Sophos Threat Report: Das sind die Bedrohungen für 2020 und darüber hinaus

Sophos Threat Report 2020 zeigt Schlüsseltrends auf:

- *Kurz und schmerzhaft: Cyber-Angreifer setzen verstärkt auf Ransomware.*
- *Still und leise: Bösartige Android-Apps agieren zunehmend als Malware-Makler.*
- *Kleine Fehler, großer Schaden: Fehlkonfigurationen machen Cloud-Umgebungen zu beliebtem Angriffsziel.*
- *Katz und Maus: Auf Machine Learning basierende Security-Systeme geraten selbst ins Visier der Angreifer.*

Wiesbaden 5. November 2019 Sophos hat heute seinen Threat Report 2020 veröffentlicht. Der Bericht gibt einen Überblick über die sich schnell entwickelnde Cyberkrimellen-Landschaft. Die Security-Experten der SophosLabs haben hierfür Veränderungen in der Bedrohungslandschaft der letzten 12 Monate untersucht und identifizieren Trends, die sich voraussichtlich 2020 auf die Cybersicherheit auswirken werden.

„Die Bedrohungslandschaft entwickelt sich weiter – rasant, in großem Ausmaß und immer weniger vorhersehbar. Die einzige worüber wir echte Gewissheit haben, ist das, was in diesem Moment passiert," sagt John Shier, Senior Security Advisor bei Sophos.
Im Threat Report 2020 hat Sophos daher ein besonderes Augenmerk darauf gelegt, wie sich die aktuellen Trends in der Cyberkiminalität im kommenden Jahr auf die Welt auswirken könnten. Der Report beschreibt, wie die gegnerische Seite immer unauffälliger wird, wie sie versteht, Fehler besser auszunutzen, ihre Aktivitäten geschickter zu verbergen und wie es ihr gelingt, modernen Erkennungstechnologien auszuweichen. Und zwar in der Cloud, über mobile Apps und in Netzwerken. „Der Threat Report 2020 ist daher weniger als Statusbericht, sondern vielmehr als Wegweiser zu verstehen, der Unternehmen helfen soll, besser zu verstehen, was sie in den kommenden Monaten erwartet und wie sie sich vorbereiten müssen," so Shier weiter.

Der SophosLabs Threat Report 2020 konzentriert sich auf wenige Kernbereiche, in denen Forscher im vergangenen Jahr besondere Entwicklungen verzeichneten. Von folgenden Bedrohungen erwarten die Sophos-Experten, dass sie bis 2020 und darüber hinaus erhebliche Auswirkungen auf die Cyber-Bedrohungslandschaft haben werden:

Ransomware-Angreifer setzen verstärkt auf automatisierte aktive Angriffe
Diese Angriffe wenden vertrauenswürdige Management-Tools von Unternehmen gegen sie, umgehen Sicherheitskontrollen und deaktivieren Sicherungskopien um so in kürzester Zeit maximale Auswirkungen zu erzielen.

Unerwünschte Apps rücken näher an Malware heran
Nachdem in diesem Jahr zunehmend Android Fleeceware-Apps, die Abonnements missbrauchen, sowie immer mehr heimliche und aggressive Adware zum Einsatz kamen, zeigt der Threat Report, wie diese und andere potenziell unerwünschte Apps (PUA) – z.B. Browser-Plug-Ins – auch in Zukunft zu Maklern für die Bereitstellung und Ausführung von Malware und dateifreien Angriffen werden.

Die größte Sicherheitslücke für Cloud Computing ist die Fehlkonfiguration
Da Cloud-Systeme immer komplexer und flexibler werden, steigt das Risiko von Bedienungsfehlern durch die Betreiber. In Kombination mit einem generellen Mangel an Transparenz werden Cloud-Computing-Umgebungen so zu einem vorhersehbar beliebten Ziel für Cyberangreifer.

Maschinelles Lernen zur Bekämpfung von Malware wird selbst angegriffen
2019 war das Jahr, in dem sich das Potenzial von Angriffen auf Sicherheitssysteme zeigte, die durch Machine Learning unterstützt werden. Die Forschung hat gezeigt, wie diese Systeme möglicherweise ausgetrickst werden können und wie Machine Learning angewendet werden kann, um sehr überzeugende gefälschte Inhalte für das Social Engineering zu generieren. Gleichzeitig wenden wiederum auch die Verteidiger maschinelles Lernen auf die Sprache an, um bösartige E-Mails und URLs zu erkennen. Es ist zu erwarten, dass dieses fortgeschrittene Katz- und Mausspiel in Zukunft immer beliebter wird.

Aus dem Netz ins Netzwerk und weitere Themen
Weitere Bereiche, die im Bedrohungsbericht 2020 behandelt werden, sind die Angriffe, die zunehmend unbemerkt über das Internet auf daran angeschlossene Geräte und Dienste erfolgen, die Rolle des Remote Desktop Protocol (RDP) als eine anhaltend beliebte Einstiegsluke für Angreifer sowie der weitere Vormarsch automatisierter aktiver Angriffe (AAA).

Alle weiteren Details und Informationen zu den Trends in der Bedrohungslandschaft und zum Verhalten von Cyberkriminellen finden Sie im ausführlichen Report unter folgendem Link **https://www.sophos.com/en-us/labs/security-threat-report.aspx**.

Über Sophos
Als ein weltweit führender Anbieter von Next-Generation-Cybersicherheit schützt Sophos mehr als 400.000 Unternehmen jeder Größe in über 150 Ländern vor den neuesten Cyberbedrohungen. Mit den SophosLabs und seinem globalen Team für Bedrohungs- und Datenanalyse schützen die Cloud- und KI-gestützten Sophos-Lösungen Endpoints (Laptops, Server und mobile Geräte) sowie Netzwerke vor sich ständig verändernden Cyberangriffen, einschließlich Ransomware, Malware, Exploits, Datenexfiltration, individuellen Hackervorstößen, Phishing und mehr. Die cloud-basierte Plattform Sophos Central integriert über APIs das gesamte Next Generation Sophos-Portfolio, von der Intercept X Endpoint-Lösung bis zur XG Firewall, in einem einzigen Synchronized-Security-System. Sophos treibt die Entwicklung zur Next Generation Cybersicherheit voran und setzt fortschrittliche Technologien, beispielsweise aus den Bereichen Cloud, Machine Learning, APIs, Automatisierung oder Managed Threat Response ein, um Unternehmen jeder Größe Schutz der Enterprise-Klasse zu bieten. Sophos vertreibt Produkte und Services exklusiv über einen globalen Channel mit mehr als 47.000 Partnern und Managed Service Providern (MSP). Sophos stellt seine innovativen, gewerblichen Technologien auch Privatanwendern via Sophos Home zur Verfügung. Das Unternehmen hat seinen Hauptsitz in Oxford, Großbritannien, und ist an der Londoner Börse unter dem Symbol "SOPH" notiert. 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
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de