Zocken statt Zombie: Security-Tipps für PC-Gamer

(ddp direct) ?Game Over? hieß es bereits für so manchen Online-Zocker. Einige Gamescom-Besucher (Köln, 21. bis 25. August) können sicherlich ein Lied davon singen, dass sie nicht von Gegnern, sondern von Hackern in die Knie gezwungen wurden. Die Sicherheitsexperten von ESET geben neue Tipps, wie der Spielespaß mit Sicherheit groß bleibt.

1. Lastpass und andere ?Passwort-Safes? nutzen

Spieler müssen heutzutage eine ganze Menge an Passwörtern im Kopf behalten. Daher ist es schon verführerisch, das gleiche Passwort mehrfach zu verwenden. Dies gilt erst recht, wenn es sich ?nur? um eine Kopierschutz-Funktion wie Ubisofts Uplay handelt. Uplay wurde dieses Jahr gehackt, Benutzernamen und (verschlüsselte) Passwörter gestohlen.

TIPP: Wenn möglich, sollten ?Wegwerfadressen? für Kopierschutz-Funktionen und andere Einmal-Anmeldungen genutzt werden. Je mehr unterschiedliche Passwörter im Einsatz sind, desto besser ist es. Das Verwenden von Lastpass oder anderen ?Passwort-Managern? erleichtert deren Verwaltung enorm.

2. Erst denken, dann ?Alt+Tab? drücken

Ein zusätzliches Browserfenster verschafft bei Spielen, wie beispielsweise MMOs, einen besseren Überblick. Bevor man jedoch mit ?Alt+Tab? in ein solches wechselt, sollte man den ?Menschenverstand-Modus? wieder einschalten. Nicht jeder Link, den man im Spiel geschickt bekommen hat, führt Gutes im Schilde. Und nicht jeder, mit dem man während des Spiels kommuniziert (selbst Team- oder Gildenmitglieder), muss nicht immer der sein, für den man ihn hält. Das US Computer Emergency Response Team (CERT) hat erst kürzlich davor gewarnt, dass (gehackte) Spieler-Accounts für die Verteilung von Malware missbraucht wurden. Dazu zählen auch Links, die auf präparierte Webseiten verweisen. Höchst gefährlich wird es, wenn gefälschte Patches oder Spieldownloads angeboten werden ? die sich letztlich als gefährliche Software entpuppen.

3. Wenn der ?God Mode? das Geld nicht wert ist

Es werden nicht wenige ?Hacks? online angeboten, um durch Wände gehen zu können oder schneller im Spiel voranzukommen. Viele davon sind allerdings nur einfach clever benannt und zu 90 Prozent reine Malware. Wer sich im sogenannten ?God Mode? Vorteile erhofft, sollte von Hacks und Cheats die Finger lassen. Ansonsten öffnet er Hackern freiwillig Tür und Tor.

4. Vorsicht beim Modding

In vielen Online Games sind Mods und Add-Ons kein Extra, sondern ein Muss. In ?World of Warcraft? ist es zum Beispiel mehr als ein ?sozialer Fauxpas?, ohne ?Damage Counter? weit kommen zu wollen. Wer entsprechende Hilfsmittel runterladen will, sollte die anbietende Webseite genauer unter die Lupe nehmen. Seiten wie ?ModDB? oder ?Curse? sind oft vertrauenswürdig. Aber auch sie können selbst erstellte Mods von Spielern beinhalten, die wiederum mit Malware versehen sind. Die Bewertungen geben einen guten Anhalt über die Güte. Ein Check der URLs mit einer Antivirensoftware hilft zudem weiter.

5. Foren lieber fern bleiben

Es kann verführerisch sein, in Game-Foren seinem Ärger Luft zu machen. Dies ist mittlerweile umso gefährlicher, weil Cyber-Kriminelle Foren als Sammelstelle von Benutzernamen und Passwörtern nutzen. Wer Foren besucht, sollte andere Benutzernamen und Kennwörter nutzen, als für die Spieleanmeldung. ?Wegwerf?-E-Mail-Adressen stellen eine einfache Alternative dazu dar.

6. Kauft kein Gold ? und falls doch, dann nicht von dem Typen aus dem Game Chat

Gold, Spielewährungen oder Level-Boosts zu kaufen, ist ein gefährliches Geschäft. Das Geld oder die Dienste, die zum Kauf angeboten werden, können genauso gut von gehackten Accounts stammen. Von ?Verkäufern? aus dem Game-Chat gehen noch höhere Gefahren aus. Kein Verkäufer ist zu 100 Prozent vertrauenswürdig, sogar so große Seiten wie IGE. Aber kleine Seiten sind nahezu Paradiese für Phishing-Versuche, Spyware und Kreditkarten-Diebstahl. Lieber gleich meiden.

7. Lieber Sicherheit als Leistung

Wenn der PC laggt, juckt es Gamern in den Fingern, die Sicherheitssoftware abzuschalten. In einer ESET-Studie unter 1000 britischen PC-Gamern gaben 30 Prozent an, vor dem Online-Spielen die Security-Funktionen zu deaktivieren. Das Fehlverhalten hatte ernste Folgen: Mehr als zwei Drittel der Teilnehmer mussten zugeben, Opfer einer Malware-Attacke gewesen zu sein. Besonders ärgerlich: Die Bereinigung und die Systemwiederherstellung dauerten im Schnitt bis zu zwei Tage.

8. Erst schauen, dann anmelden

Webseiten, die Spiele-Logins verlangen, sollte man kritisch betrachten. Dies gilt auch für professionell gestaltete und vertrauenswürdig aussehende Pages. Blizzard, die Macher von ?World of Warcraft?, warnen: ?Jemand, der es bewusst auf Battle.net Accounts abgesehen hat, könnte eine Seite zu genau diesem Zweck erstellen, wie eine Fanseite oder Forum für ein Blizzard Spiel. Wenn Du Dich dann mit Deinen Battle.net Benutzernamen und Passwort auf dieser Webseite registrierst, hast Du demjenigen auch sofort die Schlüssel zu Deinem Account übergeben.?

9. Doppelt gemoppelt hält besser: Zwei-Faktor-Authentifizierung

Die Sicherheit des Spiele-Accounts steht und fällt mit der Einwahlsicherheit. Experten empfehlen die Zwei-Faktor-Authentifizierung, um Kriminellen die Arbeit enorm zu erschweren. Dazu bieten sich Smartphone-Apps oder physische Geräte an. Falls eine Authentifizierungs-App vorhanden ist, sollte diese auch genutzt werden. Diese schützt auch dann, wenn andere Webseiten gehackt und eigene Anmeldedaten gestohlen wurden.

Shortlink zu dieser Pressemitteilung:
http://shortpr.com/1tw43u

Permanentlink zu dieser Pressemitteilung:
http://www.themenportal.de/it-hightech/zocken-statt-zombie-security-tipps-fuer-pc-gamer-39532

Pressekontakt

ESET Deutschland GmbH

Herr Michael Klatte
Talstraße 84
07743 Jena

michael.klatte@eset.de

Firmenkontakt

ESET Deutschland GmbH

Herr Michael Klatte
Talstraße 84
07743 Jena

eset.de
michael.klatte@eset.de

Der slowakische Antivirenhersteller ESET schützt seit 1992 mit modernsten Antivirenlösungen Unternehmen und Privatanwender vor Malware aller Art. Das Unternehmen gilt - dank der vielfach ausgezeichneten ThreatSense-Engine - als Vorreiter bei der proaktiven Bekämpfung selbst unbekannter Viren, Trojaner und anderer Bedrohungen.

Die hohe Malwareerkennung und Geschwindigkeit sowie eine minimale Systembelastung zeichnen nicht nur die Top-Produkte ESET NOD32 Antivirus und ESET Smart Security aus. Inzwischen vertrauen mehr als 100 Millionen PC-Anwender weltweit den ESET-Lösungen.

Für Firmenkunden bietet ESET umfassenden Malware-Schutz an, der auch Lösungen für Mailserver, Netzwerk-Gateways und Fileserver unterschiedlicher Serverbetriebssysteme und E-Mail-Serverplattformen umfasst. Sie gewährleisten proaktiven und präzisen Antivirenschutz für High-Traffic-Server und umfangreiche Dateisysteme.

ESET beschäftigt in seiner Unternehmenszentrale in Bratislava (Slowakei) und in der Niederlassung in San Diego (USA) mehr als 500 Mitarbeiter. ESET betreibt zudem eigene Büros in Prag (Tschechische Republik), Bristol (UK), Buenos Aires (Argentinien), Singapur und Jena (Deutschland). ESET-Lösungen sind über ein weltweites Partnernetzwerk in mehr als 180 Ländern vertreten.