5 Lebenszeichen sicherer Netzwerke

Wie ein Arzt bei einem Patienten sollten Sie die Lebenszeichen Ihres Netzwerks überwachen.

Ein Arzt achtet routinemäßig vorrangig auf Körpertemperatur, Puls, Atmung und Blutdruck. Der erste Schritt bei der Diagnose von Krankheiten ist, diese Lebenszeichen auf Änderungen zu überprüfen. Dabei steht oft nicht ihr spezifischer Wert im Vordergrund, sondern dessen Veränderung im Laufe der Zeit bei einem bestimmten Patienten.

Wir haben für Sie die fünf wichtigsten Lebenszeichen von Netzwerken zusammengestellt, die Sie zum Schutz Ihres Unternehmens überwachen sollten.

1: Neue Clients und Server

Anzeichen: In Ihrem Netzwerk wimmelt es vor Servern und Clients – und Unternehmen fügen im Rahmen des regulären Betriebs ständig neue hinzu. Unbekannte Server im Netzwerk und unerwartete Clients, die mit diesen kommunizieren, können jedoch ein Anzeichen für unerwünschte Aktivitäten sein.

Diagnose: Ein neuer, unbekannter Dateiserver in Ihrem Netzwerk kann Anzeichen einer versuchten Datenexfiltration sein. Ein neuer SubSeven/Back Orifice/SVN-Server kann auf eine Hintertür eines Hackers hinweisen. Ein neuer Server könnte für unrechtmäßige Dateifreigaben verwendet werden.

2: Scans

Anzeichen: Ungewöhnliche oder vermehrte Scans im Netzwerk können darauf hinweisen, dass in Ihre Systeme eingedrungen wurden und Sie die Angreifer schnell finden und stoppen müssen.

Diagnose: Scans nach offenen und verfügbaren Diensten sind eine gängige Ausspähtechnik von Hackern, die Ihr Netzwerk infiltriert haben. Computerwürmer nutzen oft willkürliche Scans, um andere verwundbare Systeme zu finden.

3: Verbotene Kommunikation

Anzeichen: Hosts mit bekanntermaßen bösartigen IP-Adressen wie Botnetze oder Kanäle für die Malware-Verteilung.

Diagnose: Kommunikation mit einem bekanntermaßen bösartigen Host kann darauf hinweisen, dass Malware heruntergeladen wird oder dass der Angreifer bereits in das Netzwerk gelangen konnten und die Malware zusätzliche Steuerungen und Exploits etabliert.

4: Volumenbasierte Aktivität

Anzeichen: Ein fortlaufend ungewöhnlicher Zuwachs an Netzwerk-Traffic und -verbindungen kann auf Angriffe wie Amplification, SYN Flood, Smurf/Fraggle, Slow Loris, Christmas Tree, LAND, IP/TCP NULL usw. hinweisen.

Diagnose: Diese Traffic-Muster signalisieren einen potenziell stattfindenden DDoS-Angriff, der Systemausfälle verursachen kann. Sie müssen diese Muster also schnell entdecken, klassifizieren und Probleme ggf. beheben können.

5: Datenexfiltration

Anzeichen: Die Datenübertragung in und aus Ihrem Netzwerk gehört zur Routine. Werden jedoch ungewöhnlich große Datenmengen aus Ihrem Netzwerk heraus übertragen – insbesondere vertrauliche Daten – sollten Sie sofort ermitteln.

Diagnose: Große Datenübertragungen könnten ein Anzeichen für Datendiebstahl sein. Bemerkt ein Unternehmen, dass seit Wochen oder gar Monaten ein Leak vertraulicher Daten besteht, können die finanziellen Konsequenzen und Rufschädigungen verheerend sein.

Das Wichtigste zusammengefasst

Neue Clients und Server, Scans, externe Kommunikationen und Datenübertragungen gehören alle zum Routinebetrieb und weisen nicht notwendigerweise auf ein Problem hin. Änderungen des Umfangs oder Musters dieser Aktivitäten können jedoch Anzeichen für unerwünschtes Verhalten sein. Die Lebenszeichen Ihres Netzwerks sind außerdem ein Frühwarnsystem. Werden sie überwacht, können Probleme schnell erkannt und behoben werden, um das Netzwerk zu schützen.

Für weitere Informationen über das Monitoring der Lebenszeichen Ihres Netzwerks mit Riverbed klicken Sie hier.