G Data deckt "Fußball Hacks" auf

(ddp direct) Die Experten der G Data SecurityLabs, der Forschungsabteilung des deutschen Anbieters von IT-Sicherheitslösungen, haben in Hackerforen Informationen gefunden, die im Zuge der EM 2012 auf erfolgreiche Angriffe auf offizielle Webseiten von europäischen Fußballclubs, Fan-Seiten und einen europäischen Fußballverband schließen lassen.

Laut Aussage des Täters, ist seine Aktion politisch motiviert (Hacktivismus): [] Fußballvereine machen enorme Umsätze, während die Wirtschaftskrise die Mittelschicht ruiniert (frei übersetzt aus dem Englischen).

Problem/Risiko: Durch die Veröffentlichung der Schwachstellen ist nicht auszuschließen, dass Online-Kriminelle versuchen werden aus den bestehenden Sicherheitslücken der Webseiten Profit zu schlagen und ihrerseits die Seiten angreifen. Gewonnene persönliche Daten könnten so für Folgeangriffe eingesetzt werden (z.B. Spam-Attacken für den Verkauf von gefälschten Tickets) oder werden an Datenhändler weiter verkauft.

G Data hat bereits mit den bisher bekannten Vereinen bzw. Webseitenbetreibern Kontakt aufgenommen und diese über das Sicherheitsproblem informiert.

Eine Aussage zur Anzahl der erfolgreich attackierten Webseiten kann nicht getroffen werden. Es ist aber nicht auszuschließen, dass es dem Täter europaweit gelungen ist, Daten im großen Stil zu erbeuten.

Webseiten von denen der Hacker Daten veröffentlicht hat:
- Europäische Fußballvereine aus Italien, Spanien, Griechenland, Zypern, Deutschland, Niederlande u.a. Erstligavereine und auch Zweitligavereine
- Laut seinen Angaben gehört auch ein europäischer Fußballverband zu den Opfern

Art der durchgesickerten Daten:
- Admin-Benutzernamen, Admin-Passwörter
- Admin-Benutzernamen, Admin-Passwörter, Host Adressen
- Benutzernamen, Benutzerpasswörter
- Benutzernamen, E-Mail Adressen
- Benutzernamen, Benutzerpasswörter, E-Mail Adressen, Benutzer IPs, Benutzertyp
- Benutzernamen, Klarnamen, E-Mail Adressen
- Benutzernamen, Klarnamen, E-Mail Adressen, vollständige Adressen, Telefonnummern (Festnetz und Mobil), Ausweisnummern, Banknamen, Kontonummern.
- Klarnamen, Schulnamen, E-Mail Adressen, Telefonnummern

Webseiten, die der Hacker als verwundbar nennt, von denen aber (noch) keine Daten veröffentlicht wurden:
- Private Fan-Blog Seite mit einem Namen, der sehr eng verbunden ist mit der UEFA EURO 2012
- Webseite eines Stadions, das offizieller Austragungsort der UEFA EURO 2012 ist

Daten, die von diesen verwundbaren Seiten potentiell durchsickern könnten:
- Fan-Blog: Benutzernamen, E-Mail Adressen, Nutzerpasswörter, Stadt, Lieblingsverein, Identität in sozialem Netzwerk.
- Stadion: Klarnamen, Passwörter, Telefonnummern, E-Mail Adressen
- Möglicherweise noch mehr Daten. Zum Beispiel kann man auf der Stadionwebseite Tickets für Konzerte etc. buchen. Bei einer Bestellung könnten also Bankdaten verlangt werden, die unter Umständen auch in den lokalen Datenbanken liegen könnten.

Wie hat der Angreifer die Seiten attackiert?
- Der Angreifer nennt in einigen Fällen SQL-Injektionen als Angriffsvektor und in anderen Fällen CRLF-Injektionen
- SQL-Injektionen: Eine Applikation wird dazu überredet SQL-Code auszuführen, denn sie normalerweise nicht ausführen würde. Gelingt es einem Angreifer, Code direkt in ein SQL-Statement einzuschleusen, dann kann er damit fast beliebige Dinge anstellen, u.a. Kopieren, Löschen oder Ändern von Daten in Datenbanken
Dominante Schwachstelle: unbereinigte bzw. ungefilterte Nutzereingaben in Eingabefeldern auf Webseiten
- CRLF-Injektionen: Ein Angreifer kann z.B. cross-site scripting Attacken und andere Exploits mit dieser Methode ausführen. Er sendet eine speziell präparierte http Anfrage an einen Webserver, um die Antworten des Webservers zu manipulieren.
Dominante Schwachstelle: unbereinigte bzw. ungefilterte Nutzereingaben in Eingabefeldern auf Webseiten
- Der Angreifer veröffentlichte eine detaillierte Angriffsanleitung für eine der Webseiten und es war uns möglich, das Bestehen der Sicherheitslücke zu verifizieren.

Motivation:
- Einerseits nennt der Angreifer in einigen der durchgesickerten Daten Spaß als sein Motiv.
- Andererseits hat er am Nachmittag des 12.6. eine Nachricht veröffentlicht, in der er seine Angriffe damit begründet, dass Fußballvereine enorme Umsätze machen, während die Wirtschaftskriese die Mittelschicht ruiniert. (frei übersetzt aus dem Englischen).

Shortlink zu dieser Pressemitteilung:
http://shortpr.com/sl1c8q

Permanentlink zu dieser Pressemitteilung:
http://www.themenportal.de/wirtschaft/g-data-deckt-fuball-hacks-auf-85327

=== Sicherheitswarnung zur Fußball-Europameisterschaft: G Data deckt "EM-Hacks" auf (Bild) ===

Die Experten der G Data SecurityLabs, der Forschungsabteilung des deutschen Anbieters von IT-Sicherheitslösungen, haben in Hackerforen Informationen gefunden, die im Zuge der EM 2012 auf erfolgreiche Angriffe auf offizielle Webseiten von europäischen Fußballclubs, Fan-Seiten und einen europäischen Fußballverband schließen lassen.

Shortlink:
http://shortpr.com/wuevq0

Permanentlink:
http://www.themenportal.de/bilder/sicherheitswarnung-zur-fussball-europameisterschaft-g-data-deckt-em-hacks-auf

Pressekontakt

G Data Software AG

Frau Kathrin Beckert
Königsallee b 178
44799 Bochum

presse@gdata.de

Firmenkontakt

G Data Software AG

Frau Kathrin Beckert
Königsallee b 178
44799 Bochum

gdata.de
presse@gdata.de

Die G Data Software AG, mit Unternehmenssitz in Bochum, ist ein innovatives und schnell expandierendes Softwarehaus mit Schwerpunkt auf IT-Sicherheitslösungen. Als Spezialist für Internetsicherheit und Pionier im Bereich Virenschutz entwickelte das 1985 in Bochum gegründete Unternehmen bereits vor mehr als 20 Jahren das erste Antiviren-Programm.G Data ist damit eines der ältesten Securitysoftware-Unternehmen der Welt.

Das Produktportfolio umfasst Sicherheitslösungen für Endkunden, den Mittelstand und für Großunternehmen. G Data Security-Lösungen sind in weltweit mehr als 90 Ländern erhältlich.

Weitere Informationen zum Unternehmen und zu G Data Security-Lösungen finden Sie unter www.gdata.de

Anlage: Bild