Shop-Risiken: Falscher Umgang mit Session-ID

Viele Shopbetreiber und Onlineshopper sind mittlerweile sensibler im Umgang mit dem Thema Sicherheit geworden. So erfolgt der Großteil der Internetbestellungen beispielsweise über gesicherte SSL-Verbindungen. Tatsächlich existieren jedoch mehr Bedrohungen als das reine Abhören der Datenleitung.

Vorsicht, denn Kundendaten könnten in falsche Hände gelangen...

Mit Hilfe einer Session-ID ordnet das Shopsystem dem Käufer eine Sitzung zu, damit beispielsweise Login-Status und Warenkorb-Inhalt während seiner Aktionen erhalten bleiben. Für die Verwendung von Session-IDs existieren im Wesentlichen zwei Bedrohungen, die wohl den meisten Shopbetreibern nicht bewußt sind:

1. Session-Hijacking

Außer der Session-ID werden meist keine eindeutigen Parameter des Käufers gespeichert. Daher reicht einem vermeintlichen Angreifer die Kenntnis der Session-ID aus, um die Sitzung des Käufers trotz bestehender SSL-Verbindung zu übernehmen. Moderne Shopsysteme bieten in der Regel, durch Vergabe wirklich zufälliger Session-IDs, einen relativ guten Schutz gegen das einfache Erraten der laufenden Session-ID.

Schleust jedoch ein Angreifer per Cross-Site-Scripting (XSS) schadhaften Code in Ihr Shopsystem ein und wird dieser vom ahnungslosen Käufer ausgeführt kann die Session-ID an den Angreifer übertragen und entsprechend die Session übernommen werden. Ist die Session erst übernommen können beispielsweise Kundendaten eingesehen oder Fehlbestellungen getätigt werden. Ein unschönes Szenario, sowohl für den Shopbetreiber als auch für den Kunden.

Eine weitere weitestgehend unbekannte Lücke, welche die Übernahme einer Session ermöglichen kann, ist das sogenannte “Referrer-Leck”. Ist die Session-ID als Parameter in der URL gespeichert und der Käufer klickt auf einen externen Link im Shop, wird die aktuelle URL aus der Adresszeile des Shops vollständig an den nächsten Webserver übertragen. Der Betreiber dieses Webservers könnte nun bei der Auswertung der referenzierenden Webseiten die entsprechende Session-ID auslesen und gegebenfalls übernehmen.

2. Session-Fixation

Bei der Session-Fixation wird die Sitzung durch den Angreifer selbst gestartet. Er schickt dem Opfer einen Link, der die gültige Session-ID enhält. Mit Umleitungsdiensten oder E-Mails im HTML-Format kann die Ziel-URL problemlos maskiert übermittelt werden. Klickt der Käufer auf den Link und meldet sich anschließend im Shop an, kann der Angreifer bei einer “schwachen” Sessionverwaltung die Sitzung übernehmen. Auch wenn mittlerweile viele Onlineshopper bereits von Phishing-Mails gehört haben, würden derartige Links in Emails dennoch häufig geklickt.

Mögliche Sicherheitsmaßnahmen

Je nach Shopsystem kann die Session-ID auch ohne “Mitschleifen” über die URL gespeichert werden. Dies kann durch Hidden Fields oder Cookies realisiert werden. Falls Sie die Session-ID doch in der URL speichern und das Shopsystem selbst entwickelt haben, verknüpfen Sie weitere Informationen wie den verwendete Browser mit der Session. Dies bietet zumindest einen einfachen Schutz.
Speichern Sie diese Information zusätzlich, damit es für eine Übernahme nicht ausreicht, nur die

Session-ID herauszufinden. Aus Datenschutzgründen ist es jedoch dringend zu vermeiden, die IP-Adresse des Nutzers zu verarbeiten. Zudem sollten Sie externe Links nur für vertrauenswürdige Seiten setzen und verhindern, dass Benutzer ihre eigenen Links über Eingabefelder hinzufügen.

Praxistipp: Halten Sie wichtige Grundsätze ein

Folgende allgemeine “Session-Spielregeln” gilt es einzuhalten. Sie bestimmen, nach welchen Aktionen eine Sitzung invalidiert wird. Diese sind mindestens:

Login: nach erfolgreicher Anmeldung muss die alte Session-ID ungültig werden und der Kunde eine neue erhalten. Dadurch wird eine Session-Fixation verhindert.
Logout: der Käufer muss die Session aktiv beenden können. Versäumt er dies, muss er per Timeout automatisch ausgeloggt werden.
Systemfehler: Bei bewussten Manipulationen durch einen Angreifer können Systemfehler auftreten. Tritt solch ein Fehler auf, sollte die Session automatisch ungültig werden. Zudem kann man die Ausgabe derartiger Fehlermeldungen in der Server-Konfiguration deaktivieren.
Diese und weitere Hinweise finden Sie auch im Maßnahmenkatalog des Bundesamts für Sicherheit in der Informationstechnik.

Weitere Beiträge zum Thema Shop-Sicherheit / Security finden Sie in unserer Blogkategorie Sicherheit.