Cyber-Sicherheitsrat Deutschland e.V.

Werkzeugkasten Cybersicherheit

Threat Hunting

Definition, Einsatzgebiete & Diskussion

Wir sind wehrhaft

Cybersicherheit erscheint uns oft als unbezwingbare Aufgabe: ein **asymmetrisches Setting**, das Angreifern einen taktischen Vorteil gegenüber Sicherheitsexperten verschafft, wachsende Möglichkeiten und die **Professionalisierung von Cyberkriminellen**, **unklare Zuständigkeiten** und regulatorische Anforderungen bei IT-Sicherheitsinstitutionen und vieles mehr.

Das kann deprimieren.

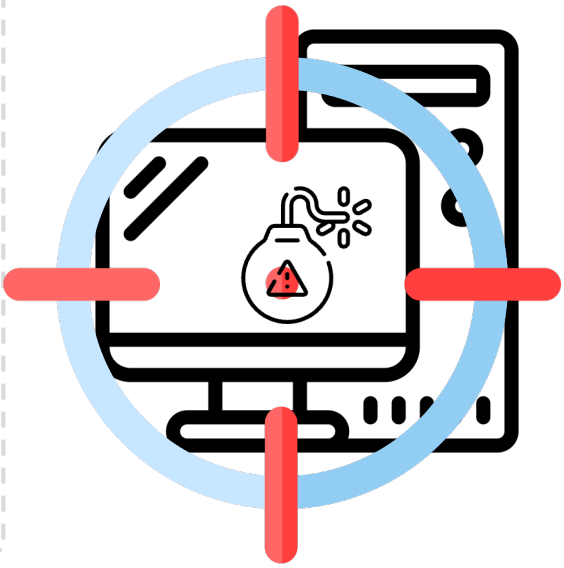
Was wir dabei oft vergessen sind die vielen Menschen, Ressourcen und Werkzeuge auf der anderen Seite, die tagtäglich daran arbeiten, Wirtschaft und Gesellschaft sicherer zu machen. In der Vergangenheit wurden **wirkungsvolle und starke Methoden** entwickelt, die nur an den richtigen Stellen genutzt werden müssen, um Angreifern einen Schritt voraus zu sein.
Es gibt für alles eine Lösung, man muss sie nur finden – vor allem im Bereich Cybersicherheit. Diese Publikationsreihe stellt übersichtsartig die wichtigsten **Methoden im Kampf gegen Cyberattacken** mit ihren Einsatzgebieten sowie Vor- und Nachteilen vor, damit zukünftig die richtigen Werkzeuge an den passenden Stellen parat stehen.

Ich wünsche Ihnen eine anregende Lektüre und interessante Einblicke in den Werkzeugkasten Cybersicherheit.

Hans-Wilhelm Dünn
Präsident
Cyber-Sicherheitsrat Deutschland e.V.

Threat Hunting – Was ist das?

Threat Hunting ist ein **proaktiver Ansatz** zur Verbesserung der Cybersicherheit. Mit dieser Methode wird aktiv nach Cyberbedrohungen in Netzwerken und Systemen gesucht, die dort **bisher unentdeckt** geblieben sind. Ziel ist es, **bösartige Akteure aufzuspüren**, die in der IT-Umgebung Sicherheitsmaßnahmen umgehen konnten.
Diese Methode ist notwendig, da Angreifer nach dem Eindringen in Systeme oft für längere Zeit **unentdeckt und heimlich in einem Netzwerk verbleiben**, um Daten zu sammeln, nach vertraulichem Material zu suchen oder Anmeldeinformationen zu erlangen.



Wie funktioniert Threat Hunting?

Threat-Hunting-Programme gehen davon aus, dass sich bereits ein **Angreifer innerhalb des Systems** befindet, auch wenn es dafür (noch) keine konkreten Anzeichen gibt. Dieser proaktive Ansatz erfordert in der Regel **manuelle Prozesse**, die von spezialisierten Fachleuten mithilfe von **automatisierten Sicherheitstools** gesteuert werden. Teilweise kommen dabei KI-basierte oder **Machine-Learning-gestützte Methoden** zum Einsatz, um große Datenmengen zu analysieren.
Durch die **gezielte Suche nach Bedrohungen** kann ein Unternehmen **frühzeitig** auf mögliche Angriffe reagieren und potenzielle Schäden vermeiden.
Mit verschiedenen Methoden wird nach **Anomalien** im System, **auffälligen Verhaltensweisen** und anderen Indikatoren für Kompromittierungen gesucht. Die Ergebnisse des Threat Huntings können verwendet werden, um die vorhandenen **Sicherheitssysteme zu optimieren** und schneller auf mögliche Angriffe zu reagieren.

Wem nutzt Threat Hunting?

Unternehmen und andere Organisationen, die über ausreichende Ressourcen verfügen, sollten Threat Hunting als wichtigen Bestandteil ihres ganzheitlichen Sicherheitskonzepts betrachten. Diese proaktive Methode kann dazu beitragen, **Bedrohungen frühzeitig zu erkennen und ihre Auswirkungen zu minimieren**. Organisationen, die nicht über ein eigenes Team von Threat Huntern verfügen, können auf **externe Anbieter** zurückgreifen. Diese können die notwendigen Ressourcen, Expertise und Technologien bereitstellen, um Threat Hunting effektiv durchzuführen.

Welche Chancen gibt es?

Threat Hunting ermöglicht es, schnell auf potenzielle Angriffe zu reagieren, indem es Hinweise auf eine Kompromittierung oder einen laufenden Angriff liefert. Dadurch können die Zeit zwischen dem Eindringen und der Entdeckung einer Bedrohung sowie die **potenziellen Folgen eines Angriffs minimiert** werden.

Durch die Ergebnisse des Threat Huntings können vorhandene Sicherheitssysteme optimiert werden. Beispielsweise können **neue Indikatoren für Bedrohungen** oder Kompromittierungen definiert und in die Sicherheits-Tools integriert werden.

Threat Hunting steigert zudem die Fähigkeiten der Sicherheitsteams, indem es ihnen erlaubt, **neue Taktiken, Techniken und Verfahren der Angreifer** zu lernen und sich entsprechend vorzubereiten. So können sie künftige Angriffe schneller erkennen und effektiver darauf reagieren.

Welche Risiken gibt es?

Threat Hunting erfordert **viel Zeit**, um nach Bedrohungen zu suchen, Daten zu sammeln und Hypothesen zu erstellen. Viele IT-Teams haben jedoch nicht genügend Zeit oder Personal, um diese Aufgaben durchzuführen. Daher müssen sie möglicherweise zusätzlich externe Dienstleister beauftragen oder verstärkt in die Ausbildung ihrer Mitarbeiter investieren.
Auf technologischer Seite werden ebenfalls **leistungsfähige Infrastrukturen** benötigt, die in der Lage sind, große Datenmengen zu verarbeiten. Diese Technologien müssen auch in die **vorhandenen Sicherheitssysteme integriert** werden können.
Threat Hunting kann manchmal **falsch-positive Ergebnisse** liefern, also Anomalien oder Indikatoren identifizieren, die keine echten Bedrohungen darstellen. Dies kann zu unnötigen Alarmen oder Untersuchungen führen, die Ressourcen verschwenden oder die Aufmerksamkeit von den wirklichen Bedrohungen ablenken.

Fazit

Threat Hunting ist eine wichtige Verteidigungsstrategie, um den neuesten Cyberbedrohungen **einen Schritt voraus** zu sein und schnell auf mögliche Angriffe reagieren zu können. Diese Methode spielt eine wichtige Rolle dabei, verdeckte Angreifer in Systemen zu finden, **bevor ein Cyberangriff eskalieren kann**. Dabei vereint sie sowohl **menschliche Expertise** als auch die Anwendung automatisierter und **skalierbarer Tools** zur Datenanalyse.
Insgesamt kann Threat Hunting einen erheblichen Beitrag zur Verbesserung der Cybersicherheit leisten. Trotzdem ist es wichtig zu beachten, dass Threat Hunting nur ein **Teil eines umfassenden Sicherheitsansatzes** ist. Unternehmen sollten sich bewusst sein, dass diese Methode Zeit, Ressourcen und Expertise erfordert und kontinuierlich angepasst und optimiert werden muss.