# Tabellenverzeichnis

# 1

# Game Hacking: Von der Raubkopie zum Cybercrime Game Hack

Dieses Buch fördert keine Piraterie, Verstöße gegen die DMCA, das EU-Urheberrecht oder andere Urheberrechte sowie Nutzungsbedingungen von Spielen. Game-Hacker wurden lebenslang für Spiele gesperrt, auf Millionen von Dollar oder Euro Schadensersatz verklagt und sogar inhaftiert.

**Was Sie aus diesem Kapitel mitnehmen**

- Ein Grundverständnis, wie Künstliche Intelligenz in Game Engines funktioniert
- Einblicke, wie Game Hacker arbeiten und warum es eine hohe Kunst ist, ein Game zu hacken
- Exemplarische Darstellung von Game Hacks und Anti-Cheat-Software
- Hinweise zur Analyse von Anti-Cheat-Mechanismen in Computerspielen
- Juristische Einschätzung aus der Helikopter-Perspektive im Hinblick auf das Cybercrime Game Hack

Wesentliche Teile des 1. Kapitels wurden mit freundlicher Genehmigung von Marius Christian Anderie entweder wörtlich oder inhaltlich aus der Masterarbeit ‚Analyse von Anti-Cheat-Mechanismen in Computerspielen', vorgelegt an der Philipps-Universität Marburg im Januar 2019, übernommen



L. Anderie, *Quick Guide Game Hacking, Blockchain und Monetarisierung,* Quick Guide, https://doi.org/10.1007/978-3-662-60859-3_1

Dass Software schon immer illegal genutzt wurde, ist nichts Neues – das gilt auch für Computerspiele. Seit Anbeginn der Games-Branche wurden illegale Raubkopien auf Schulhöfen getauscht oder verkauft. Zu faszinierend war das neue verpixelte Produkt Videogame auf Diskette, als dass sich Schüler der Attraktivität hätten entziehen können. Die Verletzung von Urheberrechten war vielen nicht klar und im Sozialkundeunterricht wusste der Lehrer auch nicht so recht, wie es um die Rechtslage bei Games bestellt ist. Im Großen und Ganzen war klar, dass man sich beim Diskettentausch oder -kauf besser nicht erwischen ließ. Gleichzeitig hat die Games-Branche die Verbreitung von Raubkopien jahrelang geduldet – schließlich konnte so die Markenbekanntheit einer Game-IP gesteigert werden. Zur Konfusion beigetragen haben seinerzeit Freeware- und Shareware-Monetarisierungsmodelle – man konnte Games (vermeintlich) kostenlos spielen.

Mit der Einführung von Konsolen-Games und Cartridges (Atari) relativierte sich der illegale Tauschhandel etwas – doch der PC (Personal Computer) beflügelte die Software-Piraterie bei Games als nicht zu unterschätzendes Phänomen. Durch erweiterte Speicherkapazitäten wurde es ermöglicht, dass immer größere Datenmengen und somit attraktivere Games illegal in Umlauf gebracht wurden.

Das Ökosystem, bei dem die Hacker über die Skills und das Know-how verfügten, die Games ‚zu knacken', die Intermediäre, die diese vertrieben, und die User, welche die Games kauften, funktionierte. Genauso wie Alkohol während der Prohibition in den USA, wurde das illegale Gut produziert (erst gehackt und dann raubkopiert) und dann über Netzwerke distribuiert. Jeder kannte ‚über ein paar Ecken' jemanden, der Games ‚billiger als im Laden' besorgen konnte (‚irgendwie vom Laster gefallen'). Unrechtsbewusstsein gab es bei den Usern eher selten. Es gab die Diskussion um das Recht auf die Privatkopie, zeitgleich häuften sich Gerüchte, dass Developer und Publisher ‚Buggy Games' in Umlauf brachten, um enttäuschte User für den Kauf legaler Games zu gewinnen.

Erst eine Kampagne der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU) im Jahre 2006 führte dazu, dass medienwirksam Hausdurchsuchungen durch die Polizei vorgenommen wurden und signifikante Strafen verhängt wurden. Ähnlich dem Ankauf von Steuersünder-CDs wurde eine Strategie der Abschreckung verfolgt. Nach

geraumer Zeit relativierten sich die GVU-Aktivitäten – einerseits sollte die Zielgruppe ‚nicht illegalisiert' werden, andererseits wurde durch den Auf- und Ausbau des Internets und des Webs die Online-Registrierung üblich. Nichtsdestotrotz gab es in Osteuropa einschließlich Russland illegale professionelle Kopierwerke, die gehackte Software über ‚Pirates' distribuierten. Die Aufgabe der Hacker war es, den Kopierschutz ‚zu knacken', was in der Regel innerhalb weniger Stunden oder Tage gelang. Oftmals wurde die Games-Software jedoch schon direkt im Development Studio gestohlen und vor dem Release-Termin illegal distribuiert.

Mit der Entwicklung von MMORPGs (Massively Multiplayer Online Role Play Games) seit dem Jahr 1999 wurden Hacker vor neue technologische Herausforderungen gestellt. Nun galt es, Cheat Software zu entwickeln, mit welchen Vorteile im Spielverlauf gegenüber Mitspielern generiert werden konnten.

> A hacker is an individual who intends to gain unauthorized access to a computer system. (…) by finding weaknesses in security protections website and computer system employ, often taking advantage of various features of the internet that makes it an open system and easy to use. (Laudon K. und Laudon J. 2019, S. 329)

Gleichzeitig galt es, für Game Development Studios diese kriminellen Aktivitäten einzudämmen. Keine einfache Aufgabe, da durch *‚reverse engineering'* und die Entwicklung von *‚rootkits'* durchaus professionelle *malicious software* entwickelt wurde, um Computerspiele zu hacken. Reverse Engineering, eine Teildisziplin des Software-Reengineering, wird von Hackern genutzt, um Games zu manipulieren.

Bruce Dang, Senior Security Development Engineering Lead bei Microsoft, erläutert das wie folgt (Dang et al. 2014, S. 3):

> (…) the reverse engineering learning process is similar to that of a foreign language acquisition for adults.

Und er sagt, dass diese ‚schwarze Kunst' von den Software-Ingenieuren und Codern zunächst einmal erlernt werden müsse, um sie dann zu bekämpfen.

Auch durch die Anbindung der Konsolen-Hardware an das Internet (2001), die Distribution von Games über Online-Plattformen wie Steam (2003) und die Entwicklung von Apps für das Smartphone (2007) wandelten sich die Anforderungen an das Game Hacking. Illegale Log-in Codes (Keys) galt es zu generieren oder von den Servern der Developer und Publisher zu stehlen – Cybercrime in seiner reinsten Form.

Allerdings gibt es durch sogenannte Expertensysteme die Möglichkeit, Cybercrime abzuwenden:

> Expertensysteme (XPS) sind angewandte KI, die Lösungen aus einer Wissensbasis ableiten und zu entsprechendem Handeln anregen. Im Bereich der Sicherheit können Sie Cyberattacken verhindern (Miranda 2019, S. 58). Cyber ist die englische Kurzform für Kybernetik, der Wissenschaft, die sich mit der Steuerung und Kommunikation von Systemen mit Maschinen und Menschen beschäftigt. Meist ist sie Teil von Begriffen, die mit der digitalen Welt und dem Internet zu tun haben, wie Cyberspace, Cybermobbing oder Cybercrime. (Miranda 2019, S. 54)

## 1.1 Cheat Engines: Künstliche Intelligenz und Black Hats

Künstliche Intelligenz wurde durch mannigfaltige Definitionen beschrieben. Deshalb bietet es sich an, eine Definition zu wählen, die von einem der bedeutendsten Unternehmen zitiert wurde, welche sich mit dem Themengebiet befassen: Google.

In einer Veröffentlichung von Google (Alphabet) aus dem Jahre 2018 wird Professor Wolfgang Wahlster, Leiter des Deutschen Forschungszentrums für Künstliche Intelligenz, in einem Interview mit folgender Definition zitiert (Google 2019, S. 23):

> Künstliche Intelligenz ist der Versuch, Leistungen, für die der Mensch Intelligenz benötigt, durch Computer erbringen zu lassen.