IT-Security sichtbar machen

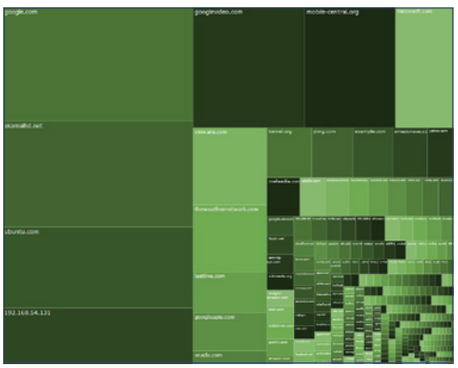
Um den Überblick im Datendschungel der IT-Security nicht zu verlieren, sind integrale Real-Time-Monitoring- und Visualisierungslösungen notwendig. Sie verschaffen dem Management sowie den IT-Security-Verantwortlichen einen transparenten Überblick über das Geschehen im Netzwerk, über Gefahren und notwendige Massnahmen.

UTM-Plattformen, XTM-Appliances, Firewalls mit Application-Control: Moderne IT-Security-Lösungen beinhalten mannigfaltige Abwehr- und Sicherheitsmechanismen, die für eine ganzheitliche IT-Security notwendig sind. Sie konsolidieren Funktionen wie Statefull Inspection Firewall, Malware Detection, Application Control, Web-Filter, Antivirus, Intrusion Prevention, SSL-VPN und Traffic Shaping in einem System.

Was grundsätzlich positiv zu werten ist, hat auch seine Kehrseite. So führt die enorme Funktionsvielfalt der Systeme zu einer erhöhten Komplexität, was sich beispielsweise bei deren Konfiguration sowie bei der Implementierung anspruchsvoller, firmenspezifischer Security-Policies bemerkbar macht. Ebenso herausfordernd ist die schier unbegrenzte Datenmenge (Big Data), die von den Sicherheitsplattformen generiert und gespeichert wird. Sie ist ohne spezifische Hilfsmittel nicht zu bewältigen. Deutlich macht dies ein aktueller Bericht des SANS-Instituts, gemäss dem sich lediglich zehn Prozent der Umfrageteilnehmer in der Lage sehen, ihre grossen Datenmengen hinsichtlich IT-Security zu analysieren und die gewonnenen Erkenntnisse in richtige Entscheidungen umzumünzen.

Vor diesem Hintergrund wird offensichtlich, dass Reporting- und Visualisierungstools notwendig sind, welche die enorme Datenmenge verdichten und das sicherheitsrelevante Geschehen im Netzwerk und am Gateway schnell und verständlich sichtbar machen können. Dabei gilt es, Rohdaten in Echtzeit zu konsolidieren, in einem übersichtlichen Dashboard zu präsentieren und nachvollziehbare, entscheidungsrelevante Berichte zu erstellen – Reports, die auf die unterschiedlichen Bedürfnissen der einzelnen Empfänger zugeschnitten sind.

DER AUTOR
Jürg Hefel,
Product Manager
WatchGuard,
BOLL Engineering
AG, Wettingen



Die Visualisierungs- und Reporting-Lösung WatchGuard Dimension verdichtet sicherheitsrelevante Informationen und macht diese in konsolidierter, verständlicher Form sichtbar.

Visualisierungslösungen sind exakt für dieses Bedürfnis geschaffen. Sie konsolidieren relevante Kennzahlen im Security-Umfeld zu einem «Big Picture» und unterstützen damit die Security-Verantwortlichen beim sofortigen Erkennen sicherheitsbezogener Vorkommnisse und Gefahren. Reports und Real-Time-Monitoring-Dienste veranschaulichen beispielsweise, welche Webseiten und Kategorien von internen Benutzern am meisten aufgerufen und welche Applikationen genutzt werden, ob vertrauliche Daten das Unternehmen unerlaubterweise verlassen, welche kritischen Aktivitäten von internen Benutzern ausgeführt werden, welche Nutzer und Anwendungen besonders viel Bandbreite verbrauchen oder wo konkrete Angriffe stattfinden und aus welchen geografischen Regionen diese stammen. Informationen dieser Art unterstützen Administratoren einerseits bei der Definition zielgerichteter Security-Policies und andererseits bei deren zeitnahen Anpassung an sich verändernde Bedrohungslagen.

Gefahren erkennen und abwehren

Moderne Visualisierungs- und Reporting-Lösungen bilden eine tragende Säule bei der zeitnahen Erkennung und wirksamen Abwehr von Gefahren. Zu den wesentlichen Leistungsmerkmalen entsprechender Plattformen gehören:

Echtzeit-Dashboard und Reports: Security-Dashboard und Reports zur Netzwerkaktivität bündeln relevante Security-Kennzahlen zu einem konsolidierten Gesamtbild (Big Picture) und verschaffen dem Management eine High-Level-Übersicht über alle wichtigen Security-Aspekte. Sie informieren beispielsweise über aktivste Benutzer, Beziehungen zwischen User und Anwendung, aktuelle Bedrohungen im Netzwerk, benötigte Bandbreite einzelner Applikationen, unüblichen Datenverkehr, geblockte Kategorien und Gefahren u.v.m.

Nebst allgemeinen selbsterklärenden Reports auf hoher Ebene stellen innovative Plattformen wie «WatchGuard Dimension» auch detaillierte Reports zur Verfügung, die auf die spezifischen Informationsbedürfnisse unterschiedlicher Zielgruppen (z. B. CEO, Leiter IT-Security, Compliance-Manager) zugeschnitten sind. Die Reports – wie beispielsweise HIPAA- und PCI-Compliance-Reports – werden automatisch generiert und verschickt.

Kacheldiagramme: Moderne Visualisierungs- und Reporting-Tools basieren auf optimierten Formen zur Datenvisualisierung. Besonders wertvoll sind dabei sogenannte Kacheldiagramme, die mit unterschiedlich grossen Flächen (Kacheln) die Aufmerksamkeit der Betrachter auf die eigentlichen «Hotspots» des Geschehens leiten. Dank Kacheln lässt sich schnell erfassen, was wo passiert und wo unmittelbarer Handlungsbedarf besteht.

Kacheldiagramme sind unübersichtlichen, langen Listen weit überlegen und im Vergleich zu Kuchendiagrammen in der Lage, auch kleinste Ereignisse darzustellen. Zudem ermöglichen sie mittels «Drill-down» das Eintauchen auf tiefere Informationsebenen und ermöglichen detaillierte Analysen einzelner Aspekte.

Weltweite Gefahren-Map: Beinhaltet die Visualisierungslösung eine interaktiv konfigurierbare «Global ThreatMap», lassen sich die Bedrohungslagen einzelner Regionen veranschaulichen und aufgrund entsprechender Erkenntnisse geeignete Abwehrmechanismen konfigurieren.

Plattformübergreifende Gesamtsicht: Ist die Visualisierungs- und Reporting-Lösung cloud- und multiplattformfähig, lassen sich sicherheitsrelevante Daten über mehrere Appliances bzw. Standorte und Kunden konsolidieren. Eine Möglichkeit, die für geografisch verteilte Firmen sowie für Managed Security Service Provider gleichermassen interessant ist.