Sicherheit für KMUs in 5 Teilen

Teil 5: Kosten und erweiterte Vorgehensweise

Kostenplan

Die **Anschaffungskosten** können wegen der Software-Lösung als eine Open-Source SIEM vernachlässigt werden, da keine Lizenzkosten hierfür anfallen.

Hardwarekosten fallen möglicherweise nur bei einer On Premise-Lösung an, falls keine geeignete Hardware im Unternehmen zur Verfügung steht. Hierbei ist zu berücksichtigen, dass das GSG-SIEM System große Datenmengen generiert, die zumindest für eine gewisse Zeit gespeichert werden müssen, teils in performanten SSDs, teils in Standard-Speicher. Nicht zu vernachlässigen bei dieser On Premise Lösung sind die Betriebskosten für Strom, Kühlung, Netzwerk und Personal zur Aufrechterhaltung des Betriebs.

Die **Betriebskosten** einer Private-Cloud Lösung sind in erster Linie von der Daten- und von der Speichermenge abhängig. Die Datenmenge wiederum ist von einer jeweils pro angeschlossenem Gerät unterschiedlichen EPS-Größe (Events per Seconds) abhängig, die Speicherdauer von der Anzahl der für die Nachverfolgung sinnvollen Zeit. Als eine erste Näherung kann der monatliche Kostenrahmen mit einer Größenordnung von 4,60 € pro angeschlossenem Gerät kalkuliert werden. Hierin sind Systemupdates und Service für die Cloud-Infrastruktur entsprechend einem Supportplan enthalten. Eine genaue und transparente Abrechnung erfolgt am Ende eines Monats.

Schulungskosten sind für eine effektive Wissensvermittlung entscheidend um sicherzustellen, dass das IT-Personal des Unternehmens in der Lage ist, das GSG-SIEM-System optimal nutzen zu können. Diese Kosten beinhalten Trainingsmodule, Workshops und möglicherweise Zertifizierungen für Teammitglieder. Ein Schulungstag kann mit 1.500.- € kalkuliert werden, zuzüglich Reisekosten.

Implementierungsplan

Alle nachfolgenden Phasen werden mit dem Unternehmen abgesprochen und z.B. in den angesprochenen Workshops behandelt.

Phase 1
In der Vorbereitungs- und Planungsphase werden zu Beginn detaillierte Sicherheitsbewertungen durchgeführt, um die spezifischen Sicherheitsanforderungen und Ziele des Unternehmens zu definieren. Dazu gehört die Auswahl der zu überwachenden Systeme und Anwendungen.

Phase 2
Die technische Implementierung umfasst die Einrichtung der Serverinfrastruktur, Installation der SIEM-Software und Konfiguration der Datenquellen. Dieser Schritt erfordert technisches Know-how in Netzwerkkonfiguration und Sicherheitsmanagement.

Phase 3
Nach der Erstkonfiguration folgen umfangreiche Tests, um sicherzustellen, dass alle Systemkomponenten korrekt funktionieren und die Daten wie erwartet verarbeitet werden. Basierend auf den Testergebnissen werden Anpassungen zur Optimierung der Leistung vorgenommen.

Phase 4
Abschließend werden alle beteiligten Mitarbeiter in der Nutzung des SIEM-Systems geschult. Nach erfolgreichen Tests und Schulungen wird das System vollständig in Betrieb genommen.

Management und Alarmierung

Das moderne GSG-SIEM nutzt komplexe Algorithmen, um Ereignisse über verschiedene Systeme und Zeitpunkte hinweg zu korrelieren. Diese Fähigkeit ermöglicht es, versteckte Muster und Zusammenhänge zu erkennen, die auf fortgeschrittene Bedrohungen hindeuten könnten.

Das System priorisiert und kategorisiert Alarme basierend auf deren Dringlichkeit und potenziellem Einfluss. Diese Alarme informieren das Sicherheitsteam über mögliche Sicherheitsvorfälle, sodass hierauf schnell reagiert werden kann.

Zusätzlich zur Alarmierung können automatisierte Workflows konfiguriert werden, um auf bestimmte Arten von Sicherheitsvorfällen zu reagieren, z.B. das Isolieren eines Netzwerksegments bei Anzeichen einer Infektion.

Zusätzliche Daten-Nutzung

Durch die Speicherung und Analyse historischer Daten kann das GSG-SIEM wertvolle Einblicke in langfristige Sicherheitstrends bieten und helfen, zukünftige Bedrohungen vorherzusagen. Für diesen Zweck ist die Dauer der Datenhaltung zu entscheiden.

Automatisierte Reporting-Funktionen erleichtern die Erstellung von Berichten für Compliance-Zwecke, was die Auditierung vereinfacht und sicherstellt, dass das Unternehmen den gesetzlichen Anforderungen entspricht.

Die fortlaufende Analyse der von dem GSG-SIEM-System generierten Daten ermöglicht es Sicherheitsteams, ihre Strategien kontinuierlich anzupassen und zu verbessern, um die Sicherheit zu maximieren.