-room/whitepapers/incident/creating-managing-incident-response-team-large-company-1821

[2] Scott J. Roberts, Incident Response is Dead… Long Live Incident Response, Blogpost, April 2015, https://sroberts.github.io/2015/04/14/ir-is-dead-long-live-ir/

[3] Rob Lee, Hunting Your Adversary – How to Operate and Leverage an Incident Response Hunt Team, Vortragsfolien, SANS SOC Summit 2015, https://files.sans.org/summit/SOC_Summit_2015/PDFs/Hunting-Your-Adversary-How-to-Opearte-and-Leverage-an-Incident-Response-Hunt-Team-Rob-Lee.pdf