Rekordzahl bei Zero-Day-Angriffen in 2021

Originalartikel

Backup

<html> <header class=„article-header“><h1 class=„articleheading“>Rekordzahl bei Zero-Day-Angriffen in 2021</h1> Patrick Howell O'Neill </header><figure class=„aufmacherbild“><figcaption class=„akwa-caption“>(Bild: JARIRIYAWAT/Shutterstock.com)</figcaption></figure> Mindestens 66 Zero-Days wurden bereits gefunden. Doch man sollte die Gründe für die Verdoppelung gegenüber dem Vorjahr differenziert betrachten. So ziemlich das Wertvollste, was ein Hacker besitzen kann, ist ein Zero-Day-Exploit – eine Möglichkeit, einen Cyberangriff über eine bisher unbekannte Sicherheitslücke zu starten. Solche Schwachstellen können auf dem freien Markt Preise von über einer Million Dollar erzielen. In diesem Jahr hat die Sicherheitsindustrie für den Cyberspace die höchste Anzahl an Zero-Days aller Zeiten abgefangen, wie sich aus mehreren Datenbanken herauslesen lässt und wie Forscher sowie Vertreter von Cybersicherheitsunternehmen in einem Gespräch mit MIT Technology Review berichten. Laut Datenbanken wie dem 0-Day Tracking Project [1] wurden in diesem Jahr mindestens 66 Zero-Days im Einsatz gefunden – fast doppelt so viele wie im Jahr 2020 und mehr als in jedem anderen Jahr der Aufzeichnungen. Doch während die Rekordzahl an sich die Aufmerksamkeit auf sich zieht, ist ihre Interpretation nicht ganz einfach. Bedeutet sie, dass mehr Zero-Days als je zuvor verwendet werden? Oder gelingt es den Verteidigern besser, die Hacker zu erwischen, die sie früher übersehen hätten? <h3 class=„subheading“ id=„nav_schnelle0“>Schnelle Verbreitung von Hacking-Tools</h3> „Wir beobachten auf jeden Fall eine Zunahme“, sagt Eric Doerr, Vizepräsident für Cloud-Sicherheit bei Microsoft. „Die interessante Frage ist: Was bedeutet das? Stürzt der Himmel ein? Ich bin der Meinung, dass es sich um ein differenziertes Phänomen handelt“. Ein Faktor, der zu der höheren Rate der gemeldeten Zero-Days beiträgt, ist die rasche weltweite Verbreitung von Hacking-Tools. Mächtige Gruppen investieren haufenweise Geld in Zero-Days, um sie für sich zu nutzen – und sie profitieren davon. An der Spitze stehen die von Regierungen gesponserten Hacker. Allein China steht im Verdacht, in diesem Jahr für neun Zero-Days verantwortlich zu sein, sagt Jared Semrau, Direktor für Schwachstellen und Exploitation bei der amerikanischen Cybersicherheitsfirma FireEye Mandiant. Die USA und ihre Verbündeten verfügen zweifellos über einige der ausgefeiltesten Hacking-Fähigkeiten, und es gibt immer mehr Gerüchte über <a

href=„https://www.nytimes.com/2021/09/20/opinion/ransomware-biden-russia.html“ rel=„external noopener“ target=„_blank“>einen aggressiveren Einsatz dieser Instrumente [2]. „Wir haben es hier mit einer Spitzengruppe hochentwickelter Spionageakteure zu tun, die definitiv auf Hochtouren arbeiten, wie wir es in den vergangenen Jahren noch nicht gesehen haben“, sagt Semrau. Nur wenige, die auf Zero-Days aus sind, haben die Fähigkeiten von Peking und Washington. Die meisten Länder, die auf der Suche nach leistungsfähigen Exploits sind [3], haben weder das Talent noch die Infrastruktur, um sie im eigenen Land zu entwickeln, und kaufen sie daher ein. <h3 class=„subheading“ id=„nav_wachsende1“>Wachsende Exploit-Industrie</h3> Es ist einfacher denn je, Zero-Days von der wachsenden Exploit-Industrie zu kaufen. Was früher unerschwinglich teuer und hochwertig war, ist jetzt leichter zugänglich. „Wir haben gesehen, wie staatliche Gruppen sich an die NSO Group [4] oder Candiru gewandt haben, diese zunehmend bekannten Dienste, die es Ländern ermöglichen, finanzielle Ressourcen gegen offensive Fähigkeiten einzutauschen“, sagt Semrau. Die Vereinigten Arabischen Emirate, die Vereinigten Staaten sowie europäische und asiatische Mächte haben allesamt Geld in die Ausnutzung von Sicherheitslücken gesteckt. Und auch Cyberkriminelle haben in den letzten Jahren Zero-Day-Angriffe genutzt [5], um Geld zu verdienen, indem sie Schwachstellen in Software gefunden haben, die es ihnen ermöglichen, einträgliche Ransomware-Programme auszuführen. „Ein Drittel der Zero-Days, die wir in letzter Zeit verfolgt haben, lassen sich direkt auf finanziell motivierte Akteure zurückführen. Sie sind raffinierter als je zuvor und spielen eine wichtige Rolle bei diesem Anstieg, der meiner Meinung nach von vielen Leuten nicht gewürdigt wird“, sagt Semrau. <figure class=„branding“> <img alt=„Mehr von MIT Technology Review“ height=„500“ src=„https://static.wallabag.it/7862d1b7aff4c3b00f37212fefade4e0e2c4cf00/64656e6965643a646174613a696d6167652f7376672b786d6c2c25334373766725323078 6d6c6e733d27687474703a2f2f7777772e77332e6f72672f323030302f737667272532307769647 4683d27363936707827253230686569676874 3d27333931707827253230766965774 26f783d27302532303025323036393625323033393127253345253343726563742532307 83d273027253230793d27302725323077696474683d27363936272532306865696768743d27333931272532306696c6c3d272532336632663266322725334525334 32f726563742533452533432f737667253345/“ class=„c3“ width=„1830“ referrerpolicy=„no-referrer“

/> [6]</figure><h3 class=„subheading“ id=„nav_sicherheitsunter2“>Sicherheitsunternehmen sind den Hackern auf der Spur</h3> Auch wenn es immer mehr Menschen gibt, die Zero-Days entwickeln oder kaufen, ist die Rekordzahl der gemeldeten Fälle nicht unbedingt eine schlechte Sache. Einige Experten sind sogar der Meinung, dass es sich dabei größtenteils um eine gute Nachricht handeln könnte. Nach Meinung der angefragten Experten ist es unwahrscheinlich, dass sich die Gesamtzahl der Zero-Day-Angriffe in einem so kurzen Zeitraum mehr als verdoppelt hat – nur die Zahl der abgefangenen Angriffe. Das deutet darauf hin, dass es den Verteidigern immer besser gelingt, Hacker auf frischer Tat zu ertappen. Eine Veränderung, die sich in diesem Trend widerspiegeln könnte, ist die Tatsache, dass mehr Geld für die Verteidigung zur Verfügung steht, nicht zuletzt durch höhere Bug-Bounties und Belohnungen, die von Technologieunternehmen für die Entdeckung neuer Zero-Day-Schwachstellen ausgesetzt werden. Aber es gibt auch bessere Werkzeuge. <h3 class=„subheading“ id=„nav_komplexere3“>Komplexere Hacks erkennbar</h3> Laut Mark Dowd, dem Gründer von Azimuth Security, sind die Verteidiger inzwischen nicht mehr nur in der Lage, relativ einfache Angriffe abzuwehren, sondern auch komplexere Hacks zu erkennen. Gruppen wie die Threat Analysis Group (TAG) von Google, das Global Research & Analysis Team (GReAT) von Kaspersky und das Threat Intelligence Center (MSTIC) von Microsoft verfügen über einen enormen Fundus an Talenten, Ressourcen und Daten – so viel, dass sie mit den Fähigkeiten eines Geheimdienstes zur Erkennung und Verfolgung gegnerischer Hacker konkurrieren können. Unternehmen wie Microsoft und CrowdStrike gehören zu denjenigen, die in großem Umfang Erkennungsmaßnahmen durchführen. Während alte Tools wie Antivirensoftware dazu führten, dass weniger Augen auf seltsame Aktivitäten gerichtet waren, kann ein großes Unternehmen heute eine kleine Anomalie auf Millionen von Rechnern aufspüren und sie bis zu dem Zero-Day zurückverfolgen, der zum Eindringen verwendet wurde. „Ein Grund dafür, dass man jetzt mehr sieht, ist, dass wir mehr finden“, sagt Doerr von Microsoft. „Wir sind besser darin, die Dinge zu beleuchten. Jetzt kann man aus dem lernen, was bei all den Unternehmenskunden passiert, was ihnen hilft, schneller schlauer zu werden. Wenn man nun etwas Neues entdeckt, wirkt sich das im schlimmsten Fall auf einen Kunden aus und nicht auf 10.000.“ Soweit die Theorie. Doch die Realität ist viel chaotischer. Zu Beginn dieses Jahres starteten mehrere Hackergruppen Angriffe gegen Microsoft Exchange E-Mail-Server. [7] Was als kritischer Zero-Day-Angriff begann, verschlimmerte sich in der Zeitspanne, als zwar eine Lösung in Form eines Updates verfügbar war [8], aber von den betroffenen Unternehmen nicht eingespielt wurde. Dieses Zeitfenster ist für Hacker immer ein beliebter Angriffspunkt. <h3 class=„subheading“ id=„nav_hacker_müssen4“>Hacker müssen heute mehr leisten</h3> Auch wenn Zero-Days mehr denn je vorkommen, sind sich die Experten in einem Punkt einig: Es wird immer schwieriger und teurer, sie auszunutzen. Bessere Abwehrmechanismen und kompliziertere Systeme bedeuten, dass Hacker mehr Arbeit leisten müssen, um in ein Ziel einzudringen, als dies noch vor zehn Jahren der Fall war. Angriffe sind heute kostspieliger und erfordern mehr Ressourcen. Doch dieser Aufwand macht sich bezahlt, da viele Unternehmen Cloud-Lösungen nutzen, können über eine einzige Schwachstelle Millionen von Kunden angegriffen werden. „Vor zehn Jahren, als noch alles vor Ort stattfand, wurden viele der Angriffe nur

von einem einzigen Unternehmen bemerkt“, sagt Doerr von Microsoft, „und nur wenige Unternehmen waren in der Lage zu verstehen, was vor sich ging“. Angesichts der verbesserten Verteidigungsmaßnahmen müssen Hacker oft mehrere Exploits miteinander verknüpfen, anstatt nur eines zu verwenden. Diese „Exploit-Ketten“ erfordern mehr Zero-Days. Der Erfolg beim Aufspüren dieser Ketten ist auch ein Grund für den steilen Anstieg der Zahlen. Heute, so Dowd von Azimuth Security, müssen Angreifer „mehr investieren und mehr riskieren, wenn sie diese Ketten haben, um ihre Ziele zu erreichen“. Ein wichtiges Signal sind die steigenden Kosten für die wertvollsten Exploits. Die begrenzten Daten, die zur Verfügung stehen, wie z. B. die öffentlichen Zero-Day-Preise von Zerodium [9], zeigen, dass die Kosten für die höchstwertigen Hacks in den letzten drei Jahren um bis zu 1150 Prozent [10] gestiegen sind. Doch der Nachfrage tut das keinen Abbruch. <header class=„a-boxheader“ data-collapse-trigger=“„>Lesen Sie auch</header><div class=„a-boxtarget a-boxcontent“ data-collapse-target=“„><article class=„a-article-teaser a-article-teaser–horizontal-layout article-teaser–articlebox a-u-no-margin-bottom a-theme“ data-cid=„0“><figure class=„a-article-teaserimage-container“> </figure> <header><h1 class=„a-article-teasertitle a-u-mb-1“>Wie eine US-Firma iPhone-Hacking-Werkzeuge an ein Regime verkauft haben soll</h1></header> [11]</article> () <hr /> URL dieses Artikels:
<small><code>https://www.heise.de/-6201206</code></small> Links in diesem Artikel:
<small><code>[1] https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit#gid=0</code></small>
<small><code>[2] https://www.nytimes.com/2021/09/20/opinion/ransomware-biden-russia.html</code></small>
<small><code>[3] https://www.heise.de/news/Cybersicherheitsstrategie-Bundesregierung-setzt-auf-Hackbacks-und-Exploits-6186893.html</code></small>
<small><code>[4] https://www.heise.de/hintergrund/Pegasus-Wie-die-NSO-Group-fuer-mehr-Transparenz-sorgen-wollte-6141498.html</code></small>
<small><code>[5] https://www.bleepingcomputer.com/news/security/new-ransomware-group-uses-sonicwall-zero-day-to-breach-networks/</code></small>
<small><code>[6] https://www.heise.de/tr/</code></small>
<small><code>[7] https://www.heise.de/news/Microsoft-Exchange-Server-China-streitet-Hacking-Vorwuerfe-westlicher-Staaten-ab-6143334.html</code></small>
<small><code>[8] https://www.heise.de/news/Jetzt-patchen-Angreifer-attackieren-Microsoft-Exchange-Server-5070309.html</code></small>
<small><code>[9] https://zerodium.com/program.html</code></small>
<small><code>[10] https://www.youtube.com/watch?t=1262&v=JlmRRS4JJd8&feature=youtu.be</code></small>
<small><code>[11] https://www.heise.de/hintergrund/Wie-eine-US-Firma-iPhone-Hacking-Werkzeuge-an-ein-Regime-verkauft-haben-soll-6194961.html</code></small>
<small><code>[12] mailto:jle@heise.de</code></small>
 Copyright © 2021 Heise Medien
</html>