softScheck

SIEM – werden Security-Tests überflüssig?

Bedrohungserkennung und -abwehr vs. Security-Testing

Ein Security Information and Event Management (SIEM) System ist ein wertvolles Werkzeug für die Überwachung und Analyse von Sicherheitswarnungen innerhalb einer IT-Umgebung. Ein SIEM-System erfasst und bündelt Log-Daten, ordnet Vorfälle und Ereignisse ein und wertet diese Informationen aus, um potenzielle Sicherheitsbedrohungen zu erkennen. Trotz seiner Nützlichkeit gibt es mehrere Gründe, warum Security-Tests weiterhin eine kritische Rolle für die Cybersicherheit eines Unternehmens spielen.

Zero-Day-Schwachstellen sind Sicherheitslücken in Software und Hardware, die dem Hersteller bisher unbekannt sind und für die es demnach noch keinen verfügbaren Patch gibt. Da sie noch nicht öffentlich bekannt sind, fehlen spezifische Signaturen oder Indikatoren für eine Anomalie, was ihre Erkennung durch traditionelle Sicherheitsmaßnahmen wie SIEM-Systeme erschwert. SIEM-Systeme hängen stark von bekannten Bedrohungssignaturen und -regeln ab, um Sicherheitsvorfälle zu identifizieren. Ohne bekannte Signaturen bleiben Zero-Day-Angriffe daher unbemerkt.

> IT-Sicherheit ist wie ein Schutzschild mit mehreren Lagen: Jede Lage bietet zusätzliche Sicherheit und verstärkt die Verteidigung gegen Angriffe von außen.

Neben Zero-Days gibt es auch andere komplexe Sicherheitslücken, die für ein SIEM schwer zu erkennen sind, insbesondere wenn sie fortschrittliche, persistente Bedrohungen (Advanced Persistent Threats, APTs) darstellen oder in hochkomplexen Netzwerkumgebungen auftreten. Beispiele hierfür sind Schwachstellen, die sich aus spezifischen Konfigurationsfehlern oder aus der Kombination mehrerer an sich nicht kritischer Fehler ergeben. Solche Schwachstellen können durch ein SIEM nur dann erkannt werden, wenn es korrekt konfiguriert ist und fortlaufend aktualisiert wird, um sich an die sich ständig verändernde Bedrohungslandschaft anzupassen. Allerdings kann selbst das beste SIEM-System ohne zusätzliche Sicherheitsmaßnahmen und Prüfungen nicht jede Schwachstelle erkennen, was die Notwendigkeit einer mehrschichtigen Sicherheitsstrategie unterstreicht.

SIEM in Kombination mit Security-Testing

SIEM-Systeme sind primär darauf ausgelegt, bekannte Bedrohungen und Anomalien zu erkennen, indem sie Log-Daten überwachen, analysieren und nach bekannten Mustern und Regeln suchen. Security-Testing hingegen zielt darauf ab, unbekannte Sicherheitslücken, Backdoors und Advanced Persistent Threats (APTs) zu identifizieren. Es wird auch getestet, inwieweit sich ein Angreifer unbemerkt vom SIEM bewegen kann, ohne von Analystenteams entdeckt zu werden. Durch simulierte Angriffe auf das SIEM und den Austausch zwischen Red und Blue Teams können die Korrelationsregeln des SIEM verfeinert und die IT-Sicherheitsmaßnahmen innerhalb des Unternehmensnetzwerks derart gestärkt werden, dass Angreifern, selbst im Falle einer unentdeckten Schwachstelle, kaum Möglichkeiten für weiterführende Angriffe bleiben.

Identifizierung und Behebung von Schwachstellen

Security-Tests identifizieren aktiv Sicherheitslücken, die von Angreifern ausgenutzt werden könnten. Diese Tests gehen über automatisierte Systeme hinaus und nutzen menschliche Kreativität, um Schwachstellen aufzudecken, die herkömmliche Sicherheitstools möglicherweise nicht finden.

Validierung der Sicherheitsmaßnahmen:

Security-Tests prüfen die Wirksamkeit der Sicherheitsrichtlinien und -prozesse eines Unternehmens. Sie zeigen auf, ob die aktuellen Sicherheitsmaßnahmen ausreichend sind, um gegen reale Angriffsszenarien zu schützen.

Simulation realer Angriffsszenarien:

Security-Tests imitieren das Verhalten eines echten Angreifers, einschließlich der Nutzung von Techniken, die darauf abzielen, die Erkennung zu vermeiden. Dies kann zeigen, ob ein SIEM System tatsächlich in der Lage ist, fortschrittliche Angriffe zu erkennen.

Aufdeckung von Schwachstellen in der Konfiguration und im Design:

Selbst wenn ein SIEM richtig konfiguriert ist, können Design- und Konfigurationsfehler die zu Sicherheitslücken führen übersehen werden. Security-Tests helfen, solche Probleme aufzudecken.