CyberMonoLog: Cyber Security Monitoring und Logging Guidelines

Monitoring und Logging, also das sukzessive Aufzeichnen und Festhalten wesentlicher Ereignisse in einem IKT-System, wie z.B. die Authentifizierung von Nutzern, das Starten von Diensten oder der Zugriff auf Ressourcen, sind wesentliche Voraussetzungen, um Cyber Angriffe zu erkennen oder zurückliegende Vorfälle professionell aufzuarbeiten. Aufgezeichnete Ereignisse geben Einblick darin, wie Systeme verwendet werden und bieten daher auch die Möglichkeit Missbrauch frühzeitig aufzudecken.

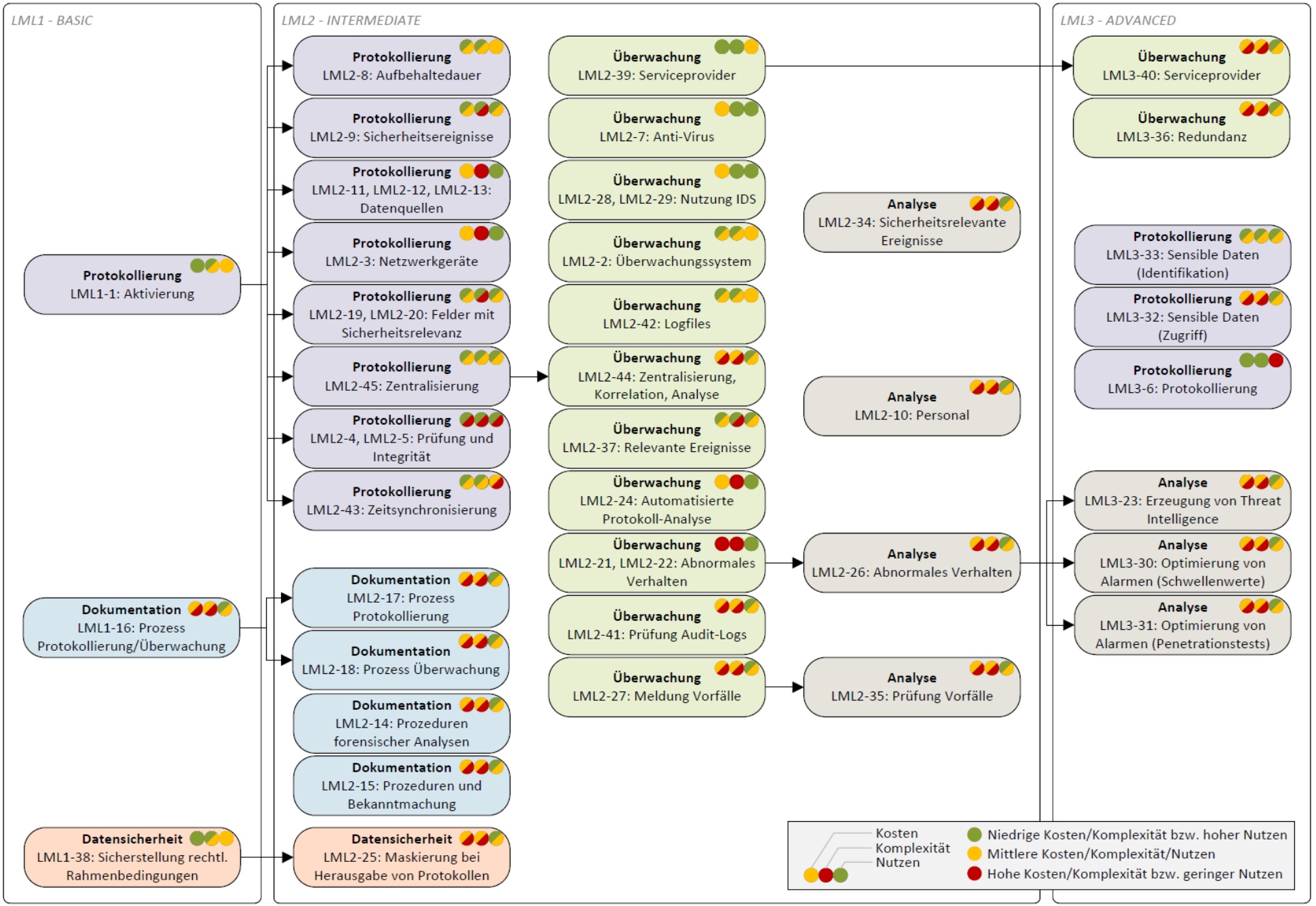
Im von der FFG geförderten KIRAS Projekt CyberMonoLog (FFG Nr. 886330) wurde der vorliegende Leitfaden zur Umsetzung von Monitoring und Logging Funktionalitäten zur Erhöhung der Informationssicherheit speziell in Klein- und Mittelständischen Unternehmen (KMUs) erarbeitet. Dafür wurden umzusetzende Maßnahmen entlang gesammelter Anforderungen aus einschlägigen Standards und Normen, insb. der ISO27000-Reihe, dem BSI Grundschutz und der CIS Top18 erarbeitet. Diese wurden weiters in sog. Log Maturity Levels (LML) unterteilt. Dabei ist vorgesehen, dass Unternehmen zuerst alle Basisanforderungen aus LML1 erfüllen, bevor diese sukzessive erhöhte Anforderungen aus LML2 und in weiterer Folge LML3 implementieren. Der Leitfaden richtet sich insbesondere an Personen, die die Verantwortung über die Cybersicherheit innerhalb des Unternehmens tragen und sowohl über die Kompetenzen zur Erhebung und Bewertung des vorherrschenden Security-Standards im Unternehmen als auch über das notwendige technische Know-How zur Umsetzung von Sicherheitsmaßnahmen verfügen (CISO, IT-Admins, SecOps, etc.). Die Umsetzung der Anforderungen muss nicht firmenintern erfolgen; der Leitfaden dient selbstverständlich auch als Grundlage für die Beauftragung von Dienstleistern, etwa zur initialen Erfassung des Ist-Standes, Abschätzung des Aufwandes zur Umsetzung fehlender Anforderungen, Priorisierung von Anforderungen oder Erstellung eines Lastenhefts.

Das Dokument umfasst zwei Teile: (1) eine grafische Übersicht von Anforderungen mit ihren jeweiligen Abhängigkeiten und Bewertungen (die Ampeln geben von links nach rechts Kosten, Komplexität und Nutzen an), (2) eine Auflistung dieser Anforderungen in tabellarischer Form, und (3) eine Ansammlung von Guidelines, um die Anforderungen zu erfüllen. Dabei können die zur Erfüllung einer Anforderung relevanten Guidelines durch Klicken auf den entsprechenden Link in der Tabelle einfach gefunden werden.

Wenden Sie das Dokument wie folgt an: Erfassen Sie Ihre Ist-Situation, indem Sie überprüfen, welche der in der nachfolgenden Tabelle genannten Anforderungen Sie bereits umgesetzt haben. Arbeiten Sie dafür die folgende Liste der Anforderungen von oben nach unten ab. Danach widmen Sie sich den noch offenen Anforderungen aus der Liste. Eine Entscheidungsgrundlage zur Umsetzung bestimmter Anforderungen sollen die beigestellten Bewertungsmetriken liefern. Anforderungen deren Erfüllung einen hohen Nutzen mit sich bringen, dabei aber nur niedrige Kosten oder Komplexität der Umsetzung nach sich ziehen, sollte der Vorrang gegeben werden. Eine grobe allgemeine Abschätzung dieser Metriken ist bereits in der Übersichtstabelle enthalten und in den jeweiligen verlinkten Guidelines konkret formuliert. Innerhalb der drei LML Stufen wurden die Anforderungen in nachfolgender Tabelle gemäß dieser Metriken sortiert, sodass kostengünstige, einfach umsetzbare, und möglichst nutzbringende Anforderungen zuerst genannt sind; aufgrund von Unterschieden in Ihrer Umgebung könnten diese Bewertungen jedoch abweichen. Haben Sie die noch zu erfüllenden Anforderungen identifiziert, bieten die verknüpften Leitfäden grundlegende Informationen zur Implementierung angemessener Maßnahmen sowie Links auf weiterführende Informationen. Sollten Sie nicht in der Lage sein, Anforderungen entsprechend umzusetzen, stellt dieser Leitfaden und die darauf basierende Bewertung der Ist-Situation eine nützliche Grundlage für die Konsultation externer Cybersicherheitsberater dar.

Die vorliegenden Guidelines erheben nicht den Anspruch eines vollständigen Implementierungsleitfadens, sondern sollen die aus öffentlichen Quellen beziehbaren Informationen zur Realisierung von Monitoring und Logging Funktionalitäten einfach für eine große Zahl unterschiedlicher Unternehmen zugänglich machen. In diesem Sinne beinhaltet das vorliegende Dokument v.a. Links auf weiterführende Literatur und bietet somit einen wesentlichen Beitrag zum erfolgreichen Start der Umsetzung.

Feedback und Anregungen zur Überarbeitung senden Sie bitte an: DDr. Florian Skopik, florian.skopik@ait.ac.at


LML1 - BASIC
LML2 - INTERMEDIATE
LML3 - ADVANCED
Protokollierung
LML1-1: Aktivierung
Dokumentation
LML1-16: Prozess Protokollierung/Überwachung
Datensicherheit
LML1-38: Sicherstellung rechtl. Rahmenbedingungen
Protokollierung
LML2-8: Aufbehaltedauer
Protokollierung
LML2-9: Sicherheitsereignisse
Protokollierung
LML2-11, LML2-12, LML2-13: Datenquellen
Protokollierung
LML2-3: Netzwerkgeräte
Protokollierung
LML2-19, LML2-20: Felder mit Sicherheitsrelevanz
Protokollierung
LML2-45: Zentralisierung
Protokollierung
LML2-4, LML2-5: Prüfung und Integrität
Protokollierung
LML2-43: Zeitsynchronisierung
Dokumentation
LML2-17: Prozess Protokollierung
Dokumentation
LML2-18: Prozess Überwachung
Dokumentation
LML2-14: Prozeduren forensischer Analysen
Dokumentation
LML2-15: Prozeduren und Bekanntmachung
Datensicherheit
LML2-25: Maskierung bei Herausgabe von Protokollen
Überwachung
LML2-39: Serviceprovider
Überwachung
LML2-7: Anti-Virus
Überwachung
LML2-28, LML2-29: Nutzung IDS
Überwachung
LML2-2: Überwachungssystem
Überwachung
LML2-42: Logfiles
Überwachung
LML2-44: Zentralisierung, Korrelation, Analyse
Überwachung
LML2-37: Relevante Ereignisse
Überwachung
LML2-24: Automatisierte Protokoll-Analyse
Überwachung
LML2-21, LML2-22: Abnormales Verhalten
Überwachung
LML2-41: Prüfung Audit-Logs
Überwachung
LML2-27: Meldung Vorfälle
Analyse
LML2-34: Sicherheitsrelevante Ereignisse
Analyse
LML2-10: Personal
Analyse
LML2-26: Abnormales Verhalten
Analyse
LML2-35: Prüfung Vorfälle
Überwachung
LML3-40: Serviceprovider
Überwachung
LML3-36: Redundanz
Protokollierung
LML3-33: Sensible Daten (Identifikation)
Protokollierung
LML3-32: Sensible Daten (Zugriff)
Protokollierung
LML3-6: Protokollierung
Analyse
LML3-23: Erzeugung von Threat Intelligence
Analyse
LML3-30: Optimierung von Alarmen (Schwellenwerte)
Analyse
LML3-31: Optimierung von Alarmen (Penetrationstests)
Kosten
Komplexität
Nutzen
Niedrige Kosten/Komplexität bzw. hoher Nutzen
Mittlere Kosten/Komplexität/Nutzen
Hohe Kosten/Komplexität bzw. geringer Nutzen

Logging Maturity Levels (LML)

LMLid	Kategorie	Anforderung	Bewertung	Guidelines
LML1-1	Protokollierung - Aktivierung	Aktivierung der Audit-Protokollierung auf allen Unternehmensgeräten [CT18-8.2/IG1] und Sicherstellung, dass ausreichend Platz für die Protokollierung zur Verfügung steht, um die im Audit-Log-Management-Prozess dokumentierten Vorgaben einzuhalten. [CT18-8.3/IG1]	Kosten: Günstig Komplexität: Einfach-Mittel Nutzen: Mittel	Logging in Windows - On-Premise Logging in Windows - Cloud Logging in Microsoft 365
LML1-38	Datensicherheit - Sicherstellung rechtlicher Rahmenbedingungen	Logfiles können persönliche Daten beinhalten, geeignete Schutzmaßnahmen der Privatsphäre sind zu treffen. [ISO2:22-8.15]	Kosten: Günstig Komplexität: Einfach-Mittel Nutzen: Mittel	Logfile Anonymisierung in Windows - On-Premise Logfile Anonymisierung in Windows - Cloud Logfile Anonymisierung in Linux Logfile Anonymisierung in MS365
LML1-16	Dokumentation - Dokumentierter Prozess Protokollierung und Überwachung	Etablierung und Pflege eines Prozesses zur Verwaltung von Audit-Logs über welchen zumindest die Erfassung, Überprüfung und Aufbewahrung von Audit-Protokollen für Unternehmensressourcen geregelt ist. Aktualisierung der Dokumentation zumindest jährlich oder bei groben Änderungen [CT18-8.1/IG1]. In Cloud-Umgebungen können die Zuständigkeiten für Log-Daten aufgeteilt werden und variieren je nach Art des genutzten Cloud-Dienstes [ISO22-8.15].	Kosten: Mittel-Teuer Komplexität: Mittel-Komplex Nutzen: Hoch-Mittel	Organisatorisch
LML2-39	Überwachung - Serviceprovider	Aufhaltung der Serviceprovider-Logs, wo möglich. Aufbewahrung der beispielsweise Authentifizierungs- und Autorisierungs-Ereignisse, sowie Datenerzeugungs-, sowie Datenlöschungs- und Benutzerverwaltungs-Ereignisse. [CT18-8.12/IG3]	Kosten: Günstig Komplexität: Einfach Nutzen: Mittel	Geloggte Aktivitäten in Windows - On-Premise Geloggte Aktivitäten in Windows - Cloud Geloggte Aktivitäten in Microsoft 365
LML2-45	Protokollierung - Zentralisierung	Soweit möglich Sammlung und Aufhaltung der Audit-Logs zentral. [CT18-8.9/IG2]	Kosten: Günstig-Mittel Komplexität: Einfach-Mittel Nutzen: Hoch-Mittel	Zentrales Logging in Windows - On-Premise Zentrales Logging in Windows - Cloud Zentrales Logging in Microsoft 365 Zentrales Logging in Linux Zentralisiertes Management und Logging
LML2-7	Überwachung - Anti-Virus	Konfiguration der Anti-Virus Software dahingehend, Wechselmedien automatisch zu prüfen [CT18-10.4/IG2] und Nutzung von verhaltensbasierter Anti-Viren Software [CT18-10.7/IG2].	Kosten: Mittel Komplexität: Einfach Nutzen: Hoch	Antimalware

LMLid	Kategorie	Anforderung	Bewertung	Guidelines
LML2-28	Überwachung - IDS	Nutzung von Host-basierten Erkennungslösungen (HIDS) auf den Assets, wo dies angemessen und möglich ist. [CT18-13.2/IG2]	Kosten: Mittel Komplexität: Einfach Nutzen: Hoch	Host basierte Intrusion Detection/Prevention
LML2-8	Protokollierung - Aufbehaltedauer	Aufbehaltung von Audit-Logs über alle Assets mindestens 90 Tage. [CT18-8.10/IG2]	Kosten: Günstig-Mittel Komplexität: Einfach-Mittel Nutzen: Mittel	Wie lange soll geloggt werden Logfile Anonymisierung in Microsoft 365
LML2-2	Überwachung - Überwachungssystem	Das Monitoring sollte ununterbrochen und in Echtzeit oder zumindest in regelmäßigen Intervallen durchgeführt werden, als auch mit großen Mengen an Daten umgehen und sich an die stetig ändernde Gefahrenlandschaft anpassen können. Neben einer Echtzeit-Benachrichtigung sollen die Werkzeuge auch in der Lage sein mit Signaturen, Daten sowie Netzwerk- und Anwendungsverhaltensmuster zu arbeiten. [ISO2:22-8.16]	Kosten: Günstig-Mittel Komplexität: Einfach-Mittel Nutzen: Mittel	Wie lange soll geloggt werden Monitoring in Windows - On-Premise Monitoring in Windows - Cloud Monitoring in Microsoft 365
LML2-42	Überwachung - Logfiles	Logfiles beinhalten eine große Menge an Informationen mit vielen für das Security-Monitoring überflüssigen Informationen. Um wichtige Ereignisse zu erkennen sollten daher geeignete Hilfsprogramme und Audit-Werkzeuge genutzt werden. [ISO2:22-8.15]	Kosten: Günstig-Mittel Komplexität: Einfach-Mittel Nutzen: Mittel	Monitoring in Windows - On-Premise Monitoring in Windows - Cloud Monitoring in Microsoft 365
LML2-9	Protokollierung - Sicherheitsereignisse	Des Weiteren wird empfohlen folgende Ereignisse aufzuzeichnen: • Erfolgreiche und abgewiesene Versuche, auf Daten und andere Ressourcen zuzugreifen • die Nutzung von Privilegien • Dateien, auf die zugegriffen wurde, und die Art des Zugriffs, einschließlich des Löschens wichtiger Datendateien • vom Zugangskontrollsystem ausgelöste Alarme • Aktivierung und Deaktivierung von Sicherheitssystemen, wie Virenschutzsystemen und Systemen zur Erkennung von Eindringlingen • Erstellung, Änderung oder Löschung von Identitäten • Transaktionen, die von Benutzern in Anwendungen ausgeführt werden. In einigen Fällen sind die Anwendungen ein Dienst oder Produkt, das von einer dritten Partei bereitgestellt oder betrieben wird. [ISO2:22-8.15]	Kosten: Günstig-Mittel Komplexität: Einfach-Komplex Nutzen: Hoch-Mittel	Was soll geloggt werden Geloggte Aktivitäten in Windows - On-Premise Geloggte Aktivitäten in Windows - Cloud Geloggte Aktivitäten in Microsoft 365
LML2-19	Protokollierung - Ereignisprotokoll-Felder mit Sicherheitsrelevanz	Sicherstellung von detaillierten Audit-Logs für Assets mit sensiblen Daten, welche zumindest die Ereignisquelle, einen Zeitstempel, die Quell- und Ziel-Adressen, sowie weitere wichtige Informationen enthalten, die bei einer späteren forensischen Analyse unterstützen können. [CT18-8.5/IG2]	Kosten: Günstig-Mittel Komplexität: Einfach-Komplex Nutzen: Hoch-Mittel	Was soll geloggt werden Geloggte Aktivitäten in Windows - On-Premise Geloggte Aktivitäten in Windows - Cloud Geloggte Aktivitäten in Microsoft 365

LMLid	Kategorie	Anforderung	Bewertung	Guidelines
LML2-20	Protokollierung - Ereignisprotokoll-Felder mit Sicherheitsrelevanz	Die Ereignisprotokolle sollten für jedes Ereignis gegebenenfalls Folgendes enthalten: • Benutzer-IDs • Systemaktivitäten • Datum und Uhrzeit sowie Einzelheiten zu den relevanten Ereignissen (z.B. An- und Abmeldung) • Netzwerkadressen und -protokolle • erfolgreiche und abgelehnte Systemzugriffsversuche • Änderungen an der Systemkonfiguration • Verwendung von Hilfsprogrammen und Anwendungen • Geräteidentität • Systemkennung und Standort [ISO2:22-8.15]	Kosten: Günstig-Mittel Komplexität: Einfach-Komplex Nutzen: Hoch-Mittel	Was soll geloggt werden Geloggte Aktivitäten in Windows - On-Premise Geloggte Aktivitäten in Windows - Cloud Geloggte Aktivitäten in Microsoft 365
LML2-37	Überwachung - Relevante Ereignisse	Überwacht werden sollten: • Ausgehender und eingehender Netz-, System- und Anwendungsverkehr • Zugang zu den Systemen, Servern, Netzwerk-Komponenten, Überwachungssystemen, kritische Anwendungen, etc. • System- und Netzkonfigurationsdateien auf kritischer oder administrativer Ebene • Ereignisprotokolle in Bezug auf System- und Netzwerkaktivitäten • Protokolle von Sicherheitstools (insbesondere Anti-Virus, IDS, Webfilter, Firewalls, DLP) • Überprüfung, ob der auszuführende Code im System laufen darf und ob er manipuliert wurde • die Nutzung von Systemressourcen (CPU, Speicherplatz, Hauptspeicher, Leitung) und deren Leistung. [ISO2:22-8.16]	Kosten: Günstig-Mittel Komplexität: Einfach-Komplex Nutzen: Hoch-Mittel	Was soll geloggt werden Geloggte Aktivitäten in Windows - On-Premise Geloggte Aktivitäten in Windows - Cloud Geloggte Aktivitäten in Microsoft 365
LML2-3	Protokollierung - Netzwerkgeräte	Netzwerkgeräte müssen ermöglichen, dass eine angemessene Protokollierung und Überwachung sowie die Aufzeichnung und Erkennung von Aktionen ermöglicht werden, die sich auf die Informationssicherheit auswirken oder von informationssicherheitstechnischer Relevanz sind [ISO2:22-8.20]	Kosten: Mittel Komplexität: Komplex Nutzen: Hoch	Was soll geloggt werden
LML2-11	Protokollierung - Datenquellen	Nutzung von DHCP Audit-Logs, um das Bestandverzeichnis des Unternehmens aktuell zu halten. Wöchentliche Überprüfung aller DHCP-Server-Audit-Logs, um das Verzeichnis aktuell zu halten. [CT18-1.4/IG2]	Kosten: Mittel Komplexität: Komplex Nutzen: Hoch	Was soll geloggt werden

LMLid	Kategorie	Anforderung	Bewertung	Guidelines
LML2-12	Protokollierung - Datenquellen	Sammelung von DNS-Anfragen Audit-Logs [CT18-8.6/IG2], URL-Aufrufs Audit-Logs [CT18-8.7/IG2], sowie Command-Line Audit-Logs [CT18-8.8/IG2].	Kosten: Mittel Komplexität: Komplex Nutzen: Hoch	Was soll geloggt werden
LML2-13	Protokollierung - Datenquellen	Zur Überprüfung und Alarmierung von Netzwerkgeräten sollen Netzwerk-Verkehrs-Logs und/oder Netzwerk-Verkehr (Full Paket Caputure) gesammelt werden. [CT18-13.6/IG2]	Kosten: Mittel Komplexität: Komplex Nutzen: Hoch	Was soll geloggt werden
LML2-29	Überwachung - IDS	Einsetzen von Netzwerk-basierte Erkennungslösungen (NIDS) oder vergleichbare Cloud-Dienste-Anbieter Dienste auf den Assets, wo dies angemessen ist. [CT18-13.3/IG2]	Kosten: Mittel Komplexität: Komplex Nutzen: Hoch	Network-Based Intrustion Detection/Prevention System (NIDS/NIPS)
LML2-24	Überwachung - Automatisierte Protokoll-Analyse	Die Loganalyse sollte durch Überwachungsmaßnahmen unterstützt werden, um abnormales Verhalten zu identifizieren und zu analysieren: • Überprüfung auf erfolgreiche und fehlgeschlagene Versuche auf geschützte Ressourcen zuzugreifen (z.B. DNS-Server, Webportale, Dateifreigaben) • Überprüfung von DNS-Logs, um ausgehende Netzwerkverbindungen zu bösartigen Servern zu identifizieren (z.B. Botnetz, Command & Control Server) • Einbeziehung von Logs der physischen Überwachung wie Ein- und Ausgänge zur Verbesserung der Erkennung • Korrelation von Protokollen für eine effiziente und genaue Analyse [ISO2:22-5.25]	Kosten: Mittel Komplexität: Komplex Nutzen: Hoch	Was soll geloggt werden
LML2-5	Protokollierung - Prüfung und Integrität	Die Ereignislogs sollen sichergestellt werden, um deren Integrität zu sichern und diese vor unbefugten Zugriff zu schützen. [ISO2:22-8.15]	Kosten: Günstig-Mittel Komplexität: Einfach-Komplex Nutzen: Hoch-Niedrig	Was soll geloggt werden Sicherheit von Log-Dateien in Windows - On-Premise Sicherheit von Log-Dateien in Windows - Cloud Sicherheit von Log-Dateien in Microsoft 365
LML2-43	Protokollierung - Zeitsynchronisierung	Zwei synchronisierte Zeitquellen für alle Enterprise-Assets hinweg sollen zur Verfügung gestellt werden. [CT18-8.4/IG2] [ISO2:22-8.15] [ISO2:22-8.18]	Kosten: Günstig-Mittel Komplexität: Einfach-Mittel Nutzen: Mittel-Niedrig	Zeitsynchronisierung in Windows Zeitsynchronisierung in Linux

LMLid	Kategorie	Anforderung	Bewertung	Guidelines
LML2-4	Protokollierung - Prüfung und Integrität	Für Anwendungen sollen geprüfte Module und Dienste verwendet werden, welche Auditing und Protokollierung ermöglichen. Beispielsweise bieten Betriebssysteme Mechanismen zur Erstellung und Verwaltung sicherer Prüfprotokolle an. [CT18-16.11/IG2]	Kosten: Mittel-Teuer Komplexität: Mittel-Komplex Nutzen: Hoch-Mittel	Organisatorisch
LML2-10	Analyse - Personal	Für die Auswertung von Alarmen muss Personal bereitgestellt und trainiert werden, um die potentiellen Gefahren akkurat einzustufen. [ISO2:22-8.16]	Kosten: Mittel-Teuer Komplexität: Mittel-Komplex Nutzen: Hoch-Mittel	Organisatorisch
LML2-14	Dokumentation - Dokumentierte Prozeduren forensischer Analysen	Für weitere forensische Analysen sind Prozeduren zur Archivierung von Logfiles sicherzustellen. [ISO2:22, 5.28]	Kosten: Mittel-Teuer Komplexität: Mittel-Komplex Nutzen: Hoch-Mittel	Organisatorisch
LML2-15	Dokumentation - Dokumentierte Prozeduren und Bekanntmachung	Die Betriebsverfahren müssen dokumentiert und dem Personal, dass sie benötigt, zur Verfügung gestellt werden. Dies umfasst zumindest die Sicherstellung des Audit-Trails, die Log- und Monitoring-Prozeduren, sowie die damit in Verbindung stehenden Verwaltungsaufgaben. [ISO2:22-5.37]	Kosten: Mittel-Teuer Komplexität: Mittel-Komplex Nutzen: Hoch-Mittel	Organisatorisch
LML2-17	Dokumentation - Dokumentierter Prozess Protokollierung	Es soll festgelegt werden, zu welchem Zweck Protokolle erstellt, welche Daten gesammelt und protokolliert werden, sowie die Anforderungen zum Schutz und zur Handhabung der Protokolldaten festgelegt werden. [ISO2:22-8.15]	Kosten: Mittel-Teuer Komplexität: Mittel-Komplex Nutzen: Hoch-Mittel	Organisatorisch
LML2-18	Dokumentation - Dokumentierter Prozess Überwachung	Der Umfang und das Ausmaß des Monitorings sollte in Übereinstimmung mit den Anforderungen des Unternehmens und der Informationssicherheit, sowie unter Berücksichtigung der einschlägigen Gesetze und Vorschriften festgelegt werden. Die Aufzeichnungen sollten für eine festgelegte Zeit aufbewahrt werden. [ISO2:22-8.16]	Kosten: Mittel-Teuer Komplexität: Mittel-Komplex Nutzen: Hoch-Mittel	Organisatorisch
LML2-21	Überwachung - Erkennung von abnormalem Verhalten	Es soll eine Baseline erstellt werden, gegen welche die Monitoringsysteme auf Anomalien prüfen. Bei der Erstellung der Baseline sollte darauf geachtet werden, dass die Ressourcenlast der Systeme unter Normal- und Peak-Zuständen sowie die übliche Zugriffszeit, der Zugriffsort als auch die Frequenz des Zugriffs jedes Nutzers oder jeder Benutzergruppe herangezogen wird. [ISO2:22-8.16]	Kosten: Mittel-Teuer Komplexität: Mittel-Komplex Nutzen: Hoch-Mittel	Organisatorisch

LMLid	Kategorie	Anforderung	Bewertung	Guidelines
LML2-22	Überwachung - Erkennung von abnormalem Verhalten	Es soll abnormales Verhalten festgestellt werden wie: • die ungeplante Beendigung von Prozessen oder Anwendungen • Aktivitäten, die typsicherweise mit Malware oder Datenverkehr in Verbindung gebracht werden, der von gefährlich eingestuften IP-Adressen oder Netzwerkdomänen ausgeht • bekannte Angriffsmerkmale (z.B. Denial of Service, Puffer overflow) • ungewöhnliches Systemverhalten, wie die Protokollierung von Tastatureingaben, Prozessinjektion und Abweichungen von Standardprotokollen • Engpässe und Überlastungen (z.B. Netzwerkwarteschlangen, Latenzzeiten und Netzwerk-Jitter) • unbefugter Zugriff (tatsächlich und versucht) auf Systeme oder Informationen • unbefugtes Durchsuchen von Geschäftsanwendungen, Systemen und Netzwerken • erfolgreiche und erfolglose Versuche auf geschützte Ressourcen zuzugreifen • ungewöhnliches Benutzer- und Systemverhalten im Verhältnis zum erwarteten Verhalten [ISO2:22-8.16]	Kosten: Teuer Komplexität: Komplex Nutzen: Hoch	SIEM bzw. zentralisiertes Logging in LML 2
LML2-25	Datensicherheit - Maskierung bei Herausgabe von Protokollen	Sollten Logfiles zur Unterstützung bei der Fehlersuche an Externe weiteregeleitet werden, so müssen diese vorab von sensible Daten bereinigt werden. Diese sind beispielsweise Usernamen, IP-Adressen, Hostnamen, Organisationsnamen, etc. [ISO2:22-5.28]	Kosten: Mittel-Teuer Komplexität: Mittel-Komplex Nutzen: Hoch-Mittel	Organisatorisch
LML2-26	Analyse - Abnormales Verhalten	Abnormale Ereignisse müssen an die zuständigen Stellen gemeldet werden, um Audits, Sicherheitsbewertungen, Schwachstellensuche und Überwachungsaktivitäten zu verbessern. [ISO2:22-8.16]	Kosten: Mittel-Teuer Komplexität: Mittel-Komplex Nutzen: Hoch-Mittel	Organisatorisch
LML2-27	Überwachung - Meldung Vorfälle	Dem Personal müssen Mechanismen zur Verfügung gestellt werden, um beobachtete oder vermutete Informationssicherheitsvorfälle zeitgerecht zu melden. [I2:22-6.8]	Kosten: Mittel-Teuer Komplexität: Mittel-Komplex Nutzen: Hoch-Mittel	Organisatorisch

LMLid	Kategorie	Anforderung	Bewertung	Guidelines
LML2-34	Analyse - Sicherheitsrelevante Ereignisse	Die Analyse von Events sollte folgende Aspekte berücksichtigen: • die erforderlichen Fähigkeiten der Experten, welche die Analyse durchführen • festgelegte Verfahren für die Analyse • die erforderlichen Attribute jedes sicherheitsrelevanten Events • Ausnahmen vorher festgelegter Regelsätze (z.B. Firewall-, IDS-, Antivirus- oder SIEM-Regeln) • bekannte Verhaltensmuster und Standard-Netzwerkverkehr im Vergleich zu anomalen Aktivitäten und Verhalten • Ergebnisse aus Trend- oder Musteranalysen • verfügbare Threat Intelligence [ISO2:22-8.15]	Kosten: Mittel-Teuer Komplexität: Mittel-Komplex Nutzen: Hoch-Mittel	Organisatorisch
LML2-35	Analyse - Prüfung Vorfälle	Überprüfung von Sicherheitsereignisse (auch vermutete wie z.B. Virenbefalls-Meldungen oder Port-Scans auf der Firewall) und Überprüfung darauf, ob es sich um Informationssicherheitsvorfälle handelt [ISO2:22-5.25, 8.15]	Kosten: Mittel-Teuer Komplexität: Mittel-Komplex Nutzen: Hoch-Mittel	Organisatorisch
LML2-41	Überwachung - Prüfung Audit-Logs	Zumindest auf wöchentlicher Basis sind die Audit-Logs zu prüfen, um Anomalien oder abnormale Ereignisse zu erkennen, die auf potentielle Gefahren hindeuten [CT18-8.11/IG2] [ISO2:22-8.15,8.16 (Networks, Systems and Applications)]	Kosten: Mittel-Teuer Komplexität: Mittel-Komplex Nutzen: Hoch-Mittel	Organisatorisch
LML2-44	Überwachung - Zentralisierung, Korrelation, Analyse	Zentrale Sammlung der Sicherheitsereignis-Logs aller Assets, um eine Log-Korrelation und Analyse zu ermöglichen. Eine Best-Practice-Implementierung erfordert die Verwendung eines SIEM, das händlerspezifische Ereigniskorrelierungsalarmierungen enthält, alternativ kann auch eine Log-Analyseplattform verwendet werden, die sicherheitsrelevante Korrelationsalarmierungen ermöglicht. [CT18-13.1/IG2]		
LML3-33	Protokollierung - Sensible Daten	Sensible Informationen sind zu identifizieren und zu überwachen, um eine unbefugte Offenlegung zu verhindern. Auch sind Kanäle, die Datenlecks ermöglichen wie beispielsweise E-Mail oder den Zugriff auf Cloud-Dienste, zu überwachen. [I2:22-8.12]	Kosten: Günstig-Mittel Komplexität: Einfach-Mittel Nutzen: Hoch-Mittel	SIEM bzw. zentralisiertes Logging in LML 3 Data Loss Prevention (DLP)

LMLid	Kategorie	Anforderung	Bewertung	Guidelines
LML3-6	Protokollierung - Schutz vor Veränderung	Nutzer, auch jene die privilegierte Rechte haben, darf es nicht möglich sein, Logs zu ihren eigenen Aktivitäten zu löschen oder zu deaktivieren. Weiters sollen keine Veränderungen an den aufgezeichneten Nachrichtentypen vorgenommen werden dürfen. Logfiles dürfen nicht bearbeitet oder gelöscht werden und es muss sichergestellt werden, dass, sollte der Speicherplatzbedarf überschritten werden, Ereignisse zu jeder Zeit aufgezeichnet werden können, ohne das alte Einträge überschrieben werden. Hierfür sollten Techniken wie kryptografisches Hashing, Aufzeichnungen in eine „append-only and read-only" Datei, sowie Aufzeichnungen in eine öffentliche Transparenzdatei verwendet werden. [I2:22-8.15]	Kosten: Günstig Komplexität: Einfach Nutzen: Niedrig	Sicherheit von Log-Dateien in Windows - On-Premise Sicherheit von Log-Dateien in Windows - Cloud Sicherheit von Log-Dateien in Microsoft 365
LML3-23	Analyse - Erzeugung von Threat Intelligence	Informationen zu Gefahren müssen gesammelt und analysiert werden, um Threat Intelligence zu erzeugen [ISO2:22-5.7]	Kosten: Mittel-Teuer Komplexität: Mittel-Komplex Nutzen: Hoch-Mittel	Organisatorisch
LML3-30	Analyse - Optimierung von Alarmen	Alarmierungsschwellenwerte sollen von Ereignissen sollten zumindest monatlich optimiert [CT18-13.11/IG3] [ISO2:22-8.16] und ein Prozesse für den Umgang mit Fehlalarmen etabliert werden, um die Zahl der künftigen Fehlalarme zu verringern. [ISO2:22-8.16]	Kosten: Mittel-Teuer Komplexität: Mittel-Komplex Nutzen: Hoch-Mittel	Organisatorisch
LML3-31	Analyse - Optimierung von Alarmen	Die etablierten Sicherheitsmaßnahmen sollen während Penetrationstests gerade stattfindende Angriffe aufzeigen. Regelsätze und Funktionen müssen falls erforderlich angepasst werden, um die bei den Tests verwendeten Techniken zu erkennen. [CT18-18.4/IG3]	Kosten: Mittel-Teuer Komplexität: Mittel-Komplex Nutzen: Hoch-Mittel	Organisatorisch
LML3-32	Protokollierung - Sensible Daten	Der Zugriff auf sensible Daten einschließlich Änderung und Löschung muss protokolliert werden. [CT18-3.14/IG3]	Kosten: Mittel-Teuer Komplexität: Mittel-Komplex Nutzen: Hoch-Mittel	Organisatorisch
LML3-36	Überwachung - Redundanz	Die für Logging und Monitoring zuständigen Systeme, Personen und Prozesse sollen redundant ausgelegt sein, dies gilt sowohl für die Protokollierung, als auch die Überwachung, die Alarmierung und die Werkzeuge für die Auswertung und die Reaktion darauf. [ISO2:22-8.16]	Kosten: Mittel-Teuer Komplexität: Mittel-Komplex Nutzen: Hoch-Mittel	Organisatorisch
LML3-40	Überwachung - Serviceprovider	Überwachung von Dienstanbietern im Einklang mit den Richtlinien des Unternehmens zur Verwaltung von Dienstanbietern. Die Überwachung kann eine periodische Neubewertung der Einhaltung der Vorschriften durch den Dienstanbieter, Überwachung der Versionshinweise des Dienstanbieters und Überwachung des Dark Web sein. [CT18-15.6/IG3]	Kosten: Mittel-Teuer Komplexität: Mittel-Komplex Nutzen: Hoch-Mittel	Organisatorisch

LML 1 Organisatorisch

Bei diesen Anforderungen handelt es sich um organisatorische Maßnahmen, die nicht einfach technisch umgesetzt werden können:

- LML1-16 Dokumentierter Prozess Protokollierung und Überwachung

Tags

- #Organisatorisch

Windows

Logging in Windows - On-Premise

Die Speicherung von Log-Einträgen ist in Windows standardmäßig aktiv, kann allerdings manuell deaktiviert, eingeschränkt, aber auch erweitert werden. Es sollte überprüft werden, ob auf allen Assets der richtige Logging Level konfiguriert ist. Für Details siehe: https://www.loggly.com/ultimate-guide/windows-logging-basics/

Es kann ebenfalls konfiguriert werden, wie viele Log-Einträge aufbehalten werden sollen: https://learn.microsoft.com/en-us/answers/questions/451919/event-log-settings-maximum-log-size-kb-windows-ser.html

Speicherplatz für Logs sollte in etwa so berechnet werden:

Speicherbedarf = Log_Größe * Dauer

- `Log_Größe` stellt die Größe des jeden Tag anfallenden Logs pro Gerät dar.
- `Dauer` stellt die Tage dar, die das gesamte Log aller Geräte gespeichert werden soll.

Erfüllte Anforderungen

- LML1-1 Protokollierung - Aktivierung

Metriken für Implementierungsentscheidungen

- Kosten
  - Günstig
    - Die Speicherung ist aktiviert, es muss lediglich die Umsetzung überprüft werden.
- Komplexität der Umsetzung
  - Einfach
    - Die Einstellungen können einfach eingesehen und überprüft werden.
- Nutzen (Impact)
  - Mittel

        - Im Falle eines Incidents können grundlegende Events nachvollzogen werden.

Logging in Windows - Cloud

In der Cloud können Logs Cloud-spezifisch über Agenten, die in den virtuellen Maschinen installiert werden, weitergeleitet werden: https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-syslog

Auch hier kann konfiguriert werden wie lange Log-Einträge aufgehoben werden sollen: https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-archive?tabs=portal-1%2Cportal-2

Erfüllte Anforderungen

- LML1-1 Protokollierung - Aktivierung

Metriken für Implementierungsentscheidungen

- Kosten
    - Günstig
        - Es fallen geringe Speicherkosten in der Cloud an.
- Komplexität der Umsetzung
    - Einfach
        - Das Logging kann im Azure Portal konfiguriert werden.
- Nutzen (Impact)
    - Mittel
        - Im Falle eines Incidents können grundlegende Events nachvollzogen werden.

Logfile Anonymisierung in Windows - On-Premise

Um den Datenschutz zu wahren, sollte darauf geachtet werden keine personenbezogenen Daten in den Logs zu verarbeiten. Hierbei sollte darauf geachtet werden im Vorhinein solche Daten nicht in das Log einfließen zu lassen, oder nur anonymisiert zu speichern.

Weitere Informationen:

- Deutscher IT-Sicherheitskongress 2015 - Risiko Logfiles: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/ITSiKongress/14ter/Vortraege-19-05-2015/Heidrich_Wegener.pdf?__blob=publicationFile&v=1
- Tool zum regelbasieren Anonymisieren von Logs: https://github.com/sys4/loganon

Erfüllte Anforderungen

- LML1-38 Datensicherheit - Sicherstellung rechtlicher Rahmenbedingungen

Metriken für Implementierungsentscheidungen

- Kosten

    - Günstig
        - Das Skript kann nach Implementierung automatisiert ausgeführt werden.
- Komplexität der Umsetzung
    - Mittel
        - Minimale Scripting-Kenntnisse sind erforderlich.
- Nutzen (Impact)
    - Mittel
        - Datenschutz-Grundlagen müssen eingehalten werden.

Logfile Anonymisierung in Windows - Cloud

Personenbezogene Daten können und werden ebenso wie On-Premise in der Cloud gespeichert, hier gelten dieselben Empfehlungen:

- Azure, Verwalten personenbezogener Daten in Log Analytics: https://learn.microsoft.com/de-de/azure/azure-monitor/logs/personal-data-mgmt

Erfüllte Anforderungen

- LML1-38 Datensicherheit - Sicherstellung rechtlicher Rahmenbedingungen

Metriken für Implementierungsentscheidungen

- Kosten
    - Günstig
        - Seitens Microsoft werden grundlegende Schnittstellen zum Löschen der personenbezogenen Daten angeboten.
- Komplexität der Umsetzung
    - Mittel
        - Es gibt eine Lösch-API.
- Nutzen (Impact)
    - Mittel
        - Datenschutz-Grundlagen müssen eingehalten werden.

Tags

- #Windows
- #Logging

Linux

Logging in Linux

Linux - On-Premise

Auf Linux-Systemen werden Logs in Dateien geschrieben, die unter `/var/log/` liegen. Beispielsweise werden Anmeldeversuche, Kernel-Events und Logs von Apache oder MySQL in dieses Verzeichnis geschrieben [1]. Logs können auch aber auch direkt an andere Prozesse geschickt werden, beispielsweise mit `systemd-journald` oder `rsyslog`. Über diese Programme können die Logs über die Kommandozeile ausgelesen, oder an andere Services und Server weitergeleitet [2,3] werden.

1. https://www.loggly.com/ultimate-guide/linux-logging-basics/
2. https://www.loggly.com/ultimate-guide/centralizing-with-syslog/
3. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/configuring_basic_system_settings/assembly_configuring-a-remote-logging-solution_configuring-basic-system-settings

Notizen

Speicherplatz für zentrale Logs sollte in etwa so berechnet werden:

Speicherbedarf = Geräte * Log_Größe * Dauer

- `Geräte` stellt die Anzahl der Geräte dar, die überwacht werden sollen.
- `Log_Größe` stellt die Größe des jeden Tag anfallenden Logs pro Gerät dar.
- `Dauer` stellt die Tage dar, wie lange das gesamte Log aller Geräte gespeichert werden soll.

Linux - Cloud

In der Cloud können Logs Cloud-spezifisch über Agenten, die in den virtuellen Maschinen installiert werden, weitergeleitet werden.

- Azure, Log Analytics Agent: https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-syslog

Erfüllte Anforderungen

- LML1-1 Protokollierung - Aktivierung

Metriken für Implementierungsentscheidungen

- Kosten
  - Günstig
    - Die Tools sind frei verfügbar und Open-Source.
- Komplexität der Umsetzung
  - Mittel
    - Linux-Kenntnisse müssen vorhanden sein.
- Nutzen (Impact)
  - Mittel
    - Im Falle eines Incidents können grundlegende Events nachvollzogen werden.

Logfile Anonymisierung in Linux

Linux - On-Premise

Um den Datenschutz zu wahren, sollte darauf geachtet werden keine personenbezogenen Daten in den Logs zu verarbeiten. Hierbei sollte darauf geachtet werden im Vorhinein solche Daten nicht in das Log einfließen zu lassen, oder nur anonymisiert zu speichern.

Weitere Informationen:

- Deutscher IT-Sicherheitskongress 2015 - Risiko Logfiles: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/ITSiKongress/14ter/Vortraege-19-05-2015/Heidrich_Wegener.pdf?__blob=publicationFile&v=1
- Tool zum regelbasieren Anonymisieren von Logs: https://github.com/sys4/loganon

Linux - Cloud

Personenbezogene Daten können und werden ebenso wie On-Premise in der Cloud gespeichert, hier gelten dieselben Empfehlungen.

- Azure, Verwalten personenbezogener Daten in Log Analytics: https://learn.microsoft.com/de-de/azure/azure-monitor/logs/personal-data-mgmt

Erfüllte Anforderungen

- LML1-38 Datensicherheit - Sicherstellung rechtlicher Rahmenbedingungen

Metriken für Implementierungsentscheidungen

- Kosten
  - Günstig
    - Das Skript kann nach Implementierung automatisiert ausgeführt werden.
- Komplexität der Umsetzung
  - Mittel
    - Minimale Scripting-Kenntnisse sind erforderlich.
- Nutzen (Impact)
  - Mittel
    - Datenschutz-Grundlagen müssen eingehalten werden.

Tags

- #Linux
- #Logging

Microsoft 365

Logging in Microsoft 365

Die Speicherung von Log-Einträgen ist in Microsoft 365 standardmäßig aktiv, kann allerdings manuell deaktiviert werden. Es sollte überprüft werden, ob das Logging im Account aktiv ist. Für Details siehe: https://learn.microsoft.com/en-us/microsoft-365/compliance/turn-audit-log-search-on-or-off?view=o365-worldwide

Log-Einträge werden standardmäßig für 90 Tage aufbehalten. Dieser Wert kann über Audit Log Retention Policies angepasst werden: https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-log-retention-policies?view=o365-worldwide

Erfüllte Anforderungen

- LML1-1 Protokollierung - Aktivierung

Metriken für Implementierungsentscheidungen

- Kosten
  - Günstig
    - Die Speicherung ist aktiviert, es muss lediglich die Umsetzung überprüft werden.
- Komplexität der Umsetzung
  - Einfach
    - Die Einstellungen können einfach eingesehen und überprüft werden.
- Nutzen (Impact)
  - Mittel
    - Im Falle eines Incidents können grundlegende Events nachvollzogen werden.

Logfile Anonymisierung in Microsoft 365

Log-Dateien werden in Microsoft 365 automatisch von persönlichen Daten bereinigt: https://learn.microsoft.com/en-us/compliance/assurance/assurance-internal-logging

Erfüllte Anforderungen

- LML1-38 Datensicherheit - Sicherstellung rechtlicher Rahmenbedingungen
- LML2-8 Protokollierung - Aufbehaltedauer

Metriken für Implementierungsentscheidungen

- Kosten
  - Günstig
    - Die Umsetzung ist automatisch aktiviert.
- Komplexität der Umsetzung
  - Einfach
    - Die Umsetzung ist automatisch aktiviert.
- Nutzen (Impact)
  - Mittel
    - Datenschutz-Grundlagen müssen eingehalten werden.

Tags

- #MS365
- #Logging

LML 2 Organisatorisch

Bei diesen Anforderungen handelt es sich um organisatorische Maßnahmen, die nicht einfach technisch umgesetzt werden können:

- LML2-4 Protokollierung - Prüfung und Integrität
- LML2-10 Analyse - Personal
- LML2-14 Dokumentierte Prozeduren forensischer Analysen
- LML2-15 Dokumentierte Prozeduren und Bekanntmachung
- LML2-17 Dokumentierter Prozess Protokollierung
- LML2-18 Dokumentierter Prozess Überwachung
- LML2-21 Überwachung - Erkennung von abnormalem Verhalten
- LML2-25 Datensicherheit - Maskierung bei Herausgabe von Protokollen
- LML2-26 Analyse - abnormales Verhalten
- LML2-27 Überwachung - Meldung Vorfälle
- LML2-34 Analyse - Aspekte
- LML2-35 Analyse - Prüfung Vorfälle
- LML2-41 Überwachung - Protokolle

Zusätzliche Informationen

LML2-4 Protokollierung - Prüfung und Integrität

Dieser Punkt wird bereits mit Implementierungshilfen für LML1-1 abgedeckt. Siehe dazu auch:

- [[LML1-MS365]]
- [[LML1-Linux]]
- [[LML1-Windows]]

Tags

- #Organisatorisch

Allgemein

Diese Anforderungen müssen Betriebssystem unabhängig technisch umgesetzt werden, um ein vollständiges Logging zu gewährleisten.

Was soll geloggt werden

Es ist wichtig aussagekräftige Werte zu loggen, um Events nachvollziehen zu können.

Hierbei müssen zwei Komponenten richtig konfiguriert werden, damit das Log-Format beidseitig verstanden wird:

1. Die Log-Quelle, also das System auf dem das Log generiert wurde, muss diese Informationen an das zentrale Logging-System weiterleiten.
2. Das zentrale System zur Speicherung von Logs muss diese Logs entgegennehmen und speichern können.

Wichtig ist auch, dass die Integrität der Ereignislogs sichergestellt wird, und diese vor unbefugten Zugriff geschützt sind. [ISO2:22-8.15]

Geloggte Daten

Die Ereignisprotokolle sollten für jedes Ereignis gegebenenfalls Folgendes enthalten:

- Benutzer-IDs
- Systemaktivitäten
- Datum und Uhrzeit sowie Einzelheiten zu den relevanten Ereignissen (z.B. An- und Abmeldung)
- Netzwerkadressen und -protokolle
- Erfolgreiche und abgelehnte Systemzugriffsversuche
- Änderungen an der Systemkonfiguration
- Verwendung von Hilfsprogrammen und Anwendungen
- Geräteidentität
- Systemkennung und Standort [ISO2:22-8.15]

Wichtig ist auch detaillierte Audit-Logs für Assets mit sensiblen Daten zu erstellen, welche zumindest die Ereignisquelle, einen Zeitstempel, die Quell- und Ziel-Adressen, sowie weitere wichtige Informationen enthalten, die bei einer späteren forensischen Analyse unterstützen. [CT18-8.5/IG2]

Wichtige Log-Informationen von eingesetzten Softwarekomponenten

Des Weiteren wird empfohlen folgende Ereignisse aufzuzeichnen:

- Erfolgreiche und abgewiesene Versuche, auf Daten und andere Ressourcen zuzugreifen
- Die Nutzung von Privilegien
- Dateien, auf die zugegriffen wurde, und die Art des Zugriffs, einschließlich des Löschens wichtiger Datendateien, vom Zugangskontrollsystem ausgelöste Alarme
- Aktivierung und Deaktivierung von Sicherheitssystemen, wie Virenschutzsysteme und Systeme zur Erkennung von Eindringlingen
- Erstellung, Änderung oder Löschung von Identitäten
- Transaktionen, die von Benutzern in Anwendungen ausgeführt werden. In einigen Fällen sind die Anwendungen ein Dienst oder Produkt, das von einer dritten Partei bereitgestellt oder betrieben wird. [ISO2:22-8.15]

Logging auf Netzwerkebene

Netzwerkgeräte müssen ermöglichen, dass eine angemessene Protokollierung und Überwachung sowie die Aufzeichnung und Erkennung von Aktionen ermöglicht werden, die sich auf die Informationssicherheit auswirken oder von informationssicherheitstechnischer Relevanz sind. [ISO2:22-8.20]

Überwacht werden sollten:

- Ausgehender und eingehender Netz-, System- und Anwendungsverkehr
- Zugang zu den Systemen, Servern, Netzwerk-Komponenten, Überwachungssysteme, kritische Anwendungen, etc.
- System- und Netzkonfigurationsdateien auf kritischer oder administrativer Ebene
- Ereignisprotokolle in Bezug auf System- und Netzwerkaktivitäten
- Protokolle von Sicherheitstools (insbesondere Anti-Virus, IDS, Webfilter, Firewalls, DLP)
- Überprüfung, ob der auszuführende Code im System laufen darf und ob er manipuliert wurde
- die Nutzung von Systemressourcen (CPU, Speicherplatz, Hauptspeicher, Leitung) und deren Leistung. [ISO2:22-8.16]

Kommunikationsdaten

Zusätzlich sollten Kommunikationsdaten und Protokolle aufgezeichnet werden:

- Nutzung von DHCP Audit-Logs, um das Bestandsverzeichnis des Unternehmens aktuell zu halten. Prüfung aller DHCP-Server-Audit-Logs wöchentlich, um das Verzeichnis aktuell zu halten. [CT18-1.4/IG2]
- Sammlung von DNS-Anfrage Audit-Logs [CT18-8.6/IG2], URL-Aufrufs Audit-Logs [CT18-8.7/IG2], sowie Command-Line Audit-Logs [CT18-8.8/IG2].
- Sammlung von Netzwerkverkehrs-Logs und/oder Netzwerkverkehr (Full Paket Capture) zur Überprüfung und Alarmierung von Netzwerkgeräten. [CT18-13.6/IG2]

Überwachungsmaßnahmen

Die Loganalyse sollte durch Überwachungsmaßnahmen unterstützt werden, um abnormales Verhalten zu identifizieren und zu analysieren:

- Überprüfung auf erfolgreiche und fehlgeschlagene Versuche auf geschützte Ressourcen zuzugreifen (z.B. DNS-Server, Webportale, Dateifreigaben)
- Überprüfung von DNS-Logs, um ausgehende Netzwerkverbindungen zu bösartigen Servern zu identifizieren (z.B. Botnetz, Command & Control Server)
- Einbeziehung von Logs der physischen Überwachung, wie Ein- und Ausgänge, zu Verbesserung der Erkennung
- Korrelation von Protokollen für eine effiziente und genaue Analyse [ISO2:22-5.25]

Erfüllte Anforderungen

- LML2-3 Protokollierung - Netzwerkgeräte
- LML2-5 Protokollierung - Prüfung und Integrität
- LML2-9 Protokollierung - Sicherheitsereignisse
- LML2-11 Protokollierung - Datenquellen
- LML2-12 Protokollierung - Datenquellen
- LML2-13 Protokollierung - Datenquellen
- LML2-19 Ereignisprotokoll-Felder mit Sicherheitsrelevanz
- LML2-20 Ereignisprotokoll-Felder mit Sicherheitsrelevanz
- LML2-24 Überwachung - Automatisierte Protokollanalyse

- LML2-37 Überwachung - relevante Ereignisse

Metriken für Implementierungsentscheidungen

- Kosten
  - Mittel
    - Es müssen viele Anforderungen überprüft und umgesetzt werden.
- Komplexität der Umsetzung
  - Komplex
    - Viele verschiedene TOMs müssen überprüft und implementiert werden.
- Nutzen (Impact)
  - Hoch
    - Flächendeckendes Logging hilft im Falle eines Incidents bei einer forensischen Untersuchung und ist Voraussetzung um aktiv Angriffe im Netzwerk zu erkennen.

Wie lange soll geloggt werden

Das Monitoring sollte ununterbrochen und in Echtzeit, oder zumindest in regelmäßigen Intervallen durchgeführt werden. Es soll auch mit großen Mengen an Daten umgehen können und sich an die stetig ändernde Gefahrenlandschaft anpassen können. Neben einer Benachrichtigung in Echtzeit sollen die Werkzeuge auch in der Lage sein mit Signaturen, Daten sowie Netzwerk- und Anwendungsverhaltensmuster zu arbeiten. [ISO2:22-8.16]

Audit-Logs über alle Assets sollten mindestens 90 Tage aufbewahrt werden. [CT18-8.10/IG2]

Erfüllte Anforderungen

- LML2-2 Überwachung - Überwachungssystem
- LML2-8 Protokollierung - Aufbehaltedauer

Metriken für Implementierungsentscheidungen

- Kosten
  - Günstig
    - Für die Speicherung der Logs wird eigene Hardware benötigt.
- Komplexität der Umsetzung
  - Mittel
    - Die Umsetzung muss geprüft werden.
- Nutzen (Impact)
  - Mittel
    - Die Nachvollziehbarkeit von Incidents muss gewährleistet werden.

Tags

- #TechnischAllgemein

Windows

Voraussetzung

- [[LML1-MS365]]

Zentrales Logging in Windows - On-Premise

In Windows Umgebungen ist es möglich Logs auf einen oder mehreren zentrale Server weiterzuleiten.

Eine genaue Beschreibung mit Beispielen wie Windows Logging zentralisiert werden kann, ist hier zu finden: https://www.loggly.com/ultimate-guide/centralizing-windows-logs/

Die Konfiguration der Ereignisweiterleitung von Microsoft wird hier erklärt: https://learn.microsoft.com/de-de/defender-for-identity/configure-event-forwarding

Verwendung der Ereignisweiterleitung zur Erkennung von Angriffen ist hier zu finden: https://learn.microsoft.com/de-de/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection

Speicherplatz sollte in etwa so berechnet werden:

Speicherbedarf = Geräte * Log_Größe * Dauer

- `Geräte` stellt die Anzahl der Geräte dar, die überwacht werden sollen.
- `Log_Größe` stellt die Größe des jeden Tag anfallenden Logs pro Gerät dar.
- `Dauer` stellt die Tage dar, wie lange der gesamte Log aller Geräte gespeichert werden soll.

Erfüllte Anforderungen

- LML2-45 Protokollierung - Zentralisierung

Metriken für Implementierungsentscheidungen

- Kosten
  - Günstig
    - Die Weiterleitung kann im Eventviewer konfiguriert werden.
- Komplexität der Umsetzung
  - Mittel
    - Log-Server und -Client müssen konfiguriert werden.
- Nutzen (Impact)
  - Hoch
    - Im Falle einer Kompromittierung eines Systems können die Log-Dateien nicht manipuliert werden und zentral eingesehen werden.

Zentrales Logging in Windows - Cloud

In Microsoft Azure gibt es den Managed Service Azure Monitor. Dieser kann unter anderem dazu genutzt werden, um Windows Event Logs zu sammeln: https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-windows-events

Erfüllte Anforderungen

- LML2-45 Protokollierung - Zentralisierung

Metriken für Implementierungsentscheidungen

- Kosten
  - Günstig
    - Der Azure Monitor wird pro GB an Log-Daten abgerechnet.
- Komplexität der Umsetzung
  - Einfach
    - Die Konfiguration erfolgt über den Azure Monitor
- Nutzen (Impact)
  - Mittel
    - Im Falle einer Kompromittierung eines Systems können die Log-Dateien nicht manipuliert werden und zentral eingesehen werden.

Monitoring in Windows - On-Premise

Es kann ein PowerShell Skript erstellt werden, das den Windows EventViewer Log durchsucht und eine E-Mail versendet, sollten gewisse Ereignisse auftreten:

- https://windowsreport.com/windows-event-viewer-email-notification/
- https://social.technet.microsoft.com/Forums/ie/en-US/6fe4133d-8858-485a-992d-42e27dd91d27/email-alert-when-an-event-id-is-triggered?forum=winserver8gen
- https://stackoverflow.com/questions/65726315/powershell-script-to-send-me-email-alerts-of-event-viewer-errors-warnings-failur

Metriken für Implementierungsentscheidungen

- Kosten
  - Günstig
    - Lediglich die initiale Umsetzung muss durchgeführt werden.
- Komplexität der Umsetzung
  - Mittel
    - PowerShell-Kenntnisse müssen vorhanden sein.
- Nutzen (Impact)
  - Mittel
    - Das Verwalten und Durchsuchen von Logging-E-Mails ist nicht effizient.

Erfüllte Anforderungen

- LML2-2 Überwachung - Überwachungssystem

- LML2-42 Überwachung - Protokolle

Monitoring in Windows - Cloud

Durch das zentrale Logging im Azure Monitor können Regeln definiert werden, die einen Alarm auslösen. Diese Alarme können verschiedenste Aktionen auslösen, beispielsweise eine E-Mail an den Administrator senden: https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-overview#manage-your-alerts-programmatically

Erfüllte Anforderungen

- LML2-2 Überwachung - Überwachungssystem
- LML2-42 Überwachung - Protokolle

Metriken für Implementierungsentscheidungen

- Kosten
  - Günstig
    - Je nach Anzahl und Häufigkeit der ausgelösten Alarme, sowie der gewählten Benachrichtigungswege, können die Kosten höher werden.
- Komplexität der Umsetzung
  - Mittel
    - Es müssen zuerst die gewünschten Alarme konfiguriert werden.
- Nutzen (Impact)
  - Mittel
    - Grundlegendes Alerting und Erkennung ist möglich.

Sicherheit von Log-Dateien in Windows - On-Premise

Nur Benutzer mit den Rollen Administrator und Event Log Readers können die Log-Einträge des Eventviewers einsehen.

Weiters kann die Integrität des Systems ebenfalls überwacht werden: https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-system-integrity

Erfüllte Anforderungen

- LML2-5 Protokollierung - Prüfung und Integrität
- LML3-6 Protokollierung - Schutz vor Veränderung

Metriken für Implementierungsentscheidungen

- Kosten
  - Günstig
    - Ist standardmäßig umgesetzt.
- Komplexität der Umsetzung
  - Einfach

        - Ist standardmäßig umgesetzt.
- Nutzen (Impact)
    - Niedrig
        - Angreifer benötigt erhöhte Rechte zum Auslesen der Daten.

Sicherheit von Log-Dateien in Windows - Cloud

Azure Monitor stellt die Integrität der Logs sicher: https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-security

Weiters können die Logs nur von bestimmen Rollen eingesehen oder verwaltet werden: https://learn.microsoft.com/en-us/azure/azure-monitor/roles-permissions-security

Erfüllte Anforderungen

- LML2-5 Protokollierung - Prüfung und Integrität
- LML3-6 Protokollierung - Schutz vor Veränderung

Metriken für Implementierungsentscheidungen

- Kosten
    - Günstig
        - Ist standardmäßig umgesetzt.
- Komplexität der Umsetzung
    - Einfach
        - Ist standardmäßig umgesetzt.
- Nutzen (Impact)
    - Niedrig
        - Angreifer benötigt erhöhte Rechte zum Auslesen der Daten.

Zeitsynchronisierung in Windows

Um Events auf verschiedenen Systemen miteinander in Verbindung bringen zu können, ist es erforderlich auf allen Systemen die Zeit synchron zu halten.

In Windows gibt es eine definierte Hierarchie, von wo Systeme ihre Zeit beziehen (z.B. der DC). Für weitere Details siehe: https://learn.microsoft.com/en-us/windows-server/networking/windows-time-service/how-the-windows-time-service-works#domain-hierarchy-based-synchronization

Erfüllte Anforderungen

- LML2-43 Protokollierung - Zeitsynchronisierung

Metriken für Implementierungsentscheidungen

- Kosten
    - Günstig

        - Ist standardmäßig umgesetzt.
- Komplexität der Umsetzung
    - Einfach
        - Ist standardmäßig umgesetzt.
- Nutzen (Impact)
    - Niedrig
        - Angreifer benötigt erhöhte Rechte zum Auslesen der Daten.

Geloggte Aktivitäten in Windows - On-Premise

Ein EventViewer kann konfiguriert werden, die Log-Einträge sind aber unveränderlich und können daher nur gelöscht aber nicht verändert werden. Interaktionen mit dem Log, beispielsweise das Löschen von Logs, werden ebenfalls im Log gespeichert:

- https://learn.microsoft.com/en-us/host-integration-server/core/how-to-change-event-viewer-settings1
- https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/planning-and-deploying-advanced-security-audit-policies

Erfüllte Anforderungen

- LML2-9 Protokollierung - Sicherheitsereignissen
- LML2-19 Ereignisprotokoll - Felder mit Sicherheitsrelevanz
- LML2-20 Ereignisprotokoll - Felder mit Sicherheitsrelevanz
- LML2-37 Überwachung - relevante Ereignisse
- LML2-39 Überwachung - Serviceprovider

Metriken für Implementierungsentscheidungen

- Kosten
    - Günstig
        - Ist standardmäßig umgesetzt.
- Komplexität der Umsetzung
    - Einfach
        - Ist standardmäßig umgesetzt.
- Nutzen (Impact)
    - Mittel
        - Das Loggen von relevanten Ereignissen ist unerlässlich um Monitoring und Incident Response zu ermöglichen.

Geloggte Aktivitäten in Windows - Cloud

Es kann konfiguriert werden, welche Ereignisse geloggt werden sollen: https://learn.microsoft.com/en-us/azure/azure-monitor/logs/basic-logs-configure?tabs=portal-1%2Cportal-2

Der Azure Monitor Log kann nur erweitert werden, also neue Einträge hinzugefügt werden, jedoch nicht manipuliert werden: https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-system-integrity

Erfüllte Anforderungen

- LML2-9 Protokollierung - Sicherheitsereignissen
- LML2-19 Ereignisprotokoll - Felder mit Sicherheitsrelevanz
- LML2-20 Ereignisprotokoll - Felder mit Sicherheitsrelevanz
- LML2-37 Überwachung - relevante Ereignisse
- LML2-39 Überwachung - Serviceprovider

Metriken für Implementierungsentscheidungen

- Kosten
  - Günstig
    - Ist einfach zu konfigurieren bzw. teilweise schon standardmäßig umgesetzt.
- Komplexität der Umsetzung
  - Einfach
    - Ist einfach zu konfigurieren bzw. teilweise schon standardmäßig umgesetzt.
- Nutzen (Impact)
  - Mittel
    - Das Loggen von relevanten Ereignissen ist unerlässlich um Monitoring und Incident Response zu ermöglichen.

Tags

- #Windows
- #Logging
- #ZentralesLogging

Linux

Voraussetzung

- [[LML1-Linux]]

Zentrales Logging in Linux

Audit-Logs sollten zentral aufbewahrt werden, um eine Gesamtanalyse von Ereignissen über alle Systeme hinweg zu ermöglichen.

Linux - On-Premise

Die gängigen Logging Lösungen unter Linux unterstützen das Schreiben von Log-Dateien in ein zentrales System:

- Konfiguration von rsyslog: https://www.loggly.com/ultimate-guide/managing-linux-logs/

- Konfiguration von syslog-ng: https://www.syslog-ng.com/technical-documents/doc/syslog-ng-open-source-edition/3.22/administration-guide/12
- Beispielkonfiguration von logstash: https://www.elastic.co/guide/en/logstash/current/config-examples.html

Linux - Cloud

Der Azure Monitor kann beispielsweise auch Linux syslog Nachrichten entgegennehmen: <Azure Monitor>

Erfüllte Anforderungen

- LML2-45 Protokollierung - Zentralisierung

Metriken für Implementierungsentscheidungen

- Kosten
  - Günstig
    - Zentrales Logging wird von gängigen (Open Source) Lösungen unterstützt.
- Komplexität der Umsetzung
  - Mittel
    - Das zentrale Logging muss konfiguriert werden.
- Nutzen (Impact)
  - Hoch
    - Zentrales Logging ermöglicht einfacheres Monitoring und Incident Response. Des weiteren ist es für Angreifer schwieriger Logeinträge zu manipulieren (da das Log auf einem zentralen Server gespeichert wird).

Zeitsynchronisierung in Linux

Um Events auf verschiedenen Systemen miteinander in Verbindung bringen zu können, ist es erforderlich auf allen Systemen die Zeit synchron zu halten.

Linux - On-Premise

Unter Linux wird empfohlen mindestens vier NTP-Server einzusetzen: https://access.redhat.com/solutions/58025

Linux - Cloud

Viele Linux Standardimages in Azure verfügen über keine vorinstallierte Zeitsynchronisation. Grundsätzlich gibt es allerdings keine weiteren Spezifika. Weitere Informationen: https://learn.microsoft.com/en-us/azure/virtual-machines/linux/time-sync

Erfüllte Anforderungen

- LML2-43 Protokollierung - Zeitsynchronisierung

Metriken für Implementierungsentscheidungen

- Kosten
  - Günstig
    - Kann mit gratis Tools umgesetzt werden.
- Komplexität der Umsetzung
  - Mittel
    - Werden bestehende Zeitserver verwendet, müssen diese nur konfiguriert werden. Sollten eigene Zeitserver verwendet werden, müssen diese aufgesetzt werden.
- Nutzen (Impact)
  - Mittel
    - Zeitsychronisation ist essentiell um den Ablauf von Angriffen nachvollziehen zu können.

Tags

- #Linux
- #Logging
- #ZentralesLogging
- #Dauer

Microsoft 365

Voraussetzung

- [[LML1-MS365]]

Zentrales Logging in Microsoft 365

In Microsoft 365 wird zentral in Microsoft 365 geloggt. Diese Informationen können allerdings noch in ein SIEM integriert werden. Dabei hilft der folgende Artikel von Microsoft:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/siem-server-integration

Erfüllte Anforderungen

- LML2-45 Protokollierung - Zentralisierung

Metriken für Implementierungsentscheidungen

- Kosten
  - Günstig
    - Für das Logging selbst fallen keine Kosten an. Die Kosten fallen auf SIEM Seite an.
- Komplexität der Umsetzung
  - Mittel
    - Logging in ein SIEM muss konfiguriert werden.
- Nutzen (Impact)

    - Mittel
        - Zentrales Logging ermöglicht einfacheres Monitoring und Incident Response. Des weiteren ist es für Angreifer schwieriger Logeinträge zu manipulieren (da das Log auf einem zentralen Server gespeichert wird).

Monitoring in Microsoft 365

Monitoring und Alerting kann direkt in Microsoft 365 über Microsoft 365 Alert Policies erfolgen. Folgender Guide erklärt wie Alerts erstellt werden können: https://o365reports.com/2022/03/10/real-time-alerting-with-microsoft-365-alert-policies/

Erfüllte Anforderungen

- LML2-2 Überwachung - Überwachungssystem
- LML2-42 Überwachung - Protokolle

Metriken für Implementierungsentscheidungen

- Kosten
    - Mittel
        - Diese Funktionalität ist nicht in allen Lizenzmodellen inkludiert.
- Komplexität der Umsetzung
    - Einfach
        - Die Konfiguration ist einfach.
- Nutzen (Impact)
    - Mittel
        - Alerting ist unerlässlich, um über potentielle Angriffe schnellstmöglich informiert zu werden.

Sicherheit von Log-Dateien in Microsoft 365

Log-Dateien können nur von Konten mit speziellen Rollen eingesehen werden. Hier gibt es auch eine Rolle, die nur lesenden Zugriff erlaubt. Für Details siehe: https://techcommunity.microsoft.com/t5/public-sector-blog/discovering-microsoft-365-logs-within-your-organization-part-1/ba-p/2823682

Erfüllte Anforderungen

- LML2-5 Protokollierung - Prüfung und Integrität
- LML3-6 Protokollierung - Schutz vor Veränderung

Metriken für Implementierungsentscheidungen

- Kosten
    - Günstig
        - Die Funktionalität ist integriert.
- Komplexität der Umsetzung

    - Einfach
        - Die Funktionalität ist bereits konfiguriert.
- Nutzen (Impact)
    - Niedrig
        - Nur privilegierte Konten sollten Einsicht bekommen.

Geloggte Aktivitäten in Microsoft 365

Die Liste an geloggten Aktivitäten wird von Microsoft gepflegt und kann nicht editiert werden. Eine Übersicht findet sich unter folgendem Link: https://learn.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide#audited-activities

Erfüllte Anforderungen

- LML2-9 Protokollierung - Sicherheitsereignisse
- LML2-19 Ereignisprotokoll - Felder mit Sicherheitsrelevanz
- LML2-20 Ereignisprotokoll - Felder mit Sicherheitsrelevanz
- LML2-37 Überwachung - relevante Ereignisse
- LML2-39 Überwachung - Serviceprovider

Metriken für Implementierungsentscheidungen

- Kosten
    - Günstig
        - Die Funktionalität ist integriert.
- Komplexität der Umsetzung
    - Einfach
        - Die Funktionalität kann nicht konfiguriert werden.
- Nutzen (Impact)
    - Mittel
        - Relevante Ereignisse müssen geloggt werden.

Tags

- #MS365
- #Logging
- #ZentralesLogging

Antimalware

computerweekly.com definiert Antimalware folgendermaßen:

> Antimalware, oft auch Anti-Malware geschrieben, ist ein spezielles Software-Programm. Es soll schädliche Programme auf individuellen Computer- und IT-Systemen verhindern, erkennen und vernichten.

https://www.computerweekly.com/de/definition/Antimalware-Anti-Malware

Host basierte Intrusion Detection bzw. Prevention ist oft ein Bestandteil von Antimalwaresoftware.

Funktionalitäten von Antimalwaresoftware

Die meisten Antimalwarelösungen sollten die automatische Prüfung von Wechselmedien unterstützen. Die meisten modernen Antimalwarelösungen sollten auch verhaltensbasierte Erkennung unterstützen.

Beispiel Windows Defender

Windows

Microsoft Windows Defender Echtzeit Schutz:

- https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963

Wechseldatenträger automatisch scannen:

- https://answers.microsoft.com/en-us/protect/forum/all/defender-to-automatically-scan-portable-drives-for/d4545417-a160-4221-96db-89fcc1cdde54

Microsoft Windows Defender ist verhaltensbasiert:

- https://learn.microsoft.com/de-de/microsoft-365/security/defender-endpoint/configure-protection-features-microsoft-defender-antivirus?view=o365-worldwide

Linux

Windows Defender für Linux:

- https://learn.microsoft.com/de-de/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint-linux?view=o365-worldwide

macOS

Windows Defender für macOS:

- https://learn.microsoft.com/de-de/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint-mac?view=o365-worldwide

Windows (in Azure)

Antimalware für Azure:

- https://learn.microsoft.com/de-de/azure/security/fundamentals/antimalware

Linux (in Azure)

Antimalware für Azure gibt es nicht für Linux, aber Defender for Cloud wird empfohlen:

- https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction

Microsoft 365

Schutz vor Schadsoftware in Microsoft 365:

- https://learn.microsoft.com/de-de/microsoft-365/security/office-365-security/anti-malware-protection?view=o365-worldwide

Erfüllte Anforderungen

- LML2-7 Überwachung - Anti-Virus

Metriken für Implementierungsentscheidungen

- Kosten
  - Mittel
    - Es können Lizenzgebühren entstehen.
- Komplexität der Umsetzung
  - Einfach
    - Die benötigten Einstellungen sollten nicht allzu komplex sein.
- Nutzen (Impact)
  - Hoch
    - Durch Antimalwaresoftware können Angriffe abgewehrt werden.

Host basierte Intrusion Detection/Prevention

Diese Funktionalität wird oft von Antimalwarelösungen bzw. Host-basierte Firewalls abgedeckt. Windows Defender deckt diese Funktionalität beispielsweise ab:
https://www.microsoft.com/security/blog/2018/11/15/whats-new-in-windows-defender-atp/.
Der Windows Defender kann für Windows und Linux bezogen werden, siehe [[LML2-7 Überwachung - Anti-Virus]].

Erfüllte Anforderungen

- LML2-28 Überwachung - IDS

Metriken für Implementierungsentscheidungen

- Kosten
  - Mittel
    - Diese Funktionalität könnte möglicherweise nur mit zusätzlicher kostenpflichtiger Software abgedeckt werden.

- Komplexität der Umsetzung
  - Einfach
    - Je nach eingesetzter Software sollte der Implementierungsaufwand gering sein.
- Nutzen (Impact)
  - Hoch
    - Durch Host basierte Intrusion Detection/Prevention können Angriffe abgewehrt werden.

Zentralisiertes Management und Logging

Die Antimalwarelösung sollte Ereignisse in ein zentrales System schreiben und zentral verwaltet werden. Für Windows Defender gibt es hier beispielsweise folgende Hilfestellung:
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/deploy-manage-report-microsoft-defender-antivirus?view=o365-worldwide

Erfüllte Anforderungen

- LML2-45 Protokollierung - Zentralisierung

Metriken für Implementierungsentscheidungen

- Kosten
  - Mittel
    - Es können Lizenzgebühren anfallen.
- Komplexität der Umsetzung
  - Einfach
    - Die Konfiguration benötigt kein besonderes Fachwissen.
- Nutzen (Impact)
  - Hoch
    - Malware auf den Endgeräten kann die Logs nicht manipulieren.

Tags

- #AntiVirus
- #Antimalware
- #Virus
- #protection
- #Defender

Network-Based Intrustion Detection/Prevention System (NIDS/NIPS)

Barracuda definiert ein IDS/IPS folgendermaßen:

> Ein Intrusion Detection System (IDS) ist ein Gerät oder eine Softwareanwendung, das bzw. die ein Netzwerk auf böswillige Aktivitäten oder Richtlinienverstöße hin überwacht. Jede böswillige Aktivität oder Sicherheitsverletzung wird normalerweise zentral mithilfe eines Sicherheitsinformations- und Ereignisverwaltungssystems gemeldet oder erfasst. Einige IDS sind in der Lage, auf Eindringversuche zu reagieren. Diese werden als Intrusion Prevention Systems (IPS) bezeichnet.

https://de.barracuda.com/glossary/intrusion-detection-system

Einsatz von IPS Systemen

On-Premise

Es gibt eine große Auswahl an kommerziellen und freien Tools. Populäre Open-Source Lösungen sind beispielsweise folgende:

- snort: https://github.com/snort3/snort3
- suricata: https://github.com/OISF/suricata
- zeek: https://github.com/zeek/zeek

Um die Anforderung zu erfüllen, sollte ein NIDS/NIPS Tool in wichtigen Netzwerkbereichen eingesetzt werden.

Azure Cloud

In Azure gibt es spezielle Lösungen für dieses Problem, wie z.B. die Azure Firewall. Für weitere Informationen siehe: https://learn.microsoft.com/en-us/security/benchmark/azure/security-control-network-security#16-deploy-network-based-intrusion-detectionintrusion-prevention-systems-idsips

Erfüllte Anforderungen

- LML2-29 Überwachung - IDS

Metriken für Implementierungsentscheidungen

- Kosten
  - Mittel
    - Es können Lizenzgebühren entstehen.
- Komplexität der Umsetzung
  - Komplex
    - Diese Tools sind komplex zu konfigurieren.
- Nutzen (Impact)
  - Hoch
    - Ein gut eingestelltes NIDS/NIPS kann Angriffe in Echtzeit erkennen und eventuell verhindern.

Tags

- #IDS/IDP
- #NIDS/NIPS

SIEM bzw. zentralisiertes Logging in LML 2

security-insider.de erklärt SIEM folgendermaßen:

> Die Abkürzung SIEM steht für Security Information and Event Management. Es handelt sich um ein softwarebasiertes Technologiekonzept aus dem Bereich des Sicherheitsmanagements, mit dem ein ganzheitlicher Blick auf die IT-Sicherheit möglich wird. SIEM stellt eine Kombination aus Security Information Management (SIM) und Security Event Management (SEM) dar. Durch das Sammeln, Korrelieren und Auswerten von Meldungen, Alarmen und Logfiles verschiedener Geräte, Netzkomponenten, Anwendungen und Security-Systeme in Echtzeit werden Angriffe, außergewöhnliche Muster oder gefährliche Trends sichtbar. Auf Basis der gewonnenen Erkenntnisse können Unternehmen oder Organisationen schnell und präzise auf Bedrohungen reagieren. Das Security Information and Event Management nutzt Verfahren des maschinellen Lernens und der Künstlichen Intelligenz (KI). SIEM-Lösungen sind auch als Services aus der Cloud verfügbar.

https://www.security-insider.de/was-ist-ein-siem-a-772821/

Ein SIEM sollte folgende Eigenschaften erfüllen:

> Zentrale Sammlung von Sicherheitsereignis-Logs aller Assets, um eine Log-Korrelation und Analyse zu ermöglichen. Eine Best-Practice-Implementierung erfordert die Verwendung eines SIEM das händlerspezifische Ereigniskorrelierungsalarmierungen enthält, alternativ kann auch eine Log-Analyseplattform verwendet werden, die sicherheitsrelevante Korrelationsalarmierungen ermöglicht. [CT18-13.1/IG2]

Einsatz eines SIEMs um abnormales Verhalten zu erkennen

Es soll abnormales Verhalten festgestellt werden wie:

- die ungeplante Beendigung von Prozessen oder Anwendungen
- Aktivitäten, die typischerweise mit Malware oder Datenverkehr in Verbindung gebracht werden, der von gefährlich eingestuften IP-Adressen oder Netzwerkdomänen ausgeht
- bekannte Angriffsmerkmale (z.B. Denial of Service, Puffer overflow)
- ungewöhnliches Systemverhalten, wie die Protokollierung von Tastatureingaben, Prozessinjektion und Abweichungen von Standardprotokollen
- Engpässe und Überlastungen (z.B. Netzwerkwarteschlangen, Latenzzeiten und Netzwerk-Jitter)
- unbefugter Zugriff (tatsächlich und versucht) auf Systeme oder Informationen
- unbefugtes Durchsuchen von Geschäftsanwendungen, Systemen und Netzwerken
- erfolgreiche und erfolglose Versuche auf geschützte Ressourcen zuzugreifen
- ungewöhnliches Benutzer- und Systemverhalten im Verhältnis zum erwarteten Verhalten [ISO2:22-8.16]

Erfüllte Anforderungen

- LML2-22 Überwachung - Erkennung von abnormalem Verhalten

Metriken für Implementierungsentscheidungen

- Kosten
  - Teuer
    - Je nach verwendetem SIEM können Lizenzkosten anfallen sowie eventuelle externe Consulting Leistungen.
- Komplexität der Umsetzung

    - Komplex
        - Die Konfiguration ist sehr komplex und benötigt eventuell externes Wissen.
- Nutzen (Impact)
    - Hoch
        - Durch ein funktionierendes SIEM können Sicherheitsvorfälle oder gefährliche Trends gut erkannt werden.

Tags

- #SIEM
- #Monitoring
- #ZentralesLogging

LML 3 Organisatorisch

Bei diesen Anforderungen handelt es sich um organisatorische Maßnahmen, die nicht einfach technisch umgesetzt werden können:

- LML3-23 Analyse - Erzeugung von Threat Intelligence
- LML3-30 Analyse - Optimierung von Alarmen
- LML3-31 Analyse - Optimierung von Alarmen
- LML3-32 Protokollierung - sensible Daten
- LML3-36 Überwachung - Redundanz
- LML3-40 Überwachung - Serviceprovider

Tags

- #Organisatorisch

SIEM bzw. zentralisiertes Logging in LML 3

Ein SIEM sollte eine Möglichkeit zur Authentifizierung haben und verschiedene Userrollen (z.B. Read-Only) unterstützen:

> Nutzer, auch jene die privilegierte Rechte haben, darf es nicht möglich sein Logs zu ihren eigenen Aktivitäten zu löschen oder zu deaktivieren. Weiters sollen keine Veränderungen an den aufgezeichneten Nachrichtentypen vorgenommen werden dürfen. Logfiles dürfen nicht bearbeitet oder gelöscht werden und es muss sichergestellt werden, dass, sollte der Speicherplatzbedarf überschritten werden, Ereignisse zu jeder Zeit aufgezeichnet werden können, ohne das alte Einträge überschrieben werden. Hierfür sollten Techniken wie kryptografisches Hashing, Aufzeichnungen in eine „append-only and read-only“ Datei, sowie Aufzeichnungen in eine öffentliche Transparenzdatei verwendet werden. [I2:22-8.15]

Erfüllte Anforderungen

- LML3-33 Protokollierung - sensible Daten

Metriken für Implementierungsentscheidungen

- Kosten
  - Günstig
    - Diese Funktionalität ist in gängigen SIEM Systemen integriert.
- Komplexität der Umsetzung
  - Mittel
    - Die Einstellungen müssen nur zu Beginn einmal konfiguriert werden. Zugriffsrechte sollten regelmäßig überprüft werden.
- Nutzen (Impact)
  - Mittel
    - Angreifer können Logeinträge nicht mehr so einfach manipulieren und somit Angriffe verschleiern.

Tags

- #SIEM
- #Monitoring
- #ZentralesLogging

Data Loss Prevention (DLP)

Die Definition von Data Loss Prevention auf computerweekly.com (https://www.computerweekly.com/de/definition/Data-Loss-Prevention-DLP):

> Data Loss Prevention (DLP) ist eine Strategie, die sensible oder kritische Informationen schützt. Der Begriff wird auch verwendet, um Software-Lösungen zu beschreiben. Dabei handelt es sich um Produkte, die unterschiedliche Sicherheitstechniken und Maßnahmen einsetzen, um die Vertraulichkeit der Daten zu gewährleisten.

Data Loss Prevention ist häufig in Antimalwarelösungen oder IPS enthalten.

Erfüllte Anforderungen

- LML3-33 Protokollierung - sensible Daten

Metriken für Implementierungsentscheidungen

- Kosten
  - Mittel
    - Je nach Umsetzung können verschiedene Lizenz- oder Hardwarekosten entstehen.
- Komplexität der Umsetzung
  - Einfach
    - Muss nur einmal zu Beginn konfiguriert werden.
- Nutzen (Impact)
  - Hoch

- Im Falle eines Incidents greifen die Maßnahmen und helfen bei der Erkennung und Verhinderung.

Tags

- #DLP