Spyware-Gefahren und wie ihr sie umgeht

DER SPION IN MEINEM SPIEL

Spy- und Ransomware bedrohen eure Privatsphäre am PC, auch in Spielen. Oft stecken Kriminelle dahinter, manchmal auch Unternehmen. Das raten Experten, um sich zu schützen. Von Michael Sonntag

Spiele sind bekanntlich tolle Unterhaltungsmedien. In den Augen von Unternehmen sind sie dagegen wirtschaftliche Erzeugnisse, aber auch wertvolle Datenspeicher. Cyberkriminelle wiederum sehen in ihnen Einlasstore für effektive Angriffe. So oder so, eine Spieldatei aus dem Internet kann mehr enthalten, als sie auf den ersten Blick preisgibt, etwa Malware oder Spyware, die besonders heimtückisch ist. Weil sie unsichtbar ist: Der Begriff Spyware bezeichnet Software, die ohne Wissen des Konsumenten mitinstalliert wird und sensible Daten sammelt. In der Vergangenheit lösten Berichte über versteckte, automatisch mitinstallierte und potenziell schädliche Programme vereinzelte Shitstorms in den Steam-Reviews aus, etwa im Fall von XCOM: Chimera Squad oder bei den Total-War-Spielen.

Wie müssen wir mit Malware und Spyware im Gaming umgehen? Wir geben einen Überblick über das Phänomen und welche Ausprägungen es annimmt. Und am allerwichtigsten: wie man sich davor schützen kann.

Der Spion im Code

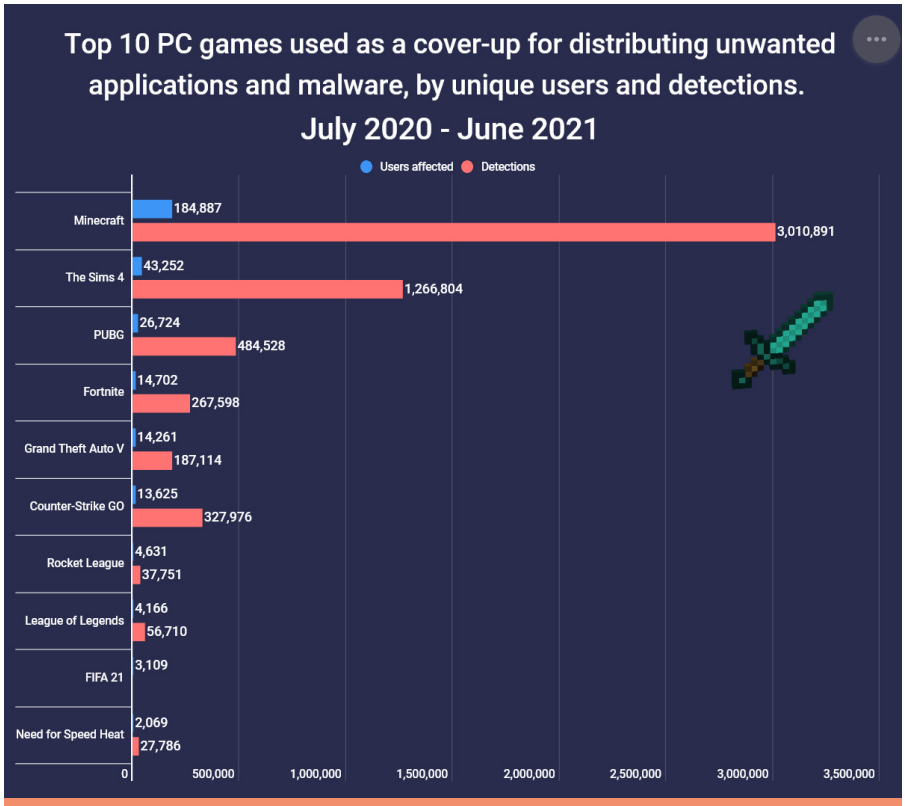
Das Feld der kriminellen Möglichkeiten mit Spyware ist unbegrenzt, weiß auch Dr. Michael Littger, Geschäftsführer des Deutschland sicher im Netz e.V. (DsiN): »Ist die Schad-Software einmal auf dem Gerät installiert, können beispielsweise Geräteeingaben protokolliert, Nachrichten gelesen oder Kameras und Mikrofone aktiviert oder gar die Kontrolle über das Gerät übernommen werden. So lassen sich umfangreiche Informationen und Bewegungsprofile im Sinne eines ›digitalen Fingerabdrucks‹ erstellen, auch sensible Daten wie Online-Banking-Zugänge oder Kreditkartendaten und Telefonnummern können erfasst werden.« Als gemeinnütziges Bündnis leistet der DsiN konkrete Hilfestellungen für IT-Sicherheit und Datenschutz für private Verbraucher und auch kleinere Unternehmen.

Natürlich wollen wir von Experte Dr. Littger wissen, wie gefährdet speziell wir Spieler sind. Antwort: Zumindest im Mainstream-Gaming lasse sich größtenteils Entwarnung geben. »Bei qualitativ hochwertigen Spielen der AAA-Klasse sind derzeit wenige Vorwürfe zu Spyware bekannt«, sagt Dr. Littger. Trotzdem sei das Phänomen Spyware nicht zu unterschätzen. Dr. Littger erklärt: »Spyware sind Computerprogramme, die meist ohne das Wissen der Nutzer:innen im Hintergrund aktiv und ohne Zustimmung Daten unbefugt erheben. Die Absichten solcher Programme sind unterschiedlich und können von privaten Beziehungen bis hin zu staatlich gelenkten Zwecken reichen.« Es gibt viele Kanäle, auf denen sich ahnungslose User unwissentlich gefährliche Malware und Spyware auf ihre Geräte holen können. Wir zeigen euch einige dieser Wege und führen hierzu auch entsprechende Gaming-Beispiele an.

Über Mods und externe Angebote

Im Herbst 2021 ermittelte das Unternehmen Atlas VPN (auch basierend auf Daten des Cyber-Security-Unternehmens Kaspersky), dass Minecraft das PC- und Mobile-Spiel mit der meisten Malware darstelle. Zwischen Juli 2020 und Juni 2021 wurden drei Millionen Fälle von Schad-Software registriert, 180.000 User waren direkt betroffen. In der Liste der PC-Spiele werden auch Die Sims 4, PUBG, Fortnite und GTA 5 aufgeführt. Im Oktober 2022 untersuchte Atlas VPN erneut, welche PC- und Mobile-Spieler den meisten Cyberangriffen ausgesetzt sind. Auch hier führt Minecraft mit insgesamt 150.000 betroffenen Usern auf beiden Plattformen. Des Weiteren finden sich auch Roblox und Need for Speed in der Liste. Dabei stammt die Malware nicht direkt von den Entwicklern selbst, sondern von externen Mods oder Angeboten von Drittanbietern. Die Dienstleistungen sind vielseitig: hübschere Texturen in Minecraft, neue Möbel in Die Sims, Items, Accounts mit hohem Level, ganz egal.

Kaspersky untersuchte im Sommer 2021 20 dieser Minecraft-Mods im Google Play Store. Die Mods geben vor, tatsächliche Spielinhalte zu sein, zielen aber in Wahrheit natürlich nur darauf ab, Berechtigungen über Endgeräte zu bekommen und so unerlaubt Werbeanzeigen zu schalten, ein kostenpflichtiges Abo abzuschließen oder Facebook-Daten zu erbeuten. Besonders tückisch: Wird die App dann vom Nutzer gemeldet und von Google entfernt, laden die Betreiber sie oft erneut hoch – mit geringen Anpassungen, um nicht sofort aufzufallen. Der DsiN beobachtet diese externen Pseu-



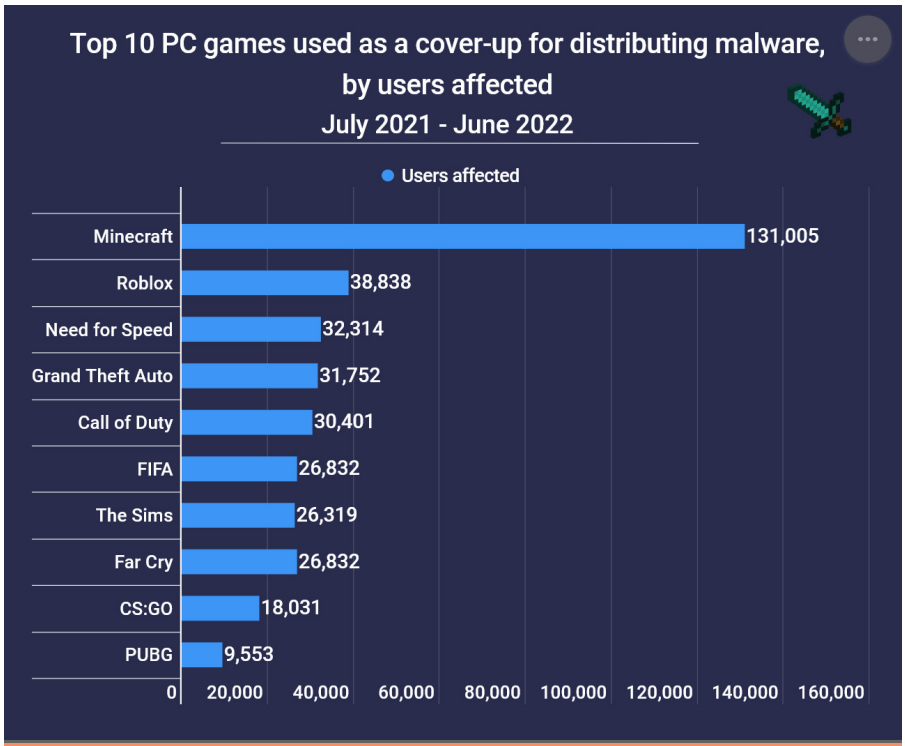
Atlas VPN ermittelte, dass Minecraft das Spiel ist, in dem die meiste Malware im Umlauf ist. Nicht durch die Entwickler, sondern durch externe Mods und Angebote.

doangebote auch bei MMOs wie World of Warcraft und Final Fantasy. »Auch In-Game-Auktionshäuser sind betroffen. Scammer teilen Links in Foren oder In-Game-Chats, mit denen sie digitale Gegenstände besonders günstig zum Kauf anbieten. Wenn der Link angeklickt wird, kann sich schädliche Software herunterladen«, so Geschäftsführer Littger. Die Opfer seien vor allem junge Spieler: »Es erscheint verlockend, ein begehrtes Item für nur wenige Euro sofort freizuschalten, das unter Umständen Monate dauern würde, um es auf normalem Wege zu erreichen. Die Täter nutzen hierbei die mangelnde digitale Kompetenz und Unvorsichtigkeit der Spieler:innen aus.«

Zuletzt stellt natürlich auch Piraterie ein gefährliches Einlasstor für Cyberkriminelle dar. Eine interessante Zahl hierzu liefert Steam eher unfreiwillig: Um ein gecracktes PC-Spiel zum Laufen zu bringen, verwenden Personen oft Spacewar!, hinter dem sich aber nicht der Retro-Klassiker von 1962 verbirgt, sondern in Wahrheit eine Testapplikation von Valve. So »spielten« am 16. Februar 2023 laut SteamDB überraschenderweise ganze 78.000 Personen das Raumschiffspiel – vermutlich um Cracks von Hogwarts Legacy oder Forza Horizon 5 zu spielen (zwei Titeln, die zu dieser Zeit auf dem Crack-Markt besonders trendeten).

Während die Testapplikation Spacewar! selbst ungefährlich ist, kann man das von den meisten Crack-Versionen nicht unbedingt behaupten. So fand das Unternehmen Avast im Sommer 2021 gefährliche Malware (insbesondere eine Mining-Software namens Crackonosh) in zahlreichen Installern gecrackter Spieleversionen, darunter etwa Fallout 4 GOTY, GTA 5 und Die Sims 4.

Quelle: AtlasVPN



Auch ein Jahr später steht Minecraft an der Spitze der mit Malware infizierten Spiele.

Mobile Games

»Generell haben Spiele auf mobilen Geräten sowie Apps ein höheres Risiko für Spyware, da über Smartphones vielfältige Informationen erhoben werden. Hier stehen Unternehmen wie Alphonso für eine recht freizügige Praxis der Datennutzung beispielsweise über das Mikrofon der Smartphones«, sagt Dr. Littger. Im Jahr 2017 berichtete T3N, dass 250 Mobile-Spiele die Belauschungs-Software von Alphonso verwenden würden (via New York Times). Dazu gehören unter anderem eher unbekannte Titel wie Tasty Dozer, Casino Coin Rush und Highway Racer.

Der DsiN sagt zu diesem Sachverhalt: »Wir empfehlen Nutzenden, die entsprechenden AGB einmal zu lesen und selbst zu entscheiden, wie sie damit umgehen. [...] Es kann derzeit davon ausgegangen werden, dass Spieler:innen in seriösen Spielen weitgehend sicher sind – vor allem auf Konsolen. Hier befindet man sich derzeit in einer bestmöglich kontrollierten Umgebung. Die Situation auf den Plattformen PC und Mobile ist aufgrund ihrer Offenheit anders.«

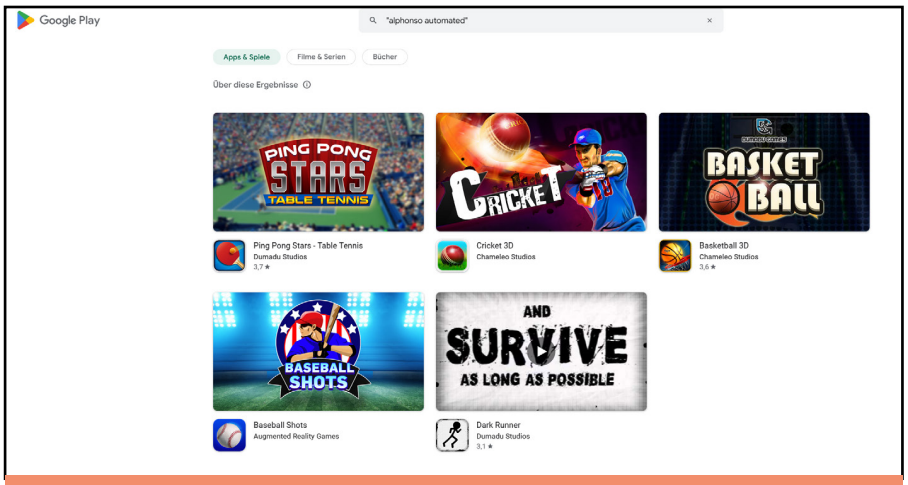
Datenerhebungen

Dass Entwickler aber auch selbst in Berührung mit Formen von Spyware kommen können, zeigte ein Skandal vor fünf Jahren: Im Juni 2018 offenbarten informatikaffine Spieler auf Reddit, dass Spiele wie Civilization 6 und Total War nicht nur den Spielcode übertragen, sondern auch gleich die Software Red Shell mitinstallieren. Diese analysiert den Erfolg und Effekt von Werbeanzeigen bei Usern. Hierbei wird festgehalten, ob der User auf eine Spielwerbung klickt und später dieses Spiel auch auf dem PC startet. Zu den gespeicherten Daten gehören laut FAQ von Red Shell folgende: Betriebssystem, Auflösung, Zeitzone, Sprache, installierte Schriftarten, Browser – genauso wie die Steam-ID und die IP-Adresse. Letztere gelten laut der DSGVO als personenbezogene Daten. Während die IP-Adresse dank der

Name of infected installer	SHA256
NBA 2K19	E497EE189E16CAEF7C881C1C311D994AE75695C5087D09051BE59B0F0051A6CF
Grand Theft Auto V	65F39206FE7B706DED5D7A2DB74E900D4FAE539421C3167233139B5B5E125B8A
Far Cry 5	4B01A9C1C7F0AF74AA1DA11F8BB3FC8ECC3719C2C6F4AD820B31108923AC7B71
The Sims 4 Seasons	7F836B445D979870172FA108A47BA953B0C02D2076CAC22A5953EB05A683EDD4
Euro Truck Simulator 2	93A3B50069C463B1158A9BB3A8E3EDF9767E8F412C1140903B9FE674D81E32F0
The Sims 4	9EC3DE9BB9462821B5D034D43A9A5DE0715FF741E0C171ADFD7697134B936FA3
Jurassic World Evolution	D8C092DE1BF9B355E9799105B146BAAB8C77C4449EAD2BDC4A5875769BB3FB8A
Fallout 4 GOTY	6A3C8A3CA0376E295A2A9005DFBA0EB55D37D5B7BF8FCF108F4FFF7778F47584
Call of Cthulhu	D7A9BF98ACA2913699B234219FF8FDAA0F635E5DD3754B23D03D5C3441D94BFB
Pro Evolution Soccer 2018	8C52E5CC07710BF7F8B51B075D9F25CD2ECE58FD11D2944C6AB9BF62B7FBFA05
We Happy Few	C6817D6AFECDB89485887C0EE2B7AC84E4180323284E53994EF70B89C77768E1

Infected installers

Wie Avast feststellte, schleusen die Hersteller in die Installer bekannter Spiele oft auch Malware und Programme, die eure PCs zu Bitcoin-Generatoren machen.



Diese Spiele verwenden eine Software von Alphonso, die auf das Handy-Mikrofon zugreift.

DSGVO verschlüsselt wird, gilt das jedoch nicht für den Namen des Geräts.

Handelt es sich bei Red Shell bereits um Spyware? Auch wenn die Betreiber widersprachen und manche Entwickler die Software verteidigten, liefen die Spieler Sturm – und das mit Erfolg. Dutzende Entwickler entfernten die Software in den darauffolgenden Monaten aus ihren Spielen, das Reddit-Team dokumentierte fleißig mit. Die Liste ist lang (Letzter Stand 26. August 2018): Wir zählen 43 Entfernungen und etwa zehn Spiele, bei denen die Entfernung noch nicht bestätigt werden konnte.

Eine gewisse Gläsernheit gehe mit manchen Spielen einher und könne in der Praxis auch nicht verhindert werden, so Doktor Littger vom DsiN. »Bei fast allen Online-Spielen werden Informationen über die Nutzer:innen gesammelt. Einige dieser Daten werden von Spielenden selbst angegeben, zum Beispiel für Verträge und Zahlungen. Andere Daten werden jedoch ohne aktives Wissen erfasst, wie zum Beispiel Informationen über den Computer und das Nutzungsverhalten. Diese Daten können beispielsweise von Werbetreibenden genutzt werden, um ein umfassendes Profil über die Spielenden zu erstellen. Wenn diese Informationen mit anderen Daten verbunden werden, können Rückschlüsse auf das persönliche Leben des Spielers gezogen werden.«

Was mit den Daten genau passiert, erfahren Spieler in den AGB der Spiele. Stimmen sie diesen zu, ist der Entwickler im Recht und fein raus. Der DsiN-Geschäftsführer erklärt: »Gaming-Unternehmen müssen ihre Nutzungsbedingungen und Datenschutzpraktiken in ihren AGB darlegen, wie beispielsweise das Speichern von Spielerstatistiken oder die Überwachung von Chats. Deshalb lohnt es sich wirklich, die AGB zu lesen und im Zweifel die Finger von Spielen mit unseriösen Datenpraktiken zu lassen.« Vollkommene Narrenfreiheit hätten die Entwickler allerdings auch nicht, betont Littger: »Auch eine Zustimmung zu den AGB stellt keinen Verzicht auf die von der DSGVO verpflichtenden Betroffenenrechte dar.« Insbesondere sind hier von Belang:

- Auskunftsrecht (Art. 15 DSGVO)
- Berichtigungs- und Löschungsrecht (Art. 16 und 17 DSGVO)
- Einschränkungsrecht (Art. 18 DSGVO)
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
- Widerspruchsrecht (Art. 21 DSGVO)

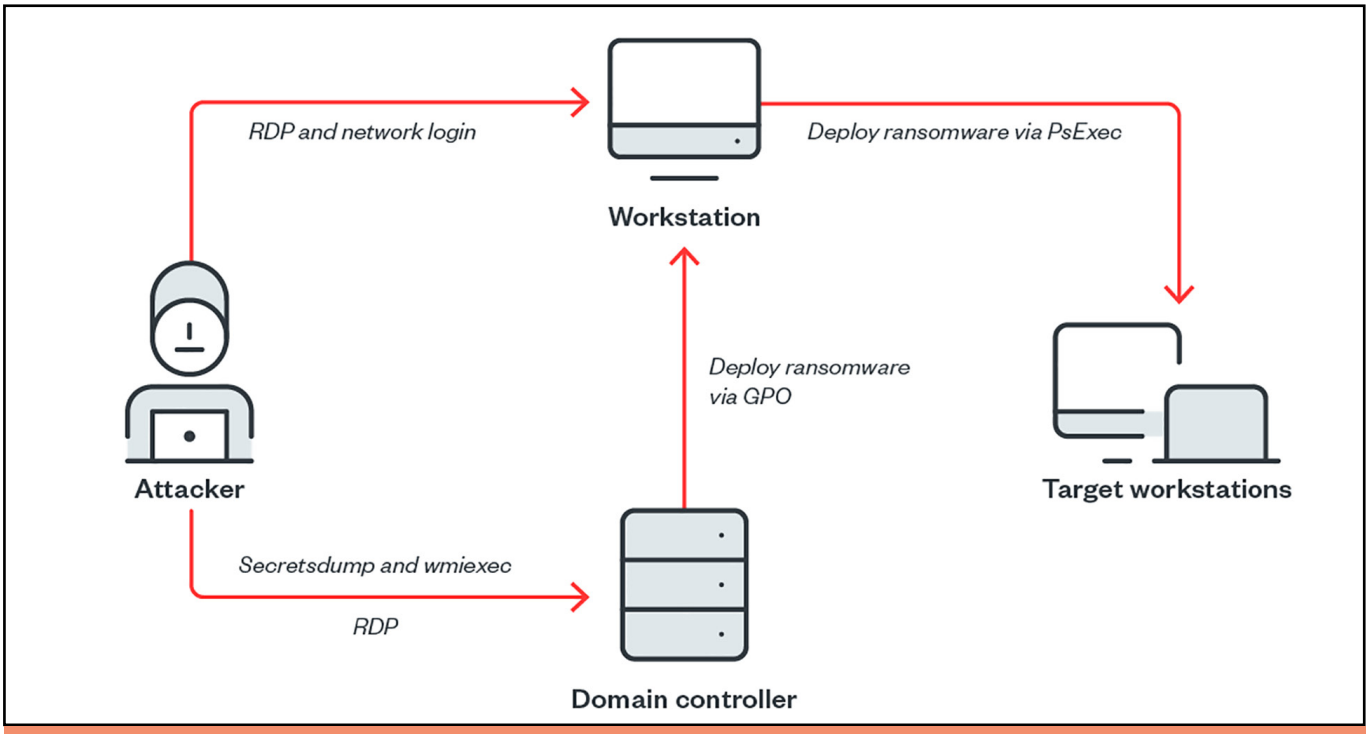
»Grundsätzlich kann die Einwilligung zur Verarbeitung personenbezogener Daten gemäß Art 7 Abs. 3 jederzeit widerrufen werden«, so Doktor Littger.

Anti-Cheat

Besonders heikel wird es dann, wenn ein eigentlich guter Vorwand einen gefährlichen Nebenaspekt mit sich bringt: Um cheaten in Spielen zu unterbinden, verwenden Entwickler mittlerweile immer stärkere Anti-Cheat-Software. So zum Beispiel auch EA bei FIFA 23. Ein andauernder Wettlauf, da die Cheat-Hersteller ebenfalls immer klügere Programme erstellen. Aber auch ein zweischneidiges Schwert: Der Anti-Cheat muss für seine völlige Effektivität auf die unterste Ebene des Betriebssystems zugreifen, den Kernel. Das ist die Schnittstelle zwischen Hardware und Software mit den meisten Zugriffsrechten und -freigaben über den PC. Damit soll die Software auch die hartnäckigste Cheat-Software stoppen, die ebenfalls im Kernel ansetzt, um möglichst unsichtbar zu bleiben. Gleichzeitig erhält der Anti-Cheat damit aber auch viel Macht über den PC. Und das ist keine, die Spieler den Spieleunternehmen normalerweise leichtfertig geben wollen. Es ist ein Dilemma, trotz aller Beteuerungen der Entwickler, dass nichts Anderweitiges mit dieser Macht getan werde. Die Praxis hat beide Situationen geliefert:

- Im April 2018 entdeckten Spieler in der Anti-Cheat-Software von Guild Wars 2 auch gefährliche Spyware.
- Im April 2020, im Falle von Valorant, das Vanguard verwendet, erwies sich die Software äußerst effektiv gegen Cheater, bisher ohne Rattenschwanz.

Nichtsdestotrotz macht diese extrem eingreifende Software ironischerweise Computer auch für Fremdeinwirkungen sehr angreifbar. Das zeigt der Fall Genshin Impact. Im August 2022 deckte die Cyber-Security-Firma Trend Micro auf, wie Kriminelle mittels der Anti-Cheat-Software von Genshin Impact den Virenschutz umgehen können, um dann Ransomware zu installieren (Erpresser-Trojaner, mit denen die Täter Zugänge blockieren und sie nur gegen Geld wieder freigeben). Während mehrere Technikmagazine (unter anderem Inside Digital) empfohlen haben, das Spiel vorerst wegen der Sicherheitslücke zu deinstallieren, arbeitet Entwickler HoYoVerse aktuell immer noch an einer Lösung. »Gamer bieten Cyberangreifern lohnende Ziele«, sagt Richard Werner, Business Consultant bei Trend Micro. Im Jahr 2019 untersuchte das Unternehmen gezielt Cyberkriminalität und Cheating im E-Sport, unter anderem in Spielen wie CoD: Warzone, Fortnite und PUBG. »So ist der Diebstahl von Login-Daten sehr interessant, weil die Opfer durchaus bereit sind, Lösegeld zu bezahlen, wenn ansonsten mühsam erspielte Erfolge verloren gehen. Auf der anderen Seite gibt es auch einen Markt, der genau diese Erfol-



Trend Micro veranschaulicht, wie Cyberkriminelle die Anti-Cheat-Software von Genshin Impact verwenden, um den Virenschutz zu umgehen und Ransomware zu installieren. Die wird man dann nur gegen Geldzahlung wieder los.

ge dann dem Höchstbietenden weiterverkauft. Zählt man Cheaten, wie zum Beispiel den Einsatz von unerlaubten Hilfsprogrammen, und auch Gambling, also unerlaubtes Wetten, hinzu, kann man sagen, dass die Gaming-Welt eine der größten Branchen im digitalen Untergrund ist.«

Politik und Gesellschaft

Begeben wir uns auf die politische und gesellschaftliche Ebene von Spyware, wird es recht vage und dystopisch. Wie der chinesische Gaming-Riese Tencent im Sommer 2021 ankündigte, plant er Gesichtserkennungstechnologie in seine Spiele einzubauen, um den übertriebenen Videospielkonsum chinesischer Jugendlicher zeitlich besser zu beschränken – ganz im Sinne der neuen kontroversen Gesetzeslage im Land.

Der Ukraine-Krieg schuf 2022 wiederum eine neue Situation – mit wachsender Skepsis gegenüber russischen Produkten: Im Frühjahr 2022 warnt das deutsche Bundesamt für Sicherheit in der Informationstechnik davor, Programme des russischen Cyber-Security-Unternehmens Kaspersky zu nutzen. Der Einfluss der russischen Regierung sei nicht mehr genau einzuschätzen. Im Falle des russischen Ego-Shooters Atomic Heart tauchten anscheinend in einer älteren Version der Private Policy Passagen auf, die besagen, dass Nutzerdaten gesammelt und möglicherweise auch an den russischen Ge-

Minecraft ist ein riesiges Einfallstor für Spyware, weil es auf unzähligen Handys und PCs installiert ist. Auf Konsole ist man vergleichsweise sicher.

Ziel darin war es, in einem Labyrinth aus Räumen Puzzleteile zu finden und zusammenzusetzen.

Populäre Spiele wie Die Sims 4 werden ebenfalls zum Einschleusen von Malware verwendet.

UNSERE EXPERTEN

Dr. Michael Littger ist der Geschäftsführer des Deutschland sicher im Netz e.V., einem gemeinnützigen Bündnis, das Verbrauchern und kleineren Unternehmen konkrete Hilfestellungen für IT-Sicherheit und Datenschutz liefert. Der Verein besteht seit 2006 und beantwortet auf seiner Website auch Fragen zu künstlicher Intelligenz sowie Passwortsicherheit.

Richard Werner ist Business Consultant bei Trend Micro, einem 1988 in Kalifornien gegründeten und seit 1992 hauptsächlich in Japan ansässigen Cyber-Security-Unternehmen, das sich als Weltmarktführer in Sachen Server-Sicherheit sieht und heute Niederlassungen in über 30 Ländern unterhält.

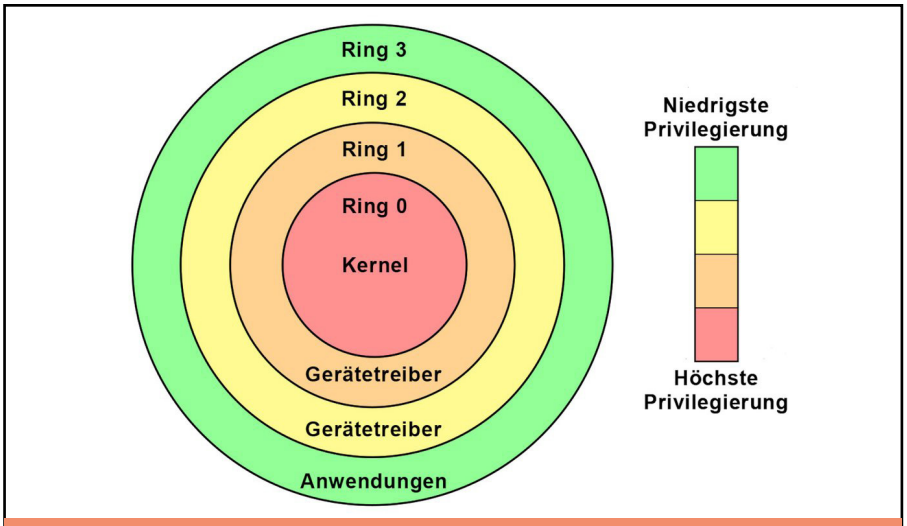
heimdienst FSB weitergegeben werden. Entwickler Mundfish widerspricht dieser Behauptung, die betreffenden Zeilen des Textes seien veraltet. Die Seite existiert ebenfalls nicht mehr. Im Artikel »The Unnerving Rise of Video Games that Spy on You« geht Wired auf viele weitere videospieltechnische und allgemein digitale Bereiche ein, die über Datenspeicherung und -fütterung in der Zukunft völlig neue Dimensionen annehmen können und werden.

Wie ihr euch schützen könnt

GameStar-Autor und Cyber-Security-Experte Wolfgang Rabenstein empfiehlt euch folgende Tipps für den sicheren Umgang:

- Wenn man sich nicht sicher ist, ob eine Datei von Viren befallen ist, muss die erste Anlaufstelle (bevor man sie ausführt!) immer der Virenscan per VirusTotal sein.
- Keine Cracks verwenden (und keinesfalls auf diesen Systemen dann auch noch Online-Banking betreiben).
- Nur vertrauenswürdige Software von vertrauenswürdigen Plattformen wie Steam, GOG.com oder Epic installieren.
- Immer die aktuellste Version von Spielen/Programmen benutzen.
- Für jeden Account ein eigenes Passwort und niemals 2x das gleiche verwenden. Das ist generell ein guter Tipp!
- Sichere, zufallsgenerierte Passwörter verwenden, auch wenn sie umständlich sind.
- Mit Passwortmanagern wie Keepass behält man hier den Überblick.

Aber was ist mit der Politik? Diese könne nicht in die Verantwortung gezogen werden, einen ultimativen Schutz im Netz zu gewährleisten, meint der DsiN. »Die Verantwortung für den Schutz vor Spyware liegt derzeit größtenteils bei den Nutzer:innen. Digitale Kompetenz ist für einen sicheren und souveränen Umgang mit digitalen Spielen unverzichtbar. Die Politik kann hier einen Beitrag leisten, indem sie die Förderung von Digitalkompetenzen in der breiten Gesellschaft vo-



Moderne Anti-Cheat-Software soll das Cheaten dort unterbinden, wo es ansetzt: direkt im Kernel, also einem zentralen Bereich, in dem die Software gleichzeitig auch viel Macht über den Rechner bekommt. Ein zweischneidiges Schwert, denn diese Macht kann ausgenutzt werden.

Selbst über CS:GO wird Malware verbreitet. Dabei sind CS-Spieler mit allen Wassern gewaschen.

rantreibt und Wirtschaft und Zivilgesellschaft ermutigt, sich zu engagieren.« Es bleibe jedoch dabei: »Spieler:innen müssen frühzeitig über Betrugsmaschen aufgeklärt werden, um diese zu erkennen und abzuwehren. Wir empfehlen, alle Arten von Internetkriminalität und unseriösen Praktiken den Betreibern zu melden.« Richard Werner von Trend Micro ergänzt dazu: »Es gibt bereits Gesetze gegen Betrug, Datendiebstahl und die Verwendung von Malware. Allerdings haben wir bei allen cyberkriminellen Aktivitäten das gleiche Problem: Die Täter sind oft schwer zu ermitteln und zu allem Überfluss meist im Ausland – bezüglich Gaming meist Südostasien. Zudem ist der entstandene Schaden nur schwer zu beziffern. Es ist deshalb für Strafverfolgungsbehörden häufig nicht möglich, die Täter zu überführen und zur Rückgabe gestohlener Daten oder auch Schadensersatz zu verurteilen. Für Verbraucher ist es daher deutlich effektiver, sich selbst zu schützen.«

Darüber hinaus empfiehlt Dr. Littger vom DsiN noch die folgenden Tipps: »Eine weitere Maßnahme zur Erhöhung der eigenen Sicherheit ist die Beschränkung der Zugriffsrechte von Apps auf Funktionen. Es empfiehlt sich auch, kritisch zu hinterfragen, ob eine App wirklich notwendig ist. Bewertungen und Austausch mit anderen Nutzer:innen können dabei hilfreich sein. Die Einrichtung einer Zwei-Faktor-Authentifizierung sowie die Nutzung von Passwortmanagern und gesonderten E-Mail-Adressen für Gaming-Konten sind weitere sinnvolle Schutzmaßnahmen. Für Streamer kann ein VPN nützlich sein, um die eigene IP-Adresse zu maskieren.« Zwei-Faktor-Authentifizierung wird ohnehin bereits von vielen Plattformen wie Blizzards Battlenet angeboten.

Zuletzt bitten wir Richard Werner von Trend Micro um eine Einschätzung zu den Gefahren von Spy- und Malware im Gaming: »Datendiebstahl und Spionage sind ein uraltes und nach wie vor hoch profitables Geschäft. Gleiches gilt für die Gaming-Industrie. Sieht man sich die Entwicklung im Bereich E-Sports und/oder Turnieren an, wird schnell deutlich, dass es dabei auch um viel Geld geht. Entsprechend groß ist der Appetit auf Daten.« Die Herausforderung sei, den legalen vom illegalen Umgang mit Daten zu unterscheiden, und das sei nicht immer einfach. »Verwendet man Freeware, Browser-Games et cetera, sollte man sich die EULAs ansehen. In Panik zu verfallen, wäre aber falsch«, betont der Business Consultant. »Ja, es passiert viel. Aber angesichts der Anzahl von Spielern ist das normal. Cyberkriminelle suchen nach Gamern und gehen dabei den Weg des geringsten Widerstandes. Ein normaler Umgang mit dem Thema Datenschutz und -sicherheit ist dennoch wichtig, sollte aber ausreichen. Cyberkriminelle haben in der Regel noch immer genügend andere Opfer, die nicht einmal dieses Minimum einhalten und deshalb deutlich einfachere Beute sind.« ★

Roblox wird gerne von Kindern genutzt. Die haben in der Regel keine Ahnung, was sie sich da einhandeln können, die Eltern sind gefragt.

2012 gab es die Reihe auch in Apples App Store, mittlerweile ist sie dort aber leider verschwunden.