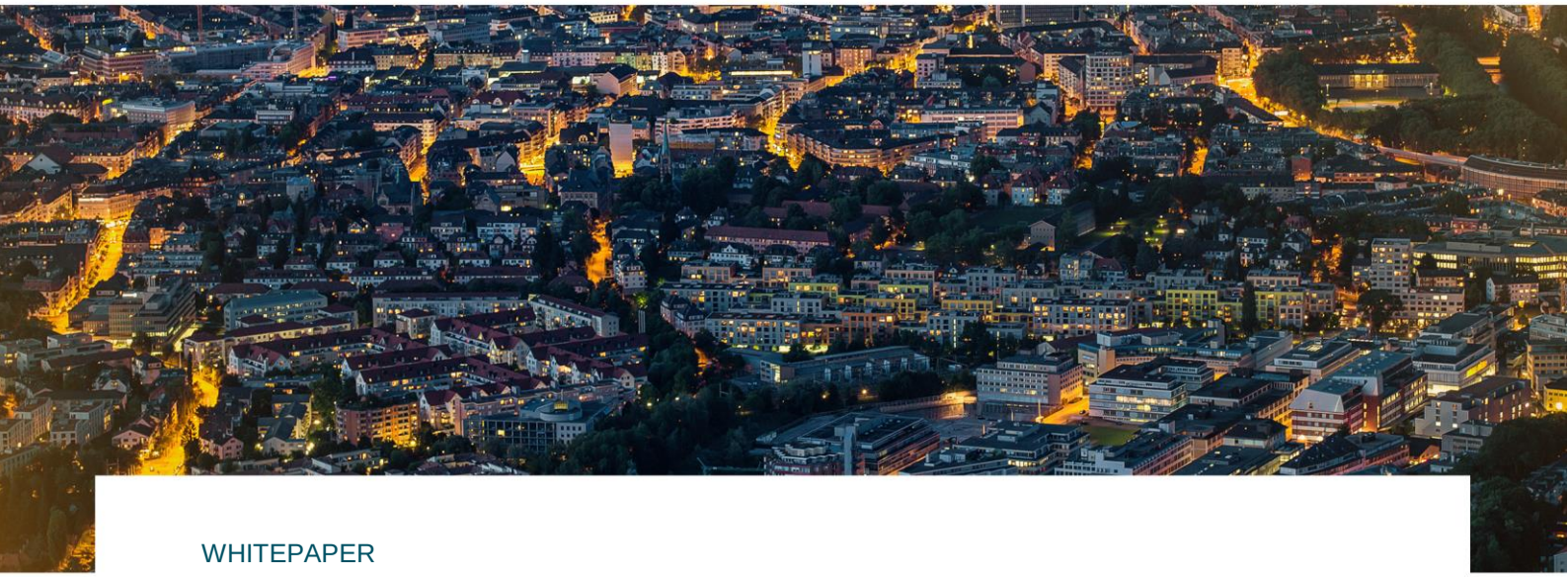
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch



WHITEPAPER

Logging, Auditing und Monitoring – Frontfühler der IT-Sicherheit

Nikola Stojanov | Produktmanager Management-Systeme | Steinhausen, 08. November 2019

Die heutige IT-Sicherheit ist damit konfrontiert, den Menschen als potenziell schwächstes Glied der Sicherheitskette, als beliebtes Angriffsziel für Cyber-Kriminelle, zu schützen. Denn Cyber-Kriminelle wenden ausgefeilte Social Engineering-Methoden an. Dabei spielt ein effektives Security Log Management eine zentrale Rolle. Welches die Herausforderungen sind und welchen Mehrwert das Security Log Management der CyOne Security bietet, erfahren Sie in diesem Whitepaper.

Meist ist es nur die Speerspitze eines raffinierten Verschleierungssystems, mit dem Ziel, die Sicherheitsmassnahmen möglichst effektiv und unbemerkt zu umgehen. Beliebte Ziele für Social Engineering-Attacken sind vor allem staatliche Stellen, aber auch zunehmend strategisch wichtige Infrastrukturen. Um solche Cyber-Attacken zu detektieren, Gegenmassnahmen einzuleiten oder mittels forensischer Datenanalyse das Schadensausmass und die Schwachstellen zu benennen, bedarf es eines guten Security Log Managements.

Denn das Logging bildet die Basis für eine erfolgreiche Ursachenanalyse. Sogar wenn ein Angriff bereits erfolgreich war und beispielsweise Daten abgeflossen sind, bleiben oft nur noch die Logs als letzte Verteidigungslinie für eine professionelle Ursachenanalyse, um die Schwachstellen und eventuell den Verantwortlichen zu identifizieren und damit bei einer Wiederherstellung des normalen Betriebes eine gleiche Cyber-Attacke zu unterbinden.

Die Entwicklung von «Logs»

In der Schifffahrt hat das Logbuch eine jahrhundertealte Tradition. Der Kapitän trägt alle wichtigen Ereignisse im Logbuch ein und kann bei Bedarf dort nachschlagen. Ganz ähnlich wird dies auch in der Softwarebranche gehandhabt, nur wird hier eine Logdatei anstelle des Logbuchs verwendet und nicht der Kapitän, sondern die Softwareapplikation eines Gerätes schreibt seine Ereignisse in diese Logdatei. Je nach Lösung wird anstelle einer Logdatei auch eine Datenbank verwendet. Hat man viele Geräte innerhalb eines Netzwerkes, werden die Logs auch zentral bei einem Server zusammengefasst.

Historisch wurden «Logs» in der Softwarebranche vor allem zur raschen Identifizierung und Behebung von Problemen und Fehlern in der Entwicklung verwendet. Heute dienen Logs vielen und sehr unterschiedlichen Funktionen innerhalb einer Organisation. Solche Funktionen sind zum Beispiel: Netzwerkperformance optimieren, Netzstabilität erhalten, Verfügbarkeit des Systems und der Komponenten gewährleisten und die Alarmierung bei dringenden Ereignissen.

Logging als organisatorische Herausforderung

Die zunehmende Verbreitung von Computersystemen in unserem Alltag führt zu einer enormen Zahl unterschiedlicher Komponenten in allen Bereichen einer Organisation. Die Gerätearten werden vielfältiger, es gibt Server, Workstations, Router, Switches, Firewalls und immer mehr auch mobile Geräte mit immer grösserer Rechenpower, die innerhalb einer Organisation operieren. Dies führt zu einer immer grösseren Zahl von Logs. Nicht nur die Zahl der Geräte wächst, auch die Anzahl Logeinträge pro Gerät kann unter Umständen sehr gross sein und wächst mit zunehmender Leistung der Geräte. Als ob das noch nicht ausreichen würde, gibt es auch immer mehr unterschiedliche Arten von Logeinträgen.

Die vielen Logs einer Organisation enthalten auch sicherheitsrelevante Meldungen. Diese Security Logs haben einen Sonderstatus und müssen speziell verarbeitet werden. Beispiele für Security Logs sind u.a. die Protokollierung von Authentisierungsversuchen durch Benutzer oder unautorisierte Zugangsversuche zu klassifizierten Daten. Nachfolgend werden die wichtigsten Begrifflichkeiten erläutert:

Logging / Log

Mit einer Logdatei oder einem Log ist eine Datei (im erweiterten Sinne auch eine Datenbank) gemeint, welche entweder die Ereignisse (events) eines Betriebssystems, die Software-Applikation oder die Kommunikationsanwendung mittels eines Nachrichteneintrags (entry/message) in einer Datei festhält. Im einfachsten Fall wird pro Nachricht eine Datei geschrieben. Die Erstellung eines Logs nennt man Logging.

Auditing

Betrifft das automatische Aufzeichnen von sicherheitskritischen Informationen zu Aktivitäten der Benutzer mit einer Applikation. Solche Informationen sind zum Beispiel: An- und Abmeldungen von Benutzern, Änderung der Benutzer- und Zugriffsrechte sowie Änderungen von sensiblen und sicherheitsrelevanten Daten. Die Speicherung der Audit-Daten muss in einem geeignet gesicherten System erfolgen.

Monitoring

Dient zur Überwachung der Logmeldungen in Echtzeit, als Basis für die Analyse der Anwendung, insbesondere der Performance.

Nutzen von Logging und Log Management

Effektives Logging erlaubt einer Organisation, frühzeitig Systemveränderungen zu entdecken und rechtzeitig darauf zu reagieren. Um einen solchen Nutzen ziehen zu können, muss man jedoch regelmässig die Logs beobachten, sprich, es braucht ein entsprechendes Monitoring der Logmeldungen.

Betriebsnutzen – Performance und Stabilität

Monitoring ist die Basis und die operative Stütze eines Netzwerk- und IT-Betreibers. Es unterstützt den Operator darin, die System-Leistung der effektiven Auslastung entsprechend zu optimieren. Hierfür beobachtet und wertet er leistungsspezifische Meldungen aus. Ebenso kann die System-Stabilität durch Analyse von Fehlermeldungen verbessert werden, indem das Monitoring Ersatz oder Erweiterung von betroffenen Geräten vorschlägt. Das Monitoring erlaubt es dem Betreiber in der Regel das System auszubalancieren, ohne dass die Benutzer davon etwas merken. Dies ist möglich, weil Massnahmen bereits vor spürbaren Symptomen für den Benutzer ergriffen werden können und damit einem Hotline-Anruf vorgreifen.

Sicherheitsnutzen – Detektion, forensische Datenbasis

Kontinuierliches Monitoring von Security Logs sind die feinsten und äussersten Fühler eines Systems, um einen Angriff zu detektieren. Einfache Angriffe, welche unter Umständen auch vom Benutzer (mit entsprechender Software) vor einem Schaden entdeckt werden, sind zwar die häufigsten, jedoch nicht zwingend die schädlichsten. Die aufwändigeren Angriffsmuster, bei denen die Angreifer sehr komplexe Angriffsvektoren fahren, haben sich in letzter Zeit gemehrt. Heute sind nicht nur staatliche Organisationen im Besitz von Tools, die einen solchen Angriff ermöglichen, vermehrt gibt es auch Fälle von kriminellen Organisationen, welche solche komplexen Angriffe fahren können.

Um diese Angriffe detektieren zu können, braucht man zwingend eine systemweite Lageübersicht und die Fähigkeit, System-Korrelationen zu fahren. Es braucht «Security Information and Event Management »-Systeme (SIEM), um frühzeitig sicherheitsrelevante Vorfälle (incidents) zu detektieren und zu melden. Meist ist ein SIEM in einem Security Operation Center (SOC) integriert. Die schiere Datenmenge, gekoppelt mit der Notwendigkeit rasch zu reagieren, bringt heute immer öfter neue Technologie, wie Künstliche Intelligenz (KI) oder eine vernetzte Wissensdatenbank, in einem SOC zum Einsatz. Anders liesse sich das heute, bei den vielen unterschiedlichen Geräten und der immensen Datenmenge von Logs, die an einem SOC zusammengetragen werden und in Echtzeit prozessiert werden müssen, kaum mehr bewerkstelligen.

Im günstigsten Fall erkennt man einen Angriff bereits, bevor Schaden entstanden ist, und kann Gegenmassnahmen einleiten und Schaden abwenden. Es gibt allerdings auch Cyber-Angriffe, die erfolgreich sind und erst nach dem entstandenen Schaden sichtbar werden. Aber auch hier ist das Security Log Management von entscheidender Bedeutung, um forensische Datenanalyse zu betreiben. Die Feststellung des Schadensausmasses ist für eine Organisation fast noch wichtiger als der Vorfall selber. Das Security Log Management ermöglicht Rückschlüsse auf die Verbesserung des Sicherheitsdispositivs, um gegen zukünftige Attacken gewappnet zu sein.

Warum braucht es ein Security Log Management?

Die schiere Masse an Daten macht effizientes Security Log Management notwendig. Insbesondere muss der Prozess der Erstellung, Übertragung, Speicherung, Analyse und des Löschens der Security-Logdaten bestimmt und geregelt werden. Vieles, das hier im Zusammenhang mit Security Log Management zur Sprache kommt, gilt auch für das generelle Logging. Wir werden uns im Weiteren jedoch auf das Security Logging konzentrieren.

«Device logs can be one of the most helpful tools…, or they can be a huge waste of space and time.»[1]

Das Ziel des Log Managements ist es sicherzustellen, dass IT-Sicherheitsmeldungen in genügend hoher Detailauflösung und für eine genügend lange Zeitperiode gespeichert werden. Die eigentliche Schwierigkeit für eine Organisation in Bezug auf das Security Log Management besteht darin, die Balance zwischen den beschränkten Log-Management-Ressourcen und dem kontinuierlichen Fluss der Logdaten zu finden.

Automatische oder routinemässige Analyse der Logs sind entscheidend für die Identifikation von Sicherheitsereignissen (*security incidents*), Policy-Zuwiderhandlungen, bösartigen Aktivitäten oder bei operativen Problemen.

Auditing Logs sind im Speziellen sehr hilfreich bei der forensischen Analyse von internen Problemen. Sie sind Voraussetzung, um operationale Trends und Langzeitengpässe zu erkennen sowie mögliche externe Angriffsversuche auszumachen. Diese müssen entsprechend geschützt abgelegt werden.

Auch der gesetzliche Rahmen muss beim Logging beachtet werden. Auf der einen Seite besteht bei gewissen Aktivitäten eine gesetzliche Pflicht für Mindestaufbewahrungszeiten, zum Beispiel für Audit-Logs. Auf der anderen Seite müssen personenbezogene Daten innerhalb einer bestimmten Frist gelöscht werden.

Das Security Log Management muss sicherstellen, dass Vertraulichkeit, Zugang, Datenintegrität sowie die benötigte Verfügbarkeit gewährleistet sind.

[1] Autor unbekannt, jedoch oft zitiert in IT-Administratorenforen.

Herausforderung eines Security Log Managements

Das Security Log Management beinhaltet die Prozesse der Erstellung, Verteilung, Speicherung, Analyse und des Löschens von Security-Log-Daten. Innerhalb einer Organisation gibt es typischerweise viele unterschiedliche Geräte und Applikationen, welche Logs generieren. Dies verkompliziert das Log Management in folgender Weise:

Viele Quellen

Logs sind innerhalb der Organisation auf viele Geräte verteilt. Ein einzelnes Gerät kann auch mehrere Logfiles haben, z.B. Netzwerkaktivitäten in einer Datei und Authentisierungs-Ereignisse in einer anderen.

Hohe Anzahl von Logmeldungen pro Gerät

Die Logmeldungen pro Gerät lassen sich oft konfigurieren. Wenn auf Systemniveau kein Prozess oder keine Policy definiert wurde, wird hier standardmässig entweder so konfiguriert, dass das Gerät keine (oder nur Error-) Meldungen oder aber möglichst alle Meldungen versendet. Es kann sogar vorkommen, dass innerhalb einer Organisation, je nach Operator, das eine oder andere Extrem eingestellt ist. Hier zeigt sich am deutlichsten der Nutzen einer systemweiten Planung und Definition des Loggings.

Inkonsistente Logmeldungen

Geräte können aus Effizienzgründen gewisse redundante Informationsteile weglassen und nur die wichtigste Information speichern. Für das Gerät selber ist sie vielleicht redundant. In einer zentralen Sammelstelle, wo die Daten analysiert werden sollen, ist sie es nicht. Es kann sich auch um unterschiedliche Formatierungen handeln, wie z.B. unterschiedliche Datum-Zeit-Schreibweisen. All das macht den Prozess der Vereinheitlichung und Speicherung der Log-Daten kompliziert.

Inkonsistente Zeitstempel

Jedes Gerät verwendet für die Logmeldung seine interne Systemzeit. Wenn diese nicht synchronisiert sind, kann die Reihenfolge von Ereignissen geräteübergreifend nicht mehr reproduziert werden.

Inkonsistente File-Formate, Standards

Die Geräte unterstützen nicht immer das gleiche File-Format, um die Logmeldungen zu speichern. Selbst wenn der gleiche Standard eingestellt ist, bleibt die effektive Implementation zwischen unterschiedlichen Geräteherstellern verschieden, so dass eine einfache automatische Auswertung nicht ohne zusätzlichen Aufwand möglich ist.

CyOne Security – flexible operative Integration für höchste Sicherheitsansprüche
CyOne Security-Geräte verfügen über ein konfigurierbares Logging, welches sowohl an den Server im Heimnetz rapportieren kann als auch an Server auf dem WLAN. Auf diese Weise hat der Kunde die Flexibilität, gewisse Monitoring-Funktionen bei Bedarf auch an externe Partner zu vergeben, z.B. für den Wartungsbetrieb. Gleichzeitig behält der Kunde aber die Kontrolle über sicherheitsrelevante Meldungen innerhalb der eigenen Organisation.

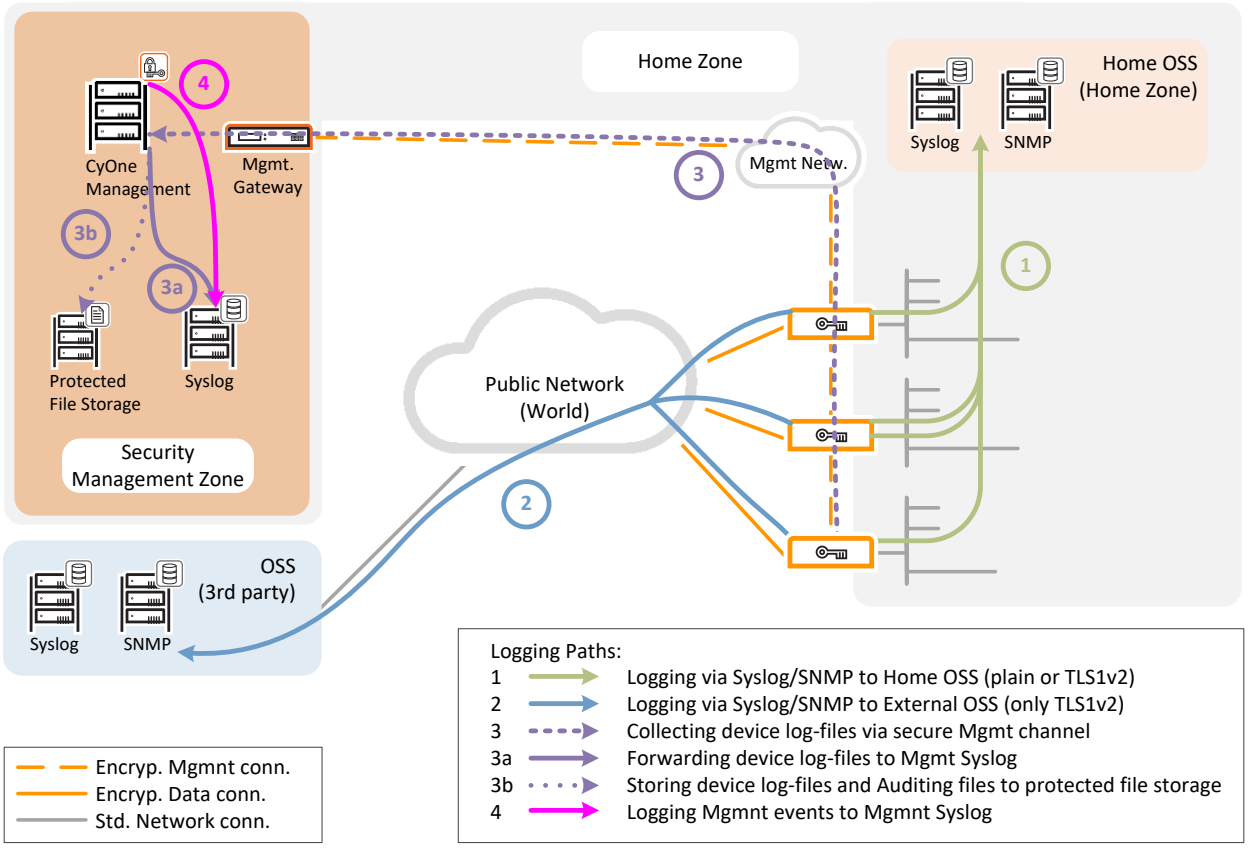


Abbildung 1 Systemaufbau mit CyOne Security-Geräten und -Management für ein sicheres Log-Reporting aus Betreibersicht

CyOne Security setzt auf verbreitete Standards wie Syslog und SNMP im Log Management und auf eine einheitliche Implementierung innerhalb der eigenen Gerätefamilie. Somit ist eine flexible Integration der CyOne Security-Geräte in ein heutiges Operation Support System (OSS) möglich, ohne dabei auf höchste Sicherheitsansprüche zu verzichten. Hierzu wird vor allem auf den Syslog Standard zurückgegriffen. Je nach Verbindung lässt sich der offene Standard oder die Secure-Variante, TLS-1v2-verschlüsselt, verwenden (siehe Abbildung 1). CyOne Security-Infrastruktur-Geräte der neusten Generation unterstützen zusätzlich SNMPv3, auch hier in der offenen wie auch in der Secure-Variante.

In der Abbildung 1 sind alle unterstützten Varianten für das Log Management mit CyOne Security-Geräten abgebildet. Je nach Systemarchitektur und Sicherheitsanforderung lassen sich Teile davon oder aber auch alle Wege umsetzen.

***1 Home OSS Logging** (Abbildung 1 – Logging Path 1)*

Die am häufigsten gewählte Variante, bei eigenem operativem Center (OSS), ist das Logging über Syslog (offen oder secure) auf dem Home Netz in das OSS. Hier sind auch alle SNMP verfügbar, ebenfalls in der offenen wie auch verschlüsselten Variante.

***2 Drittbetreiber OSS** (Abbildung 1 – Logging Path 2)*

Sollte eine Drittfirma sich um den operativen Betrieb kümmern, so besteht die Möglichkeit, dass die CyOne Security-Geräte auf der Worldseite ebenfalls Logging-Meldungen absetzen können. Hier steht jedoch nur noch die verschlüsselte Variante (TLS 1v2) zur Verfügung und im Fall von SNMP nur noch ein reduziertes Set.

***3 Geräte-Logs sammeln durch CyOne Management** (Abbildung 1 – Logging Path 3)*

Die Geräte-Logs lassen sich auch durch das CyOne Management über den sicher verschlüsselten Management-Kanal einsammeln. Das CyOne Management ist durch den hochsicher verschlüsselten Management-Kanal und den CyOne Management Gateway optimal geschützt, um höchsten Sicherheitsanforderungen zu genügen.

3a Geräte-Logs an Syslog innerhalb der Security Management Zone
(Abbildung 1 – Logging Path 3a)

Um zusätzlich Sicherheit zu gewährleisten, können die Gerätelogs zusätzlich vom CyOne Management an einen Syslog-Server innerhalb der hochsicheren Management Zone geleitet werden. Auch hier kann wahlweise der offene oder verschlüsselte (TLS 1v2) Syslog Standard verwendet werden.

***3b Geräte-Log Files speichern in Management Zone** (Abbildung 1 – Logging Path 3b)*

Die Geräte-Logs können zusätzlich an einem speziell geschützten Speicherort innerhalb der Management Zone abgelegt werden, um so die Redundanz zu erhöhen und zusätzlich vor eventuellen Manipulationen durch einen potenziellen Angreifer zu schützen.

***4 Syslog-Meldungen der CyOne Management Systems** (Abbildung 1 – Logging Path 4)*

Das CyOne Management-System kann auch eigene Ereignismeldungen via Syslog an einen Syslog-Server in der Management Zone versenden.

Durch diese vielfältigen Konfigurationsmöglichkeiten ist so eine individuelle Systemintegration möglich. Die Flexibilität und die hohe Sicherheit der CyOne Security-Lösung legt die Basis für ein verlässliches und vertrauenswürdiges Logging im operativen Kontext. Bei richtiger Planung und Verwendung von zusätzlichen Lösungen von Dritten lässt sich das CyOne Security-Logging ebenso in ein Security Operation Center (SOC) integrieren.

CyOne Security Logging – Stützpfeiler im Ernstfall

«No matter how extensive you're logging, log files are worthless if you cannot trust their integrity. The first thing most hackers will do is try to alter log files to hide their presence. To protect against this, you should record logs both locally and to a remote log server. This provides redundancy and an extra layer of security as you can compare the two sets of logs against one another -- any differences will indicate suspicious activity.»[2]

Die Grundpfeiler des Security Log Managements sind die Datenintegrität, die Vertraulichkeit und der sichere Datenzugang: Eine Meldung, der man nicht vertrauen kann, ist wertlos, wenn nicht sogar schädlich. Logmeldungen sind auch beliebte Angriffspunkte von Hackern. CyOne Security geht in diesen Belangen keine Kompromisse ein, die Geräte erfüllen die Anforderungen für die höchste Sicherheitsstufe. Nicht nur findet eine vollständige Trennung der Kommunikationskanäle durch eine quantenrechnersichere Chiffrierung statt, die Geräte verfügen ausserdem über einen Tamperschutz, um auch physisch gegen Manipulationen gefeit zu sein.

Das Schlüsselelement ist jedoch das zentrale Management von CyOne Security, welches sich, abgeschottet durch ein Management Gateway, in einer hochsicheren Zone befindet. CyOne Security-Geräte werden online über das zentrale Management konfiguriert. Das Monitoring der Geräte für die Betriebsstabilität kann wahlweise über einen «externen» Syslog-Server, das heisst ausserhalb der hochsicheren Management Zone, betrieben werden oder innerhalb der hochsicheren Management Zone. Auf diese Weise lässt sich die Zonierung auf das jeweilige Betreiberszenario optimal anpassen.

Das CyOne Management-System, CMS-1200, erlaubt zudem das Abholen und Ablegen der Geräte-Logmeldungen, um diese zentral beim Management-System zu speichern und archivieren. Die abgeholten Geräte-Logs können wahlweise auch an einen Syslog-Server in der hochsicheren Management Zone weitergereicht werden. Auf diese Weise wird eine flexible Loganalyse durch Tools von Drittanbietern gewährleistet und die Integrität der Daten gewahrt.

Der neuste Release des CyOne Management-Systems geht mit der integrierten Auditing-Funktionalität sogar noch einen Schritt weiter. Die sicherheitsrelevanten Aktivitäten am zentralen Management-System werden so verdichtet gesammelt und erlauben einen effektiven Zugang zu Veränderungen der Sicherheitskonfigurationen. Hierbei unterscheidet die Management-Lösung von CyOne Security zwischen zwei Auditing-Funktionalitäten: Unit- und Application-Auditing.

Das Unit Auditing speichert jede an das Gerät (Unit) gesandte Konfiguration lokal ab. Innerhalb der Management-Lösung hat der Administrator die Möglichkeit, die Konfigurationen pro Gerät zwischen unterschiedlichen Zeitpunkten zu vergleichen. Dies geschieht direkt über ein integriertes graphisches User Interface. Das Application-Auditing ist das Audit Log, um die Benutzer-Aktivität innerhalb der Management-Software zu protokollieren. Hierbei wird einerseits ein Tageslog geführt, andererseits werden alle Datenbank-Änderungen als Reports abgelegt, um mittels externer Vergleichs-Tools bei Bedarf vertiefte zusätzliche Analysen zu fahren.

Last, but not least ist mit der CyOne Management-Lösung eine benutzerspezifische Definition des Zugangs zu den abgelegten Logdaten möglich, ohne die operative Funktionalität dadurch zu beeinträchtigen. So kann der Zugang zu heiklen und personenspezifischen Daten noch weiter eingeschränkt werden. Die Ablage der Logdaten ist so umsetzbar, dass die Logdaten grundsätzlich vor Manipulationen geschützt sind.

---

[2] Michael Cobb, Computer Weekly, 29. Aug. 2018

Der realistische Ernstfall

Heutige Hacker-Angriffe werden immer intelligenter und ausgefeilter. Die Angreifer haben oft detailliertes Fachwissen und entsprechende Tools, um Standard-Abwehrmechanismen zu umgehen oder auszuschalten. Weiter sind die Logs für Angreifer ein beliebtes und wichtiges Ziel: Hier lassen sich Spuren verwischen oder sogar Alarme verhindern. In diesem Kontext gilt ganz besonders: Das Logging ist nur so gut und hilfreich, wie die Datenintegrität und Vertraulichkeit gewahrt ist. Ebenso muss ein sicherer Zugang, geschützt vor jeglicher Manipulation auch in einem Notfallszenario gewährleistet werden. Ohne diese Eigenschaften sind die Logmeldungen wertlos, wenn nicht sogar schädlich. Ganz besonders wichtig ist dies bei hochsensiblen Daten, wo sich der Aufwand eines organisierten Angriffes lohnt.

Die Angreifer wissen um die Bedeutung der Logmeldungen und werden versuchen, diese wenn immer möglich zu manipulieren. Damit lassen sich Spuren verwischen, die Aufschlüsse über den Angriff oder den Angreifer zulassen. Bei genügend Systemwissen liesse sich unter Umständen sogar ein Alarm verzögern, wenn nicht sogar verhindern. Um cleveren Spionen oder aufwändigen Social-Engineering-Angriffen, wie sie heute existieren, auf die Spur zu kommen, braucht es vor allem auch Logmeldungen, auf die sich mögliche SIEM oder SOC abstützen können.

Auch im Fall eines erfolgten Angriffs sind verlässliche Logmeldungen entscheidend, um eine forensische Datenanalyse vornehmen zu können. Nehmen wir einmal an, Ihr System wurde attackiert. Sie haben die Attacke festgestellt und werden als Nächstes prüfen, ob sie erfolgreich war und anschliessend das Schadensausmass ausloten. Ob ein Versuch am äusseren Schutzwall abgeprallt ist, nur bis zum inneren Schutzwall gelangte oder gar ohne Ausmass war, hat grundlegend verschiedene Reaktionen zur Folge. Wenn Sie immer von einem grössten anzunehmenden Unfall (GAU) ausgehen, kann der Angreifer mit einem einfachen Angriffsversuch bereits erheblichen Schaden auslösen. Aber ebenso, wenn Sie nur von einem versuchten Angriff ausgehen, der Angreifer jedoch alle geschützten Daten komplett abziehen konnte.

Nicht- oder Falsch-Einschätzung des Angriffs ist mitunter eines der wichtigsten Ziele eines ausgeklügelten Angriffs, wie zum Beispiel von einer staatlichen oder kriminellen Organisation. Hier die datenforensische Analyse auf Logdaten mit höchster Datenintegrität und Vertraulichkeit abzustützen ist massgebend und entscheidet, ob die Analyse im Blindflug startet oder einem roten Faden zur Orientierung folgen kann.

Wir müssen heute davon ausgehen, dass Angreifer über die Schwachstellen bei Standardprodukten besser und frühzeitiger Bescheid wissen als wir Betreiber und Hersteller von Sicherheitselementen. Dadurch sind sie uns einen Schritt voraus. CyOne Security-Geräte bieten hiervor Schutz, da sie sowohl in den CyOne Security-Geräten als auch im Management-System über proprietäre und ausgefeilte Schutz- und Trennmechanismen verfügen.

CyOne Security ist der vertrauenswürdige Partner für sichere IT-Infrastruktur

Aufgrund der zunehmenden Vernetzung und vielfältigen Nutzung von Geräten innerhalb einer Organisation braucht es ein professionelles Log Management, um die Übersicht zu bewahren. Standardisierte Lösungen sind notwendig, um die Interoperabilität im Betrieb und deren Stabilität zu gewährleisten. Security Log Management bedarf erhöhter Zugangs- und Vertraulichkeitskontrolle, um auch im Ernstfall verlässliche Analysen vornehmen zu können.

CyOne Security-Geräte unterstützen deshalb nicht nur Standardtechnologien, wie Syslog und SNMP, um die Interoperabilität mit Drittherstellern zu gewährleisten. CyOne Security entwickelt auch eigene gehärtete Geräte und Management-Lösungen, um höchste Sicherheit und Datenintegrität in neuralgischen Systemkomponenten sicherzustellen. Mit der eigenen Sicherheitsmanagement-Lösung können die Sicherheitselemente geschützt konfiguriert, aber auch die Security-Logdaten sicher und zentral verwaltet werden. Somit wird für Sie als Betreiber ein zentrales und hochsensibles Element mit höchsten Sicherheitsstandards professionell aus einer Hand umgesetzt.

Setzen Sie auf die langjährige Erfahrung und die 360°-Sicherheitskompetenz der CyOne Security. Als rein schweizerisches Unternehmen bieten wir den kundenspezifischen Risiken angepasste, umfassende Sicherheitskonzepte und -lösungen auf höchstem Niveau an; für Product Security, System Security sowie Operational Security.

Beginnen Sie heute, Ihre vertraulichen Daten und Kommunikation zu schützen: mit einem effektiven Security Log Management.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren Cyber Security-Experten Ihre aktuellen und zukünftigen Sicherheitsbedürfnisse und entsprechende Sicherheitslösungen.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.