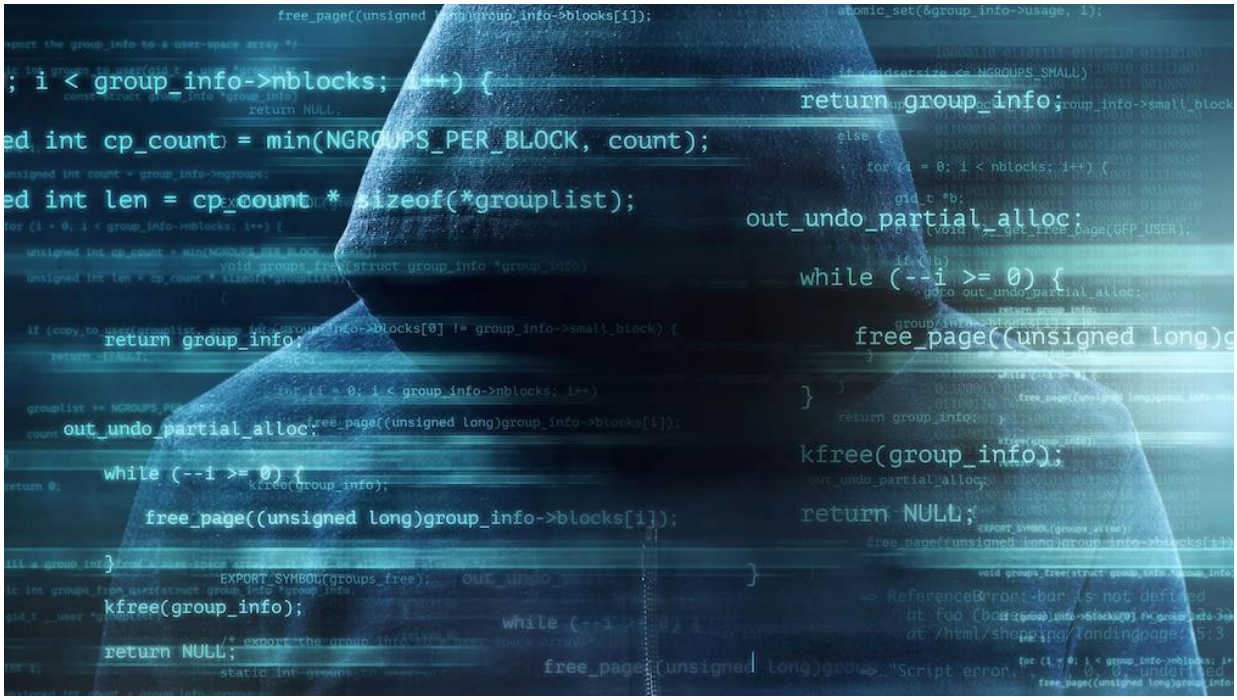
DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Anleitung Zero-Day-Exploits - Darum sind sie so gefährlich

Zero-Day-Exploits: Darum sind sie so gefährlich



Zero-Day-Exploits: So gefährlich sind die Sicherheitslücken. Aber Sie können sich schützen. Foto: iStock.com/shapecharge

26.04.2023, 15:12 Uhr

Zero-Day-Exploits nutzen Schwachstellen aus, für die es noch keinen Patch gibt. Warum diese Sicherheitslücken so gefährlich sind, lesen Sie hier.
Inhaltsverzeichnis

Sicherheitslücken sind an sich schon gefährlich, weil es in der Regel dauert, bis alle Betroffenen die nötigen Sicherheits-Updates installiert haben. Noch gefährlicher sind Zero-Day-Exploits für die User. Bei solchen Sicherheitslücken gibt es nämlich noch gar keinen Patch, obwohl Kriminelle sie schon für Angriffe nutzen. Das macht es für die Nutzerinnen und Nutzer besonders schwierig, sich zu schützen. COMPUTER BILD erklärt, was Sie zu diesen Lücken wissen müssen und wie es gelingt, den PC abzusichern.

Was ist ein Zero-Day-Exploit?

Zero Day, also Tag null, meint die Zeitspanne, die ein Hersteller nach dem Bekanntwerden einer Sicherheitslücke hat, um einen Patch zu entwickeln und zu veröffentlichen – er hat also gar keine Zeit. Ein Zero-Day-Exploit ist eine Malware, die solch eine Schwachstelle ausnutzt. Wenn Hacker einen derartigen Angriffsvektor finden und ihn für sich behalten, können sie ihn so lange nutzen, bis der Hersteller die Lücke bemerkt und schließt. Das dauert mitunter Tage, Wochen oder sogar Monate.

Warum sind Zero-Day-Angriffe so gefährlich?

Eine Sicherheitslücke ermöglicht nicht vorgesehene Zugriffe, das Erschleichen von höheren Rechten oder sogar das Vorbeischleichen an Schutzmaßnahmen. Ist die Lücke bekannt, kann der Hersteller reagieren und sie schließen. Auch die Hersteller von Antivirus-Software können Maßnahmen ergreifen, damit die Schutzprogramme das Ausnutzen der Lücke bemerken. Bei Zero-Days gibt es nur wenig Schutz gegen die Angriffe. Je nach Art der Lücke sind Zero-Day-Exploits daher in der Lage, unbemerkt Daten zu stehlen, Systeme zu infizieren, zu spionieren oder Ähnliches. Gute Antivirus-Software überwacht zwar ständig kritische Bereiche des Systems, um eben solche Angriffe zu entdecken, trotzdem klappt das nicht immer.

Handel mit Zero-Days

Unter Hackern – und Geheimdiensten – sind Zero-Day-Lücken extrem begehrt. Die Kriminellen handeln sogar damit. Für kritische Zero-Days in Windows zahlen sie schon mal eine Million US-Dollar oder mehr. Große Hersteller haben deshalb Bug-Bounty-Programme, die ebenfalls eine Belohnung für das Finden von Schwachstellen bieten. Haben Hacker oder Geheimdienste einen Zero-Day-Exploit, halten sie die Lücke geheim und nutzen den Exploit für ihre Zwecke. Geheimdienste verwenden die Schadsoftware zum Ausspionieren von mutmaßlichen Terroristen. Sie stehen dafür aber immer wieder in der Kritik, weil das Vorhandensein der Lücken alle Nutzerinnen und Nutzer gefährdet. Zudem könnten Hacker die Exploits stehlen, was beispielsweise bei der NSA schon passiert ist.

Bekannte Beispiele von Zero-Day-Angriffen

- **Stuxnet:** Der bekannteste Fall eines Zero-Day ist Stuxnet. Der Zero-Day-Exploit tauchte 2010 zum ersten Mal auf und zielte darauf, das iranische Atomprogramm zu sabotieren. Dazu infizierte der Wurm PCs in der Herstellung und brachte die Steuerungsprogramme von Maschinen in Urananreicherungsanlagen dazu, unerwartete Befehle auszuführen. Aktiv war der Wurm wohl bereits seit 2005. Die Lücke blieb also fünf Jahre lang unentdeckt!
- **Microsoft Word:** 2017 ermöglichte ein Zero-Day-Exploit Angreifern das Stehlen von Anmeldedaten zum Online-Banking. Die Nutzerinnen und Nutzer sahen nur die Abfrage "Remote-Content laden" mit der Aufforderung, einem anderem Programm den Zugriff zu erlauben. Wer das tat, war seine Anmeldedaten los.
- **iOS:** 2020 sorgte eine Zero-Day-Schwachstelle dafür, dass Angreifer iOS-Geräte aus der Ferne manipulieren konnten.

So schützen Sie sich vor Zero-Days

Einige Antivirus-Hersteller werben mit einem Exploit-Schutz oder einem Zero-Day-Schutz. Das sind Module, die kritische Bereiche überwachen und auf Auffälligkeiten achten. Oft kommt maschinelles Lernen zum Einsatz, um Angriffe auch dann zu erkennen, wenn die Malware unbekannt ist. Das ist neben einer guten Firewall der beste technische Schutz vor Zero-Day-Angriffen. Einen vollständigen Schutz gegen gibt es aber nicht. Hilfreich: Installieren Sie Software generell nur aus vertrauenswürdigen Quellen. Halten Sie Betriebssystem und Programme auf dem neuesten Stand, damit Patches zum Schließen von Zero-Days auf Ihrem PC ankommen. Setzen Sie sich mit typischen Phishing-Maschen auseinander, da Zero-Day-Exploits ebenfalls über E-Mail-Anhänge verbreitet werden.

Quelle: https://www.computerbild.de/artikel/cb-Tipps-Sicherheit-Was-ist-ein-Zero-Day-Exploit-33413091.html