

## Attacke verdeutlicht Gefahr unsicherer Webentwicklung



### Massenweise SQL-Injections: Tausende Webserver automatisch mit Trojaner-Links verseucht

Von Armin Barnitzke

11. Januar 2008

Die Surfgefahr bleibt angespannt – über eine automatisierte Attacke auf SQL-Injection-Verwundbarkeiten haben Cybergangster tausende von Webseiten mit Links auf chinesische Trojaner-Server verseucht. Vermutlich dient ein Bot-Netz aus gekaperten PCs als Ausgangsbasis. Für Experten stellen solche automatisierten SQL-Attacken eine neue Qualität dar.

Kurz nachdem Trojaner-verteilmende Werbebanner auf populären Internetseiten wie Myspace und Blick.ch für Aufregung gesorgt haben („[Werbebanner schleusen Trojaner ein](#)“), sorgt nun eine andere massive Webattacke für Surfgefahr: Tausende von Webseiten wurden mit böartigen Iframes verseucht, die auf ein chinesische Trojaner-Server verweisen. Diese nutzen wohl vor allem kürzlich bekannt gewordene Schwachstellen im Real Player aus, um die PCs der ahnungslosen Surfer mit Malware zu infizieren.

Der Security-Experte Bjoan Zdrnja des Internet Storm Center (ISC): „Wenn man nach der Adresse der Malware-Seite uc8010.com googelt, findet man Tausende von betroffenen Seiten, die alle auf uc8010.com zeigen.“ Dazu gehören die Verbandsgemeinde Heidesheim am Rhein oder der österreichische Restaurant-Führer. Sogar die Presseseiten des Security-Spezialisten CA waren betroffen, sind aber inzwischen bereinigt.

Nach [Analysen](#) des Internet Storm Center wurden die Angriffe wohl über automatisierte Scripts durchgeführt, die eine SQL-Verwundbarkeit in Webanwendungen ausnutzt. Bei einer SQL-Injection wird durch ein nicht ordentlich abgesichertes Eingabefeld in der Webanwendung ein SQL-Kommando an die dahinter liegende Datenbank eingeschleust.

Zdrnja: „Fast alle betroffenen Seiten nutzen den Microsoft-Webserver IIS und die Redmonder Datenbank MS SQL-Server.“ Der Experte hat aber keine Zweifel ihre automatisierte Attacke – die vermutlich ein Bot-Netz aus gekaperten PCs als Ausgangsbasis nutzt – so variieren, dass auch Seiten auf Basis von PHP und MySQL angegriffen werden.

Für das ISC ein weiteres Beispiel, das die Notwendigkeit der sicheren Webentwicklung unterstreicht. Laut Liste des Open Web Application Security Project (OWASP) rangieren Injection-Schwachstellen hinter Cross Site Scripting auf Platz zwei der Liste der gefährlichsten Webverwundbarkeiten.

Automatisierte SQL-Injektionen sind für Security-Experte Stefan Strobel eine neue Qualität. Bisläng kannte der Chef des Beratungshauses cirosec vor allem gezielte SQL-Attacken auf einzelne Server. Als Schutzmaßnahme empfiehlt er Unternehmen die Installation einer Web

cirosec GmbH  
Edisonstraße 21  
74076 Heilbronn  
Tel: 07131 / 59455-0  
Fax: 07131 / 59455-99  
info@cirosec.de  
[www.cirosec.de](http://www.cirosec.de)

## Application Firewall

Solche WAFs gibt es – etwa von der Regensburger Art of Defence – als Zusatzsoftware für den Webserver bereits für einige Tausend Euro. Spezielle Webschutz-Appliances sind ab 15000 Euro erhältlich, Highend-Kisten für die Absicherung kompletter Rechenzentren kosten rund 70000 Euro, so Strobel.

Und auch die Konfiguration solcher Lösung sei nicht so kompliziert wie oft befürchtet. Den Aufwand schätzt Strobel auf wenige Stunden bis zwei Tage – je nach Komplexität der Webanwendung. „Aber wenn eine WAF richtig konfiguriert ist, dann haben Sie das Problem SQL-Injection gelöst.“ Denn solche Lösungen lassen nur erlaubte SQL-Kommandos durch.

Zudem können spezielle Verwundbarkeits-Scans Schwachstellen in der Webanwendung aufdecken. Via Internet mietbare Dienstleistungen von Qualys oder Foundstone/McAfee würden aber nur gängige Schwachstellen finde, so Strobel. Er plädiert daher für Tests vor Ort mit entsprechendem Know-how und Tools.

***computerzeitung.de 11.01.2008***