«THE POWER TO CONTROL» – AUF DEM WEG ZUR KONSOLIDIERTEN SICHERHEIT

Neue Angriffsformen, mehrstufige Attacken, gut organisierte Hackergruppen, eine Vielzahl verletzlicher Systeme ... Klassische Firewalls reichen nicht mehr aus, um eine Rundum-Sicherheit für die IT zu gewährleisten. Benötigt wird vielmehr ein übergreifender Ansatz mit integralen Konfigurations-, Analyse- und Kontrollfunktionen.

Die Next Generation UTM Appliances von Fortinet bilden die zentrale Instanz zur Gewährung einer umfassenden IT-Security.

IT-Security-Verantwortliche sind mit stetig komplexer werdenden Rahmenbedingungen konfrontiert, mit einer Vielfalt an Systemen, Technologien und Applikationen, die allesamt gesichert werden müssen. Es reicht nicht aus, einen wirksamen Perimeter-Schutz zu etablieren, wenn gleichzeitig Web-Shops, WLAN-Infrastrukturen, Mail-Systeme oder Datenbanken ungeschützt bleiben.
Ein wichtiger sicherheitsrelevanter Faktor ist die zunehmende Verletzlichkeit der Firmen bzw. deren Abhängigkeit von funktionierenden, stets verfügbaren Systemen, Daten und Applikationen. Dies verschafft Themen wie Patch Management und Vulnerability Scans besondere Bedeutung. Beachtenswert ist zudem der Trend hin zur Einbindung privater mobiler Devices ins Firmennetz (BOYD). Diese Entwicklung bringt statische Security-Policies an ihre Grenzen. Technologien wie Benutzer- und Geräte-Authentifizierung, IPSEC und SSL VPN, Datenverschlüsselung, Device-Härtung, Verschleierung, Konformitätsüberprüfung etc. sind ein Muss.

Grosse Herausforderungen an die IT-Security stellen ferner die vermehrte Nutzung von Virtualisierungs-Technologien und Cloud-basierten Diensten sowie die rasante Zunahme von Web-2.0-Anwendungen. Diese sind verbunden mit neuen Schwachstellen, zusätzlichen Angriffszielen sowie mit neuen Formen der Bedrohung. User, Systeme und Programme lassen sich nicht mehr klar definierten IP-Adressen oder TCP-Ports zuordnen. Folglich reichen für deren Kontrolle konventionelle Technologien wie Paketfilter, Content Filter oder IDS/IPS alleine nicht mehr aus.

UMFASSENDE IT-SECURITY DANK INTEGRALEM ANSATZ

Faktoren dieser Art führen dazu, dass konventionelle Firewalls nicht in der Lage sind, eine umfassende Sicherheit zu gewährleisten. Benötigt wird vielmehr ein übergreifender, konsolidierter Ansatz mit integralen Konfigurations-, Analyse- und Kontrollfunktionen. Geradezu wegweisend in diesem Bereich sind die Next Generation UTM Appliances von Fortinet. Sie verschaffen den für die IT-Security zuständigen Personen einen stets aktuellen Überblick über das aktuelle Gefährdungspotenzial und bilden eine leistungsfähige Plattform zur Durchsetzung firmenweiter Security Policies. Zu den wichtigsten Leistungsmerkmalen zählen:

Kontrolle von Usern, Applikationen, Devices
Die granulare Definition, welche Applikationen – oder Teile davon – wann und für wen zugelassen oder gesperrt sind (User based Policy Enforcement), ermöglicht die Umsetzung von Sicherheits-Policies auf User-, Device- und Applikationsebene. Dadurch ist es beispielsweise möglich, HTTPS firmenweit freizugeben, hingegen Online-Browser-Spiele zu blockieren und die Freigabe von Social-Media-Applikationen zeitabhängig zu steuern.

Blockieren von Schadcode und Angriffen
Die Next Generation UTM Appliances von Fortinet mit integrierter «Application Control» sind in der Lage, den gesamten Datenverkehr beziehungsweise User, Devices und Applikationen in Echtzeit zu überwachen, zu visualisieren und – wenn nötig – auf Basis der definierten Security-Policies und stets aktualisierter Signaturen aktiv ins Geschehen einzugreifen. Selbst verschlüsselter Code, der über Protokolle wie HTTPS, POP3S, SMTPS und IMAPS transportiert wird, kann analysiert werden.

Minimale Latenz, maximale Verfügbarkeit
Sicherheitsmassnahmen sind ressourcenintensiv und müssen in Echtzeit und ohne spürbare Beeinträchtigung der System- und Netzwerkleistung zur Verfügung stehen. Vor diesem Hintergrund setzt Fortinet auf eine Kombination aus selbst entwickelter Hochleistungs-Hardware, speziellen Prozessoren und Beschleunigungs-Chips. Dadurch werden spezifische Security-Aufgaben wie IPS, AV-Inspection, SSL-Entschlüsselung oder User- und Application-Control in einer dedizierten Umgebung parallel ausgeführt und beschleunigt.