Gehackte BusinessWeek-Site verteilt Trojaner

Der Antiviren-Hersteller Sophos berichtet, dass auf den Seiten des Wirtschaftsportals böser JavaScript-Code lauert.

heise Security Summary News-Meldung vom 15.09.2008

Einem Bericht des Antiviren-Herstellers Sophos zu Folge wurde die Website des bekannten US-Wirtschaftsmagazins “BusinessWeek“ kompromittiert, so dass sie Besuchern Schadsoftware von russischen Servern unterjubelte.

Offenbar wurde das Portal Opfer eines SQL-Injection-Angriffs, über den Code in die dynamisch erstellten Seiten eingebettet wurde.

Googles Safebrowsing-Liste bestätigt die Analyse. Bei den Tests der Google-Roboter versuchten während der vergangenen 90 Tage 216 Seiten ohne Zustimmung des Anwenders Software zu installieren, also sogenannte Drive-by-Downloads durchzuführen.

Dazu nutzt das eingebettete JavaScript meist bekannte Sicherheitslücken in Browsern aus. Bevorzugtes Ziel ist in der Regel der Internet Explorer, aber auch Firefox-Anwender, die nicht die aktuelle Version einsetzen, laufen Gefahr, dass ihr System über Sicherheitslükken infiziert wird.

Der Vorfall bestätigt eindrücklich die Analyse der Anti-Phishing Working Group, die seit Beginn des Jahres einen dramatischen Anstieg bei der Zahl der Sites beobachtet, über die Crimeware verteilt wird.

Die Parallele zu den seit etwa einem halben Jahr systematisch ausgenutzten Sicherheitslücken in Web-Applikationen, die mit Datenbanken kommunizieren und dabei nicht ausreichend gesichert sind, liegt auf der Hand.