Blind-Spot-Analyse mithilfe der MITRE ATT&CK Matrix und XDR

HERAUSFORDERUNGEN BEI DER STRUKTURIERUNG SICHERHEITSRELEVANTER LOGS IM SIEM

Bei dem Versuch, die Infrastruktur so sicher wie möglich zu gestalten und vor Angreifern zu schützen, stehen die IT-Sicherheitsteams vor zahlreichen Herausforderungen. Tägliche Änderungen an den IT-Systemen und ständig neue Sicherheitslücken erschweren diese Aufgabe zusätzlich. Ein wichtiger Aspekt dabei ist, den Überblick nicht zu verlieren und ein strukturiertes Vorgehen zu entwickeln. Doch wo fängt man an und wann ist eine Infrastruktur sicher? Zur Strukturierung kann hier die MITRE ATT&CK Matrix herangezogen werden.

In einer IT-Infrastruktur ist eine Vielzahl von Produkten zur Erhöhung der Sicherheit im Einsatz. Das wohl bekannteste Tool ist die Firewall. Mit der E-Mail als Einfallstor Nummer eins für Schadsoftware gehören aber auch E-Mail-Security-Gateways und Endpunkt-Virenscanner zur Grundausstattung. Diese werden von den Verantwortlichen in den Unternehmen meist noch durch Intrusion-Detection-and-Prevention-(IDS/IPS)-Systeme sowie Extended-Detection-and-Response-(XDR)-Lösungen ergänzt.

Alle diese Sicherheitskomponenten – aber auch die meisten anderen Systeme heutiger IT-Infrastrukturen – protokollieren umfangreiche Informationen über durchgeführte Änderungen oder erfolgte Zugriffe. Viele moderne Angriffsformen lassen sich erst durch die Zusammenschau dieser Informationen identifizieren. Die MITRE „Adversarial Tactics, Techniques and Common Knowledge"-(ATT&CK)-Matrix kann dabei helfen, diese Daten zu strukturieren und zu entscheiden, welche Daten sicherheitsrelevant sind und welche fehlen, um einen Angriff möglichst schnell zu erkennen.

WAS IST DAS MITRE ATT&CK-FRAMEWORK

Die MITRE ATT&CK Matrix wurde von der Organisation MITRE entwickelt, die sich mit verschiedenen Programmen im Bereich IT-Sicherheit engagiert. Neben der Enterprise Matrix gibt es noch eine Matrix für mobile Betriebssysteme und eine für Industrial Control Systems (ICS).

Das ATT&CK-Framework stellt Informationen über Cyberbedrohungen und Vorgehensweisen von Angreifergruppen zur Verfügung, setzt sich mit den verschiedenen Phasen eines Hackerangriffs auseinander und ordnet den Phasen Angriffstechniken zu, die auf realen Ereignissen basieren. Dabei werden die Techniken innerhalb der Enterprise Matrix aktuell in die folgenden 14 Taktiken als Spalten eingeordnet.

- **Reconnaissance**
  Hier sammeln Angreifer Informationen für einen späteren Angriff.
- **Ressource Development**
  Beschaffung von Ressourcen, die für einen späteren Angriff genutzt werden können
- **Initial Access**
  Der Angreifer verschafft sich Zugriff zum Unternehmensnetzwerk.
- **Execution**
  Ausführung von Schadsoftware
- **Persistence**
  Der Angreifer verfestigt den Zugriff, um längerfristigen Zugang zu den Systemen zu behalten.
- **Privilege Escalation**
  Verschaffen von höheren Berechtigungen im Unternehmensnetzwerk
- **Defense Evasion**
  Verwischen von Spuren, um unerkannt zu bleiben
- **Credential Access**
  Der Angreifer versucht, an die Zugangsdaten des Benutzers zu kommen.
- **Discovery**
  Aufbau eines umfassenden Überblicks über das Unternehmensnetzwerk
- **Lateral Movement**
  Verbreitung im Netzwerk und Kompromittierung von weiteren Systemen
- **Collection**
  Sammeln von relevanten Unternehmensdaten
- **Command and Control**
  Erlangen der Kontrolle über die Systeme
- **Exfiltration**
  Daten auslesen und stehlen
- **Impact**
  Manipulation oder Beschädigung der Systeme und Daten

In der Matrix werden die einzelnen Techniken dann in die Spalte mit der jeweiligen Taktik einsortiert und beschrieben. Die Beschreibung gibt Empfehlungen, wie sich diese Angriffe erkennen lassen, und erläutert Möglichkeiten zur Vorbeugung oder Reduzierung der Angriffsfläche. Darüber hinaus werden Beispiele für bekannte Angriffe oder Schadprogramme aufgeführt, die sich dieser Technik bedienen.

Mithilfe dieser Einordnung kann abgeleitet werden, welche Protokolle oder Log-Informationen für die Erkennung wichtig sind. Man sollte zudem sicherstellen, dass diese Informationen in das zentrale Security-Information-and-Event-Management-(SIEM)-System einfließen.

Ein Beispiel: Eine Technik in der Phase „Defense Evasion" ist Indicator Removal. Konkret geht es hier darum, dass Angreifer im Unternehmensnetzwerk versuchen, durch das Ändern oder

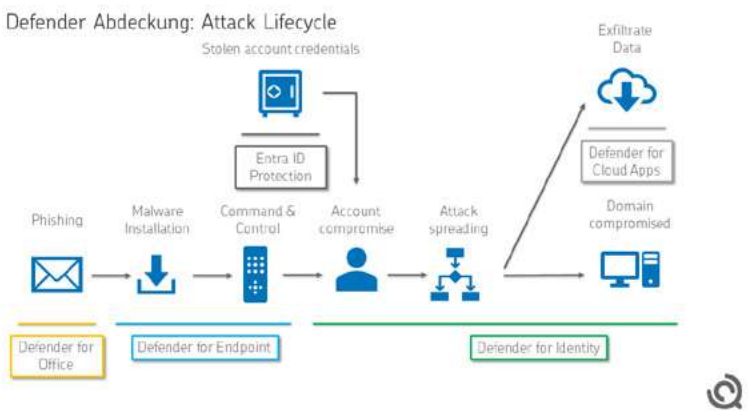

Abbildung 1: Darstellung eines Attack-Lifecycles durch Defender XDR (Bild: Net at Work GmbH)

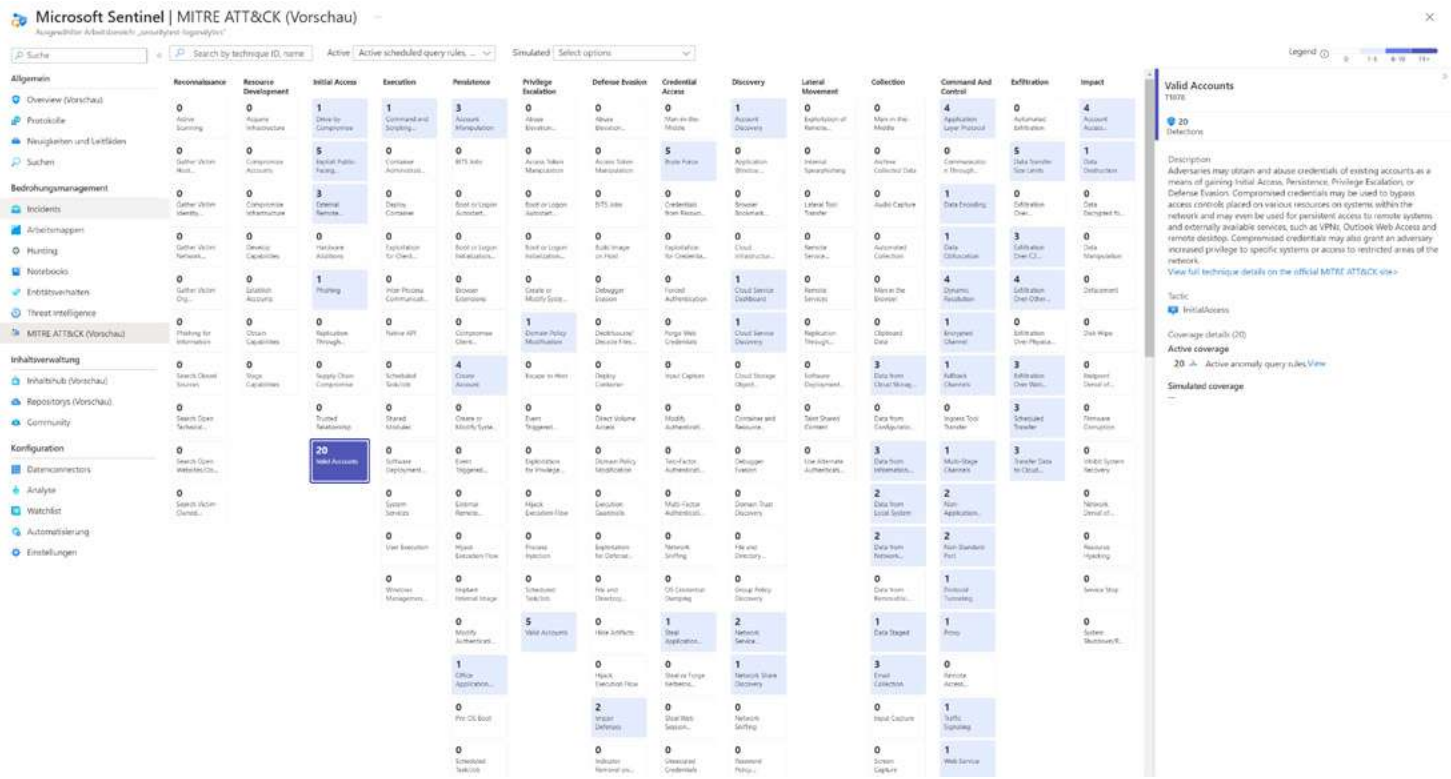

Abbildung 2: Screenshot aus Sentinel, der die Techniken und Taktiken der MITRE ATT&CK Matrix innerhalb von Sentinel abbildet (Bild: Net at Work GmbH)

Löschen von Informationen oder Dateien den Angriff zu verschleiern, um möglichst lange unerkannt zu bleiben. Als Beispiel sei das Löschen des Windows Event Logs genannt. Für die Erkennung sollte sichergestellt sein, dass entsprechende Löschbefehle per Powershell oder das Löschen von „.evtx"-Dateien an das SIEM übermittelt werden.

ABDECKUNG BEI MICROSOFT

Wie bereits erwähnt, besteht die Herausforderung nun darin, festzustellen, welche Informationen durch die eingesetzten Sicherheitslösungen schon vorhanden sind und an welchen Stellen durch Mangel an Protokollen eine Erkennung verhindert wird. Dort, wo die Informationslage Lücken aufweist, spricht man von sogenannten Blind Spots.

Mit der Microsoft XDR-Technologie können viele Infrastrukturbereiche beleuchtet werden:

- **Endpunkte** – von Clients und Servern bis zu Netzwerkgeräten
- **Identitäten** – hybride Identitäten im lokalen Active Directory und Entra ID
- **E-Mail und Collaboration Tools** – Kommunikation via Chat oder E-Mail und Austausch von Links oder Dateien
- **Cloud Apps** – Kommunikation und Datenverbindung zu Microsoft 365 sowie anderen Cloud-Diensten und Apps

Die Informationen aus diesen Bereichen ermöglichen die Erkennung von Angriffen aus vielen Techniken der MITRE ATT&CK Matrix. Der Grad der Abdeckung lässt sich zum Beispiel über die MITRE Engenuity ATT&CK-Evaluations (https://mitre-engenuity.org/) ermitteln. Dabei werden anhand von Simulationen die Techniken realer Bedrohungsszenarien ausgewertet und geprüft, wie und auf welcher Datengrundlage die jeweilige Sicherheitslösung die Technik erkennt. Mithilfe dieser Beispiele bekommt man eine erste Einschätzung darüber, wie gut die Abdeckung ist und hat eine Vergleichsmöglichkeit für die Lösungen verschiedener Hersteller.

Werden nicht alle Bereiche der Umgebung durch eine Lösung wie beispielsweise Microsoft XDR abgedeckt und fehlen auf Basis der ATT&CK-Evaluations-Bewertung noch Datenquellen zur vollständigen Abdeckung der Angriffsphasen und -techniken, sollte die Verantwortlichen in den Unternehmen die Informationen aus weiteren Produkten hinzuziehen.

ERWEITERUNG MIT SIEM

Alle sicherheitsrelevanten Informationen sollten dann in einem SIEM zusammengeführt und gespeichert werden, um sie zentral verarbeiten und Korrelationen zwischen verschiedenen Ereignissen aus unterschiedlichen Systemen herstellen zu können. Hier werden alle zuvor identifizierten Sicherheitslösungen und sicherheitsrelevanten Datenquellen angeschlossen.

Das von Microsoft in Azure angebotene SIEM- &-SOAR-Produkt Microsoft Sentinel profitiert von einer Integration der MITRE ATT&CK Matrix. An Microsoft Sentinel sind Sicherheitssysteme wie die Microsoft XDR-Plattform, Firewalls oder VPN-Gateways per Daten-Connectoren

angebunden. Die angeschlossenen Log-Quellen werden mit Analyseregeln untersucht, und jede Regel kann einer oder mehreren Taktiken zugeordnet werden. Somit ergibt sich eine Übersicht, welche Techniken und Taktiken der MITRE ATT&CK Matrix gut abgedeckt sind und wo Blind Spots vorhanden sind.

BLIND SPOTS SCHLIEßEN

Wurden nun mit der integrierten ATT&CK Matrix in Microsoft Sentinel die Blind Spots ermittelt, muss man als Nächstes für die Schließung dieser Lücken sorgen. Dabei hilft das folgende Vorgehen:

1. **Priorisierung**
   Je nachdem wie viele Phasen oder Techniken ohne angebundene Datenquellen ermittelt wurden, ist hier eine Priorisierung unerlässlich, um nicht den Fokus zu verlieren. Die Priorisierung kann sich jedoch bei verschiedenen Organisationen unterscheiden. Hierbei können zum Beispiel spezielle Branchenbedrohungen oder regionale Bedrohungen eine Rolle spielen. Des Weiteren kann auch eine Einordnung nach Angriffsgruppen bei der Priorisierung helfen. Werden die Angriffsgruppen ermittelt, die eine entsprechende Relevanz für das Unternehmen haben, kann sich die Blind-Spot-Analyse auf die eingesetzten Techniken fokussieren.

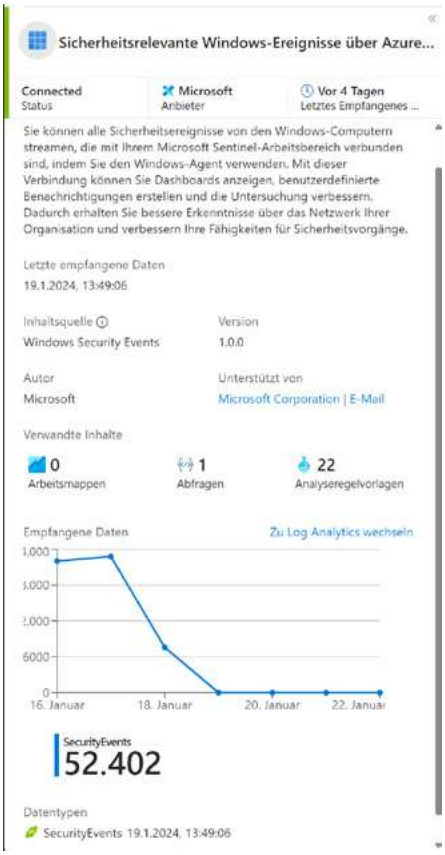

Abbildung 3: Beispiel eines Daten-Connectors (Bild: Net at Work GmbH)

2. **Identifizierung der Datenquelle**
   Wurden die fehlenden Bereiche ermittelt, wird als Nächstes geklärt, ob die Daten prinzipiell bereits im SIEM vorhanden sind beziehungsweise ob überhaupt Protokollinformationen sinnvoll zur Identifizierung genutzt werden können. Um die notwendigen Datenquellen zu ermitteln, kann wieder die MITRE ATT&CK Matrix zu Rate gezogen werden.

3. **Anbindung von Datenquellen**
   Fehlende Log-informationen müssen nun per Daten-Connector angebunden werden. Wurde beispielsweise ermittelt, dass bestimmte Event Logs von Windows-Servern zur Erkennung von Angriffen dienen können, kann ein Event Log Forwarding eingerichtet werden. Sind hingegen zusätzliche Firewall-Logs erforderlich, kann eine Syslog-Anbindung an Microsoft Sentinel helfen, die Informationslücke zu schließen. Für viele Produkte stehen bereits vorgefertigte Connectoren zur Verfügung, die nur konfiguriert werden müssen.

4. **Analyseregeln**
   Wenn die Daten bereits vorhanden waren oder nun durch zusätzliche Anpassungen oder neue Daten-Connectoren vorhanden sind, sollte das SIEM bei Auffälligkeiten mindestens alarmieren. Dafür werden Analyseregeln eingerichtet, die per Abfragesprache Logs durchsuchen und einen Alarm auslösen, wenn die Abfrage ein entsprechendes Ergebnis zurückgibt. Diese Analyseregeln werden mit den MITRE ATT&CK-Techniken verknüpft, sodass dann auch in der integrierten Matrix die Abdeckung weiter visualisiert werden kann. In dem Beispiel von oben für die Technik „Indicator Removal" kann so etwa das Löschen des Windows Security-Logs einen Alarm auslösen. Dafür wird zunächst das relevante Event mit der ID „1102" per Event Log Forwarding vom Domain Controller an Microsoft Sentinel angebunden. Das Event wird immer dann protokolliert, wenn das Security-Log gelöscht wird. In einer Analyseregel wird das Aufkommen dieses Events also abgefragt und mit der Technik „T1070 – Indicator Removal on Host" verknüpft.

5. **Visualisierung**
   Bei einigen Daten kann eine zusätzliche grafische Aufbereitung der Logs sinnvoll sein. So kann im Analysefall schnell ein Überblick gewonnen werden. Die Aufbereitung in Form von Grafiken oder Tabellen ist ebenfalls mit Microsoft Sentinel möglich.

FAZIT

Die Analyse vieler Daten und die Ausarbeitung der relevanten Daten zur Angriffserkennung ist mit steigender Komplexität in IT-Infrastrukturen eine Herausforderung. Neuerungen bei Angriffsmustern oder neuartige Bedrohungen machen diese Aufgabe nicht leichter. Mit der MITRE ATT&CK Matrix und einer strukturierten Einbindung in ein SIEM ist es jedoch möglich, die Blind Spots im Blick zu behalten und die Abdeckung über die Angriffsphasen zu optimieren. ■

THOMAS WELSLAU
ist Competence Lead Security bei Net at Work GmbH.