12.06.2014
WM 2014

So schützen sich Fußballfans vor Cyber-Fouls

Bei sportlichen Großereignissen spielen auch Cyberkriminelle ihr Spiel. Die Sicherheitsexperten von G DATA rechnen während der WM 2014 mit einem Anstieg von Online-Betrugsfällen und geben Tipps, wie sich Fußballfans - zuhause oder in Brasilien - vor Datendieben schützen können.

Ahnungslose Fußballfans werden leicht zu Opfern von Cyberkriminellen. Als besonders gefährlich stuft G DATA Spam-Mails und manipulierte Internetseiten ein, die den Empfängern Eintrittskarten, Flüge oder exklusive Videos versprechen. Ziel der Täter ist es, an persönliche Daten wie Kreditkarten-Informationen oder Zugangsdaten für E-Mail-Konten zu gelangen oder Fan-PCs mit Schadcode zu infizieren. Der Anbieter von Sicherheitslösungen zeigt, mit welchen Betrugsmaschen Cyberkriminelle auf die Jagd gehen:

Manipulation bekannter Internetseiten

Der Song „'54, '74, '90, 2010“ war in Deutschland ein WM-Hit, so dass viele Fußballfans auch dieses Jahr auf einen stimmungsvollen Song hoffen und die Webseite der beliebten Band besuchen. Kriminelle hackten und manipulierten die Internetseite der Sportfreunde Stiller. G DATA erkannte die Manipulation und warnte die Betreiber der Seite. Vor und während der WM 2014 muss damit gerechnet werden, dass Cyberkriminelle versuchen werden, bekannte Webseiten mit Fußball-Bezug zu kompromittieren.

Ticket-Verkauf

Spam-Mails oder Internetseiten versprechen die besten Plätze zum günstigen Preis. Internetnutzer sollten die Angebote genau prüfen. Der Verkauf von Eintrittskarten läuft über den Weltfußballverband FIFA. Fans können Karten regulär nur über die FIFA oder durch Gewinnspiele der offiziellen Sponsoren beziehen. Bei Käufen über Verkaufsplattformen ist Vorsicht geboten, denn hier können Betrüger lauern.

Auch bei angeblichen Ticketbestätigungen sollte man vorsichtig sein, oftmals sind Schaddateien an den vermeintlichen PDFs angehängt.

Eine weitere Masche: WM-Spam-Mails, die per Link auf angebliche Verkaufsseiten führen. Dort haben es die Täter auf persönliche Daten wie z. B. Kreditkarten-Informationen abgesehen oder sie versuchen, per Drive-by-Download unzureichend geschützte Rechner mit einem Computerschädling zu verseuchen.

Angebote für Flüge und Übernachtungen

Günstige Hotels und preiswerte Flüge sind während einer WM bei Fans heiß begehrt. Doch das vermeintliche Schnäppchen für Kurzentschlossene kann sich schnell als Betrug entpuppen. Gefälschte Angebote werden per Mail verschickt, um die Empfänger auf

Schadcode-Webseiten zu locken oder für vermeintliche Flug- und Hoteltickets bezahlen zu lassen, die es gar nicht gibt.

Exklusive News und Videos

Eine beliebte Masche bei Cyberkriminellen ist das Versenden von Spam-Mails, die exklusive Nachrichten oder Videos versprechen. Damit wollen die Täter die Empfänger auf kompromittierte Webseiten locken, um den PC mit Schadcode zu infizieren.

Was Fußballfans in Brasilien beachten sollten:

- Ungesicherte öffentliche WLAN-Funknetze meiden - Cyberkriminelle warten nur darauf, den Datenverkehr mitlesen zu können und sensible Daten zu stehlen.
- Online-Shopping oder Bankgeschäfte niemals über solche Verbindungen tätigen.
- Vorsicht bei der Nutzung von Internetcafés – hier sollten niemals vertrauliche eingegeben werden.
- Am besten eine separate E-Mail-Adresse für den Aufenthalt in Brasilien anlegen.

Wichtige Schutzmaßnahmen – nicht nur in WM-Zeiten

Die G DATA-Experten geben außerdem Tipps für den Schutz gegen Cyberkriminelle, die generell beherzigt werden sollten:

- Auf dem PC sollte eine aktuelle Sicherheitslösung verwendet werden.
- Mobilgeräte wie Smartphones oder Tablets sollten mit einer Security-App ausgestattet sein. So sind diese unterwegs vor Schadsoftware und gefährlichen Apps geschützt.
- Bei Sicherheitslösungen für Mobilgeräte sollte der Diebstahlschutz aktiviert sein.
- Bei Notebooks bietet es sich an, sensible Daten auf der Festplatte zu verschlüsseln. So haben Langfinger keine Chance, an die Daten zu gelangen.
- Sperrnummern notieren: Fußball-Fans, die nach Brasilien reisen, sollten sich die Servicenummern ihres Mobilfunkanbieters sowie der Kredit- und EC-Kartendienstleister notieren. Bei Verlust kann so die betroffene Karte umgehend gesperrt werden.
- Funkverbindungen sollten nur dann genutzt werden, wenn diese auch benötigt werden. Per Bluetooth oder WLAN versenden Angreifer Dateien, die mit Schadcode gespickt sind.
- Das Betriebssystem, die eingesetzte Software und Apps sollten immer auf dem aktuellsten Stand gehalten werden.
- **Immer genau hinsehen:** Unseriöse E-Mails mit verlockenden Angeboten, angeblichen Buchungsbestätigungen oder unbekannten Gewinnspielbenachrichtigungen zur WM sofort löschen, Dateianhänge und eingefügte Links nicht anklicken!