Bayerisches Ministerialblatt

BayMBl. 2024 Nr. 557 20. November 2024

2003.4-J

Dienstvereinbarung über die Nutzung der Software Microsoft Sentinel bei den Gerichten und Staatsanwaltschaften im Geschäftsbereich des Bayerischen Staatsministeriums der Justiz

Bekanntmachung des Bayerischen Staatsministeriums der Justiz

vom 27. September 2024, Az. H4 - 1500E - VI - 9730/2022

Zur Gewährleistung der schutzwürdigen Interessen und Belange der Bediensteten schließen das **Bayerische Staatsministerium der Justiz** und der **Hauptpersonalrat bei dem Bayerischen Staatsministerium der Justiz**, der **Hauptrichterrat der ordentlichen Gerichtsbarkeit** sowie der **Hauptstaatsanwaltsrat** (im Folgenden: Hauptpersonalvertretungen) gemäß Art. 73 in Verbindung mit Art. 75a Abs. 1 des Bayerischen Personalvertretungsgesetzes (BayPVG) sowie Art. 27 Abs. 5, Art. 31 und Art. 37 Abs. 1 in Verbindung mit Art. 28 Abs. 1 Nr. 9 des Bayerischen Richter- und Staatsanwaltsgesetzes (BayRiStAG) folgende Dienstvereinbarung:

1. Gegenstand und Geltungsbereich

1.1 Gegenstand dieser Dienstvereinbarung ist die Einführung eines SIEM (Security Information and Event Management) Systems im Geschäftsbereich des Bayerischen Staatsministeriums der Justiz mit Ausnahme des Justizvollzugs. Um den Angriffsszenarien auf schutzbedürftige Komponenten im Justiznetz zu begegnen, wird als Ergänzung zu den gängigen Abwehrmechanismen zur Anomaliedetektion ein sog. SIEM System eingeführt. Hierzu wird die KI-gestützte Cloudsoftware Microsoft Sentinel verwendet, welche anfallende Logdateien untereinander abgleicht und so Angriffsmuster auch in komplexen und verteilten Szenarien erkennt.

1.2 Die datenschutzrechtlichen, dienstrechtlichen und tarifrechtlichen Bestimmungen bleiben unberührt.

2. Begriffsbestimmungen

2.1 Verhaltenskontrolle: Jede Maßnahme zur Überprüfung oder Auswertung des Verhaltens des einzelnen Beschäftigten durch Datenverarbeitungsprogramme.

2.2 Leistungskontrolle: Jede Maßnahme zur Überprüfung oder Auswertung der Qualität oder Quantität der Leistung des einzelnen Beschäftigten durch Datenverarbeitungsprogramme.

3. Zustimmung zur Einführung und Anwendung

3.1 Die Hauptpersonalvertretungen stimmen der Einführung und Anwendung des SIEM Systems Microsoft Sentinel gemäß Art. 70 Abs. 1 in Verbindung mit Art. 75a Abs. 1 Nr. 1 BayPVG sowie Art. 17 Abs. 4, Art. 28 Abs. 1 Nr. 9a und Art. 37 Abs. 1 BayRiStAG zu. Sie sind bei erheblichen Änderungen des Kollaborationswerkzeugs Microsoft Sentinel zu beteiligen.

3.2 Die genutzten Funktionen ergeben sich aus der Anlage. Eine Änderung der Anlage erfolgt nur mit Zustimmung der Hauptpersonalvertretungen. Eine Änderung der Dienstvereinbarung ist hierfür nicht erforderlich.

Die Hauptpersonalvertretungen sind vor der Freigabe neuer Funktionen von Microsoft Sentinel zu beteiligen.

4. Leistungs- und Verhaltenskontrolle durch die Auswertung der Logdateien

4.1 Das SIEM System ist ausschließlich für die Detektion von Sicherheitsvorfällen eingerichtet. Es erfolgt keine anderweitige Nutzung. Eine Leistungs- und Verhaltenskontrolle von Bediensteten durch die Erfassung und Verarbeitung der verschränkten Logdateien findet hierbei mit Ausnahme der in Nrn. 4.2 und 4.3 geregelten Fälle nicht statt.

4.2 Ausgenommen sind Fälle, in denen ein akuter Sicherheitsvorfall durch das System gemeldet wird. In diesem Fall wird zwar keine Leistungs-, aber falls für die Aufklärung und Behebung des Sicherheitsvorfalls notwendig, eine Verhaltenskontrolle durchgeführt. Diese wird in einem Rahmen durchgeführt, der zur Rekonstruierung des Hergangs und zur Feststellung des Schadensausmaßes notwendig ist. Die Verhaltenskontrolle wird nach dem Grundsatz der Datensparsamkeit durchgeführt und umfasst die im Zeitraum des Alarms der kontaktierten Systeme des Benutzerendgeräts sowie die genutzten technischen Dienste. Die Kontrolle wird durch ein eigenes, auf diesen Anwendungsfall spezialisiertes Team des Betriebsdienstleisters durchgeführt (Sog. SOC => Security Operation Center). Dieses befindet sich nicht in der Organisationsstruktur des bajTECH Projektes. Alle beteiligten Mitarbeiter sind im Rahmen des Gesetzes über die förmliche Verpflichtung nichtbeamteter Personen auf gewissenhafte Erfüllung seiner Obliegenheiten verpflichtet. Weiterhin werden die Mitarbeiter im Rahmen eines gesonderten NDA (Non Disclosure Agreement) zur Verschwiegenheit verpflichtet.

4.3 Ausgenommen sind ebenso Fälle, in denen eine individuelle Verhaltens- und Leistungskontrolle wegen eines durch konkrete Tatsachen begründeten Verdachts auf einen dienst-, arbeits-, datenschutz- oder strafrechtlichen Verstoß erforderlich ist.

In diesem Fall ist der oder die Bedienstete vor Beginn über den Umfang und den Zweck der Maßnahme zu unterrichten und gegebenenfalls zur Stellungnahme aufzufordern, soweit nicht Gründe der Unaufschiebbarkeit oder der Geheimhaltungsbedürftigkeit einer Maßnahme (z. B. strafrechtliche oder disziplinarrechtliche Ermittlungen) entgegenstehen. Die zuständige Personalvertretung ist unverzüglich zu unterrichten, soweit dies durch den Betroffenen beantragt wird. Der Betroffene ist hierüber zu belehren. Nach Beendigung der Maßnahmen sind der Betroffene sowie die von ihm eingeschaltete Personalvertretung über den Ausgang der Maßnahme zu unterrichten.

Zu diesem Zweck hergestellte Auswertungen sind nach Gebrauch unverzüglich zu vernichten, soweit Rechtsvorschriften nicht entgegenstehen.

5. Informationspflicht

Die Hauptpersonalvertretungen erhalten einen im Monatszyklus angefertigten Bericht, aus welchem die Anzahl der gemeldeten Alarme des Systems sowie die aus diesen Alarmen generierten Sicherheitsvorfälle hervorgehen. Die übermittelten Daten können auf Anfrage der Hauptpersonalvertretungen mit Zustimmung des StMJ erweitert werden.

6. Datenzugriff und Schweigepflicht

6.1 Der Zugriff auf Daten in Verfahren im Sinne der Nr. 4.2 darf nur durch Dienst- bzw. Fachvorgesetzte sowie von ihnen beauftragte Mitarbeiter erfolgen. Letztere sind der Personal-, Richter- oder Staatsanwaltsvertretung namentlich mitzuteilen. Die Zugriffe sind für die Kontrollzwecke zu dokumentieren. Hierbei ist mindestens festzuhalten, wer wann und mit welcher Eingabe welche Auswertung erzielt hat. Unberührt bleibt der Zugriff durch technische Mitarbeiter zur Wahrnehmung von deren Aufgaben.

6.2 Alle Personen, die Zugriff auf solche Daten haben, unterliegen einer besonderen Verschwiegenheitspflicht, diese ist Teil ihrer Dienstaufgaben. Sie gilt auch gegenüber Vorgesetzten aus anderen Bereichen. Sie sind hierüber gesondert zu belehren.

7. Inkrafttreten, Laufzeit

7.1 Die Dienstvereinbarung tritt mit der Unterzeichnung in Kraft. Sie kann von jeder Partei mit einer Frist von drei Monaten zum Ende eines Kalendermonats schriftlich gekündigt werden.

7.2 Nach Außerkrafttreten der Dienstvereinbarung wegen Kündigung gelten ihre Regelungen bis zum Abschluss einer neuen Dienstvereinbarung weiter.

München, den 12. September 2024

Bayerisches Staatsministerium der Justiz

Dr. Winfried B r e c h m a n n
Ministerialdirektor

München, den 17. September 2024

Hauptpersonalrat

Ralf S i m o n
Amtmann im Justizvollzugsdienst

Nürnberg, den 23. September 2024

Hauptrichterrat

Ingrid D e m m e l
Vorsitzende Richterin am Oberlandesgericht

Rosenheim, den 27. September 2024

Hauptstaatsanwaltsrat

Gunther S c h a r b e r t
Oberstaatsanwalt

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.

Impressum

Herausgeber:
Bayerische Staatskanzlei, Franz-Josef-Strauß-Ring 1, 80539 München
Postanschrift: Postfach 220011, 80535 München
Telefon: +49 (0)89 2165-0, E-Mail: direkt@bayern.de

Technische Umsetzung:
Bayerische Staatsbibliothek, Ludwigstraße 16, 80539 München

Druck:
Justizvollzugsanstalt Landsberg am Lech, Hindenburgring 12, 86899 Landsberg am Lech
Telefon: +49 (0)8191 126-725, Telefax: +49 (0)8191 126-855, E-Mail: druckerei.ll@jv.bayern.de

ISSN 2627-3411

Erscheinungshinweis / Bezugsbedingungen:
Das Bayerische Ministerialblatt (BayMBl.) erscheint nach Bedarf, regelmäßiger Tag der Veröffentlichung ist Mittwoch. Es wird im Internet auf der Verkündungsplattform Bayern www.verkuendung.bayern.de veröffentlicht. Das dort eingestellte elektronische PDF/A-Dokument ist die amtlich verkündete Fassung. Die Verkündungsplattform Bayern ist für jedermann kostenfrei verfügbar.
Ein Ausdruck der verkündeten Amtsblätter kann bei der Justizvollzugsanstalt Landsberg am Lech gegen Entgelt bestellt werden. Nähere Angaben zu den Bezugsbedingungen können der Verkündungsplattform Bayern entnommen werden.