Neue Strategien für Netzwerk- und Endpoint-IT-Sicherheit

Schutzstatus erhöhen, Komplexität senken und Automatisierungsgrad erhöhen

Wiesbaden, 11. November 2016 – In vielen Unternehmen hat die IT-Security heute eine hohe Priorität und es wird versucht, das Netz und die Daten mit Hilfe unterschiedlicher Security-Tools vor den Aktivitäten von Hackern und Cyber-Kriminellen zu schützen. Doch die Silo-orientierten Ansätze aus der Vergangenheit zeigen heute deutliche Nachteile: die Security benötigt viel Administrationszeit, Reaktionszeiten im Falle eine Angriffs sind zu lange und die Sicherheit hält mit den Entwicklungen der Angreifer nicht Schritt. Gemeinsam mit dem internationalen Marktforschungsunternehmen IDC hat Sophos auf Basis von aktuellen Umfrageergebnissen die fünf wichtigsten Anforderungen an die IT-Security identifiziert. Mit einer Drei-Punkte-Strategie können Unternehmen diese wieder in den Griff bekommen und ihr Sicherheitslevel der Bedrohungslage anpassen.

IT-Sicherheit ist häufig zu komplex

In der Umfrage von Sophos und IDC gaben 48 Prozent der Befragten Unternehmen an, dass die Konfiguration und das Management die wichtigsten Faktoren für die Komplexität der Sicherheitsumgebung sind. Das zweite große Manko ist die hierfür erforderliche Expertise. 37 Prozent gaben an, dass für die vielen benötigten Security-Systeme zu viel spezifische Fachkenntnisse erforderlich sind. Der Silo-orientierte Ansatz aus der Vergangenheit wurde von nahezu einem Viertel der Befragten als Grund für die hohe Komplexität genannt.

Ungenügender Wissensstand

Um vor Gefahren durch Hacker und Angreifer aus dem Internet sicher zu sein, muss der Sicherheitsstatus im Unternehmen jederzeit messbar sein. 79 Prozent der befragten Unternehmen können dazu jedoch keine definitive Aussage treffen. Um die Sicherheit im Unternehmen zu steigern, sehen 55 Prozent der Befragten die Notwendigkeit, dass die einzelnen Security-Tools vernetzt miteinander kommunizieren.

Fünf Dinge, die eine IT-Sicherheitslösung können muss

1. Schnelle und zielgenaue Reaktion bei Störfällen
2. Hohe Real-Time Erkennung
3. Hoch automatisierte Schadensbeseitigung
4. Integrierter Security-Ansatz
5. Übergreifendes Reporting

Ganz gleich wie groß oder verzweigt ein Unternehmen ist – das Wichtigste für Security-Lösungen ist eine schnelle und zielgenaue Reaktion bei Störfällen. Diese kann aber nur dann erfolgen, wenn das System eine hohe Real-Time-Erkennung mit einer möglichst hoch automatisierten Schadenbeseitigung bietet. Hierfür wird ein

integrierter Security-Ansatz benötigt, bei dem alle Instanzen und Komponenten intelligent miteinander kommunizieren, um mögliche Angriffe schneller zu erkennen und abzuwehren. Selbstverständlich müssen nicht nur IT-Administratoren, sondern im Sinne der Compliance und Risikobewertung auch das Management genau wissen, wie sicher das Unternehmen ist und welche Gefahren abgewendet werden. Dafür ist einerseits ein detailliertes und übergreifendes Reporting für IT-Administratoren wichtig, andererseits aber auch der Business-orientierte Ansatz, der dem Management eine klare Aussage über den aktuellen Sicherheitsstatus gibt.

„IT-Security lag bisher hauptsächlich im Verantwortungsbereich der IT und wird nun immer mehr zum Management-Thema in Unternehmen. Aber egal auf welcher Ebene: alle Beteiligten brauchen die Gewissheit, dass das Unternehmen optimal geschützt ist und ein Schaden durch Angriffe weitestgehend ausgeschlossen ist“, erklärt Michael Veit, Sicherheitsexperte bei Sophos. „Möglich ist dieses heute durch eine intelligente und vernetzte Security, die den raffinierten Angriffen gewachsen ist.“

Drei Empfehlungen zur Steigerung der IT-Security
Die Security ist an einem Wendepunkt angelangt und muss neu gedacht werden. Die bisherigen Schutzsysteme sind den immer raffinierteren Angriffsmethoden nicht mehr gewachsen. Darüber hinaus ist eine hohe Automatisierung der Security wichtig, um auf die vielschichtigen Angriffe schnell genug und vor allem mit den richtigen Aktionen zu reagieren. Auch ist eine immer komplexer werdende und zeitintensive Administration der IT-Security nicht zielführend. Innovative Konzepte und Technologien wie die Cloud-basierte Security helfen dabei, die Sicherheit für das Unternehmen im Griff zu haben.

Eine Infografik von IDC und Sophos steht zum Download bereit unter:
http://www.tc-communications.de/presse_lounge/sophos.html

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