

Cheater in Spielen

ARMEE DER BETRÜG

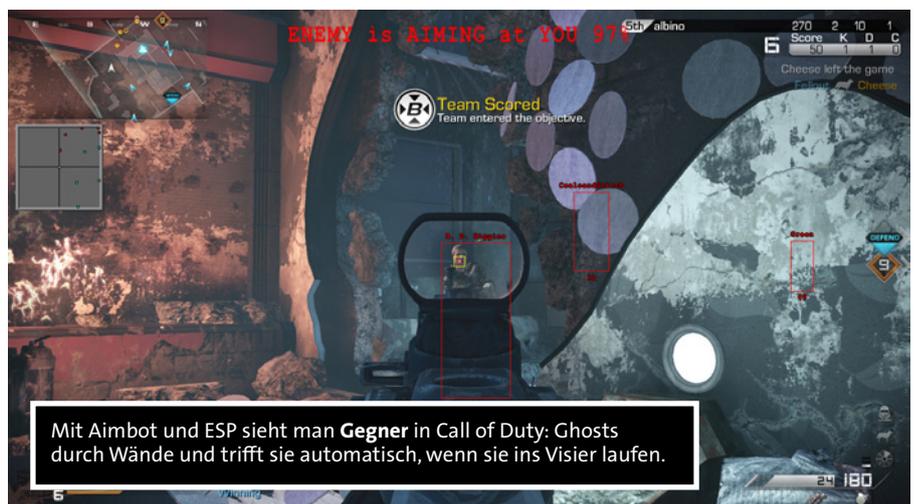
Das Cheaten in Online-Spielen hat sich zum Wettrüsten entwickelt: Hacker verkaufen professionelle Betrugstools, die Spielehersteller antworten mit immer aggressiveren Sperren - und die normalen Spieler geraten zwischen die Fronten. Eine Bestandsaufnahme. Von Dennis Kogel

Wir sind ein digitaler Gott unter 32 Sterblichen. Beim Sprint durch die Korridore eines ausgebrannten Gefängnisses im chinesischen Kuntun-Gebirge sehen wir unsere Feinde auch durch Wände hindurch. Sobald sie um die Ecke biegen, bringen wir sie binnen eines Herzschlags mit präzisen Kopfschüssen zu Fall. Noch dazu sind wir auf der Map »Operation Spind« von **Battlefield 4** immer genau da, wo unser Team uns braucht, auf einer kleinen Übersichtskarte beobachten wir nämlich den kompletten Schlachtverlauf. Virtuell allmächtig, so muss sich Neo in der Matrix gefühlt haben. Gestockt hat uns der Aufstieg zum Gott 15 Euro. Wir cheaten in **Battlefield 4** – und nichts und niemand hält uns auf.

Okay, wir fühlen uns schmutzig. So schmutzig, als hätten wir gerade von der verbotenen Keksdose genascht oder heimlich eine Zigarette geraucht: Cheaten bereitet uns ein Hochgefühl, das fast schon an einen Drogenrausch erinnert – aber es ist falsch, zutiefst falsch. Weil es ehrlichen Spielern den Spaß verdirbt, das Spiel für sie kaputt macht. Das schlechte Gewissen alleine scheint viele Schummler jedoch nicht auf-

zuhalten, um das Betrügen in Onlinespielen hat sich eine regelrechte Schattenindustrie entwickelt: Professionelle Cheat-Tools gibt's zu kaufen, Tausende Spieler greifen zu - und machen ihren Gegnern das Leben zur Hölle. Zugleich ist das bewusste Betrügen ein Thema, über das die meisten Publisher so gerne sprechen wie über eine Darmspiegelung. Riot Games, die Macher von **League of Legends**, entscheiden sich »aus Sicherheitsgründen« gegen ein Interview. Der **Battlefield**-Entwickler Dice ist laut Electronic Arts

zu beschäftigt damit, Bugs zu beheben, um auch noch über Schummler Auskunft zu geben. Und Activision Blizzard gibt gleich gar keine Gründe dafür, warum man unsere Fragen zu **Call of Duty** nicht beantworten will. Die Pressestellen sprechen von einem »heiklen Thema«. Kein Wunder, die Hersteller wollen den Anschein erwecken, dass sie Betrüger aktiv und erfolgreich bekämpfen. Alles gut, hier gibt's keine Cheater, bitte weitergehen! Zugleich wurzelt die Schweigsamkeit tatsächlich in Sicherheitsbedenken.



Mit Aimbot und ESP sieht man **Gegner** in **Call of Duty: Ghosts** durch Wände und trifft sie automatisch, wenn sie ins Visier laufen.



Bild: Warner Bros Pictures

»Es ist eine knifflige Situation«, gesteht Gary Newman, der Macher des Source-Engine-Sandkastens **Garry's Mod** und des Survival-Spiels **Rust**: »Man möchte zwar gerne sagen, wie die eigenen Anti-Cheat-Systeme funktionieren – aber sobald man das macht, finden die Hacker einen Weg, sie auszuhebeln.« Doch selbst wenn Entwickler beim Thema Betrugsbekämpfung keinen Mucks von sich geben, gibt es für viele Betrugsbekämpfungstools bereits regelrechte Umgehungsstraßen. Denn für die meisten populären Onlinespiele – **Battlefield 4**, **Call of Duty: Ghosts**, **World of Warcraft**, **Rust**, **DayZ** und viele mehr – sind Cheats nur eine schnelle Suchanfrage entfernt.

Es gibt keine offiziellen Zahlen darüber, wie viele Spieler tatsächlich cheaten, Anhaltspunkte liefern allerdings die Meldungen über erwischte und gebannte Betrüger. So verzeichnet die Statistik-Website PBBans.com zu unserem Redaktionsschluss über 41.000 gesperrte **Battlefield 3**-Accounts. Angesichts der laut EA über 15 Millionen Verkäufe klingt das erst mal nach wenig, doch das sind ja auch nur die Schummler, die erwischt werden – es gibt eine Dunkelziffer. »Ich würde sagen, bei 32 Leuten ist in Battlefield 4 immer mindestens ein Cheater dabei«, erzählt Samuel Steiner. »Das ist wie beim Bodybuilding. Die besten nehmen Steroide.« Hacks sind Steiners Job, auf seiner kostenpflichtigen Seite Hackerbot.net rezensiert der 22-jährige Schweizer aktuelle Cheat-Programme. Am beliebtesten sind natürlich die Shooter-Schergewichte **Battlefield** und **Call of Duty**, dicht gefolgt vom **Defense of the Ancients**-Ableger **League of Legends**. Gefragt sind vor allem Aimbots, also Zielprogramme, die das präzise Schie-

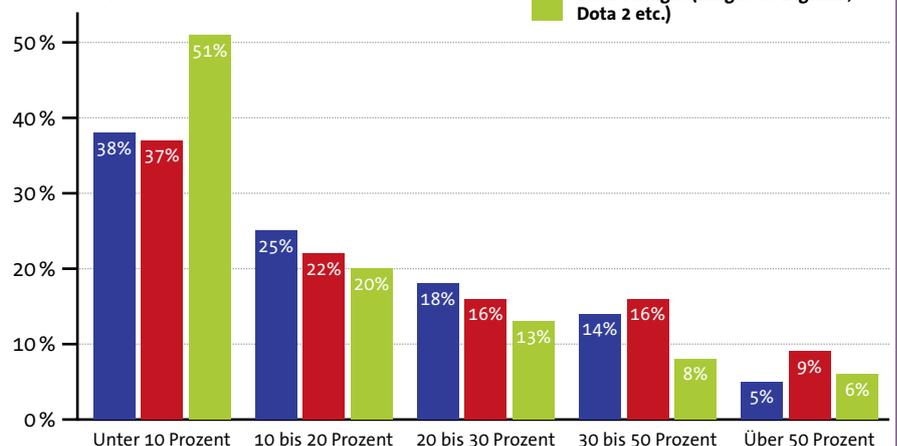
ßen automatisieren, sowie sogenannte ESP-Tools (»Extra Sensory Perception«), die etwa die Position aller Gegner mit Punkten oder Rechtecken direkt in der Spielansicht markiert – auch durch Wände hindurch.

Sollten Steiners Aussagen stimmen, dann blickt in so gut wie jedem populären Onlinespiel irgendjemand durch Mauern und verteilt per Aimbot mühelose Kopfschüsse. Fällt das nicht auf? »Nein, nein! Einen Aimbot bemerkst du überhaupt nicht«, erwidert Steiner. Selbst der schwerwiegendste Hack, der die Spielbalance aus den Fugen bringt, ist also gar nicht so leicht zu entdecken. »Natürlich, die ganz offensichtlichen

Cheat-Anfänger werden den Aimbot so einrichten, dass er innerhalb einer Tausendstelsekunde auf den Kopf des Gegners zielt und schießt. Das ist offensichtlich. Aber wenn man es professionell macht, dann zielt der Bot sehr langsam, wartet 0,2 Sekunden und schießt dann. So mache ich das auch. Und bei mir merkt nie jemand etwas.« Dass Spieler nichts merken, ist in der Hektik einer Shooter-Partie nur verständlich. Zumindest die Anti-Cheat-Mechanismen der Publisher sollten jedoch Alarm schlagen, egal ob ein Aimbot nun 0,0001 Sekunden zum Zielen braucht oder 0,2. Wer **Battlefield 4** installiert, installiert nämlich auch die Anti-Cheat-Software PunkBuster, die Cheats un-

Umfrage Cheater-Anteil

Wie hoch schätzen Sie den Cheater-Anteil in Onlinespielen ein?



Ergebnis: Den Cheater-Anteil schätzen die Teilnehmer über alle Genres hinweg ungefähr gleich hoch ein, auch wenn Dota-Ableger als etwas sicherer gelten. Generell glaubt jeweils über die Hälfte der Teilnehmer, dass maximal 20 Prozent der Spieler schummeln.

Quelle: Onlineumfrage mit 5.000 Teilnehmern

Konsolen-Cheats

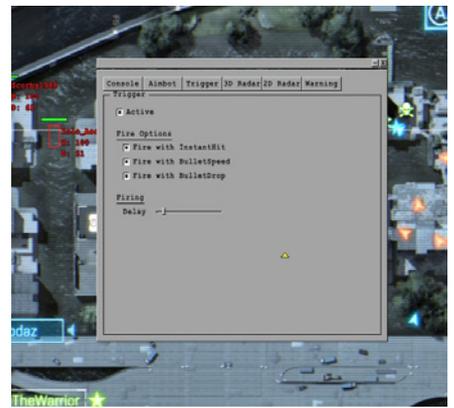
Mit Abstand am meisten geschummelt wird auf dem PC, weil sich darauf problemlos Dateien verändern und Zusatztools installieren lassen. Die geschlossenen Datei-Ökosysteme der Konsolen machen das Betrügen fast unmöglich. Aber nur fast. Beispielsweise kann man sich einen sogenannten Packet Sniffer anschaffen, ein externes Modul, das an die Konsole gekoppelt wird und dann erfasst, welche Daten sie mit den Servern austauscht. Alternativ lässt sich ein PC mit entsprechendem Sniffer-Programm anschließen, die ins Netz gesendeten Daten kann ein Hacker dann manipulieren. Außerdem lassen sich die Konsolen modden, man schraubt an ihrem Innenleben herum und verkabelt beispielsweise das Mainboard neu, damit andere Betriebssysteme sowie Programme aufgespielt werden können. All diese Methoden sind jedoch umständlich und erfordern Vorwissen, erwischt und gesperrt werden kann man trotzdem. »Wer cheaten will, soll sich lieber einen Windows-PC kaufen, das ist günstiger«, sagt auch Samuel Steiner von Hackerbot.net. Noch dazu sind im Netz zwielichtige Gestalten unterwegs, die als Konsolen-Cheats getarnte Schadsoftware feilbieten. Steiner führt aus: »Das sind alles Betrüger, die dir sagen, dass du nur einen USB-Stick mit dem Cheat drauf anschließen musst.« Der PC ist und bleibt für Schummler die komfortabelste Plattform. Zum Leidwesen der ehrlichen Spieler.



Schummeln auf den Konsolen ist möglich: In **Grand Theft Auto Online** erschlichen sich Hacker Unsummen von Geld.



Für die Konsolenversion von **Call of Duty Ghosts** gibt es angeblich Cheats zum Download. Doch die sind gefälscht.



Bei vielen Betrugstools lassen sich die **Cheat-Einstellungen** komfortabel in einem Menü festlegen.

terbinden soll. Auf Steam soll Valves hausinternes System VAC (Valve Anti Cheat) die Spieler vor Hackern schützen. Warum greifen diese Schutzmechanismen ins Leere?

»Gegen Cheater vorzugehen, kostet Geld, das allerdings keinen direkten Umsatz bringt«, erklärt Teut Weidemann den Umstand, dass sich viele Entwickler bei der Betrugsbekämpfung wenig Mühe zu geben scheinen. Weidemann ist einer der ersten professionellen deutschen Spieledesigner, hat unter anderem den Online-Shooter **Söldner: Secret Wars** (2004) veröffentlicht und weiß, wo bei vielen Studios und Publishern die Prioritäten liegen. Zuletzt arbeitete er am browserbasierten **Siedler Online**. »Anti-Cheat-Mechanismen einzubauen, bedeutet einen großen Aufwand. Nur erfahrene Teams wissen, wie das überhaupt geht. Und die Publisher machen es sich einfach. Die lizenzieren beispielsweise PunkBuster – und das war's! Was sie nicht wissen, ist, dass PunkBuster gegen »Noobies«, gegen Anfänger schützt, aber nicht gegen professionelle Cheat-Entwickler.« Samuel Steiner kann das bestätigen. Unerfahrene Cheater findet man auf der Seite **MPGH.net**, dem wahrscheinlich größten Cheat-Forum. Dort laden sie kostenlose Cheats runter, die manchmal funktionieren, manchmal aber vollgepackt sind mit Viren. Einen Rechner hat Steiner so schon verloren. »Wenn man Gratissachen benutzt, wird man schnell gebannt. Wenn man hingegen für einen Hack zahlt, hat man keine Probleme«, erklärt Steiner.

»Bei mir merkt nie jemand etwas«

Wie professionelles Cheaten funktioniert, möchten wir im Selbstversuch herausfinden. Wir bitten Steiner um Hilfe, er empfiehlt uns eine einschlägige Website, deren Namen wir lieber

unerwähnt lassen – wir wollen ja niemanden zum Betrügen verleiten. An unserem Ziel erwartet uns keine Schattenwelt, kein schummriger Schwarzmarkt, keine HTML gewordene **Star Wars**-Cantina: Die Seite sieht aus wie jedes beliebige Spieleforum: Fadenkreuze, Spiele-Icons, ein Link zu einer Facebook-Präsenz. Um die hausinterne Betrugssoftware zu nutzen, müssen wir uns erst im Forum anmelden. Im groß beworbenen Kaufmenü haben wir dann die Wahl zwischen mehreren Cheat-Abos. Drei Monate **Call of Duty** mit der kompletten Serie seit **Call of Duty 2** gibt es im Sonderangebot für 40 Euro. Für Cheats in Early-Access-Titeln wie **Rust** oder **DayZ** zahlt man etwas weniger, für besonders beliebte Spiele wie **Battlefield** etwas mehr. Das Komplettpaket mit allen unterstützten Spielen kostet 15 Euro pro Woche. Gezahlt wird komfortabel und fast schon erschreckend gewöhnlich per Paypal. Wenige Minuten nach Zahlungseingang bekommen wir eine private Nachricht. Darin enthalten: der Download-Link und Installationsanleitungen in mehreren Sprachen, darunter Deutsch. Die Cheat-Software lässt sich leicht einrichten, um sie nutzen zu können, müssen wir uns allerdings mit meinem Foren-Account einloggen. Selbst Schummelprogramme kommen heutzutage nicht ohne Kopierschutz aus. Die Software selbst entpuppt sich als schmucklos und funktional. Aus einer langen Liste von Spielen suchen wir uns ein passendes aus und laden die Cheat-Dateien runter. Wenn wir das Tool beim Spielstart laufen lassen, »injiziert« es den Cheat direkt in die Programmdateien. Per Tastendruck können wir dann

Direkt in der Spielansicht zeigt uns dieser Hack für Battlefield 4 die Positionen aller Spieler an – sehr nützlich, wenn man im **Bomber** sitzt.



Umfrage Cheater-Geständnis

Haben Sie schon einmal in einem Onlinespiel gecheatet?



Ergebnis: Das kommt überraschend, fast ein Viertel der Umfrage-Teilnehmer haben schon mal in einem Onlinespiel betrogen.

Haben Sie in einem Online-Shooter gecheatet?



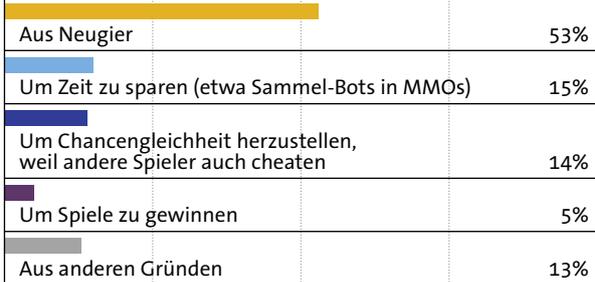
Ergebnis: Drei Fünftel der Teilnehmer, die schon einmal in einem Onlinespiel geschummelt haben, haben das in einem Shooter getan.

Haben Sie in einem anderen Onlinespiel gecheatet, etwa in einem MMO oder in einem Dota-Ableger?



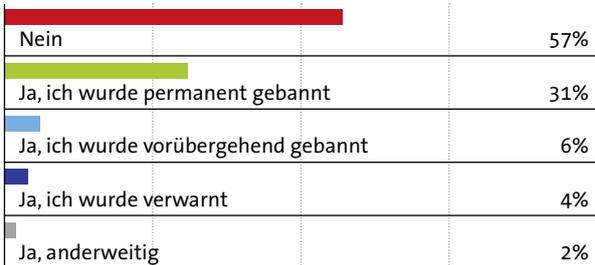
Ergebnis: Online-Shooter sind bei Cheatern offensichtlich deutlich beliebter als andere Genres, weniger als ein Drittel der Schummler sind beispielsweise in MMOs oder Dotas aktiv.

Warum haben Sie den Cheat verwendet?



Ergebnis: Über die Hälfte der Cheater haben die Betrugstools eingesetzt, weil sie wissen wollten, wie sich das anfühlt. Auch Zeitersparnis oder Ärger über andere Betrüger verleiten zum Schummeln. Der unbedingte Siegeswille motivierte hingegen nur einen Bruchteil der von uns befragten Cheater.

Wurden Sie fürs Cheaten bestraft?



Ergebnis: Die Erfahrungen von fast 60 Prozent der Teilnehmer decken sich mit unseren eigenen im Schummel-Selbstversuch, das Cheaten blieb unentdeckt und straffrei.

Quelle: Onlineumfrage mit 5.000 Teilnehmern

direkt im Spiel ein Menü aufrufen, das uns alle relevanten Parameter mit Schieberegler bestimmen lässt. Wie lange soll der Aimbot warten, bevor er sich aufschaltet? Auf welche Bereiche soll gezielt werden? In welcher Farbe sollen die Rechtecke erstrahlen, die uns die Position aller Spieler durch Wände hindurch verraten? Wie »hacken« fühlt sich das nicht an, es ist erstaunlich leicht. Professionelles Cheaten ist barrierefreies Cheaten. Wir folgen Samuel Steiners Rat, deaktivieren auffällige Kopfschüsse und stellen den Aimbot auf 0,2 Sekunden Verzögerung. Niemand scheint etwas zu merken. Beim Start der Partie meldet das Spiel eine Anti-Cheat-Prüfung, die bleibt aber folgenlos. Erwartet haben wir etwas völlig anderes. Eine sofortige Sperrung unseres Accounts zum Beispiel. Stattdessen passiert nichts. Ist PunkBuster machtlos?

»Die Messlatte liegt heute viel höher«, sagt Tony Ray, »in den späten 90ern konnte jeder Skripte runterladen und damit Hacks für so gut wie jedes Multiplayer-Spiel erstellen. Heutzutage müssen Cheat-Autoren ziemlich fortgeschrittene Programmierer sein.« Ray ist der Chef von Even Balance Inc. und hat bereits anno 2000 mit PunkBuster eines der ersten Anti-Cheat-Tools entwickelt. Denn ihn und seine Mitstreiter nervte damals die Betrügerflut im Multiplayer-Modus von **Half-Life**. Valve jedoch verweigerte Rays Team die Unterstützung und trieb lieber sein eigenes Anti-Cheat-System VAC voran –

selbst das Angebot der PunkBuster-Macher, ihr Tool für einen symbolischen Dollar in Steam zu integrieren, schlugen Gabe Newell & Co. aus. Ray und seine Mitstreiter gaben nicht auf, gründeten Even Balance und strickten PunkBuster zur allgemein verwendbaren Betrugsbekämpfungs-Software um. Heute ist es das meistgenutzte Anti-Cheat-Tool. Hersteller, die Even Balance anheuern, bezahlen monatlich für deren Service und müssen Punkbuster fest im Spiel verankern. Dann scannt es unter anderem im Arbeitsspeicher der Spieler nach bekannten Betrugsprogrammen. Ray, der Schummler gerne als »kleine Versager« bezeichnet, führt aus: »Die meisten Cheats sind heutzutage kommerziell, die Betrüger bezahlen auch noch dafür. Trotzdem werden sie immer noch erwischt.« Außer, wenn sie – wie

wir selbst – nicht erwischt werden. Der Sinn eines Schutzwalls sollte ja die schnelle und automatische Bekämpfung aktiver Cheater sein, doch bei unserem Selbstversuch blieb PunkBuster still. Tony Ray jedoch besteht darauf, dass seine Software funktioniert. »Die meisten kommerziellen Seiten erwecken einen falschen Eindruck, weil sie ihre Foren aggressiv moderieren«, winkt Ray ab. »Wir überwachen die Foren und sehen, dass sich die Cheat-Käufer ständig beschweren, weil sie erwischt wurden, obwohl die Seite hundertprozentige Sicherheit »garantiert«. Doch die Betreiber löschen diese Einträge, damit Kunden nicht abgeschreckt werden.« Überprüfen lässt sich das schwer. Allerdings sieht man Cheat-Entwickler, die PunkBuster regelrecht auslachen. Beispielsweise knipst Tony Rays Software automatisch Bilder des



Garry Newman (rechts) klagt über die Cheater-Flut in **Rust** – dabei ist sein Survival-Spiel gerade erst in der Alpha-Phase.

Umfrage Strafen

Wie sollten Cheater beim ersten Vergehen bestraft werden?

Permanenter Bann	54%
Vorübergehender Bann	36%
Verwarnung	6%
Andere Strafe oder gar nicht	4%

Ergebnis: Über die Hälfte der Teilnehmer sind der Meinung, dass Cheater hart bestraft und permanent gesperrt werden sollten. Blöd nur, dass diese harten Maßnahmen manchmal die Falschen treffen – nämlich komplett unschuldige Spieler.

Wurden Sie schon einmal in einem Onlinespiel fürs Cheaten bestraft, obwohl sie nicht gecheatet haben?

Ja, ich wurde permanent gebannt	16%
Ja, ich wurde vorübergehend gebannt	18%
Ja, ich wurde verwarnet	12%
Ja, anderweitig	5%
Nein	49%

Ergebnis: Rund die Hälfte der Teilnehmer wurde schon einmal bestraft, obwohl sie gar nicht geschummelt haben. Die aktuellen Anti-Cheat-Tools haben also klare Schwächen.

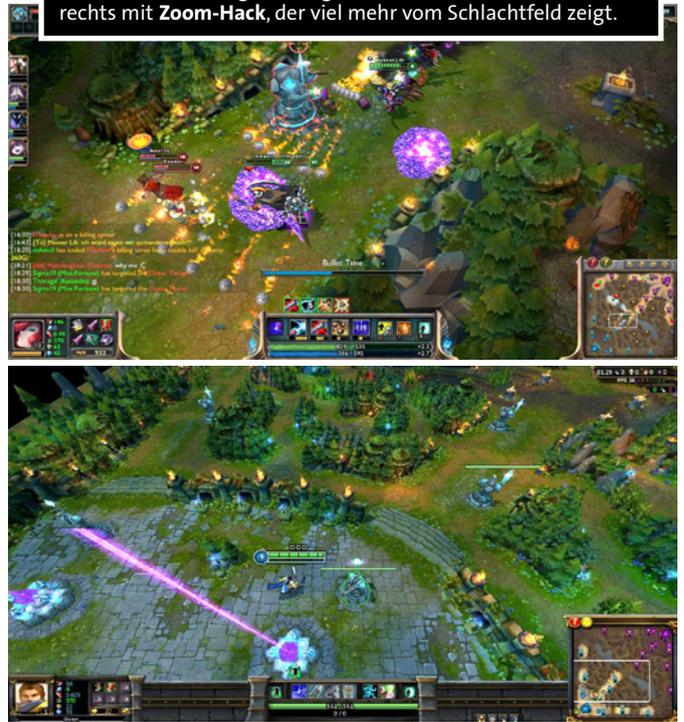
Quelle: Onlineumfrage mit 5.000 Teilnehmern

laufenden Spiels und wertet sie dann aus. Sind darauf irgendwelche Hacks zu sehen, werden Spieler gebannt. An sich eine clevere Methode, dennoch grinsen moderne Cheat-Entwickler da nur müde. Denn ihre Programme manipulieren die PunkBuster-Screenshots einfach nebenher im laufenden Betrieb. Gerade solche fortgeschrittenen Methoden bereiten vielen Entwicklern große Probleme.

»Es ist außer Kontrolle«, beschreibt Garry Newman die Situation in seinem Survival-Spiel **Rust**. Darin versuchen Online-Spieler, in einem lebensfeindlichen Tal zu überleben. Sie jagen Tiere, basteln Waffen und konstruieren behelfsmäßige Hütten aus Holz, um sich vor anderen Spielern zu schützen. Doch einige davon spielen nicht fair. Auf vielen Servern – teilweise sogar auf den offiziellen Servern des Entwicklerteams – haben Cheater kleine Imperien des Schreckens errichtet, die den blutigen Überlebenskampf noch gemeiner werden lassen. Von gewaltigen Türmen, die gewöhnliche Spieler nicht errichten könnten, fliegen **Rust**-Cheater per Flug-Hack über die Karte und jagen Anfänger. Werden sie beschossen, beschleunigen sie ihren Charakter auf irrsinnige Geschwindigkeiten und flüchten. **Rust** läuft über Steam, vor Cheats schützen sollte es eigentlich Valves eigenes System VAC. Das funktioniert aber nicht. »Unsere Idealvorstellung ist, die Anti-Cheat-Arbeit an jemand anderen abzugeben«, sagt Newman »Wir sollten uns auf das Spiel konzentrieren, nicht darauf, Betrüger zu bekämpfen.« Wenige Tage nach unserem Interview baut Newman trotzdem sein eigenes Anti-Cheat-Tool in **Rust** ein: CheatPunch. An einem Wochenende werden 4.621 Spieler durch CheatPunch gesperrt. Doch bereits wenige Tage später haben die Cheater ihre Programme aktualisiert. Auch im von uns getesteten Tool ist **Rust** schnell wieder dabei. Logisch, die Hacker haben ihren guten Ruf zu verlieren. Und ihre zahlende Kundschaft.

Cheat- und Anti-Cheat-Entwickler liefern sich also ein konstantes Wettrüsten. Das bestätigt auch eine der seltenen Aussagen des Valve-Chefs Gabe Newell zum Steam-System VAC. Auf Reddit schreibt Newell: »Die meisten kommerziellen Cheats müssen sich mit einem Server verbinden, um zu verifizieren, dass der Cheater die Entwickler bezahlt hat. VAC hat nach Cheat-Programmen gesucht, hat dann im DNS-Cache gecheckt, ob die Nutzer auf den dementsprechenden

Oben sehen Sie League of Legends in der normalen Ansicht, rechts mit **Zoom-Hack**, der viel mehr vom Schlachtfeld zeigt.



Cheat-Seiten unterwegs waren und dann nochmal überprüft, ob das Programm versucht, diesen Cheat-Server zu erreichen. So haben wir über 570 Cheater gefunden.« Diese Methode hat 13 Tage lang gewirkt, doch der Kampf geht weiter. Es geht für Valve nicht direkt darum, zu gewinnen – sondern dem Gegner die Arbeit so schwer zu machen, dass er das Handtuch wirft. »Diese Cheats sind teuer zu erstellen und es ist teuer, sie aufzuspüren. Wir wollen, dass ihre Entwicklung teurer wird als der Umsatz, den Hacker damit machen«, erklärt Newell. Laut Schätzungen ist dieses Unterfangen Valve zwei bis vier Milliarden Dollar wert. Man darf also davon ausgehen, dass die Steam-Betreiber mehr Geld und damit einen längeren Atem haben als die Cheat-Entwickler, nach einer besonders eleganten Lösung klingt das aber nicht. Ganz im Gegenteil, denn die teuren Anti-Maßnahmen treffen auch gerne mal die Falschen.

Mitte 2013 entzündete sich die Spielerwut an der Bannwelle Nummer 81518. Zahlreiche Fans wurden permanent aus **Battlefield 3** ausgesperrt, weil sie die Cheat Engine installiert hatten, ein Tool, mit dem Werte und Funktionen modifiziert werden können – allerdings nur in Offline-Spielen. So lassen sich vor allem in älteren Programmen spaßige Experimente anstellen. Doch sobald die Cheat Engine während einer **Battlefield**-Partie aktiv und mit einem beliebigen Windows-Programm verbunden war (der Taschenrechner hat gereicht), wurde PunkBuster aktiv und setzte Spieler auf die Bannliste. Die Betroffenen waren entgeistert. »Ähm ... ja, ich habe die Cheat Engine auf dem Rechner, und das reicht denen schon?«, schreibt ein Betroffener im deutschen PCX-Forum: »Und als Nächstes werde ich noch auf Diebstahl verklagt, nur weil ich dank meines Schraubenziehers theoretisch dazu in der Lage wäre?« Den Opfern der Bannwelle blieb nur der Hilferuf Richtung Even Balance, das je-

Umfrage Kaufverweigerung

Sind Cheater auf den Servern ein Grund, den Nachfolger eines Onlinespiels nicht mehr zu kaufen?

Ja	35%
Nein	65%

Ergebnis: Immerhin ein Drittel der Spieler würde beim Nachfolger nicht mehr zugreifen, wenn sie in einem Online-Titel zu sehr von Cheatern genervt wurden. Das wäre ein empfindlicher Verlust für den Publisher - und eine gute Motivation, bessere Anti-Cheat-Tools zu entwickeln.

Quelle: Onlineumfrage mit 5.000 Teilnehmern

Interview



Cheats für beliebte Spiele sind oft nur eine Suchanfrage entfernt und komfortabel zu bekommen. Doch warum schummeln manche Spieler überhaupt? Wir sprechen mit Samuel Steiner, der für die Website Hackerbot.com Schummelprogramme testet - und dafür natürlich auch selbst in Spielen betrügt.

GameStar Warum cheatest du?

Samuel Steiner Ich mache das, damit ich mich nicht so anstrengen muss, um das Spiel zu erleben. Ich spiele eben nicht, um mich im Wettbewerb mit anderen zu messen, sondern einfach zum Abschalten. Außerdem kann ein Aimbot hier und da auch lustig sein. Ich versuche allerdings, das Erlebnis meiner Mitspieler nicht allzu groß zu beeinflussen. Battlefield 2 war mein erster Shooter, und da wird man vielleicht mal Dritter oder Vierter in einem Match, aber Erster und Zweiter ist unglaublich schwer, weil es eben Hacker gibt. Das wusste ich damals nicht. Das ist wie im Bodybuilding. Die besten nehmen Steroide. Die cheaten!

► Wie hast du die Cheater-Szene erlebt?

◀ Es gibt unterschiedliche Arten von Hackern. Es gibt diejenigen, die dem Klischee entsprechen und im Keller der Eltern leben. Von denen kenne ich mittlerweile ein paar, mit denen ich auch zusammenarbeite. Und dann gibt es diejenigen, die einfach nur fertige Cheats herunterladen. Die unterteilen sich nochmals in Spieler, die das nur zum Spaß machen, sowie Spieler, die Macht ausüben und andere Menschen beherrschen möchten. Machtmenschen sind dann auch die Cheater, die wirklich nerven, die in Call of Duty jeden mit dem Aimbot abknallen und eigentlich allen das Spiel verderben. Das kennen wir doch alle, und von diesem Spielertyp

gibt es viele. Ich wäre froh, wenn das anders wäre. Die geben uns Cheatern nur einen schlechten Ruf.

► Gibt es also gutes Cheaten und schlechtes Cheaten?

◀ Vor allem bei Shootern sind Cheats mehr destruktiv als konstruktiv. Ich persönlich bin in diesem Feld tätig, weil ich Geld verdienen muss, so einfach ist das. Es macht mir nicht wirklich Spaß, in Shootern zu hacken. Ich weiß, wie es ist, auf der anderen Seite zu stehen und abgeschossen zu werden. In MMOs und Free2Play-MMOs, da hatte ich Spaß am Betrügen, in Battlefield und Call of Duty aber eher weniger. Und wenn man mal eine Stunde mit Hacks gespielt hat, dann ist der Spaß irgendwie auch vorbei.

► Nimmt das Cheaten den Spielen ihren Reiz?

◀ Ja, es wird langweilig. Ein großer Teil des Spaßes besteht ja darin, dass es schwer ist, die Leute abzuschießen, dass es schwer ist, diese coolen neuen Waffen freizuschalten. Wann man Hacks verwendet, wird das alles einfach und völlig selbstverständlich. Natürlich gibt es Leute, die dann immer noch Spaß haben. Das ist eine psychologische Sache, etwa weil sie Machtmenschen sind. Als normaler Mensch hast du nicht lange Spaß am Hacken.

► Hast du beim Cheaten kein schlechtes Gewissen?

◀ Ja und nein. Natürlich ist es nicht schön, wenn man anderen den Spaß verdirbt. Als Christ bin ich aber der Überzeugung, dass wir uns mit Wichtigerem beschäftigen können als mit PC-Spielen. Die Hacks minimieren die Zeit, die man im Spiel verbringt – für die Cheater selbst durch die erhöhte Effizienz, für alle anderen, weil ihnen der Spaß verdorben wird. Also führen die Hacks insgesamt zu weniger Spielzeit und damit eventuell zu einer höheren Chance, dass der Spieler über sein Leben nachdenken kann. Es mag nur eine kleine Hilfe sein, aber über Hunderttausende Spielern hinweg macht es hoffentlich einen Unterschied.

doch keine Unterstützung anbieten wollte. Die Chance, den Bann wieder rückgängig zu machen, ist gering. »Die Beschwerden sind wahrscheinlich begründet«, gesteht Tony Ray zu, wiegelt dann jedoch ab: »Die meisten Leute sind einen übermäßig freundlichen Kundenservice gewohnt. Wir arbeiten ganz anders. Jede Einsicht, die wir Cheatern in unsere Prozesse geben, schwächt unser System. Diese Erfahrung haben wir leider schon gemacht.« Even Balance gibt keine Infos preis – und verweigert oft Hilfe. Blöd für Spieler, die gar nichts falsch gemacht hat. »Ich vermute mal, es ist möglich, dass ein Nutzer vergessen hat, die Cheat Engine nach einem Singleplayer-Spiel auszuschalten und dann Battlefield 4 gestartet hat. Oder dass er Cheat Engine gemeinsam mit Battlefield in einen Ordner gepackt hat – aber Nutzer müssen eben verantwortungsvoll handeln, wenn sie einem Multiplayer-Spiel beitreten«, wehrt Ray ab. Selbst schuld also. Wer nicht aufpasst, wird wegen Betrugs gebannt, während echte Cheater ungestraft davonkommen, zumindest eine Zeit lang. Immer wieder spülen Bannwellen unschuldige Spieler zu Hunderten aus **Battlefield**, **Call of Duty** und anderen Online-Spielen. Doch wenn es so schwierig ist, Cheats zu unterbinden, warum weichen Publisher dann nicht einfach auf Anwälte aus?

»Das ist so, wie wenn jemand im Schwimmbad wiederholt vom Beckenrand springt, obwohl das verboten ist«, sagt der Rechtsanwalt Stephan Mathé. »Den kann man

rauswerfen, aber viel mehr ist nicht möglich. Grundsätzlich braucht man eine sogenannte Anspruchsnorm, wenn man jemanden verklagen möchte. Die zu finden, dürfte bei Cheatern schwer sein.« Und was ist mit Cheat-Entwicklern? »Da gäbe es theoretisch Anknüpfungspunkte, etwa wenn die Hacks auf verbotene Weise in die urheberrechtlich geschützte Software eingreifen. Dann könnte man gegebenenfalls auf Unterlassung und Schadensersatz klagen. Wenn ein Spiel durch solche Software beeinträchtigt wird und der Betreiber dadurch Schaden erleidet, dann wäre auch das möglicherweise gerichtlich verfolgbare.« Hätte, wäre, könnte, wirklich vielversprechend klingt das nicht.

Stattdessen geraten just die Entwickler von Anti-Cheat-Tools vermehrt ins Visier von Anwälten und Datenschützern. Damit Valves

VAC 570 Cheater stoppen konnte, musste Valve die Browser-Chroniken der Steam-Nutzer durchforsten. »Nein, wir lesen nicht eure Browser-Historie! Eure Porno-Seiten interessieren uns nicht«, schreibt Gabe Newell auf Reddit. Das mag stimmen, die technische Möglichkeit zur Spionage hätte VAC aber. PunkBuster wiederum überwacht wie erwähnt den Arbeitsspeicher, analysiert Bilder des Spielgeschehens und überträgt die IP-Adressen der Spieler. Zugleich speichert das Tool zumindest Teile des Hardware-Profils; Hinweise deuten darauf hin, dass die Seriennummern von Festplatten erfasst werden. Aus dem verwendeten Download- oder CD-Key kann das Schutzprogramm zudem jedem Spieler eine eindeutige Identifikationsnummer zuweisen, die sogenannte GUID (Globally Unique Identifier). In Kombination mit der IP-Adresse und den gespeicherten Hardware-Angaben ließen sich so Spielerprofile basteln, die genau Auskunft darüber geben, wer wie lange was gespielt

Maßnahmen treffen oft die Falschen



Teut Weidemann (rechts) hat unter anderem an **Siedler Online** mitgewirkt, das alle Aktionen der Spieler vom Server überprüfen lässt.



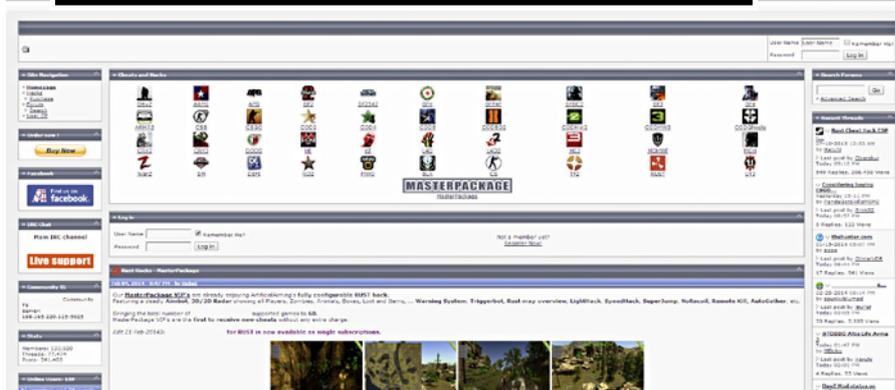
hat – das ist datenschutzrechtlich bedenklich. »Wir scannen keine Festplatten und sammeln keine personenbezogenen Daten, sie werden vom System ausgeblockt und nicht übers Netz gesendet«, beschwichtigt der PunkBuster-Chef Tony Ray und fügt dann hinzu: »Und damit das klar ist: IP-Adressen und Screenshots sind für uns keine personenbezogenen Daten.« Zumindest in Deutschland stimmt das für IP-Adressen jedoch nicht. »Das war lange umstritten und hängt vom Einzelfall ab, zum Beispiel ob es eine statistische oder dynamische Adresse ist. Der herrschenden Meinung nach können sogar beide personenbezogene Daten sein«, erklärt Stephan Mathé. »Grundsätzlich dürfte es so sein, dass das Ausspähen von Kunden-PCs für den Betrieb der Tools kaum notwendig ist, daher dürfte dies unzulässig sein.« Spieler, die diesen Prozessen nicht zustimmen, haben aber Pech. Die Nutzung von Anti-Cheat-Tools wie PunkBuster ist zwar theoretisch freiwillig, ohne Einwilligung zum Rechnerscan kann auf vielen Servern aber nicht gespielt werden. Der Kampf gegen Hacker treibt unschöne Blüten.

»Das ist eine rechtliche Grauzone«, sagt auch Teut Weidemann. Statt Anwälten und Klagewellen hat er eine andere, eine elegante Lösung parat: »Ich würde den Cheat-Entwickler einstellen. Dadurch wäre sein Cheat-Programm weg vom Markt, und ich hätte sein Know-How für meine Anti-Cheat-Programme. Und schon habe ich meine Ruhe.« Das könnte klappen. Die Hacker-Teams sind klein, mehr

als vier Programmierer arbeiten selten an einem Tool. Auf der von uns besuchten Seite gibt es sogar nur einen einzigen Programmierer, alle anderen Mitarbeiter kümmern sich um die Kunden. Der Cheat als Bewerbungsmappe ist trotzdem eine Seltenheit.

Wer schummelt, hat von Anwälten nichts zu befürchten, wer Schummel-Tools entwickelt wahrscheinlich auch nicht. Mit Cheat-

Gekauft werden die Cheats in **Foren**, die leicht zu finden sind und aussehen wie jede beliebige Spieleseite – Facebook-Präsenz inklusive.



Bastlern zusammenarbeiten wollen Publisher und Entwickler jedoch kaum. Gegen sie vorzugehen, führt wiederum höchstens zu vorübergehendem Waffenstillstand – bis PunkBuster, VAC und CheatPunch dann eben wieder ausgehebelt werden. Ein verfluchter Teufelskreis, die Atmosphäre in vielen Spielen regelrecht vergiftet. »Man fragt sich einfach immer irgendwie, ob alles mit rechten Dingen zugeht. Da wird man vielleicht Dritter oder Viertes in einem Match, aber Erster oder Zweiter ist unglaublich schwer. Weil es eben stets Hacker gibt«, sagt Samuel Steiner, der selbst Hacks benutzt. Ob diese Einschätzung stimmt, können wir nicht überprüfen, sie illustriert aber ein grundsätzliches Problem: Wenn jeder Spieler jederzeit Cheats benutzen kann, wie

kann man dann sicher sein, dass das nicht jeder auch tatsächlich tut? Selbst Spieler, die einfach gut sind, sehen sich

daher oft mit Betrugsvorwürfen konfrontiert; der Verdacht ist immer da. »Das entzweit die Community, stört den Spaß und es kostet eventuell sogar Kunden«, sagt Teut Weidemann. »Man hört dann auf, online zu spielen, und kauft sich die Fortsetzung nicht mehr. Publisher unterschätzen diesen Effekt.« Oder, noch schlimmer: Die Cheat-Opfer fangen selbst an, zu schummeln. Um die Chancen auszugleichen. Wir müssen spon-

tan an den Radsport denken: Die Doping-Skandale von Jan Ullrich, Lance Armstrong und anderen prominenten Fahrern eine verquere Logik offenbarten: Die Sportler griffen zur Spritze, weil sie wussten, dass ihre Konkurrenten ebenfalls dopten. Wenn jeder betrügt, wird der Wettbewerb doch wieder fair, oder? Nein, der Wettbewerb geht kaputt, und der Sport mit dazu. Und das gilt auch für den Sport am Bildschirm, also das Kräffemessen in Onlinespielen. Wenn jeder schummelt, spielt Können keine Rolle mehr. Und Spaß erst recht nicht. Zugleich verliert auch für die Cheater selbst das Spiel seinen Reiz, es fehlt die Herausforderung. Wer wie ein Halbgott durch die Gegner pflügt, hat auf Dauer eher wenig Spaß. Wie also können Spiele sicher werden vor Cheatern?

Um das zu verstehen, muss man erst begreifen, wie moderne Cheats funktionieren. »Beliebte Cheats wie die Leuchtskins, mit denen man Spieler durch Häuser hindurch sieht, zeigen, dass das Spiel alle Informationen über alle Spieler immer an alle Clients schickt«, erklärt Teut Weidemann. »Mein Client weiß, wo alle anderen Spieler stehen.« Heißt: Alle relevanten Informationen befinden sich auf dem eigenen Rechner, er zeigt sie nur normalerweise nicht an. Der Cheat muss da nur einen kleinen Kippschalter umlegen, von unsichtbar auf sichtbar schalten. Besonders raffinierte Betrügereien verändern dabei nicht einmal den Client.

»Ich würde den Cheat-Entwickler einstellen«

Das sagt der Anwalt



Anti-Cheat-Maßnahmen treffen manchmal die Falschen. Was man dann tun, wenn der eigene Account ungerechtfertigt gesperrt wird, weiß Stephan Mathé. Mathé ist Fachanwalt für Wirtschafts- und Medienrecht bei der Hamburger Kanzlei Rode Mathé und war früher Produktmanager bei Eidos.

GameStar Wer muss beweisen, dass ich gecheatet habe?

Stephan Mathé Das Vorliegen dieser Vertragsverletzung muss im Streitfall derjenige beweisen, der sich darauf beruft, also der Publisher. Im Falle eines ungerechtfertigten Bans (etwa bei einem gehackten Account) sollte sich der betroffene Spieler also zunächst an den Support wenden und darlegen, warum ihn keine Schuld trifft. Der Support hat Einblick in den Account und kann in der Regel nachvollziehen, wo das Problem liegt. Vor allem bei großen Spielen hat man dann aber mit dem Support eines externen Anti-Cheat-Dienstleisters zu tun. Und der ist selten hilfreich. Be-

sonders bei großen Onlinespielen kann der Support zudem überlastet sein. Eine angemessene Zeit zur Reaktion muss man dem Spielbetreiber schon geben. Die rechtliche Situation ändert sich dadurch aber nicht. Kommt der Spieler beim externen Dienstleister nicht weiter, kann er sich direkt an den Publisher wenden, denn der ist ja sein direkter Vertragspartner.

► Was kann ich machen, wenn nichts mehr weiterhilft?

◀ Stellt der Publisher auf stur, kann der Spieler als letztes Mittel auf Vertragserfüllung klagen. Er müsste dann nur vortragen, dass ihm der Publisher die Möglichkeit zum Spielen genommen hat und der Publisher müsste beweisen, dass dies zu Recht geschah. Kann er das nicht, gewinnt der Spieler und darf weiterspielen. Alternativ könnte sich der Spieler auch überlegen, dass durch den unberechtigten Ban das Vertrauensverhältnis insgesamt so zerrüttet ist, dass er stattdessen sein Geld zurückhaben möchte. Damit könnte man durchaus erfolgreich sein. Nur müsste sich der Spieler dann den Betrag anrechnen lassen, den er bereits in der Vergangenheit abgespielt hat. Er bekäme also nicht alles zurück.

»Professionelle Cheat-Entwickler hängen das Programm so in Windows ein, dass es außerhalb des Clients funktioniert«, führt Weidemann aus. »Ich erinnere mich an Hacks, bei denen das Programm die Grafikkarte ausgelesen und an optischen Mustern erkannt hat, wo man im Level gerade stand. Dann gab das Tool entsprechende Maus-Impulse ab, um automatisch auf die richtigen Stellen zu zielen. Das kann gar nicht entdeckt werden.« Je mehr Berechnungen Spiele auf den eigenen Rechner abladen, desto anfälliger werden sie also für Cheats. Gibt es überhaupt noch Spiele, in denen nicht betrogen werden kann? Ja, und sie haben sogar etwas gemeinsam.

»In Spielen von Wargaming kann man nicht cheaten«, sagt der Community Manager Enrico Loenicker über **World of Tanks**. »Alle spielrelevanten Berechnungen werden auf unseren Servern durchgeführt und nicht auf den Rechnern der Spieler. Das heißt, dass es schlicht unmöglich ist, die Ladezeit zu verkürzen, Unmengen an Gold zu bekommen oder unzerstörbar zu werden. »Hacks« im klassischen Sinne, wie man sie vielleicht aus anderen Spielen kennt, sind nahezu unmöglich.« Auch **League of Legends** lässt dem Client nur wenig Spielraum und gilt somit als gut geschützt. »Es ist unglaublich schwer, dieses Spiel zu hacken«, sagt Samuel Steiner. »Der eigene Rechner kennt einfach die Positionen der Gegner nicht. Alles, was im Fog of War liegt, ist unklar.« Tatsächlich gibt es weitaus weniger Seiten, die Cheats für **World of Tanks** oder **League of Legends**

Der Cheat legt einen kleinen Schalter um

anbieten als für andere Multiplayer-Spiele, obwohl beide zig Millionen Fans haben. Zwar gibt es Angebote, die drehen sich aber meist um In-game-Währung oder Rangaufstiege. Ausnahmen gibt es jedoch auch bei **World of Tanks**. Weil der Panzer-Shooter den Ursprung der Tracer-Linien von Artilleriefeuer im Client berechnete, entstand prompt ein Cheat, der die Position eigentlich unsichtbarer Artilleriegeschütze anzeigte. Wargaming musste das Tracer-F Feuer zeitweise komplett abstellen. Auch **League of Legends** ist nicht völlig sicher: »Man kann den Zoom hacken, sodass man einen größeren Kartenausschnitt sieht, und man kann per Bot Talentkombos automatisch auslösen lassen«, sagt Steiner. Auch die Reichweite der eigenen Angriffe lässt sich mit einem Cheat anzeigen. »So bekommt man mehr Informationen über den eigenen Charakter und was er machen kann. Aber das ist nicht wirklich ein Hack, oder?« Nun, kein klassischer Hack im Sinne eines Aimbots oder ESP, aber dennoch ein unfairer Vorteil und Gift für den Wettbewerb. Besser als die chaotische Cheat-Situation in vielen Shootern klingt das jedoch allemal. Warum lassen nicht noch mehr Spiele alle relevanten Informationen serverseitig berechnen?

»Weil auch das Aufwand bedeutet. Es kostet Rechenzeit, es kostet Bandbreite«, sagt Teut Weidemann. Serverbasierte Spiele sind komplex, sie erfordern einen perfekt angepassten Netzcode und leistungsstarke Server, um stabil genug für alle Nutzer zu laufen. »Das sparen sich viele Publisher. Auf Kosten der Kunden.« Weidemann möchte es mit Blue Byte anders machen: »Deswegen sind bei uns Anti-Cheat-Tools von Anfang an eingeplant gewesen. Wenn eine Betrügerei bekannt wird, dann schrillen die Alarmglocken, und sie wird innerhalb von 24 Stunden ausgemerzt. Da machen wir auch Hotfixes, fahren also die Server runter. Das ist gefährlich für ein Onlinespiel, weil es einen ganzen Server kaputt machen kann. Bei unserem Siedler Online ist es so, dass alle Entscheidungen vom Server getroffen werden. Der Client kann also nichts tun, das der Server nicht erlauben muss.« Wichtig ist auch, und das wird Tony Ray und Even Balance Inc. wahrscheinlich maßlos ärgern, dass Publisher und Entwickler die Anti-Cheat-Arbeit selbst in die Hand nehmen. »Das wird alles intern geregelt«, sagt Enrico Loenicker über Wargaming. »Wir sind die Experten für unsere Produkte. Das Thema ist uns wichtig, und daher möchten

Cheat-Historie

Cheats haben Tradition, schon die ersten Entwickler bauten Betrügereien in ihre Spiele ein. Allerdings nicht für Spieler, sondern für die Entwickler selbst. Cheats erleichterten es, bestimmte Aspekte des Spiels zu testen. Einer der ersten Cheat-Codes stammt aus Matthew Smiths Jump&Run **Manic Miner**, das anno 1983 für den ZX Spectrum erschien: Wer die Zahl 6031769 (übrigens Smiths Führerscheinnummer) eingab, konnte alle Levels direkt anspringen, statt stets von vorne anfangen zu müssen. Das nutzen die Spieler natürlich aus, in Spieleheften wurden damals regelmäßig Cheatcodes abgedruckt. Zudem entstand eine kleine Cheat-Industrie, die spezielle Betrugsmodule für die Konsolen produzierte. Die Modulserie »Game Genie« erlaubte NES-Spielern unter anderem, abgeschaltete Spielelemente wieder zu aktivieren. Gebaut wurde »Game Genie« nicht von zwielichtigen Hinterhofbastlern, sondern von Codemasters – der britische Publisher und Entwickler ist heute für seine F1-Rennspiele und die Colin McRae-Serie bekannt. Die goldenen Zeiten des »offiziellen« Betrugs sind jedoch vorüber, auch wenn es nach wie vor im Laden erhältliche Cheat-Module gibt, etwa für das Nintendo DS. Von den Entwicklern eingebaute Schummelcodes dienen heute aber allenfalls als Easter-Eggs oder sind nur in speziellen, unfertigen Versionen verfügbar. Dank besserer Tools brauchen die Entwickler sie nämlich nicht mehr unbedingt zum Testen. Wer trotzdem noch einmal in Nostalgie schwelgen möchte, kann in den Fußzeilen dieses Reports berühmte Cheatcodes nachlesen.



Codemasters **Game Genie**-Modul erlaubte NES-Fans, ihre Spiele zu manipulieren.



wir es nicht in externe Hände geben. Das erhöht gleichzeitig die Effizienz und verringert natürlich das Risiko, dass Informationen zu unseren internen Werkzeugen und Abläufen nach außen dringen.« Weidemann stimmt zu: »Wer PunkBuster geknackt hat, hat alle Spiele geknackt.« Eigene Lösungen zeigen hingegen – wenn auch nur kurzfristig – Erfolg, etwa Garry Newmans CheatPunch.

»Wichtig ist, dass die Community sieht: Die tun etwas dagegen«, sagt Teut Weidemann. Denn selbst wenn in einem Spiel nur wenige Cheater aktiv sind, vergiftet das Misstrauen die Atmosphäre. Dieses Misstrauen führt zu wütenden Cheat-Vorwürfen, zu überzogenen Bannwellen. In den Quartalszahlen der Aktionärsversammlung sieht man das vielleicht nicht, in Foren und in Chats dafür umso mehr. Spiele entwickeln sich weiter. Vom Einzelprodukt zum Service, der gepflegt werden muss. Die eigene Plattform zu sichern, ist eine Grundaufgabe der Publisher und eine, der viele bislang kaum nachkommen. Zu Lasten der Spieler, denen kopfschießende Halbgötter den Spaß verderben. Dennis Kogel / GR



Enrico Loenicker (rechts), der Community Manager von Wargaming, ist sich sicher: In **World of Tanks** wird nicht betrogen.

