20 Jahre Cyberbedrohung

Sophos gibt einen umfassenden Rückblick auf Cyberbedrohungen und Ereignisse der vergangen zwei Jahrzehnte und zeigt die verschiedenen Epochen auf, in denen Würmer, Stuxnet oder Ransomware dominierten

Das Ende des Jahres ist immer ein guter Zeitpunkt, um die aktuelle Cyber-Bedrohungslandschaft zu betrachten und Prognosen darüber zu wagen, wohin sie sich entwickeln könnte. Jährliche Berichte wie der Sophos 2021 Threat Report unterstützen diesen Prozess. Sie liefern eine anschauliche Übersicht über die wichtigsten Bedrohungsereignisse der letzten zwölf Monate und zeigen Trends und zukünftige Schutzmaßnahmen auf. Aber ein Rückblick über mehrere Jahre hinaus bietet eine wertvolle zusätzliche Perspektive und ermöglicht es zu verstehen, wie verschiedene Cyberbedrohungen und das Verhalten von Angreifern entstehen und sich weiterentwickeln. Zudem liefert ein längerfristiger Rückblick zusätzlichen Kontext und wichtige Erkenntnisse über derzeitige und zukünftige Entwicklungen.

Der neue Report „Cyberthreats: A 20-Year Retrospective“ von John Shier, Senior Security Advisor bei Sophos, gibt einen ausführlichen Überblick über die Cyberbedrohungen und Ereignisse, die in den vergangenen 20 Jahren den größten Einfluss auf die Sicherheitslandschaft hatten. Der Bericht zeigt auf, wie schnell sich die Security-Bedrohungen ändern,wie Angreifer aus der Vergangenheit lernen und sich mit immer größerer Geschwindigkeit weiterentwickeln.

Die drei wesentlichen Epochen der Cyberbedrohungen

2000 bis 2004 – In den ersten Jahren des Jahrtausends wurde ein Wurm nach dem anderen auf die Welt losgelassen. Sie wüteten im Internet mit Infektionsraten, die sich in weniger als zehn Sekunden verdoppeln konnten. Etwa zehn Prozent aller mit dem Internet verbundenen Hosts waren betroffen und irgendwann waren Würmer für 25 Prozent aller Spam-Mails verantwortlich. Viele missbrauchten Schwachstellen, für die bereits Patches zur Verfügung standen. Mindestens einer zeigte eine konstante Entwicklung hin zur Überlistung der Sicherheitserkennung. Diese Würmer verursachten insgesamt rund 100 Milliarden Dollar an Kosten zur Schadensbegrenzung. Sie ebneten den Weg für Botnets, die massiv Spam verbreiten und rücksichtslos zur Monetarisierung eingesetzt werden.

2005 bis 2012 – Dies ist die Epoche, in der Cyberkriminalität zu einem Geschäft wurde. Gut organisierte Spammer zielten mit Pharma-Scams und Malvertising auf die Anwender ab. Die Landschaft wurde durch Exploit-Kits und staatlich gesponserte Bedrohungen und ihre fortschrittlichen, teuren Tools für immer verändert. Das Storm-Botnet, das den Spitznamen „der größte Supercomputer der Welt“ trägt, hat schätzungsweise zwischen einer und zehn Millionen Geräte kompromittiert. Im Jahr 2009/2010 zeigte Stuxnet der Welt, wie Cyberwaffen gegen physische Systeme eingesetzt werden können. Zudem ermöglichte der Aufstieg der Kryptowährungen Angreifern eine neue Möglichkeit, Geld zu verdienen – und zwar Lösegeld.

2012 bis heute – In den letzten Jahren hatte keine Cyberbedrohung einen schädlicheren Einfluss gehabt als Ransomware. Bis heute belaufen sich die Schäden und die Auswirkungen der Lösegeldforderung auf Billionen von Dollar. Darüber hinaus gab und gibt es in dieser Ära die transformatorischen Angriffe von Wannacry und NotPetya sowie die Weiterentwicklung und Fortsetzung der Botnets. Zudem kennzeichnen noch mehr Würmer, Spam und das Aufkommen von staatlich gesponserten Cyberwaffen die aktuelle Entwicklung. Heute sind Diebstahl bei Online-Zahlungen, immer raffinierteres Phishing sowie der Rückgang der Online-

Privatsphäre ebenfalls Teil der ständig wachsenden, immer komplexeren Bedrohungslandschaft. Zudem stehen alle Tools heute als „Everything-as-a-Service“ (XaaS) zur Verfügung. So sind Cyberattacken selbst für Cyberkriminelle möglich, die nicht über technisches und intellektuelles Know-how verfügen.

Der komplette Report „Cyberthreats: A 20-Year Retrospective“ von John Shier steht **hier** als Download bereit

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 53.000 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. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
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