rt-solutions.de
experts you can trust.

Gesamtkonzeption einer SIEM-Lösung

Vor wenigen Jahren noch war IT-Security ein Thema, das belächelt wurde. Investitionen wurden nicht getätigt, da IT-Security selten Marktanteile gewinnt oder Kosten einspart. Es wurden nur vereinzelt Sicherheitslücken oder Angriffe auf Unternehmen bekannt. Das hat sich in den letzten Jahren entscheidend gewandelt. Unternehmen werden regelmäßig und zielgerichtet von professionellen Hackern angegriffen. Cyber-Kriminalität und Innentäter haben sich zur ernsthaften Bedrohung für Unternehmen entwickelt.

Compliance-Richtlinien und internationale Standards fordern die Analyse der Log-Dateien, um Security-Incidents zu erkennen und, wie zukünftig von der EU gefordert, diese auch zu melden. Werden Angriffe bereits in den ersten Angriffsphasen erkannt, lässt sich größerer Schaden abwenden. Dazu ist es notwendig, Ereignis-Logs und Netzwerkverkehr miteinander zu korrelieren, um in Echtzeit auf Bedrohungen und Angriffe reagieren zu können.

Um diese Aufgaben bewältigen zu können, werden SIEM-Produkte eingesetzt. Vor dem Einsatz eines SIEM-Produktes benötigt jedes Unternehmen ein Gesamtkonzept, welches die unternehmensspezifischen Anforderungen und Randbedingungen in Einklang bringt mit den vorhandenen Prozessen, Personen und Produktfunktionalitäten. Nur dann kann auch ein SIEM-Produkt optimal und kosteneffizient eingesetzt werden. Ein SIEM-Produkt ist dann Teil einer ganzheitlichen SIEM-Lösung.

Die Gesamtkonzeption liefert als Ergebnis:

1. Einsatzzweck und Anwendungsfälle der SIEM-Lösung inklusive der Sicherheits- und Datenschutzanforderungen.
2. Eine Gesamtarchitektur mit den wesentlichen SIEM-Funktionselementen, zu unterstützenden Quellsystemen und anzubindenden Zielsystemen (z.B. Ticket-, Alerting, Reporting-Systeme).
3. Wesentliche Analyseregeln für Alarme und Warnmeldungen incl. Adressaten sowie notwendige Reports je Anwendungsfall.
4. Beschreibung der Einbindung in die Betriebs- und Unterstützungsprozesse zur Gewährleistung eines effizienten Betriebes sowie einer nachhaltigen Weiterentwicklung des Systems.
5. Beschreibung der Einbindung in das Incident-Management für eine effektive, effiziente und zeitnahe Behandlung von Sicherheitsvorfällen, Bedrohungen und Schwachstellen.
6. Sicherheitsmaßnahmen und Berechtigung zur Sicherstellung von Integrität und Vertraulichkeit der verarbeiteten Daten.
7. Abschätzung der Skalierungsanforderungen aller SIEM-Komponenten
8. Abschätzung des Aufwandes für Implementierung und Betrieb hinsichtlich personeller Ressourcen und Qualifikationen.
9. Gegenüberstellung von Nutzwert und Kosten der SIEM-Lösung
10. Anforderungsliste und Bewertungsmaßstab für einen Produktvergleich der verschiedenen Anbieter am Markt.