Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Schützen Sie sich persönlich
- Schützen Sie Ihren Computer und Ihre Accounts
- Tipps für Eltern

Online-Spiele – geschützt und sicher

Überblick

Online-Spiele bieten viel Unterhaltung, bergen aber auch ihre ganz eigenen Risiken. In diesem Newsletter besprechen wir, was Sie zu Ihrem eigenen Schutz und dem Ihrer Familie im Rahmen von Online-Spielen tun können.

Gastautor

Jake Williams ist der Gründer von und führender Berater bei Rendition Infosec, ein zertifizierter SANS Ausbilder und Co-Autor verschiedener SANS Kurse. Er ist auf Twitter als **@MalwareJake** aktiv und bloggt regelmäßig unter **malwarejake.blogspot.com**.

Schützen Sie sich persönlich

Die Tatsache, dass Sie mit Menschen auf der ganzen Welt spielen und kommunizieren können, macht Online-Spiele so interessant. Sehr oft kennen Sie die Personen nicht einmal, mit denen Sie da gerade ein Spiel bestreiten. Während ein Großteil der Spieler auf Unterhaltung aus ist, gibt es aber auch diejenigen, die Ihnen schaden wollen. Hier sind einige Schritte, die Sie zu Ihrem Schutz befolgen sollten:

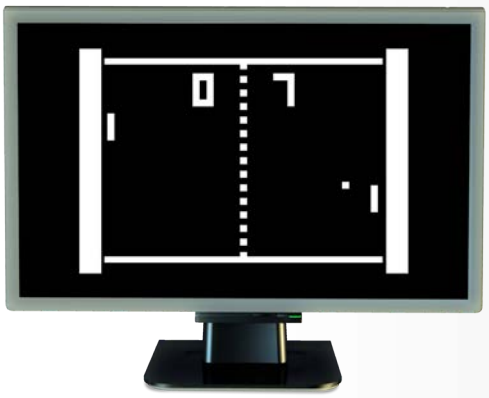
- Seien Sie insbesondere bei Nachrichten achtsam, die Sie zu einer Handlung auffordern, wie z.B. einen Link aufzurufen oder eine Datei herunterzuladen. Genau wie bei Phishingangriffen werden Kriminelle versuchen Sie zu Handlungen zu verleiten die Ihren Computer infizieren. Wenn eine Nachricht verdächtig erscheint oder sich der Inhalt zu gut anhört um wahr zu sein, rechnen Sie immer mit einem verdeckten Angriff.
- Viele Online-Spiele haben ihre eigenen Märkte, auf denen Sie virtuelle Güter handeln, eintauschen oder sogar kaufen können. Genau wie in der wirklichen Welt gibt es auch hier Betrüger, die Sie durch Tricks um Ihr Geld bringen wollen oder es direkt zu stehlen versuchen.
- Seien Sie sehr vorsichtig bei allen Geschäften, bei denen echtes Geld zum Kauf von spielinternen Artikeln genutzt wird, und andersherum natürlich auch. Wickeln Sie diese Geschäfte nur auf Marktplätzen mit einem guten Ruf ab.
- Beschränken Sie die Menge der Informationen, die Sie oder Ihre Kinder online teilen. Geben Sie nie detaillierte persönliche Informationen wie Ihr Passwort oder Ihre Wohnanschrift weiter.
- Viele Webseiten, wie z.B. die Ihrer Bank, nutzen Sicherheitsfragen um Ihre Identität zu bestätigen. Angreifer sind dafür bekannt, diese Antworten durch Anfreunden mit ihren Opfern in Online-Spielen zu erbeuten. Merken Sie sich, dass Sie keinerlei Verpflichtung unterliegen Fragen zu beantworten, die Ihnen Fremde während eines Spiels stellen.

Sichern Sie Ihr System und Ihre Accounts

Der nächste Schritt ist das Absichern Ihres Computers. Bösewichte werden versuchen, den Computer oder Ihre

Online-Spiele – geschützt und sicher

Spieleaccounts zu übernehmen - Sie müssen sie daher gut schützen.



Die wichtigsten Punkte zum eigenen Schutz bei Online-Spielen sind die Nutzung starker Passwörter, die Absicherung Ihres Computers und die Nutzung Ihres gesunden Menschenverstandes, wenn Sie mit Fremden kommunizieren oder ungewöhnliche Nachrichten oder Anfragen erhalten.

- Nutzen Sie sowohl für Ihren Computer als auch für Ihre Spieleaccounts starke Passwörter. Angreifer können dadurch Ihre Passwörter nicht ohne größeren Aufwand erraten und werden daran gehindert Ihre Accounts zu übernehmen. Wenn ein Spiel eine Zwei-Wege-Anmeldung anbietet, aktivieren Sie diese. Stellen Sie zudem sicher, dass jeder Ihrer Spieleaccounts ein eigenes Passwort nutzt. Somit besteht kein Zweifel daran, dass alle anderen Spieleaccounts unbetroffen sind, wenn ein Account kompromittiert wird.
- Schützen Sie Ihren Computer, indem Sie immer die neueste Version des Betriebssystems und der Spiele nutzen. Genau wie bei dem Betriebssystem und bei Webbrowsern hat auch veraltete Spiele-Software häufig bekannte Verwundbarkeiten, die Angreifer ausnutzen können um Ihren Computer anzugreifen. Indem Sie Ihren Computer und Ihre Anwendungen aktuell halten, räumen Sie die meisten dieser Verwundbarkeiten aus.
- Nutzen Sie ein Antivirus-Programm und stellen Sie sicher, dass es aktuell ist und all Ihre Dateien in Echtzeit überprüft.
- Laden Sie Spiele nur von vertrauenswürdigen Webseiten herunter. Wenn Sie weitere Software benötigen, um ein Spiel starten zu können, beziehen Sie diese von der Herstellerwebseite oder einer anderen bekannten, vertrauenswürdigen Quelle. Angreifer erstellen häufig nachgeahmte oder infizierte Versionen eines Spiels und verteilen sie über ihre eigenen Server. Wenn Sie eine dieser Versionen installieren, haben die Bösewichte vollen Zugriff auf Ihren Computer.
- Spieleerweiterungen, die oft von der Nutzergemeinschaft erstellt werden, ergänzen die Spiele meistens um neue Funktionen und Möglichkeiten. Angreifer infizieren diese Erweiterungen jedoch manchmal mit Schadsoftware, die von Antivirus-Programmen schwer zu erkennen sein kann. Genau wie beim Herunterladen von Spielen und Programmen sollten Sie daher sicherstellen, Erweiterungen nur von vertrauenswürdigen Quellen zu beziehen. Wenn eine Erweiterung die Deaktivierung Ihres Antivirus-Programms oder Ihrer Firewall erfordert, benutzen Sie diese Erweiterung besser nicht.
- Untergrundmärkte sind entstanden, um Mogeleien und Betrügereien (cheating) in Spielen zu unterstützen. Neben der Tatsache, dass derartiges Verhalten unethisch ist, können viele dieser Cheating-Programme oder Erweiterungen einfach nur Rootkits sein, die wohl gefährlichste Art von Schadsoftware. Installieren oder nutzen Sie daher nie eines dieser Mogelprogramme.

Online-Spiele – geschützt und sicher

- Viele Spielehersteller geben auf Ihren Webseiten Hinweise, wie Sie sich selbst gegen Gefahren absichern können. Beherzigen Sie diese!
- Auch auf Ihren Mobilgeräten müssen sie beim Online-Spielen genauso umsichtig vorgehen, wie auf Ihrem Computer. Angreifer beginnen bereits mobile Plattformen ins Visier zu nehmen.

Tipps für Eltern

Achten Sie als Elternteil darauf, dass Ihre Kinder die obigen Schritte ebenfalls befolgen bzw. führen Sie diese für jüngere Kinder durch. Klären Sie Ihre Kinder über die Risiken auf, die bei Online-Spielen bestehen. Bildung und ein offener Dialog sind die effektivsten Mittel um Ihre Kinder zu schützen. Um das Gespräch rund um die Sicherheit mit Ihrem Kind zu führen, könnten Sie sich die Spiele und Online-Welten, in denen sich die Kinder bewegen, von ihnen selbst zeigen und erklären lassen. Spielen Sie vielleicht sogar eine Runde mit ihnen. Lassen Sie sich zudem die verschiedenen Leute beschreiben, die die Kinder online kennenlernen. Online-Spiele können einen großen Anteil am Sozialleben Ihrer Kinder haben; indem Sie mit Ihnen sprechen oder ein offenes Ohr bieten, können Sie frühzeitig Probleme identifizieren und sie viel besser schützen als jede Technologie es könnte.

Weiterführende Informationen

Social Engineering:	http://www.securingthehuman.org/ouch/2014#november2014
Phishing Angriffe:	http://www.securingthehuman.org/ouch/2013#february2013
Passwörter:	http://www.securingthehuman.org/ouch/2013#october2013
Was ist Antivirus?:	http://www.securingthehuman.org/ouch/2014#december2014
Sicher im Netz:	https://www.sicher-im-netz.de/online-spiele

Informieren Sie Sich

Abonnieren Sie den monatlichen OUCH! Security Awareness Newsletter, greifen Sie auf die OUCH! Archive zu und lernen Sie mehr über SANS Security Awareness Angebote unter http://www.securingthehuman.org.

Deutsche Ausgabe

OUCH! wurde aus dem Englischen übersetzt von Marek Kreul und René Wiedewilt. Beide arbeiten für das CERT eines deutschen IT-Dienstleisters und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis