Cyberkriminalität 2021: Ransomware weiterhin der Platzhirsch - und die Angriffe werden noch pointierter

Im aktuellen Sophos Threat Report 2021 geben die Sophos-Experten ihre Einschätzungen zu den kommenden IT-Security-Trends aus unterschiedlichen Blickwinkeln ab.

Sophos präsentiert seinen aktuellen Sophos Threat Report 2021. Daraus geht hervor, dass Ransomware, insbesondere mit dem Phänomen der Sekundär-Erpressung sowie die sich

schnell verändernden Verhaltensweisen von Cyberkriminellen die Bedrohungslandschaft und die IT-Security im kommenden Jahr maßgeblich prägen werden. Der Sophos Threat Report wurde von den SophosLabs, Threat Huntern, dem Rapid-Respons-Team sowie Cloud- und KI-Experten verfasst und

liefert sowohl einen umfassenden Überblick zu den Sicherheitsbedrohungen des abgelaufenen Jahres als auch einen Ausblick auf die voraussichtlichen Gefahren im kommenden Jahr.

Die Sophos-Experten prognostizieren drei wichtige Security-Trends für 2021:

1. Die Kluft zwischen den Fähigkeiten und Ressourcen der verschiedenen Ransomware-Akteure vergrößert sich weiter. Versierte Ransomware-Kriminelle verfeinern und ändern ihre Taktiken, Techniken und Verfahren kontinuierlich, um größere Organisationen und Unternehmen mit

Lösegeldforderungen in Millionenhöhe ins Visier zu nehmen. Im Jahr 2020 gehörten zu dieser Ransomware-Kategorie beispielsweise Ryuk und RagnarLocker. Zudem rechnen die Sophos-Experten mit einer steigenden Zahl an Ransomware-Neueinsteigern. Diese arbeiten meist mit menügesteuerter Miet-Ransomware wie Dharma, mit der sie viele Ziele mit kleinen Lösegeldforderungen attackieren können.

Einen weiteren Ransomware-Trend für 2021 bildet die sogenannte „Sekundär- Erpressung". Neben der Datenverschlüsselung stehlen die Angreifer hierbei auch sensible oder vertrauliche Informationen und drohen damit, sie bei Nichterfüllung der Forderungen zu veröffentlichen.

Populäre Beispiele für diesen Ansatz sind die Ransomware-Familien Maze, RagnerLocker, Netwalker und REvil.

„Das Ransomware-Geschäftsmodell ist dynamisch und komplex. Im Jahr 2020 sahen wir bei Sophos einen klaren Trend darin, dass sich die Angreifer hinsichtlich ihrer Fähigkeiten und Ziele unterscheiden.

Auffällig war zudem, dass „Best-of-Breed"-Tools bei bestimmten Ransomware-Familien immer wieder zum Einsatz kamen und kommen", sagt Chester Wisniewski, Principal Research Scientist bei Sophos. „Einige Ransomware-Familien wie Maze schienen zu verschwinden, aber die bei diesen Attacken verwendeten Werkzeuge und Techniken tauchten unter dem Deckmantel einer neuen

Ransomware wie Egregor wieder auf. Das Verschwinden bekannter Spieler auf dem Ransomware-Markt ist also kein Anzeichen für Entwarnung, denn wenn eine Bedrohung verschwindet, nimmt schnell eine andere ihren Platz ein. In vielerlei Hinsicht ist es fast unmöglich vorherzusagen, wie

Ransomware-Attacken zukünftig aussehen. Aber die Angriffstrends, die Anfang 2020 im Sophos Threat Report diskutiert wurden, werden voraussichtlich auch im Jahr 2021 anhalten."

2. Alltägliche Bedrohungen wie Malware einschließlich Loader-Programmen und Botnets oder opportunistische Hacker, die mit Zugangsdaten handeln, stellen weiterhin eine große Herausforderung für IT-Sicherheitsteams dar. Solche Angriffe sind so konzipiert, dass sie von ihrem Ziel wichtige Daten sammeln und diese an ein Command-and-Control-Netzwerk übermitteln.

Dort überprüfen die Eindringlinge jedes kompromittierte Gerät auf seine Geolokalisierung und andere Informationen von hohem Wert und verkaufen diese Informationen an den Meistbietenden, etwa an eine große Ransomware-Gruppe. Beispielsweise setzte Ryuk in diesem Jahr den Buer

Loader ein, um Ransomware bei den Opfern zu platzieren. „Gerade alltägliche Malware sollte nicht als ‚Grundrauschen' abgetan werden, da diese Angriffe mit vielen einzelnen Attacken das Sicherheitswarnsystem regelrecht verstopfen können. Aus unseren Analysen geht klar hervor, dass auch diese Angriffe sehr ernst genommen werden müssen, da jede einzelne Infektion zur Infektion eines ganzen Systems führen kann. Sobald Malware blockiert oder entfernt und der kompromittierte Rechner gesäubert ist, schließen viele das Kapitel final ab", so Wisniewski. „Vielen ist aber möglicherweise nicht bewusst, dass der Angriff wahrscheinlich gegen mehr als nur einen Rechner gerichtet war und dass scheinbar einfach abgeblockte Malware wie Emotet oder Buer Loader in der Folge Tür und Tor für fortgeschrittenere Angriffe mit z.B. Ryuk oder Netwalker führen kann. Diese bemerken IT-Abteilungen vielfach erst dann, wenn die Ransomware zum Einsatz kommt. Eine Unterschätzung dieser ‚geringfügigen' Infektionen kann sich also als sehr kostspielig erweisen."

3. Cyberkriminelle missbrauchen zunehmend legitime Werkzeuge, bekannte Hilfsprogramme und weit verbreitete Netzwerkziele, um sich Sicherheitsmaßnahmen zu entziehen. Der Missbrauch von häufig genutzten Standardprogrammen ermöglicht es Cyberkriminellen, sich unter dem Radar im Netzwerk zu bewegen, bis sie den Angriff starten. Staatlich motivierte Angreifer haben zudem den Vorteil, dass die Verwendung neutraler Programme die Zuordnung im Fall der Aufdeckung erschwert. Im Jahr 2020 berichtete Sophos bereits über die breite Palette solcher Standard-Angriffstools.

„Der Missbrauch alltäglicher Tools und Techniken zur Verschleierung eines Angriffs stellt traditionelle Sicherheitsansätze in Frage, da die Verwendung solcher Programme nicht automatisch eine Warnung auslöst. Hier kommt der schnell wachsende Bereich des Threat Hunting durch ein Expertenteam und die kontrollierte Reaktion auf Bedrohungen erst richtig zur Geltung", sagt Wisniewski. „Diese Experten kennen die subtilen Anomalien und Spuren eines Angriffs, nach denen man suchen muss. Dazu gehört zum Beispiel ein legitimes Werkzeug, das zur falschen Zeit oder am falschen Ort eingesetzt wird. Für geschulte Threat Hunter oder IT-Manager, die Endpoint Detection and Response (EDR)-Funktionen nutzen, sind diese Zeichen wertvolle Hinweise, um vor einem potenziellen Eindringling und einem laufenden Angriff zu warnen."

Zu den weiteren Trends des Sophos Threat Report 2021 gehören:

Angriffe auf Server: Cyberkriminelle nehmen Server-Plattformen unter Windows und Linux ins Visier und nutzen diese Plattformen, um Organisationen von Innen heraus anzugreifen.

Die COVID-19-Pandemie hat Auswirkungen auf die IT-Sicherheit. Hierzu gehört beispielswiese die Absicherung im Home-Office mit persönlichen Netzwerken, die auf sehr unterschiedlichen Sicherheitsniveaus basieren.

Sicherheitsherausforderung an Cloud-Umgebungen. Bei Cloud Computing stehen Unternehmen allerdings vor anderen Herausforderungen als bei einem traditionellen Unternehmensnetzwerk.

Standarddienste wie RDP und VPN stehen nach wie vor im Fokus der Angreifer. Dabei wird RDP auch genutzt, um sich innerhalb der Netzwerke weiter auszubreiten.

Anwendungen, die traditionell als „potenziell unerwünscht“ (PUA) gekennzeichnet wurden, weil sie eine Fülle von Werbung liefern. Diese verwenden Taktiken, die zunehmend nicht mehr von ffensichtlicher Malware zu unterscheiden sind.

Das überraschende Wiederauftauchen eines alten Fehlers: VelvetSweatshop ist eine Standardkennwortfunktion für frühere Microsoft Excel-Versionen, die dazu verwendet wurde, bösartige Makros oder andere kritischen Inhalte in Dokumenten zu verbergen und so der Bedrohungserkennung zu entgehen.

Die Notwendigkeit, Ansätze aus der Epidemiologie anzuwenden. Diese helfen dabei, unentdeckte und unbekannte Cyber-Bedrohungen zu quantifizieren, um Lücken bei der Erkennung zu schließen, Risiken besser einzuschätzen und Prioritäten zu definieren.

Einen Überblick über den Sophos Threat Report 2021 gibt Chester Wisniewski im folgendem Video: https://vimeo.com/477657457/70615ef85a

Zwei weitere Artikel zum Sophos Threat Report 2021 stehen unter:

Introduction to the 2021 Threat Report

Cybersecurity: a 20-year retrospective