22.05.2015 – 18:34 Uhr

Huawei stellt beim Huawei Network Congress 2015 die Advanced Persistent Threat Big Data Security Solution vor

-- Die zentralen Informationsbestände von Unternehmen vor fortgeschrittener, andauernder Bedrohung über Cloud, Pipe und Geräte schützen

Peking (ots/PRNewswire) - Huawei hat beim Huawei Network Congress (HNC) 2015 seine Sicherheitslösung mittels großer Datenmengen gegen fortgeschrittene, andauernde Bedrohung, Advanced Persistent Threat (APT) Big Data Security Solution, vorgestellt. Die Lösung schützt die zentralen Informationsbestände von Unternehmen vor APT-Angriffen durch komplett zusammenhängenden Netzwerkschutz für Cloud, Pipe und Geräte. Die Lösung nutzt die FireHunter-Serie der Sandbox-Sicherheitsprodukte von Huawei, Cybersecurity Intelligent System (CIS) und die USG6000V-Serie von Software-Firewallprodukten. Huawei kündigte zudem Pläne an, eine Cloud Clean Alliance (CCA) zu gründen, um weltweit in Echtzeit Reinigungsleistungen für Denial-of-Service (DDoS)-Angriffe anzubieten und schützt die Bandbreitenverfügbarkeit von Links und die Unterbrechungsfreiheit von Rechenzentrumsdiensten.

"Während die Entwicklung des Internet der Dinge (IoT) das Leben bequemer macht, vergrößert sie auch die Bedrohungen für die Netzwerksicherheit", sagte Liu Lizhu, General Manager der Produktlinie Network Security, Switch and Enterprise Communications bei Huawei. "Aufgrund fehlender Verschlüsselungspraktiken bei Authentifizierung und Übertragung haben 70% der IoT-Geräte Sicherheitslücken. Dadurch können sich potenziell Sicherheitsvorfälle ergeben, die sich in jedem Winkel unseres Lebens ausbreiten. Der Einsatz von IoT erhöht jedoch in großem Maße die Anzahl von Zielen für Angriffe auf die Sicherheit. Dadurch werden IoT-Geräte zum Sprungbrett für APT-Angriffe und ein Ziel von Botnetz-Attacken."

Vor diesem Hintergrund demonstriert Huawei seinen Einsatz für den Schutz gegen APT- und DDoS-Angriffe mit der Herausgabe der APT Big Data Security Solution, die die präzise Erkennung und Abwendung von APT-Angriffen ermöglicht.

FireHunter Sandbox-Sicherheitsprodukte von Huawei

Die neue FireHunter-Serie von Sandbox-Sicherheitsprodukten von Huawei wird auf der RSA Conference 2015 herausgebracht und ist darauf ausgelegt, APT-Angriffe mit fortgeschrittener Malware zu erkennen und davor zu schützen, dass diese Angriffe ins Unternehmensnetzwerk vordringen. Ausgestattet mit einem Reputationssystem und mehrschichtiger Kontrolltechnologie können die FireHunter Sicherheits-Sandboxen mehr als 180.000 Dateien täglich überprüfen. Damit erreichen sie die 1,5-fache Kontrollgeschwindigkeit von anderen, derzeit erhältlichen Produkten, was der branchenweit höchsten Geschwindigkeit entspricht. Es handelt sich um das einzige Produkt seiner Art in China und um eins von dreien weltweit, das eine Zero-Day-Schwachstellenerkennung für Internetseiten unterstützt. So wurden beispielsweise in einem Projekt, das die Sicherheits-Sandbox von Huawei einsetzte, erfolgreich 230 unbekannte Bedrohung innerhalb von zwei Monaten entdeckt. 72 davon war man niemals zuvor in der Branche begegnet.

Cyber-security Intelligent System

Das CIS-System von Huawei bietet Unternehmensnetzwerken frühzeitige Warnung und Schutz vor APT-Angriffen. "APT-Angriffe geschehen sehr heimlich und entgehen häufig der Sicherheitserkennung. Indem sie sich in normalen Netzwerkzugängen verstecken, können APT-Angriffe nach erfolgreichem Eindringen für lange Zeit unentdeckt bleiben. Während der Inkubationszeit verbreitet sich die APT-Angriffsmalware weiter, bis sie erfolgreich relevante Informationen gestohlen hat", so Liu Lizhu weiter.

Basierend auf einer Plattform für große Datenmengen führt das CIS-System umfangreiche Korrelationsanalysen von Massendaten durch, so etwa des relevanten Datenverkehrs, von Protokollen, Kontexten und externen Informationen. Auf diese Weise werden mehr als 350 Arten von verdächtigem Verhalten aufgedeckt, was mehr als doppelt so viel ist wie im Branchendurchschnitt. Das System markiert anschließend die befallenen Ziele rechtzeitig, um ein weiteres Eindringen der APT-Angriffe zu verhindern. Außerdem spürt es schnell und präzise den Ursprung auf und blockiert und entfernt die APT-Angriffe, die während des Prozesses entdeckt wurden.

USG6000V-Software-Firewall-Serie von Huawei

Zusätzlich zu Hardware-Sicherheitsgeräten kann die APT Big Data Security Solution von Huawei Sicherheitsbedrohungen in Cloud, Pipe und Geräten blockieren und entfernen, indem sie virtualisierte, plattformübergreifende Software-Firewalls nutzt. Die USG6000V-Software-Firewall-Serie von Huawei kann je nach Serviceanfragen flexibel auf agilen Switches und agilen Routern eingesetzt werden und bietet sämtlichen Geräteelementen des Netzwerkes Sicherheit. USG6000V von Huawei ermöglicht universelle Netzwerksicherheit, indem seine umfassenden Sicherheitsfunktionen mit einem Agile Controller oder anderen, softwaredefinierten Netzwerkcontrollern (SDN) eingebunden werden. Durch die Annahme des neuesten Data Plane Development Kit (DPDK) von Intel, die Nutzung von Single-Root-I/O-Virtualisierungstechnologie (SR-IOV) und eine HyperScan Software-Musterabgleichsmaschine kann jede USG6000V-Software-Firewall von Huawei bis zu 40 GBit/s Leistung erbringen, das Fünffache des Branchendurchschnitts.

Cloud Clean Alliance

Huawei hat bei der HNC 2015 angekündigt, Partnerschaften mit Unternehmen wie China Telecom und Qingsong Technology einzugehen, um die Cloud Clean Alliance zu begründen. Die Allianz zielt darauf ab, eine Service-on-Chip (SoC)-Plattform basiert auf einer Cloud für große Datenmengen einzurichten, um die Anti-DDoS-Ressourcen von Telekommunikationsbetreibern und Internet-Datenzentren (IDCs) von großer und mittlerer Größe weltweit zu vereinigen und somit Analysen und Antworten auf DDoS-Angriffe in Echtzeit bieten. Nach ihrer Gründung wird die Cloud Clean Alliance einen umfassenden, weltweiten DDoS-Traffic-Reinigungsdienst bieten, der Endnutzern, Partnern und Huawei Nutzen bringt.

Während zunehmend mehr Einzelpersonen, Unternehmen, Organisationen und Institutionen in die vernetztere Welt eintreten, ist eine sichere Netzwerkumgebung fundamental für Unternehmen, um agilere Geschäftsformen zu entwickeln. "Sicherheitsanwendungen müssen flexible Einsatzmöglichkeiten haben, die die Umsetzung von verschiedenartigeren Geschäftsmodellen von Unternehmen unterstützen", sagte Liu Lizhu. Die APT Big Data Security Solution von Huawei und die Cloud Clean Alliance werden Kunden dabei unterstützen, eine sauberere und sicherere Netzwerkumgebung aufzubauen, um agile Geschäftsformen zu ermöglichen.

###

Informationen zu Huawei

Huawei ist ein führender weltweiter Anbieter von Lösungen für die Informations- und Kommunikationstechnologie (IKT). Unser Ziel ist es, durch eine besser vernetzte Welt das Leben zu bereichern und Effizienz zu steigern. Wir agieren als verantwortliches Unternehmen, ermöglichen Innovationen für die Informationsgesellschaft und leisten einen gemeinschaftlichen Beitrag in der Branche. Angetrieben von kundenzentrierter Innovation und offenen Partnerschaften hat Huawei ein Portfolio von durchgehenden IKT-Lösungen zusammengestellt, das den Kunden Wettbewerbsvorteile für Telekommunikations- und Unternehmensnetzwerke, Geräte und Cloud Computing verschafft. Webseite: www.huawei.com [http://www.huawei.com/]

Web site: http://www.huawei.com/

Kontakt:

KONTAKT: Jason Ding, +86-10-8288-2876, Dingwenjie@huawei.com

Diese Meldung kann unter https://www.presseportal.ch/de/pm/100053057/100773037 abgerufen werden.