Anlage zur Dienstvereinbarung über die Nutzung eines Security Information and Event Managements (SIEM) für den Geschäftsbereich des Bayerischen Staatsministeriums der Justiz

In dieser Anlage werden die Funktionen von Microsoft Sentinel näher erläutern. Microsoft Sentinel ist eine Cloud-basierte SIEM-Lösung (Security Information and Event Management), die speziell für Unternehmen und Behörden entwickelt wurde. Mit Sentinel können Bedrohungen in Echtzeit erkannt, untersucht und auf diese automatisiert reagiert werden. Durch dieses Vorgehen steigt die Fähigkeit der bayerischen Justiz auf bislang noch unbekannte und/oder zielgerichtete Angriffe zu reagieren, in erheblichem Maße. Die Funktionsgruppen von Microsoft Sentinel können in fünf verschiedene Hauptkategorien unterteilt werden, welche im Folgenden beschrieben werden.

Freigegebene Funktionskategorien

1. Logdatensammlung

Microsoft Sentinel sammelt Log-Daten von verschiedenen Quellen. Diese Sammlung ist die Grundvoraussetzung für die Angriffserkennung. Zu den Quellen zählen Firewalls, Server, Netzwerkgeräte und Arbeitsplatzgeräte. Die gesammelten Daten bestehen z. B. aus Auslastungswerten der Prozessoren und des Speichers, Fehler- und Warnmeldungen, geblockte Zugriffe, generelle Metriken über Dateisystem, Anwendungen und Netzwerkaktivität.

2. Analyse

Die Logdateien werden mit Methoden, die von stetig lernender künstlicher Intelligenz gestützt werden (sog. Machine-Learning Algorithmen) voranalysiert, die einzelnen Meldungen werden auf mögliche Anomalien priorisiert.

Die Machine-Learning-Algorithmen von Sentinel sind darauf trainiert, verschiedene Arten von Bedrohungen zu erkennen, wie beispielsweise Malware-Infektionen: Sentinel kann ungewöhnliche Aktivitäten auf Endpunkten erkennen, die auf eine

Malware-Infektion hinweisen, wie beispielsweise das Herunterladen von verdächtigen Dateien oder das Ausführen von ungewöhnlichen Prozessen.

3. Korrelation

Sentinel kann verschiedene Ereignisse aus den Logdateien miteinander in Beziehung setzen, um Bedrohungen zu erkennen. Grundlage hierfür ist das Verschränken der analysierten Logdateien, aus denen die KI-Prozesse Bedrohungsmuster herauslesen können.

Ein Beispiel für die Korrelation wäre das Erkennen von Angriffen auf mehrere Endpunkte oder Server innerhalb eines bestimmten Zeitraums. Sentinel kann die Informationen aus verschiedenen Log-Dateien zusammenführen und analysieren, um festzustellen, ob es sich um eine koordinierte Attacke handelt. Durch die Korrelation von Daten kann Sentinel Bedrohungen effektiver erkennen und priorisieren als es herkömmliche Sicherheitssysteme für sich alleine könnten.

4. Benutzer- und Entitätsanalyse

Die User and Entity Behavior Analytics (UEBA) kann ungewöhnliche Aktivitäten auf Benutzerkonten erkennen, die auf eine mögliche Bedrohung hinweisen. Hierzu zählen beispielsweise ungewöhnliche Anmeldeversuche, das Versenden von E-Mails an verdächtige Empfangsadressen oder ein ungewöhnlich hohes Aufkommen von Verschlüsselungsoperationen. Durch die Analyse des Benutzerverhaltens kann Sentinel potenzielle Bedrohungen frühzeitig erkennen und verhindern. An dieser Stelle werden personenbezogene Daten verarbeitet.

Grundlage für die Benutzer- und Entitätsanalyse ist ein sog. Baselining, in dem Nutzergewohnheiten zuordenbar aufgenommen werden. Hierfür werden Daten ausschließlich aus bereits bestehenden Logdateien verwendet, um Referenzwerte für das normale Nutzerverhalten zu erhalten. Erst durch diese Referenzwerte können sicherheitsrelevante Anomalien bestimmt werden. Zu den verwendeten abstrahierten Daten gehören z. B. der Status der Antivirenprogramme, Firewalleinstellungen oder Kommunikationsbeziehungen der verwendeten IP-Adressen. Zu den verwendeten direkt zuordenbaren Daten zählen z. B. die Anzahl der Anmeldungen in einem bestimmten Zeitraum, die verwendeten Geräte des Benutzers oder auch die aufgerufenen Anwendungen.

Sowie dieses Baselining abgeschlossen ist, können Bedrohungen, die den Benutzer selbst als Eingangstor verwenden, durch eine Veränderung des bisherigen Verhaltens erkannt und verhindert werden. Diese Angriffe sind oftmals mit herkömmlichen Mitteln nicht zu erfassen. Grund hierfür ist, dass fortgeschrittene Angriffsszenarien aus einer Vielzahl verteilter Schritte bestehen, die für sich genommen kaum oder gar nicht von erlaubten Tätigkeiten zu unterscheiden sind.

5. Automatisierte Reaktion

Sentinel kann automatisierte Reaktionen auf Bedrohungen auslösen, um den Schaden zu minimieren. Beispiele sind die Deaktivierung von Rechten zur Verschlüsselung, Beendigung von Prozessen, die eine Bedrohung darstellen bis hin zur Deaktivierung eines Netzwerkports, wenn die Bedrohung sicher festgestellt werden kann. Ebenfalls wird IT-Sicherheitspersonal automatisch alarmiert, wenn eine potentielle Bedrohung festgestellt wird.

Eine Änderung dieser Anlage bedarf der Zustimmung der Hauptpersonalvertretungen.