Sicherheit für KMUs in 5 Teilen

Teil 1: Risiken und Konsequenzen

Einleitung

Für Klein- und Mittelständige Unternehmen (KMUs) ist die Kenntnis ihrer Assets und deren möglichen Probleme durch das vorhandene Monitoring normalerweise hinreichend bekannt. Ist das Gerät noch in Ordnung, läuft der Dienst noch, dies sind alles Informationen, die zu proaktiven Maßnahmen führen und damit Schäden und Ausfallzeiten für das Unternehmen reduzieren. Jedoch ist hierin das Monitoring des Netzwerkes und der Cyber-Vorfälle nicht integriert.

In unserer zunehmend vernetzten Welt hängt die Sicherheit von Unternehmen immer stärker von fortschrittlichen Sicherheitssystemen ab. Ein wesentliches und derzeitig effizientestes Element in diesem Sicherheitsgefüge ist das Security Information and Event Management (SIEM). Dieser Abschnitt beleuchtet nicht nur die erheblichen Risiken, denen Unternehmen ohne ein solches System ausgesetzt sind, sondern diskutiert auch die tiefgreifenden rechtlichen Konsequenzen, die daraus entstehen können.

Schwachstellen erkennen

Ohne SIEM bleibt eine Vielzahl von Sicherheitsvorfällen von der Entdeckung unbemerkt, was zu gravierenden Schäden führen kann. SIEM-Systeme sind darauf ausgelegt, Anomalien und Bedrohungen in Echtzeit zu erkennen und zu analysieren. Diese Fähigkeit ermöglicht es Unternehmen, proaktiv Maßnahmen zu ergreifen, bevor kleine Sicherheitslücken zu schwerwiegenden Sicherheitsverletzungen eskalieren. Ein gut implementiertes SIEM bietet die Augen und Ohren, die notwendig sind, um die IT-Sicherheitslandschaft rund um die Uhr zu überwachen und zu schützen.

Rechtliche Konsequenzen

Unternehmen sind nicht nur ethisch, sondern auch gesetzlich verpflichtet, angemessene Maßnahmen zum Schutz personenbezogener Daten und zur Sicherstellung der IT-Sicherheit zu treffen. Das Fehlen eines effektiven SIEM-Systems kann bei

Datenschutzverletzungen zu erheblichen Bußgeldern und rechtlichen Konsequenzen führen. Das IT-Sicherheitsgesetz sowie die „Network and Information Security (NIS) Directive“, auch bekannt als NIS 2, fordern ein Umdenken bezüglich des aktuellen Sicherheitsniveaus. Dies gilt insbesondere für Unternehmen, die als Zulieferer oder Partner größerer Unternehmen agieren. Hierbei ist proaktives Handeln nicht nur empfohlen, sondern oft gesetzlich vorgeschrieben.

Fallbeispiele

Beispiel 1: Einzelhandelsunternehmen

Situation: Ein größeres Einzelhandelsunternehmen erlebte einen massiven Datenverlust, der die persönlichen Informationen von Millionen von Kunden freilegte. Dies geschah durch eine Malware-Infektion, die durch eine anfänglich unbemerkte Sicherheitslücke in einem ihrer Zahlungssysteme eingeschleust wurde.

Problem: Das Unternehmen hatte kein SIEM-System implementiert. Die Malware-Aktivität und der Datenabfluss blieben über Monate hinweg unentdeckt, weil keine adäquaten Überwachungssysteme vorhanden waren, die diese Anomalien hätten erkennen und Alarm schlagen können.

Konsequenzen: Nachdem der Vorfall bekannt wurde, litt das Unternehmen unter schweren Reputationsschäden und finanziellen Verlusten durch Rechtsstreitigkeiten und Bußgelder. Der Vorfall führte zu einer Überarbeitung ihrer Sicherheitsstrategie, einschließlich der Implementierung eines SIEM-Systems.

Beispiel 2: Compliance-Verstoß in der Finanzbranche

Situation: Ein mittelgroßes Finanzdienstleistungsunternehmen wurde von einer Regulierungsbehörde wegen Nicht-Einhaltung von Compliance-Anforderungen gerügt. Das Unternehmen konnte nicht nachweisen, dass es über ausreichende Kontrollmechanismen verfügte, um Sicherheitsvorfälle zu erkennen um darauf reagieren zu können.

Problem: Das Unternehmen nutzte ein veraltetes System zur Überwachung seiner Netzwerke, das nicht in der Lage war, die umfangreichen Datenströme effektiv zu analysieren und verdächtige Aktivitäten zu identifizieren.

Konsequenzen: Das Unternehmen musste eine hohe Geldstrafe zahlen und zusätzlich umfangreiche Investitionen in moderne SIEM-Technologien tätigen, um zukünftige Verstöße zu vermeiden und Compliance-Anforderungen zu erfüllen.