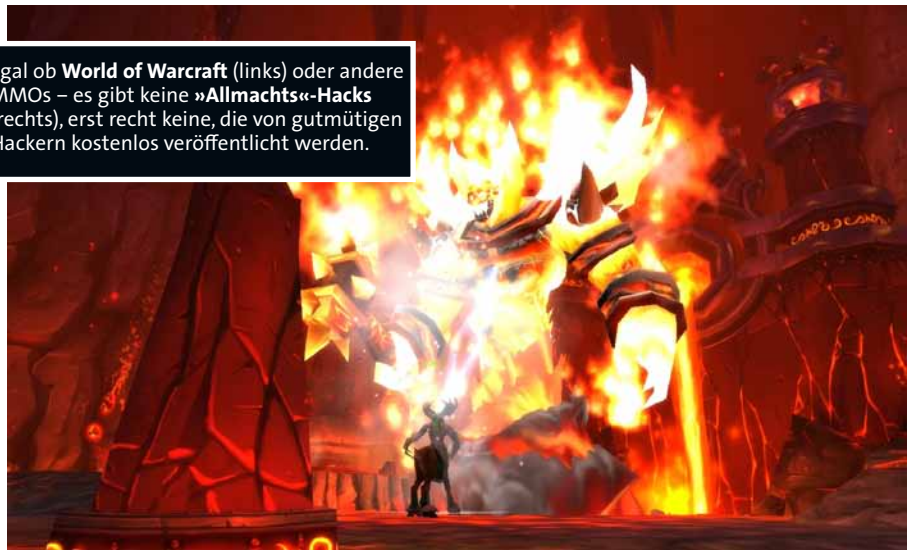
Der Feind in meinem Account

Cybergangster jagen nicht nur nach Online-Banking-Daten, längst sind auch Spieler und ihre Accounts lukrative Ziele der Schattenwelt. GameStar zeigt, wie die Kriminellen arbeiten, was Steam, WoW & Co. so attraktiv macht und wie Sie sich schützen können. Von Moritz Jäger

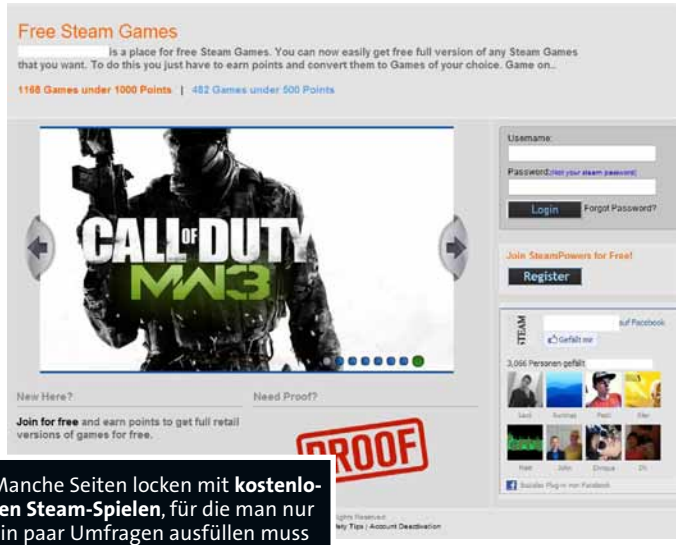
Das Angebot klingt verlockend: Ein Hacker hat ein Programm geschrieben, das den Steam-Kopierschutz aushebelt und dem eigenen Account über 100 geklaute Spiele hinzufügt. Dafür müssen Sie nur das Programm herunterladen (das es natürlich umsonst gibt, angeblich ein »Protestakt« gegen die hohen Spielepreise) und mit administrativen Rechten auf Ihrem System installieren. Den Virenschutz sollen Sie gemäß der Anleitung abschalten, weil Sie ja ein illegales Tool verwenden. Nun noch die Zugangsdaten für Steam eingeben, schon sind alle Spiele freigeschaltet – so zumindest der Plan. Die Realität sieht anders aus: Das Programm bricht mit einer Fehlermeldung ab, Sie zucken mit den Achseln und gehen ins Bett.

Als Sie am nächsten Tag weiterspielen möchten, scheint es wie verhext: Das Steam-Login, das gestern noch einwandfrei funktioniert hat, ist nun scheinbar ungültig. Dazu meldet sich ein Bekannter per Instant Messenger und fragt an, warum Sie denn Ihren jahrelangen Spitznamen geändert haben. Langsam beschleicht Sie ein dumpfes Gefühl: Ihr Account wurde gehackt. Ihr Account mit allen Spielen. Ihr Account, in dem Sie der Bequemlichkeit halber natürlich Ihre Zahlungsdaten für Bankeinzug oder Kreditkarte abgespeichert haben. Und wo haben Sie das Steam-Passwort sonst noch im Einsatz? Bei Facebook? Twitter? E-Mail-Konten?

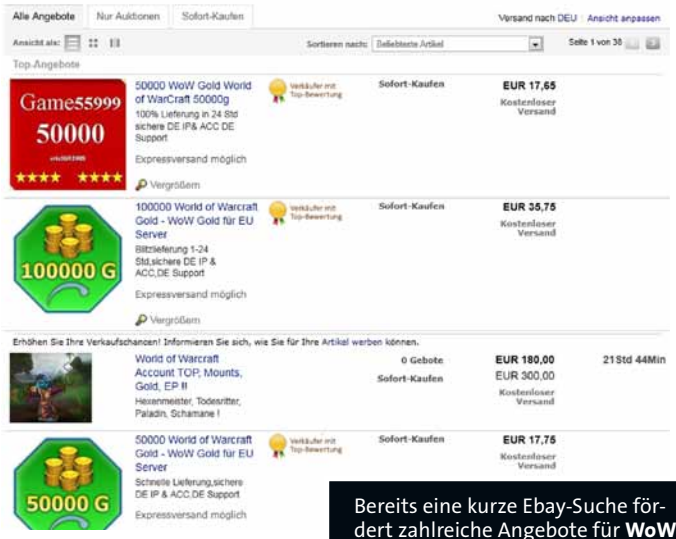


Egal ob **World of Warcraft** (links) oder andere MMOs – es gibt keine **»Allmachts«-Hacks** (rechts), erst recht keine, die von gutmütigen Hackern kostenlos veröffentlicht werden.

 2010 schätzte Symantec den Wert eines gestohlenen E-Mail-Kontos auf 1 bis 18 US-Dollar, 100 Kreditkarten gibt es ab 100 US-Dollar.



Manche Seiten locken mit **kostenlosen Steam-Spielen**, für die man nur ein paar Umfragen ausfüllen muss – inklusive Facebook-Plugin und »Beweis«-Stempel.



Bereits eine kurze Ebay-Suche fördert zahlreiche Angebote für **WoW-Gold** zutage – nicht alle Münzen stammen aus legalen Quellen.

Dieses Beispiel ist nur einer von vielen Wegen, auf denen Kriminelle Systeme infizieren. Die Attacken sind keineswegs auf Steam beschränkt, im Gegenteil: Mal locken die Tools mit Zugängen zu Betas von **Diablo 3** oder **Halo 4**, mal versprechen sie Gold für **World of Warcraft**, mal kostenlose Microsoft-Punkte für Xbox Live, mal Gegenstände in **Farmville**. All diesen Angriffen ist gemein: Die Nutzer bekommen nicht, was ihnen versprochen wird. Sondern jede Menge Ärger.

Denn die Tools scannen persönliche Daten und spielen ungehindert Schadsoftware (Malware) auf die Rechner der Opfer – die meist im ersten Installationsschritt die Sicherheitsfunktionen (Virenscanner, Firewall etc.) ihrer Systeme abgeschaltet haben. »Phishing« nennt sich diese Art des Kontenklaus, das »Angeln« nach Zugangsdaten. Ist der Account erstmal in fremden Händen, hilft meist nur noch ein Hilferuf an den Support. Wir klären auf, wie die Kriminellen arbeiten, was Steam, **WoW** & Co. so attraktiv macht – und wie Sie sich schützen können.

Dass sich die Kriminellen nun vermehrt auf Spieler stürzen, kann Christian Funk vom Virenscanner-Hersteller Kaspersky durchaus nachvollziehen – es geht natürlich ums Geld: »Cyberkriminelle haben heutzutage nur noch finanzielle Motivation. Spieler-Konten werfen zwar im Vergleich zu Kreditkartendaten oder Online-Banking-Trojanern weniger Profit ab, dafür ist das Risiko, erwischt und verurteilt zu werden, deutlich geringer.« Denn nur in wenigen Ländern gibt es entsprechende Gesetze; Ermittlungsbehörden lächeln meist nur milde, wenn der geliebte **World of Warcraft**-Paladin gestohlen wurde. »Mitgeschnittene Zugangsdaten können automatisiert bei anderen Internetservices wie sozialen Netzwerken, Auktionshäusern, Mailprovidern oder Onlineversendern ausprobiert werden und so weitere Konten offenlegen«, führt Funk weiter aus. Heißt: Wenn ein Passwort erstmal geklaut ist, ist kein Account mehr sicher, der dieselben Zugangsdaten verwendet. Und die Bedrohung wächst: Aktuell kenne man bei Kaspersky rund 2,7 Millionen Schädlinge, die auf Spieler zielen.

Candid Wüest, angestellt beim Kaspersky-Konkurrenten Symantec, warnt neben den eigentlichen Schadprogrammen auch vor häufigen Attacken über manipulierte Webseiten. Seine Firma entdeckt täglich über 13.000 neue (!) Seiten, die Malware verbreiten. Diese Seiten attackieren den Browser des Besuchers mit Hilfe so genannter Drive-By-Attacken. Dabei reicht es, wenn der Nutzer eine speziell präparierte Website lediglich besucht – im Hintergrund klopft die Malware dann den Browser und die installierten Plugins auf Schwachstellen ab. Wenn das Angriffstool fündig wird, nutzt es die Schwachstellen automatisch aus und infiziert den Rechner. Relativ neu ist Drive-By-Spam: Dabei wird der Rechner bereits infiziert, wenn man eine HTML-Mail nur ansieht. Lösung: E-Mails als Text öffnen.

Grundsätzlich verfolgen die Kriminellen laut Candid Wüest zwei Methoden: »Klassische Phishing-Angriffe locken Opfer per E-Mail oder über anderen Messaging-Dienste auf nachgebaute Webseiten, um Benutzername und Passwort zu entlocken. Eine andere weit verbreitete Art sind lokale Trojaner, die beispielsweise per Keylogger eingegebene Passwörter aufzeichnen. Beide Attacken haben es in erster Linie auf die Accounts abgesehen, sammeln zum Teil aber auch weitere Daten wie Mail-Adressen oder die Passwörter anderer Anwendungen.«

Neben den »richtigen« Spielern sieht Alexander Vukcevic von der Software-Firma Avira auch Casual-Gamer im Visier. Denn Casual Games sind sehr zugänglich und zahlreich, sprechen also eine große Zielgruppe an. »Kriminelle können Spieler mit Bonusinhalten locken, für die dann höhere Beträge vom Konto abgebucht werden, ohne dass der Anwender einer Bezahlung bewusst zugestimmt hat«, führt Vukcevic aus. Gerade im Bereich der mobilen Spiele sei dies ein gängiger Betrugsfall. Sean Sullivan vom Virenscanner-Hersteller F-Secure nennt noch eine andere Gefährdung: »Spieler suchen im Web nach Informationen über ihre Lieblingsspiele, was sich Kriminelle zu Nutze machen. Im Fall von **Farmville** etwa wurden 2010 die Suchergebnisse bei Google & Co. gezielt mit Seiten infiltriert, die neben vermeintlichen Infos vor allem Trojaner enthielten. Diese Schadsoftware versuchte, die Zugangsdaten von Facebook auszuspionieren, um anschließend an der Pinnwand der Nutzer Spam zu veröffentlichen.«

2,7 Millionen Viren lauern auf Spieler

Gekaperte Spielekonten bringen auf mehrere Arten Gewinn. Der Trend zu DLCs und In-Game-Verkäufen etwa sorgt dafür, dass viele Nutzer ihre Zahlungsdaten hinterlegen, um sie nicht jedes Mal neu eingeben zu müssen. So können die Kriminellen Kreditkarten- und Bankdaten sammeln. Allerdings heben sie das Geld nur selten direkt ab, diesen Job erledigen so genannte Money Mules. Dabei handelt es sich oft um nichtsahnende Menschen, denen per E-Mail ein Job angeboten wird: Sie müssen Geld auf einem Konto empfangen und an ein anderes überweisen oder über Transferdienste wie Western Union weiterleiten. Wenn einer dieser gutgläubigen Geldwäscher den Behörden ins Netz geht, kann er nur selten die Hintermänner nennen – er ist sich ja oft nicht einmal bewusst, dass er etwas Illegales tut.

Die zweite Gewinnmöglichkeit besteht in virtuellen Gütern. Gold, Items, Charaktere – auf Ebay oder in einschlägigen Foren gibt es für nahezu jedes Online-Rollenspiel zahlreiche Angebote. Vor allem virtuelle Währung wird nicht mehr nur durch die berüchtigten Goldfarmer erwirtschaftet, sondern direkt aus den Accounts gestohlen. Die kriminellen Anbieter überwachen oftmals mehrere gekaperte Spielerkonten, um sie erst dann leerzuräumen, wenn die entsprechenden »Bestellungen« eingegangen sind.

Beim Angriff auf Sonys **Playstation Network** erbeuteten Hacker Anfang 2011 Millionen Kundendaten.

Weitere Umsätze erzielen die Hacker mit zusätzlich abgegriffenen Daten: E-Mail-Konten, andere Passwörter – nahezu alle auf einem PC gespeicherten Informationen finden im Internet Abnehmer. Wenn ein Trojaner auf dem System installiert ist, kann dieses Schadprogramm noch dazu unbemerkt weitere Komponenten nachladen, etwa um den PC einem Botnet hinzuzufügen – also einem verdeckten »Netzwerk«, das für illegale Zwecke genutzt oder vermietet wird – etwa für den Versand von Spam oder Denial-of-Service-Attacken.

Selbst wenn es die Hersteller immer wieder versprechen, gibt es keine Einzellösung, die Spieler vor allen Attacken schützt. Der Trick liegt darin, sich mit möglichst vielen Sicherheitsmaßnahmen zu schützen, ohne dass diese zu umständlich werden. Grundsätzlich sollte auf allen Systemen eine Anti-Malware-Software installiert sein. Ob Sie sich für eine kostenlose oder kostenpflichtige Variante entscheiden, liegt bei Ihnen, Hilfestellungen zur Auswahl bieten Tests wie die unserer Schwesterzeitschrift PC Welt unter GameStar.de/Quicklink/7737. Schlanke Anti-Viren-Software wie Avira Free Antivirus beeinflusst kaum die Systemleistung – Sie können ohne Performance-Einbußen spielen.

Im nächsten Schritt geht es darum, die Angriffsfläche zu minimieren. Hauptziele sind inzwischen Browser und installierte Erweiterungen und Plugins. Dementsprechend ist es egal, welchen Browser Sie bevorzugen, wichtig ist, die aktuellste Version zu verwenden. Gleiches gilt für Plugins wie JavaScript, Flash oder den PDF-Reader. Ein nützliches und kostenloses Tool hierfür ist der Secunia Personal Software Inspector (GameStar.de/Quicklink/ 7738). Der listet alle auf dem Rechner installierten Programme auf und überprüft in einer Datenbank, ob aktuellere Versionen verfügbar sind.

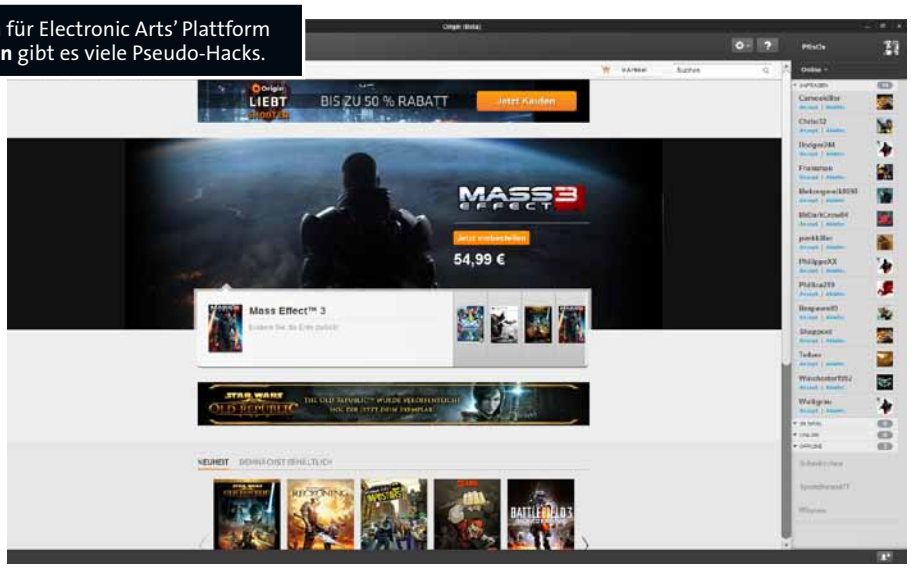
Wenn das System erstmal grundlegend geschützt ist, geht es um den Schutz der Konten. Sinnvoll ist, eine Zwei-Faktoren-Anmeldung zu aktivieren, falls das Konto sie anbietet. Diese Technik schützt normalerweise die externen Zugänge von Unternehmensnetzwerken, verbreitet sich aber inzwischen auch bei Web- und Spieledienssten. So bieten etwa Google Mail, Ebay und PayPal, aber auch Blizzard und Square Enix spezielle Anmelde-Tokens. Die gibt es entweder als Smartphone-Apps oder als Hardware, ein bekannter Vertreter von Letzterer ist Blizzards Battlenet-Authenticator. Wie alle anderen Tokens erzeugt auch dieses schlüsselanhängergroße Gerätchen Zahlenkombinationen, die nur kurze Zeit gültig sind und bei der Anmeldung abgefragt werden. Eine andere Form dieser Technik verwendet Valve mit Steam Guard: Wenn sich ein PC erstmals anmeldet, schickt Steam Guard einen Freischalt-Code an die mit dem Konto verknüpfte Mail-Adresse. Erst nach der Eingabe des Codes wird der Account freigegeben.

Für finanzielle Transaktionen wiederum sollten Sie nach Möglichkeit externe Dienste wie etwa PayPal nutzen. Die haben den Vorteil, dass der Spieleanbieter keinen direkten Zugriff auf Kreditkarten- oder Kontodaten hat. Damit wird der eigentliche Account, selbst wenn er gehackt wird, deutlich uninteressanter. Außerdem sind Sie auch geschützt, wenn die Server des Anbieters direkt gehackt werden. Ein Beispiel dafür ist die Attacke auf Sonys Playstation Network letztes Jahr, bei der die Angreifer Millionen Kontodaten erbeuteten. Auch das Steam-Network wurde Ende 2011 attackiert.

Als Letztes sollten Sie sich dem Problem der mehrfachen Passwörter annehmen, damit ein gestohlener Spiele-Zugang nicht auch noch den Weg zu ihren E-Mails oder ihrem Online-Banking ebnet. Am besten klappt das mit Tools zur Passwort-Verwaltung – etwa den kostenlosen Varianten LastPass (GameStar.de/Quicklink/7739) und KeePass (GameStar.de/Quicklink/7740). Beide Tools speichern Zugangsdaten verschlüsselt ab und füllen sie auf Wunsch direkt ins Eingabefeld – Sie müssen nur ein Master-Passwort definieren und nach dem Browserstart eingeben. Manche Spiele wie **Star Wars: The Old Republic** bieten zudem die Möglichkeit, Sicherheitsfragen zu definieren, die man beim Login beantworten muss.

Gamer sind lukrative Ziele

Die wichtigste Sicherheitsebene ist allerdings ein gesundes Misstrauen. Wenn ein Spieleangebot zu gut, eine Einladung zu verlockend ist, dann ist das höchstwahrscheinlich zu schön, um wahr zu sein. Denn der Spielemarkt ist viel zu groß, als dass die Kriminellen die Spieler künftig in Ruhe lassen würden. Genaue Zahlen zum Schwarzmarkt sind naturgemäß schwer zu bekommen, Christian Funk von Kaspersky versucht sich dennoch an einer vorsichtigen Schätzung. 2011 hat er eine Hochrechnung für ein »großes Online-Rollenspiel« aufgestellt und dazu einen Verkaufskanal für Items und Accounts beobachtet. Demnach könnte der illegale Handel alleine für dieses Spiel ein jährliches Volumen von rund 15 Millionen Euro erreichen: Funk umreißt die Bedrohung: »Diese Hochrechnung ist zwar nicht repräsentativ, zeigt aber die Größe des Marktes, der bedient werden möchte. Die Dunkelziffer ist um ein Vielfaches höher«. Das Verbrechen ist also sowieso schon überall. Laden Sie es nicht auch noch auf Ihren eigenen PC ein. Moritz Jäger / GR



Auch für Electronic Arts' Plattform **Origin** gibt es viele Pseudo-Hacks.