



Security Heartbeat: Jetzt sprechen Firewall und Endpoints miteinander

Bahnbrechende IT-Sicherheitstechnologie realisiert erstmals Synchronized Security – mit der neuen Sophos XG Firewall als Plattform

Wiesbaden, 9. November 2015. [Sophos](#), führender Anbieter von IT-Sicherheitslösungen für Endpoint und Netzwerk, hat heute den ersten Synchronized-Security-Schutz gegen die immer raffinierteren Cyberattacken vorgestellt. Plattform dafür ist die neue Next Generation Firewall „Sophos XG Series“, die den Sophos Security Heartbeat™ als zentrales Kommunikationselement einführt. Diese Technologie sorgt für eine direkte Verbindung zwischen Next Generation Firewalls mit Endpoint-Sicherheitslösungen der nächsten Generation. Die Systeme teilen also ihr Wissen und ermöglichen eine bedeutend schnellere Aufdeckung von Attacken, die automatische Isolation infizierter Geräte sowie eine schnellere Behebung des Problems. Auf diese Weise ermöglicht Security Heartbeat Unternehmen und Organisationen jeder Größenordnung, ihre Abwehrketten gegen die zunehmend versierten Attacken zu stärken – und das mit wesentlich weniger Zeit- und Mitarbeiteraufwand, als bislang zur Untersuchung und Lösung von Sicherheitsvorfällen notwendig war.

Der Sophos Security Heartbeat pulsiert ständig im System und übermittelt zwischen Endpoints und der Firewall Informationen über verdächtiges Verhalten einzelner Geräte oder bösartige Attacken in Echtzeit. Indem diese traditionell bislang getrennten Produkte nun die Möglichkeit bekommen, direkt miteinander zu kommunizieren, kann Security Heartbeat eine sofortige Aktion einleiten, um einen Malwareausbruch oder Datendiebstahl zu unterbinden. Dabei nutzt die Sophos XG Firewall Daten von Sophos Endpoint Protection, um Geräte zu isolieren oder Zugriffsrechte einzuschränken, während die Endpoint-Lösung sich darum kümmert, den potentiell entstandenen Schaden zu beheben. Auf diese Weise können IT-Verantwortliche von den Möglichkeiten der Advanced Threat Protection profitieren, ohne zusätzliche Agenten, komplexe Management-, Logging- oder Analysetools anschaffen zu müssen. Security Heartbeat ist als Teil der Sophos XG Firewall und in mit Sophos Cloud gemanagten Endpoint-Protection-Lösungen automatisch integriert und sofort einsatzbereit.

“Mit dem heutigen Tag hat Sophos den nächsten, großen Schritt in Sachen Next Generation IT-Security gemacht. Unternehmen jeglicher Größenordnung benötigen Sicherheit sowohl für Endgeräte als auch das Netzwerk – es sind zwei Grundfesten jeder IT-Sicherheitsstrategie. Allerdings haben diese Lösungen zu lange nicht miteinander geredet, sie arbeiteten als isolierte Silos und waren dadurch häufig ineffektiv und nicht komfortabel in der Verwaltung“, so Sophos-CEO Kris Hagerman. „Sophos ist nun der einzige Anbieter, der marktführende Netzwerk- und Endpoint-Sicherheitslösungen mit einer koordinierten Technologie verbindet. Wir nennen das Synchronized Security.“

Christian Christiansen, Vice President of Security Products beim Marktforscher IDC: „Kein anderes Unternehmen ist momentan in der Lage, diese Art von synchronisierter und integrierter Kommunikation zwischen Endpoint- und Netzwerk-Security-Produkten zu bieten. Die daraus resultierenden Zeit- und Ressourceneinsparungen sind gerade für den KMU-Bereich sehr attraktiv; ebenso wie die Möglichkeit, den immer ausgeklügelteren Cyberangriffen Paroli bieten zu können.“

Wie funktioniert der Security Heartbeat™?

- Wenn ein neues, von Sophos geschütztes Endgerät dem Netzwerk zugefügt wird, verbindet sich sein Security Heartbeat automatisch mit der lokalen Sophos XG Firewall und kommuniziert den Sicherheitsstatus dieses Geräts.
- Sobald die Firewall verdächtigen Datenverkehr registriert oder ein Malwarebefall auf dem Endpoint festgestellt wird, übermittelt der Security Heartbeat diese Information in Echtzeit über eine gesicherte Verbindung.
- In den Report fließen alle wichtigen Details wie Computername, Username und Prozessinformationen in Zusammenhang mit der Bedrohung ein.
- Die Firewall ist in der Lage, das befallene Endgerät automatisch von jeglichen gerouteten oder Remote-Netzwerken zu isolieren, sowie zusätzliche Maßnahmen auf dem Endgerät einzuleiten, um das Risiko zu minimieren und Datenverlust vorzubeugen.
- Nachdem die Gefahr gebannt ist, kommuniziert das Endgerät via Security Heartbeat seinen aktualisierten, positiven Sicherheitsstatus an das Netzwerk, das in Folge den „normalen“ Service für diesen Endpoint wieder aktiviert.

Jon Oltsik, Senior Analyst beim Marktforscher ESG: „Dieser Launch ist ein großer Schritt in Richtung synchronisierter Sicherheitslösungen. Nachdem ich die Sophos XG Firewall zusammen mit einem von Sophos geschützten Endpoint in Aktion gesehen habe, steht für mich fest, dass der Security Heartbeat das Risiko für Unternehmen erheblich reduzieren kann, in dem er die Entdeckung und Einleitung entsprechenden Aktionen stark beschleunigt. Es ist eben nicht nur eine Integration des Management-Interfaces, sondern der Austausch valider Daten zwischen zwei Produkten. Gerade Unternehmen, die sich keine eigenen, großen IT-Sicherheitsteams leisten können, hilft dieser Ansatz, um die Produktivität zu erhöhen und gleichzeitig IT-Sicherheitsaufgaben effektiv zu gestalten.“

Die neuen Features der Sophos XG Firewall:

Basierend auf Sophos' marktführenden UTM- und Next-Generation-Firewall-Lösungen vereint die neue Sophos XG Firewall bewährte Technologien von Sophos und Cyberoam und bietet folgende Features:

- **Network Security Control Center.** Das innovative Interface verschafft einen sofortigen Überblick über den Netzwerk-Status sowie potenzielle Gefahren und ermöglicht schnelle Entscheidungen.
- **Einheitliches Policy-Modell.** Das vereinfachte Policy-Management mit vorkonfigurierten Templates für Business Apps macht die Konfiguration so einfach wie nie.
- **User- und App-Risikoanalyse.** Ein sogenannter App Risk Score hilft dabei, gefährdete Nutzer oder Anwendungen, sowie potenzielle Security Hotspots auszumachen.

- **User Threat Quotient.** IT-Admins können nutzerbasierte Policies erstellen, die auf dem individuellen Verhalten und dem Sicherheitsstatus des betroffenen Computers oder Mobilgeräts basieren.
- **Sophos Firewall Manager.** Das zentrale und umfangreiche Managementtool für mehrere Firewalls ist für Sophos Partner und MSPs kostenlos.
- **Zentralisiertes Cloud Management.** Sophos-Partner und MSPs können mehrere Sophos XG Firewall Installationen in der Cloud managen, indem sie den Sophos Cloud Firewall Manager nutzen.
- **Security Heartbeat.** Diese einzigartige Technologie verbindet Firewall und Endpoint auf intelligente Weise und ermöglicht so den Informationsaustausch, sowie verbesserten Schutz vor modernen Bedrohungen.
- **Verschiedenste Appliance-Größen.** Die umfassende Appliance-Reihe reicht vom neuen Einstiegsmodell XG 85(w) bis zum High-End-Modell XG 750.
- **Flexible Hardware.** Das Betriebssystem der Sophos XG Firewall läuft auch auf Sophos SG Appliances und Cyberoam NG Appliances.
- **Flexible Bereitstellung.** Kunden können die XG Firewall als Hardware, Software oder Virtual Appliance ordern – alle Features sind bei jeder Bereitstellungsart verfügbar.

Über Sophos

Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos' Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.

Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos

Jörg Schindler, PR Manager CEEMEA

joerg.schindler@sophos.com, +49-721-25516-263

TC Communications

Arno Lücht, +49-8081-954619

Thilo Christ, +49-8081-954617

Christiane Capps, +49-174-3335550

Ulrike Masztalerz, +49-30-55248198

sophos@tc-communications.de