

Web 2.0:

Worauf man achten sollte

Unter dem Begriff Web 2.0 erfreuen sich soziale Netzwerke, Videos und benutzergenerierte Inhalte in interaktiven Portalen wachsender Beliebtheit. Doch was dem Anwender gefällt, sollte dem IT-Verantwortlichen Sorgen bereiten. Denn wer die neuen Gefahren aus dem Web 2.0 nicht kennt, kann sich und seine Benutzer nicht ausreichend davor schützen.

SQL-Injections: Interaktive Web 2.0-Webseiten mit Ajax-Technologie (Asynchronous Javascript and XML) machen es Angreifern leichter, Sicherheitslücken in Web-Anwendungen auszunutzen. Wird eine Lücke beispielsweise in einer beliebten Blogsoftware bekannt, können entsprechende Würmer tausende von Blogs innerhalb von Minuten mit Malware infizieren.

Drive-by-Downloads durch Iframes: Wer sich früher mit Trojanern oder Spyware infizierte, hatte wohl eine Hackerseite oder ein pornografisches Lockangebot besucht. Heute können sich Benutzer beim Besuch legitimer Websites beispielsweise von Banken oder Nachrichtenportalen infizieren – ohne dass sie es selber merken. Schuld daran sind unsichtbare Iframes mit Schadcode, die Angreifer z.B. per SQL-Injection in eine seriöse Website einschleust haben.

Gefahr durch Mashups: Immer mehr anerkannte Websites beziehen ihre Inhalte aus unterschiedlichsten Quellen – das Schlagwort ist hier Mashup. Dadurch reicht bereits die Infektion einer einzigen Quelle aus, um über zahlreiche angesehene Webseiten Schadcodes an nichtsahnende Benutzer auszuliefern.

Videos als Einfallstor: Durch Sicherheitslücken in Abspielsoftware wie dem Windows Media Player können manipulierte Videoclips beispielsweise von YouTube zum Einfallstor für Spyware werden.

Kontinuierliche Kontrolle notwendig: Im Web 2.0 ist eine fortlaufende Kontrolle aller von Benutzern angefragten Webseiten auf böartige Codes erforderlich, denn statische URL-Filter reichen nicht mehr aus. Eine Alternative sind moderne Cloud Computing-basierende Sicherheitsdienste, die von möglichst vielen Nutzern angefragte Webseiten kontinuierlich und fast in Echtzeit auf Schadprogramme prüfen.

Quelle: Dietmar Schnabel, Sales Director bei Blue Coat Systems