DEM HACKER AUF DER SPUR

Bei Cyber Defense reden alle von Incident Detection und Incident Response. Doch was beinhaltet dies und welche Schritte führen dorthin? Unser Hackerszenario zeigt, was es braucht, um einen Angriff zu erkennen.

→ **VON MANUEL KRUCKER**

In den letzten Jahren haben Cyberkriminelle ihre Geschäftsfelder ausgebaut und professionalisiert. Ihre Angriffe sind häufiger erfolgreich und verursachen grössere Schäden. Gleichzeitig nimmt die Komplexität der IT zu, auch weil immer mehr Partner involviert sind und Zugriff auf Unternehmens-Netzwerke erhalten. Vor diesem Hintergrund hat sich die Cyber Security weiterentwickelt. Da Angriffe immer wahrscheinlicher werden, reichen präventive Massnahmen allein nicht mehr aus. Angriffe müssen detektiert werden und Reaktionen möglich sein, um kostspielige Schäden zu minimieren.

EIN REALISTISCHES ANGRIFFSSZENARIO

Wie wird dies schrittweise umgesetzt und was sind dabei die Herausforderungen? Stellen Sie sich folgendes Angriffsszenario vor: Pirmin, ein Mitarbeiter der fiktiven Firma Demo Kraftwerke AG, erhält ein E-Mail von einem Strombezüger und will es noch schnell vor Feierabend beantworten. Unbedacht klickt er auf die Word-Datei im Anhang. Der Absender ist Pirmin schliesslich bekannt, von daher wird keine Gefahr erkannt. Unbemerkt startet im Hintergrund ein bösartiges Makro, das mit noch unbekannter Signatur durch alle Schleusen kam, und infiziert zuerst seinen PC, dann weitere Systeme der Infrastruktur. Infolge dessen stürzen zwei Server der Demo Kraftwerke AG ab.

LOGS: TRANSPARENZ SCHAFFEN & SPUREN AUFZEICHNEN

Zentrales Log Management ist ein wichtiger Bestandteil in der Cyber Security. Es ermöglicht, effizient nach Informationen zu suchen und Vorgänge in der IT-Infrastruktur nachzuvollziehen. Wie hilft ein Log Management konkret? In den Logs finden sich Spuren, die ein Angriff hinterlässt: Die E-Mail-Logs offenbaren das bösartige E-Mail mit Attachment, Prozess-Logs der Workstation zeigen die Ausführung eines Makros und Firewall-Logs zeigen eine Verbindung zwischen Pirmins Workstation und den abgestürzten Servern. Das Log Management muss eine gewisse Maturität aufweisen und folgende Herausforderungen meistern:

- Integration möglichst vieler Logquellen
- Automatische Erkennung von versiegten Logquellen
- Normalisierung von Logs (vers. Formate konsolidieren, strukturieren)
- Verwendung von gespeicherten und geteilten Suchanfragen
- Entwicklung von kundenspezifischen Berichten und Alarmen.

Zum Autor

Manuel Krucker: Eidg. Dipl. Inf. Ing. ETH. Cyber Security Consultant. Mehr als neun Jahre Erfahrung als Penetration Tester.

Zum Unternehmen: terreActive AG ist Spezialist für den Betrieb und die Überwachung von IT-Sicherheitsinfrastrukturen. Ein eigenes, ISO zertifiziertes Security Operations Center (SOC) bekämpft Cyberangriffe und steht 24/7 im Einsatz. Das 1996 in Aarau gegründete Schweizer Unternehmen bietet zusätzlich zum Betrieb Konzepte, Audits und Engineering-Dienstleistungen für die Cyber Security an.

Mehr als 60 Mitarbeitende sichern den Erfolg der Kunden, darunter Banken, Versicherungen, Spitäler, öffentliche Verwaltungen, e-Shops, Industrieunternehmen und IT-Service Provider.

Mehr Informationen: www.security.ch

SOC: SYSTEME ÜBERWACHEN & ANALYSE DURCHFÜHREN

Logs sammeln alleine hilft nicht, um Angriffe analysieren zu können. Idealerweise versetzt man sich in die Lage des Angreifers, um zu verstehen, welche Eintrittstüren er benutzt, welche Schwachstellen er ausnutzt und welche Ziele er nach seinem erfolgreichen Zugriff verfolgt. Diese Spurensuche, sowie die permanente Überwachung der IT sollte von einem SOC (Security Operations Center) durchgeführt werden. Durch die Aufzeichnung der Logs können alle Verbindungen zu den Servern auch rückwirkend vom SOC-Team untersucht und zur Erfüllung der Compliance Richtlinien gespeichert werden. Bei unserem Angriffsszenario bemerkt das SOC-Team die abgestürzten Server und leitet eine Untersuchung ein. Diese führt dazu, dass die Workstation von Pirmin als interner Ursprung einer Attacke identifiziert wird. Man hat den Hackerangriff erkannt.

Wie können aber Angriffe identifiziert werden, die keine so offensichtlichen Spuren hinterlassen?

SIEM: ANGRIFF DETEKTIEREN & ANALYSE BESCHLEUNIGEN

Verfügt ein Unternehmen neben Log Management und SOC auch noch über ein SIEM (Security Information and Event Management), so bietet dies einen wertvollen Mehrwert. Sogenannte Use Cases (Definition eines Angriffs) sorgen dann dafür, dass verschiedene Logeinträge korrelieren, also in Zusammenhang und Abhängigkeit gebracht werden, um Angriffsszenarien automatisch zu detektieren.

Hätte die Demo Kraftwerk AG ein SIEM, so würde die Konstellation, dass ein Powershell-Prozess durch ein Makro aufgerufen wird, eine Detektion und damit einen Alarm auslösen. Dadurch würde das SOC automatisch bereits beim Beginn des Angriffs informiert und hätte Kenntnis vom Vorfall, noch bevor die zwei Server abstürzen. Man hätte wertvolle Zeit gewonnen, um den Schaden zu minimieren.

Ein SIEM bietet standardisierte Use Cases für verschiedene Anwendungen out-of-the-

Bild: iStock.com/gorodenkoff

Im SOC fahnden Security Analysten nach Spuren von Angreifern.

box und kann von einem Security Engineer für kundenspezifische Anforderungen mit weiteren Use Cases ergänzt werden. Achtet man darauf, dass Use Cases für verschiedene Phasen eines Angriffs (der Cyber Kill Chain) vorhanden sind, steigt die Wahrscheinlichkeit, ihn zu entdecken. Für eine automatische Priorisierung der Alarme wird das SIEM an das Inventar-System angebunden und Geräte als auch Benutzer werden anhand ihres Risikoprofils klassifiziert.

Auch das beste SIEM wird bei der Inbetriebnahme Fehlalarme produzieren, weshalb es in der Einführungsphase auf die Situation im Unternehmen abgestimmt werden muss. Im laufenden Betrieb werden vom SOC kontinuierlich Anpassungen der Use Cases vorgenommen, um die Detektion zu optimieren.

INCIDENT RESPONSE: PROZESSE FÜR DAS HANDLING

Achtung, die (Security-)Reise ist hier noch nicht zu Ende, nur weil man ein Log Management, ein SOC und ein SIEM im Einsatz hat. Diese Mittel helfen, Angriffe zu erkennen und eine erste Triage vorzunehmen. Handelt es sich um einen kritischen Vorfall, sollte ein Incident ausgelöst werden, der einem klar definierten Prozess mit den Phasen Bestätigung, Analyse, Eindämmung, Wiederherstellung und Post-Incident-Analyse folgt. Der Prozess beinhaltet verschiedene Eskalationsstufen und adressiert auch Aspekte wie die interne und externe Kommunikation.

Der Incident-Response-Prozess, wie auch die Behandlung eines Vorfalls, sind komplex und Entscheidungen müssen teils unter hohem Zeitdruck gefällt werden. In unserem Beispiel hat eine Analyse ergeben, dass von Pirmins Workstation aus bösartige Software heruntergeladen wurde. Dadurch wird der Incident bestätigt und als Malware-Angriff klassiert. Dies führt dazu, dass eine entsprechende Handlungsroutine gemäss vordefiniertem Playbook ausgelöst wird.

Im Playbook, einem wichtigen Arbeitstool im SOC, ist genau beschrieben, welche Aufgaben in welcher Reihenfolge durchgeführt werden müssen. Dies kann beispielsweise die Sperrung von Benutzern, Konfigurationsänderungen von Firewalls, die Isolierung von Servern oder die Information der Geschäftsleitung beinhalten.

CYBER SECURITY UMFASST MEHRERE BESTANDTEILE

Um der Bedrohungslage gerecht zu werden, muss Cyber Security mit Incident Detection und Incident Response ergänzt werden, damit Angriffe erkannt und proaktiv Massnahmen ergriffen werden können. Zentrales Log Management, ein SOC, ein SIEM sowie ein klar definierter Incident-Prozess sind die wesentlichen Bestandteile.

Der Aufbau und der Betrieb sollten langfristig und etappenweise geplant werden. Ein SOC- oder SIEM-Workshop hilft Unternehmen, die richtige Lösung zu designen und die Umsetzung zu planen und durchzuführen. Je nach Unternehmensgrösse ist es sinnvoll über einen externen Bezug des Security-Fachwissens oder einzelner Dienstleistungen nachzudenken. ←

Dieser Beitrag wurde von der **terreActive AG** zur Verfügung gestellt und stellt die Sicht des Unternehmens dar. Computerworld übernimmt für dessen Inhalt keine Verantwortung.