FORTINET

Bedrohungserkennung und Reaktionsmaßnahmen: 5 Top-Tipps für Ihre Kaufentscheidung

Inhalt

Zusammen-fassung

Die ausgefeilten Angriffsstrategien heutiger Cyberkrimineller sind für Security-Teams eine enorme Herausforderung und große Chance zugleich: Einerseits müssen für eine erfolgreiche Cyberabwehr viele Angriffswege und unterschiedlichste Anzeichen bösartiger Aktivitäten überwacht werden (was selbst für erfahrene Sicherheitsexperten kompliziert und zeitaufwendig sein kann), andererseits lässt sich mit den richtigen Technologien die Sicherheitslage gut einschätzen und das Security-Team kann wirksame Reaktionsmaßnahmen ergreifen, bevor Schaden entsteht. Allerdings: Damit dieser Balance-Akt zwischen Prävention und frühzeitiger Eindämmung gelingt, sollten vor einer Investition in eine Plattform für die Bedrohungserkennung und Reaktionsmaßnahmen einige wichtige Fragen geklärt werden.

Einleitung

Bei Investitionen in die Cybersecurity haben sich die meisten Unternehmen bislang auf präventive Maßnahmen konzentriert. Laut Gartner ist das mittlerweile zu wenig. So heißt es in einer Research Note des Analystenhauses: „Angesichts der Komplexität der Bedrohungserkennung genügt es heute bei der Bedrohungsabwehr nicht mehr, einfach ein erstklassiges Produkt zu kaufen. Notwendig ist die Kombination mehrerer Erkennungstechnologien, die mit verschiedenen Methoden – auch über APIs – genügend Telemetriedaten sammeln und korrekt analysieren, um die Nadel im Daten-Heuhaufen zu finden.“[1]

Die gute Nachricht: Immer mehr Verantwortliche in Unternehmen erkennen, dass die Komplexität der Security-Infrastruktur und des Alarm-Managements eine ständige Herausforderung ist. 75 % der Unternehmen wollen deshalb ihre Cybersecurity-Anbieter stärker konsolidieren und viele Einzelprodukte durch Plattformen ersetzen.[2]

Wie bei jeder Technologie gibt es auch bei Erkennungs- und Reaktionsplattformen große Unterschiede. Und nicht jede Lösung ist für jedes Unternehmen geeignet: Angriffsflächen, vorhandene Abwehrmaßnahmen gegen einzelne Angriffsphasen, Erkennungstechnologien und der

Integrationsgrad können stark variieren. Wie Gartner zu Recht feststellt, ist der Stack für ein Unternehmen optimal, der die Monitoring-Ziele am effizientesten zum besten Preis-Leistungs-Verhältnis erfüllt.[3] Und nicht zu vergessen: Die beste Sicherheitstechnologie zeigt ihre Leistungsstärke erst, wenn dahinter ein kompetentes Security-Team und durchdachte Prozesse stehen. Die Menschen sind also für eine wirksame Verteidigung nach wie vor unerlässlich.

Fünf wichtige Fragen vor der Investition in eine Erkennungs- und Reaktionsplattform

Angenommen, Sie möchten eine Plattform für die Bedrohungserkennung und Reaktionsmaßnahmen einführen oder müssen Ihren Ansatz für das Risikomanagement anpassen. Dann sollten Sie die folgenden fünf entscheidende Fragen vor jeder neuen Investition klären.

1. Was lässt sich überprüfen?

Bedrohungsakteure können auf unterschiedlichste Weise in Ihr Unternehmen eindringen, z. B. per E-Mail, in Internet--Downloads, in Diensten oder über extern sichtbare Anwendungen und Assets. Es gibt viele Angriffsziele in Ihrem Unternehmen, die von Endbenutzergeräten, Anwendungsservern bis hin zu IoT- und OT-Systemen reichen. Dazu kommen noch unternehmensexterne Ziele wie Software-as-a-Service oder die Public-Cloud-Infrastruktur.

Diese dynamische, hochkomplexe Bedrohungslage erfordert Technologien, die damit mithalten können. Gartner dazu: „Je mehr Perspektiven ein Stack bietet, desto mehr Bedrohungen lassen sich damit erkennen bzw. desto aus-

sagekräftiger sind die Alarmmeldungen. Zumindest sollte der Stack eine strategische Sicht auf die Art von Bedrohungen bieten, die von größtem Interesse sind."[4] Grundsätzlich gilt: Man kann nur in den Bereichen eine Bedrohung erkennen, die die Technologie überprüfen kann. Folglich müssen Sie sicherstellen, dass die Monitoring- und Inspektionsfunktionen der Plattform wirklich alle Angriffsvektoren und Angriffsflächen abdecken.

2. Greift der Schutz in allen Angriffsphasen?

Viele Angriffe durchlaufen heute mehrere Phasen. Dadurch sollen präventive Sicherheitsmaßnahmen umgangen werden, damit sich die Angreifer länger im Unternehmensnetzwerk verbergen und maximalen Schaden anrichten können. Das MITRE ATT&CK-Framework und die Cyber-Kill-Chain – das Modell zum Ablauf eines Cyberangriffs von Lockheed Martin – zeigen die üblichen Phasen und regelmäßig verwendeten Taktiken: Vorbereitung und Durchführung des Angriffs bis hin zu Aktivitäten nach der Kompromittierung und dem Eindringen. Die gute Nachricht: Je mehr Phasen ein Bedrohungsakteur vor dem Erreichen seines eigentlichen Ziels durchführt, desto größer ist die Chance für das Unternehmen, den Angriff rechtzeitig zu erkennen und zu stoppen.

Laut Gartner sollte „am besten ein Erkennungs-Stack gefunden werden, der in der Angriffsphase funktioniert und aussagekräftige Alarme für Ihre Überwachungsziele liefert".[5] Dafür muss eine Security-Operations-Plattform allerdings Schutz vor sämtlichen Angriffs- und Verbreitungswegen sowie allen Phasen der Cyber-Kill-Chain bieten – vom Ausspähen in der Erkundungsphase, dem Herausfinden der geeigneten Angriffsmethode (Manipulation), dem Einschleusen und Ausführen der ersten Angriffsschritte und Ausnutzen von Schwachstellen (Exploit) bis hin zum Installieren einer Backdoor oder Malware, der Kontrolle per Fernzugriff (Command-Control, C2) und weiteren Aktionen zum Erreichen des Angriffsziels.

3. Welche Technologien werden zur Erkennung eingesetzt?

Nur weil Sie Aktivitäten über Angriffsvektoren und entlang der Cyber-Kill-Chain hinweg untersuchen können, heißt das nicht automatisch, dass Sie Angriffe auch erkennen können. Das liegt daran, dass Angriffe zunehmend so aufgebaut sind, dass sie wie legitime Dienste oder Aktionen aussehen oder diese sogar ausnutzen. Nach Gartner sind „einige Methoden sehr einfach und sogar deterministisch, andere erfordern umfassende Kenntnisse über Bedrohungen oder eine komplexe Datenanalyse. Obwohl es keine beste Methode gibt, sind einige Methoden dennoch bei bestimmten Bedrohungen wirksamer als bei anderen."[6]

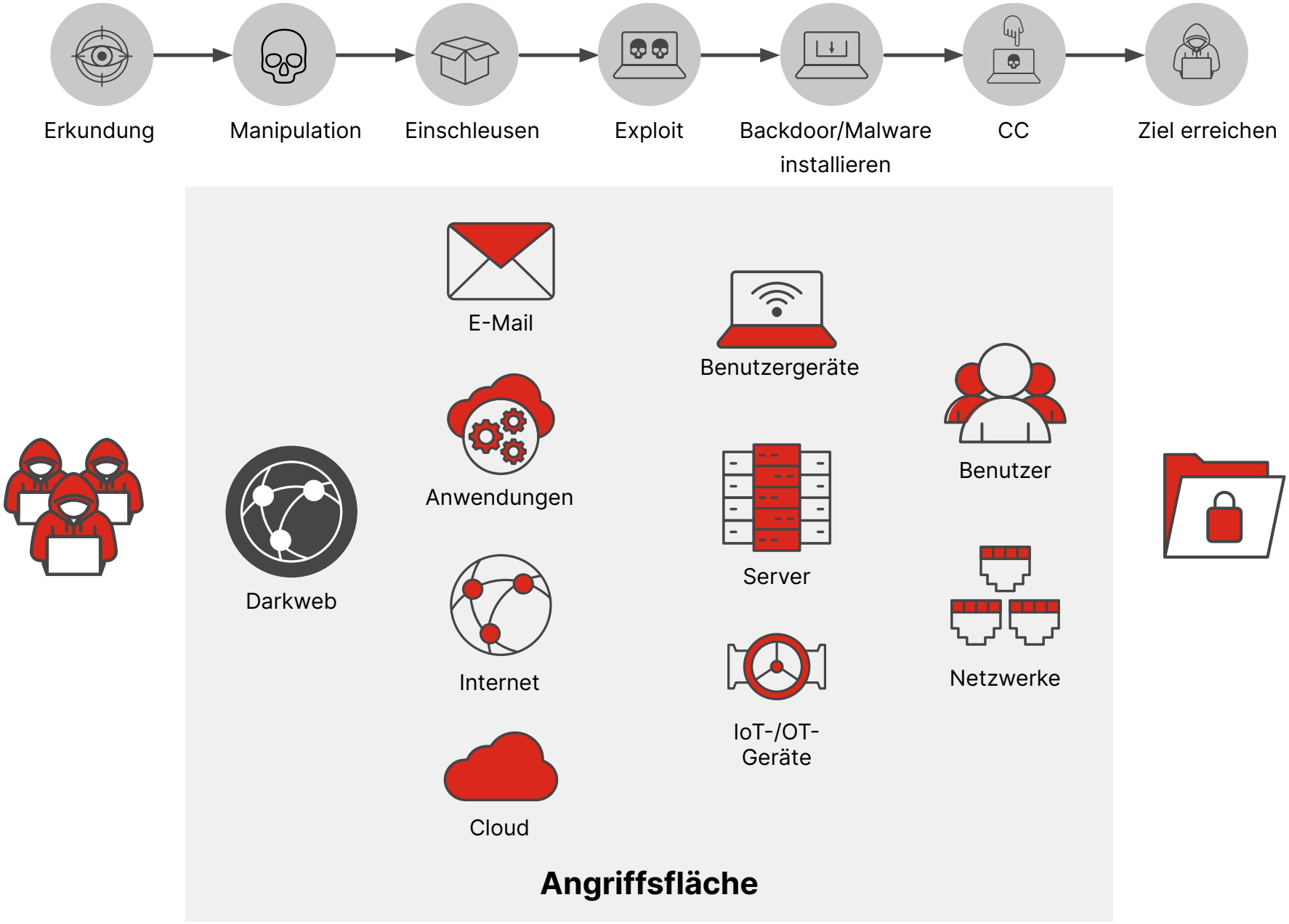

Abbildung 1: Angriffsfläche und Cyber-Kill-Chain-Phasen, für die die Bedrohungserkennung und Reaktionsmaßnahmen greifen müssen

Bedrohungsinformationen und Kompromittierungsindikatoren sind zwar hochpräzise, liefern aber keine nützlichen Prognosen, wie man sie mit Regeln und Heuristik erhält. Das Problem: Regeln und Heuristik führen häufig zu falsch positiven Ergebnissen, also Fehlalarmen. Statische Machine- oder Deep-Learning-Modelle sind weitaus besser für Prognosen geeignet, haben jedoch anfangs oft eine wenig vertrauenswürdige Wahrscheinlichkeit. Wird es dann mal besser mit der Wahrscheinlichkeit, lässt sich das allerdings dauerhaft nur schwer aufrechterhalten. Die Verhaltensanalyse bietet einige der besten Prädiktoren – sofern es Prozesse gibt, die bekannte Taktiken, Techniken oder Verfahren genau identifizieren können. Die Erkennung anomaler Aktivitäten, die womöglich nicht autorisiert oder legitim sind, ist für Security-Teams meistens extrem zeitaufwendig. Deshalb ist es so wichtig, dass Sie für Ihr Unternehmen und Ihr Team den passenden Mix aus Erkennungstechnologien finden.

4. Von wem (oder was) wird eine Reaktion erwartet?

Die Erkennung ist nur der erste Schritt. Um das Risiko zu begrenzen, müssen Vorfälle validiert und eingedämmt werden. Ebenfalls ist ein umfassender Untersuchungs- und Remediation-Prozess notwendig, um zu einem sicheren Betrieb zurückzukehren.

Diese Funktion haben bislang erfahrene Sicherheitsexperten übernommen, die auch weiterhin für diesen Prozess unverzichtbar sind. Laut Gartner lassen sich Ziele, Prozesse und

Aktivitäten aber auch gut mit standardisierten Reaktionen regeln – allerdings nicht auf präskriptiver Ebene. Wenn es konkret darum geht, was genau bei jedem vom Angriff betroffenen Objekt zu tun ist und außerdem die spezielle Art des laufenden Angriffs berücksichtigt werden muss, braucht es andere Lösungen.[7]

Unternehmen müssen entscheiden, inwieweit sie sich auf die gesammelte Expertise des Security-Teams verlassen möchten oder ob dieses institutionalisierte Wissen in Prozessen dokumentiert werden soll, die mit einer Plattform orchestriert und automatisiert werden können. Eine starke SecOps-Strategie stützt sich in der Regel auf beides – es kommt nur auf das richtige Verhältnis an. Und das ist von Unternehmen zu Unternehmen unterschiedlich.

5. Kann Ihr Team alles allein übernehmen?

Selbst ein optimal ausgerüstetes, orchestriertes und automatisiertes System funktioniert nicht von selbst. Das sieht auch Gartner so: „Die letzte und oft schwierigste Herausforderung ist der Betrieb … Ein Großteil der damit verbundenen Arbeit hat nichts mit der Fehlerbehebung oder Korrekturen zu tun, sondern besteht vielmehr aus kritischem Denken und Untersuchungen auf Expertenebene.“[8]

Klären Sie, ob Ihr Security-Team die Plattform Ihrer Wahl selbst betreiben kann oder ob Sie sich bei der Bedrohungserkennung und bei Reaktionsmaßnahmen besser auf externe Experten verlassen sollten. Beim Outsourcing haben Sie einige Optionen: Sie können alles vorübergehend oder dauerhaft auslagern, sich Unterstützung für alle Bereiche holen oder nur einen speziellen Schutz für bestimmte Aufgaben buchen. Wichtig dabei: Durch Outsourcing sind Sie nicht automatisch vor allen Cyberrisiken geschützt, sondern greifen lediglich auf das Fachwissen und Experten eines externen Anbieters zurück. Wenn Sie sich also für ein Outsourcing entscheiden, sollten Sie unbedingt eine Plattform von einem zuverlässigen Partner mit der nötigen Security-Kompetenz wählen, der Sie wirklich unterstützen kann.

Fazit

Die Komplexität, mit der heutige Bedrohungsakteure bei Angriffen vorgehen, ist für Ihr Unternehmen sowohl eine Herausforderung und Chance zugleich. Grundsätzlich gilt: Mit einem effektiven Erkennungssystem, das die gesamte Angriffsfläche und Cyber-Kill-Chain mit zuverlässigen Technologien sicher schützt und wirksame Reaktionen ermöglicht, können Sie Ihr Cyberrisiko erheblich reduzieren.

[1] „The Journey to SOC in Three Steps: Step 2 Building the Detection Stack and Establishing Security Operations". Gartner, 19. Dezember 2022.

[2] „Gartner Survey Shows 75% of Organizations are Pursuing Security Vendor Consolidation in 2022". Gartner, 13. September 2022.

[3] „The Journey to SOC in Three Steps: Step 2 Building the Detection Stack and Establishing Security Operations". Gartner, 19. Dezember 2022.

[4] Ebd.

[5] Ebd.

[6] Ebd.

[7] Ebd.

[8] Ebd.

FORTINET

www.fortinet.com/de

22. März 2024 9:32 Uhr

2504903-0-0-DE