Sicherheit für KMUs in 5 Teilen

Zusammenfassung der 5-teiligen Serie

Teil 1: Risiken und Konsequenzen

Die Serie beginnt mit einer Betrachtung der erheblichen Risiken, denen Unternehmen ohne ein Security Information and Event Management (SIEM)-System ausgesetzt sind. Ohne SIEM bleibt eine Vielzahl von Sicherheitsvorfällen unentdeckt, was zu signifikanten finanziellen und rechtlichen Konsequenzen führen kann. Der erste Teil hebt hervor, wie ein SIEM-System dazu beiträgt, diese Risiken zu minimieren, indem es fortlaufende Überwachung und Echtzeit-Bedrohungserkennung bietet.

Teil 2: Grundlagen und die Bedeutung von Logs

Im zweiten Teil wird erläutert, was SIEM ist und welche Rolle es in der modernen Cybersicherheit spielt. Besonders wird auf die Bedeutung von Log-Daten eingegangen, die eine kritische Ressource für die Überwachung und Analyse von Sicherheitsereignissen darstellen. Dieser Abschnitt betont die Notwendigkeit der Sammlung und Analyse von Log-Daten als Grundlage für effektive Sicherheitsmaßnahmen.

Teil 3: Entscheidungsfindung und Auswahl

Der dritte Teil behandelt den Prozess der Entscheidungsfindung und Auswahl eines SIEM-Systems, das besonders für KMUs geeignet ist. Hervorgehoben werden die Vorteile von kosteneffizienten, benutzerfreundlichen und skalierbaren Open Source-SIEM-Lösungen. Zudem werden wichtige Eigenschaften eines fortschrittlichen SIEM-Systems erörtert, darunter umfassende Datenerfassung, erweiterte Analysefunktionen, Echtzeit-Ereignisüberwachung und -reaktion, Konfigurations- und Compliance-Überwachung, Integration und Skalierbarkeit, sowie ein benutzerfreundliches

Dashboard und Reporting. Besonders betont wird die Bedeutung einer aktiven Community und umfassenden Unterstützung.

Teil 4: Installation des SIEM-Systems – G-SIEM

Dieser vorletzte Teil führt durch den Prozess der Installation und Konfiguration eines SIEM-Systems, hier beispielhaft dargestellt am G-SIEM. Die Schritte von der Vorbereitung über die Installation bis hin zur Feinabstimmung werden detailliert beschrieben, um Unternehmen eine klare Vorstellung davon zu geben, was die Inbetriebnahme eines SIEM-Systems erfordert.

Teil 5: Kosten und erweiterte Vorgehensweise

Der letzte und 5.Teil der SIEM-Serie fokussiert auf die Kosten, die Planung der Implementierung, die Wartung und den Service und das fortlaufende Management mit der Alarmierung des G-SIEM Systems nach der erfolgreich abgeschlossenen Testphase der Implementierung. Dieser Teil beleuchtet die entscheidenden Aspekte, die für die Aufrechterhaltung der Leistungsfähigkeit und Effektivität eines SIEM-Systems in einem Unternehmen erforderlich sind.

Abschließende Worte

Diese Artikelserie bietet KMUs eine umfassende Einführung in die Bedeutung, Implementierung und Nutzung von SIEM-Systemen. Von den initialen Überlegungen zur Auswahl eines Systems bis hin zur technischen Einrichtung und dem operativen Betrieb werden Leser befähigt, informierte Entscheidungen zu treffen, die zur Stärkung ihrer Sicherheitsstellung beitragen. Mit dem Einsatz eines SIEM-Systems können Unternehmen nicht nur ihre Compliance-Anforderungen effektiver managen, sondern auch eine robustere Verteidigung gegen Cyber-Bedrohungen aufbauen und damit die NIS2-Richtlinie in den meisten Punkten erfüllen.

Gerne sind wir bereit Sie zu beraten und für Sie die erforderlichen Schritte zu unternehmen. Kommen Sie auf Ihre GSG, Global Service Group GmbH, zu.

Verantwortlich und direkter Ansprechpartner:
Dr. Frank H. Thiele, ft@gsg-edv.de, 06154 6039 390
GSG Global Service Group GmbH, Im Seesengrund 19, 64372 Ober-Ramstadt
https://gsg-edv.de