

PRESSEINFORMATION

Aschheim-Dornach, 20. Mai 2009

Neues Betriebssystem für UTM Appliances setzt Standards

WatchGuard stellt Fireware XTM OS vor

Der Netzwerksicherheitsspezialist WatchGuard Technologies hat jetzt ein neues Betriebssystem für seine Sicherheitslösungen vorgestellt. Die Fireware XTM erweitert die Möglichkeiten der Unified Threat Management (UTM)-Appliances um eine Vielzahl neuer Sicherheitsmerkmale sowie Netzwerk- und Management-Funktionalitäten. So bietet das neue Betriebssystem die vollständige HTTPS-Prüfung und Sicherheit für VoIP, Instant Messaging und Peer-to-Peer Applikationen. Im Netzwerkumfeld eröffnet die Fireware XTM Potenziale wie Clustering oder Load-Balancing. Die Administration wird um die Möglichkeit zur rollenbasierten Zugangskontrolle (Role-based Access Control, RBAC), zentrales Multi-Box Management und erweiterte Reporting-Funktionen ergänzt. „Diese Kombination macht die Fireware XTM zu unserem stärksten Betriebssystem. Sie wird den ständig wachsenden Bedrohungen im heutigen, dynamischen Geschäftsumfeld gerecht und gibt den Anwendern die Chance, ihre Sicherheitsanforderungen bedarfsgerecht zu erfüllen“, so Eric Aarrestad, Vize-Präsident Marketing bei WatchGuard.

Erweiterte Sicherheitsfunktionen für Unternehmen

HTTPS-Verbindungen werden hauptsächlich für den Online-Zahlungsverkehr verwendet oder für die Transaktion sensibler Daten in Firmennetzwerken. Da diese Übertragungen verschlüsselt sind, können Administratoren sie nicht kontrollieren. Sie werden deshalb zum Ziel für Sicherheitsangriffe wie beispielsweise Hijacking von HTTPS-Cookies. Dank der Proxy-Technologie von WatchGuard's neuer Fireware XTM können HTTPS-Datenströme abgefangen, gescannt und wieder zusammengebaut werden. Netzwerkadministratoren können so sicherstellen, dass kein Nutzer gefährliche Dateitypen erhält.

Mit einem Wachstum von 20,1 Prozent verbreitet sich die VoIP-Technologie rasant und wird damit auch zum Angriffspunkt in Unternehmensnetzwerken. DoS-Attacken, Directory Harvesting und Voice-Phishing („Vishing“) gewinnen an Popularität. Im Gegensatz zu anderen UTM-Lösungen bietet die Fireware XTM zum Schutz eine Übersetzung von Netzwerkadressen für SIP und H.323 Protokolle. So werden VoIP-Systeme gegen Logging-Angriffe wie Buffer Overflows geschützt.



Auch Botnetze gehören heute zu den wesentlichen Sicherheitsbedrohungen. Sie nutzen dieselben Protokolle wie seriösen Geschäftsapplikationen. Instant Messaging bildet eine besondere Schwachstelle, doch das neue Betriebssystem von WatchGuard schützt auch diese Anwendungen. Neben der Prüfung der Applikation werden Ports und Protokolle identifiziert und validiert. Darüber hinaus arbeitet das P2P-Blocking Hand in Hand mit der HTTPS-Bestimmung und identifiziert so auch verschlüsselte Botnetze.

Fireware XTM: Netzwerksicherheit und leichteres Management

Unternehmensnetzwerke müssen heute ständige Verfügbarkeit und hohen Datendurchsatz gewährleisten. Fireware XTM ermöglicht dies durch vollständiges Appliance-Clustering. Dank des neuen Betriebssystems können Administratoren die UTM-Lösungen auf flexible Weise nutzen: Unterstützt wird beispielsweise die HTTP-Weiterleitung zur Entlastung des Cache von Proxy Servern oder die Mehrfachnutzung von VPN-Tunneln. Darüber hinaus sichert die Fireware XTM VPN-Verbindungen auch auf Reisen zwischen zwei Zugangspunkten.

Das neue Betriebssystem erlaubt Administratoren ein Management ihrer UTM-Appliance nach den eigenen Bedürfnissen. Zum einen stehen dafür verschiedene Oberflächen und Eingabeoptionen bereit. Zum anderen kann der Zugriff dank RBAC sicher gestaltet werden. Auch zur Erfüllung von Standardisierungs- und Automatisierungsanforderungen trägt die Fireware XTM bei. Durch erweiterte Reports und neue Filtermöglichkeiten behalten Administratoren ihre Systeme im Blick und können benötigte Informationen rasch aufrufen.

Die Fireware XTM steht für WatchGuard LiveSecurity-Kunden zum Gratis-Download zur Verfügung. Das Betriebssystem läuft auf allen „e-Series“-Modellen der WatchGuard-Produktfamilien Edge, Core und Peak. Weitere Informationen unter <http://www.watchguard.com/products/fireware-xtm.asp>.

Weitere Informationen:

WatchGuard Technologies GmbH

Michael Haas – Regional Sales Manager

IOM Business Center, Max-Planck-Str. 4 – 85609 Aschheim-Dornach

Tel.: +49 6151 60 95 05 – Fax +49 6151 60 95 05

michael.haas@watchguard.com – www.watchguard.de

Presse- und Öffentlichkeitsarbeit:

Press'n'Relations GmbH

Anne Zozo

Magirusstr. 33 – 89077 Ulm

Tel.: +49 731 962 87 18 – Fax: +49 731 962 87 97

az@press-n-relations.de – www.press-n-relations.de

Über WatchGuard Technologies

Seit 1996 entwickelt WatchGuard preisgekrönte XTM (Extensible Threat Management)-Lösungen für den umfassenden Netzwerkschutz kleiner und mittlerer Unternehmen (KMUs). Die aus Firewall, VPN und Sicherheitsdiensten bestehenden Produkte sind je nach Kundenanforderung in vielen Skalierungen und Preisklassen erhältlich. Mit Hilfe seines Händlernetzwerks aus über 7000 Partnern in 20 Ländern weltweit hat WatchGuard bereits mehr als eine halbe Million seiner markanten roten Security-Appliances an Kunden verschiedenster Branchen verkauft – darunter Gesundheitswesen, Bildung und Einzelhandel. Das in Privatbesitz befindliche Unternehmen hat seinen Hauptsitz in Seattle im US-Bundesstaat Washington und unterhält Niederlassungen in Nord- und Südamerika, Europa sowie im Raum Asien-Pazifik. <http://www.watchguard.com/international/de/corporate/>