Cisco und IBM bündeln Kräfte im Kampf gegen Cyberkriminalität

Die beiden großen Player im IT-Sicherheitsmarkt beabsichtigen, die Effizienz von IT-Security für Kunden zu verbessern durch Technologieintegration, kombinierte Services und Zusammenarbeit bei Threat Intelligence

New York, NY, USA - 31 Mai 2017: Cisco und IBM Security haben heute bekannt gegeben, dass sie zusammenarbeiten, um der wachsenden globale Bedrohung durch Cyberkriminalität zu begegnen. In dieser neuen Partnerschaft werden Cisco und IBM Security eng zum Nutzen von Kunden zusammenarbeiten - über Produkte, Dienstleistungen und den Bereich der Sicherheitsforschung hinweg. Cisco Sicherheitslösungen werden mit QRadar von IBM integriert, um Organisationen über Netzwerke, Endpunkte und Clouds hinweg besser zu schützen. Kunden profitieren auch von der Bandbreite der IBM Global Services-Unterstützung von Cisco-Produkten in Managed Security Service Provider (MSSP) -Angeboten. Die Zusammenarbeit schafft auch eine neue Verbindung zwischen den IBM X-Force- und Cisco Talos-Sicherheitsforschungsteams, die mit der Zusammenarbeit bei der Threat-Intelligence-Forschung und der Koordination bei großen Cyber-Security-Vorfällen beginnen wird. Eines der Kernprobleme, die sich auf Sicherheitsteams auswirken, ist die weite Verbreitung von Sicherheitstools, die nicht untereinander kommunizieren oder wenig integrierbar sind. Eine aktuelle Cisco-Umfrage von 3.000 Chief Security Officers ergab, dass 65 Prozent ihrer Organisationen zwischen sechs und 50 verschiedene Sicherheitsprodukte nutzen. Die Verwaltung solcher Komplexität ist eine herausfordernde Aufgabe für Sicherheitsteams und kann zu potenziellen Sicherheitslücken führen.

Die Cisco- und IBM Security-Partnerschaft konzentriert sich darauf, Organisationen zu helfen, die Zeit zu reduzieren, die erforderlich ist, um Bedrohungen zu erkennen und zu abzumildern. Sie bietet Organisationen integrierte Tools, um ihnen zu helfen, die Reaktion auf Angriffe mit größerer Geschwindigkeit und Genauigkeit stärker zu automatisieren. "Die neue Zusammenarbeit zwischen Cisco und IBM im Bereich Cybersecurity unterstreicht die Notwendigkeit, herstellerübergreifende, durchgängig integrierte Sicherheitslösungen zu schaffen - anstelle von Insellösungen, die Einzelprobleme adressieren, aber keine durchgängige IT-Sicherheitskonzeption unterstützen", sagt Christian Nern, Head of Security Software Sales, IBM DACH.

"In der Cyber-Sicherheit ist ein datengesteuertes Vorgehen der einzige Weg, um den Bedrohungen, die sich auf den Geschäftsbetrieb auswirken können, einen Schritt voraus zu sein", ergänzt Bill Heinrich, Leiter der Abteilung für Informationssicherheit bei BNSF Railway. Sicherheitslösungen über Netzwerke und Clouds hinweg integrieren

Die Kosten für Datenverluste in Unternehmen steigen weiter an. Im Jahr 2016 fand das Ponemon-Institut heraus, daß die Kosten bei den befragten Unternehmen auf einem Höchststand waren mit bis zu 4 Millionen US-$ je Vorfall - ein Anstieg um 29 Prozent in den letzten drei Jahren. Eine langsame Reaktion kann auch Auswirkungen auf die Kosten für einen Sicherheitsvorfall haben - Vorfälle, deren Bewältigung länger als 30 Tage dauern, können im siebenstelligen Bereich höhere Kosten verursachen also solche, die innerhalb von 30 Tagen entschärft werden.

Diese steigenden Kosten sind Treiber für die Notwendigkeit, Bedrohungen schneller zu erkennen und zu blockieren in einem integrierten Ansatz zur Verteidigung. Die Kombination von Ciscos Best-of-Breed-Sicherheitsangeboten und dem architektonischen Ansatz, der mit der IBM Cognitive Security Operations Platform integriert ist, hilft Kunden dabei, ihre Organisationen effektiver vom Netzwerk bis zum Endpunkt der Cloud abzusichern. Als Teil der Zusammenarbeit wird Cisco neue Anwendungen für die QRadar Security Analytics-Plattform von IBM bereitstellen.

Die ersten beiden neuen Anwendungen sollen dazu beitragen, dass Sicherheitsteams fortgeschrittene Bedrohungen besser verstehen und darauf reagieren können. Sie werden auf der IBM Security App Exchange verfügbar werden und verbessern die

Benutzererfahrung. Sie helfen Kunden, Vorfälle effektiver zu identifizieren und zu beheben, wenn diese mit Ciscos Next-Generation Firewall (NGFW), Next Generation Generation Intrusion Protection System (NGIPS) und Advanced Malware Protection (AMP) und Threat Grid arbeiten. Darüber hinaus wird die IBM Resilient Incident Response Plattform (IRP) mit Cisco Threat Grid integriert, um Sicherheitsteams mit vertiefteen Einblicken zu versorgen, um auf Vorfälle schneller zu reagieren.

Zum Beispiel können Analysten in der IRP Indikatoren für Vorfälle mit Hilfe der Threat Intelligence von Cisco Threat Grid nachschlagen oder verdächtige Malware mit Sandbox-Technologie untersuchen. Damit können Sicherheitsteams für ihre Reaktion wertvolle Vorfalldaten gewinnen. "Ciscos architektonischer Ansatz zur Sicherheit ermöglicht es Unternehmen, einmal eine Bedrohung zu erkennen und dann überall zu stoppen. Durch die Kombination von Ciscos umfangreichem Security-Portfolio mit dem IBM Security-Operations-Betrieb und der Response-Plattform bringen Cisco und IBM Best-of-Breed-Produkte und -Lösungen in das Netzwerk, den Endpunkt und die Cloud, gepaart mit fortschrittlichen Analysen- und Orchestrierungsfunktionen ", sagt David Ulevitch, SVP und General Manager, Cisco Security. "Es wird erwartet, daß Cybercrime die Welt bis zu 6 Billionen US$ jährlich bis 2021 kosten kann.

Deshalb ist IBM ein Befürworter der offenen Zusammenarbeit im Kampf gegen Bedrohungen, um die Attraktivität von Cyberangriffen deutlich zu senken", sagt Marc van Zadelhoff, General Manager, IBM Security. "Mit Ciscos Unterstützung des IBM Immunsystems zur Cyberverteidigung können gemeinsame Kunden ihre Fähigkeiten erheblich erweitern - durch die Verwendung von kognitiven Technologien wie IBM Watson für Cyber Security. Auch die Tatsache, daß die IBM X-Force und Cisco Talos Teams zusammenarbeiten, ist ein enormer Vorteil im Kampf gegen Cyberkriminalität. " Threat Intelligence und Managed Services IBM X-Force und Cisco Talos Forschungsteams werden künftig in der Sicherheitsforschung zusammenarbeiten, um anspruchsvolle Cybersicherheitsprobleme bei gemeinsamen Kunden zu lösen, indem die jeweils führenden Experten hier im Verbund arbeiten.

Für gemeinsame Kunden wird IBM eine Integration zwischen X-Force Exchange und Cisco Threat Grid bereitstellen. Diese Integration erweitert die historische und Echtzeit-Datenbasis in der Threat Intelligence, die Sicherheitsanalysten für tiefere Einsichten korrelieren lassen können. Zum Beispiel haben Cisco und IBM kürzlich die Threat Intelligence-Daten im Rahmen der jüngsten WannaCry-Ransomware-Angriffe geteilt. Die Teams koordinierten ihre Reaktionen und die Forscher tauschten Einblicke aus in der Ausbreitung der Malware. Sie arbeiten weiterhin an dieser Untersuchung zusammen, um sicherzustellen, dass gemeinsame Kunden und die Branche die jeweils wichtigsten Informationen erhalten können.

Durch diese erweiterte Zusammenarbeit wird das IBM Managed Security Services-Team, das Sicherheit für über 3.700 Kunden weltweit steuert, mit Cisco zusammenarbeiten, um neue Dienste zu erbringen, die darauf abzielen, die Komplexität weiter zu reduzieren. Eines der ersten Angebote ist für den wachsenden Hybridwolkenmarkt konzipiert. Da Enterprise-Kunden immer stärker die Sicherheitsinfrastruktur zu öffentlichen und privaten Cloud-Anbietern migrieren, stellt IBM Security Managed Security Services zur Unterstützung von Cisco Security-Plattformen in führenden Public Cloud Services zur Verfügung. Weitere Informationen: ibm.com/security und newsroom.cisco.com

Kontaktinformation

Hans-Jürgen Rehm

IBM Kommunikation 07034-151887 0171-5566940 hansrehm@de.ibm.com

---