Zero-Day-Angriffe: Die bösartigen Unbekannten - Schutzmassnahmen gegen Cyberattacken auf verborgene Sicherheitslücken

Zero-Day-Schwachstellen und entsprechende Exploit-Kits sind äusserst wertvoll auf dem Schwarzmarkt. Cyberkriminelle, die etwa an staatlicher oder Industriespionage beteiligt sind, nutzen diese Schwachstellen als Einfallstor, um hochentwickelte Angriffe durchzuführen oder sensible Daten zu stehlen. Der durchschnittliche Lebenszyklus einer Zero-Day-Sicherheitslücke bis zu ihrem öffentlichen Bekanntwerden beträgt dabei rund sieben Jahre – Exploit-Kits für Angreifer stehen dagegen häufig bereits nach nicht einmal einem Monat zur Verfügung, so eine unabhängige Analyse durch Sicherheitsforscher des amerikanischen Think-Tanks Rand Corporation. Obwohl die Anzahl der Zero-Day-Angriffe steigt, sind viele Unternehmen schlecht vorbereitet, um sich gegen diese Attacken zu wehren. Auch, weil klassische Sicherheitstools sich hauptsächlich gegen bekannte Bedrohungen richten.

Zero-Day-Schwachstellen und -Exploits: Definition und Funktionsweise

Eine Zero-Day-Schwachstelle ist, einfach ausgedrückt, ein ungepatchtes Softwareproblem, das dem Softwarehersteller oder Antivirenanbietern bisher unbekannt ist. Es stehen daher keine Sicherheitspatches zur Verfügung, um den Fehler zu beheben. Zero-Day-Schwachstellen können in jeder Art von Software vorhanden sein und treten insbesondere bei Browser- und Betriebssystemsoftware sowie bei weitverbreiteter Software von Unternehmen wie beispielsweise Adobe auf. Ein Zero-Day-Exploit ist der Code, den Angreifer verwenden, um eine Zero-Day-Schwachstelle auszunutzen und ein System oder Gerät zu kompromittieren. So können Hacker unbemerkt durch die Nutzung des Exploits Zugriff auf Daten oder Netzwerke erhalten oder Malware auf einem Gerät installieren.

Das Zeitfenster zwischen der Entdeckung einer Zero-Day-Schwachstelle und der Veröffentlichung eines Patches zur Behebung des Fehlers ist eine wertvolle Gelegenheit für Angreifer, die Lücke auszunutzen. Deswegen werden Zero-Day-Schwachstellen häufig von Cyberkriminellen lukrativ auf dem Schwarzmarkt gehandelt. Die Preise für Zero-Day-Schwachstellen und Exploit-Kits sind sehr unterschiedlich, können aber bis zu 5.000 US-Dollar oder mehr einbringen. Ein Remote-Exploit für Firefox beispielsweise erzielt Schätzungen zufolge Spitzenpreise von bis zu 200.000 Dollar, ein fortschrittlicher Exploit für Google Chrome zwischen 500.000 und einer Million Dollar. Natürlich sind auch Schwachstellen, die in mehreren Versionen eines grossen Betriebssystems oder einer Software vorhanden sind, wertvoller als solche, die nur in einer einzigen System- oder Softwareversion existieren.

Massnahmen zum Schutz vor Zero-Day-Angriffen

Unternehmen, die einen proaktiven Sicherheitsansatz verfolgen, sind besser gerüstet, um sich gegen Zero-Day-Angreifer zu verteidigen. Aufgrund ihrer Unbekanntheit umgehen Zero-Day-Exploits den Schutz durch traditionelle Antiviren-Signaturen. Verhaltensbasierte Sicherheitslösungen wie Endpoint Detection and Response (EDR) können dagegen einen Zero-Day-Angriffe mithilfe von Heuristiken oder Algorithmen zur VeSicherheitsansatzrhaltensüberwachung erkennen. Diese Technologien überwachen hierfür Endpunkt- und Netzwerkereignisse und speichern diese Informationen in einer zentralen Datenbank. Mithilfe von Verhaltensanalyse werden die Daten auf Anomalien wie selten auftretende Prozesse, ungewöhnliche oder unbekannte Verbindungen und andere verdächtige Aktivitäten untersucht. Dieser Vorgang kann automatisiert werden, wobei Anomalien Warnmeldungen für sofortige Massnahmen oder weiterführende Untersuchungen auslösen.

Unternehmensinterne Datentransparenz für Sicherheitsteams ist ein weiterer Schlüssel zur frühzeitigen Erkennung eines Zero-Day-Angriffs. Durch eine Überwachung aller Datenzugriffe und -aktivitäten auf anomales Verhalten können Unternehmen schnell Sicherheitsverstösse identifizieren und eindämmen, bevor es zum Datendiebstahl kommt. Data Loss Prevention-Lösungen, die kontextbasierte Klassifikation verwenden, können sensible Geschäftsinformationen, geistiges Eigentum und personenbezogene Daten sowohl in strukturierter Form in Datenbanken als auch in unstrukturierter Form, beispielsweise Dokumente, Bilder, E-Mails, Audio- oder Video-Daten, klassifizieren. Mithilfe von Richtlinien, Kontrollen und Verschlüsselung lassen sich so sensible Daten sowohl im Ruhezustand, in Bewegung und bei Verwendung vor Diebstahl schützen, selbst, wenn es Cyberkriminellen gelingt, einen Zero-Day-Angriff durchzuführen und das Unternehmen einen Sicherheitsverstoss erleidet.

Softwareschwachstellen und die damit verbundenen Zero-Day-Attacken werden auch zukünftig eine unvermeidbare Bedrohung bleiben. Jedoch können Unternehmen durch einen mehrschichtigen und proaktiven Sicherheitsansatz die Risiken und Folgeschäden eines Zero-Day-Angriffs deutlich minimieren.