Webanwendungssicherheit

Den Missbrauch des Vertrauenskontextes verhindern

Vertrauenskontext ist das Umfeld, das bestimmt, wie viel Vertrauen wir einer Sache entgegenbringen. Auf das Spendenformular, das in der Bank am Schalter liegt, übertragen wir das (in der Regel hohe) Vertrauen, welches wir der Bank selbst entgegenbringen. Wäre die Hilfsorganisation nicht seriös, würde unsere Bank das Formular nicht auslegen. Dasselbe Formular in der Fußgängerzone von einem unbekannten Vermittler verteilt hätte es deutlich schwerer, bei uns die Schwelle des Misstrauens zu überwinden. Oder: Der unglaublichen Enthüllungsstory schenken wir eher Glauben, wenn wir sie in der Süddeutschen lesen (hoher Vertrauenskontext) als wenn wir sie dem Exklusiv-Bericht der Regenbogenpresse entnehmen (geringer Vertrauenskontext).

Voraussetzung dafür, dass diese Art der Herleitung von Vertrauen funktioniert, ist, dass wir uns der Echtheit der Kriterien, die wir für die Bewertung des Vertrauens heranziehen, auch versichern können. Zeigt uns der Finanzberater die Zeitschrift 'Finanztest', in der die von ihm gelobte Geldanlage entsprechend gut abgeschnitten hat, dann werden wir ihm nicht unterstellen, dass er das Heft gefälscht hat. Das wäre wohl zu aufwändig und am Kiosk könnten wir uns jederzeit von der Echtheit überzeugen. So etwas kommt also im täglichen Leben in der Regel nicht vor. Und falls doch, dann haben wir eine Reihe von Merkmalen, die uns bei der Einschätzung helfen und Misstrauen aufkommen lassen, wenn da was nicht stimmt.

So vorgeprägt begeben wir uns ins Web und übersehen dabei, dass die vermeintlich sicheren Kriterien, die den Vertrauenskontext herstellen, höchst manipulierbar sind. Eine Webseite, die exakt so aussieht wie die uns vertraute Anmeldemaske zum Online-Banking macht uns Glauben, dass wir uns auch auf der Website der Bank – in vertrauenswürdigem Umfeld – befinden. Wir bedenken nicht, dass es für einen Betrüger außerordentlich leicht ist, eine gefälschte Webseite, womöglich noch mit einem ähnlich klingenden Namen, irgendwo im Internet abzulegen. Und so geben wir unsere Zugangsdaten ohne weitere Echtheitsprüfung in die Anmeldemaske ein und damit geradewegs in die falschen Hände.

Website-Spoofing und Phishing

Das vorliegende Beispiel zeigt, wie man es nicht machen sollte: Eine Versteigerungsplattform verschickt an ihre Nutzer alle paar Wochen eine Werbemail. Da der Fokus nicht auf der Sicherheit, sondern einzig auf dem Erzeugen von Kauflust liegt, ist diese peppig und deshalb im HTML-Format aufgemacht. Im Gegensatz zu einer E-Mail im Textformat, in der ein enthaltener Link genauso dargestellt

wird, wie er beim Klick auch an den Browser übergeben wird, lassen sich in HTML-Mails die Links hinter Texten oder Grafiken verstecken. Im Fuß der E-Mail heißt es "Klicken Sie hier, wenn Sie unseren Newsletter nicht mehr erhalten möchten". Der Anwender wird durch den regelmäßigen Erhalt dieser E-Mail regelrecht konditioniert und hinterfragt die Echtheit nicht mehr. So wird er jede E-Mail mit demselben Look-and-Feel ganz selbstverständlich als authentisch einstufen.

Für einen Betrüger ist es nun ganz einfach, diesen Sachverhalt auszunutzen, um in die Accounts von Benutzern einzudringen. Die Masche hat als Phishing um sich gegriffen und bisher ist der Schaden wohl nur deshalb noch halbwegs begrenzt, weil die Ausführung zumeist dilettantisch ist.

Ein Phishing-Angriff ist äußerst einfach umzusetzen und kann anonym ausgeführt werden, ohne dass eine Spur zum Betrüger zurückführt. Die Wahrscheinlichkeit, dass der ausgewählte Benutzer darauf reinfällt, bzw. die Erfolgsquote bei einem in der Breite ausgeführten Angriff hängt nun nur noch vom Geschick des Angreifers bzw. der Höhe des betriebenen Aufwandes ab: Eine Verlinkung zu einem Gewinnspiel erhöht die Klickrate wesentlich. Die Verwendung einer Webadresse, die so ähnlich klingt wie die der Versteigerungsplattform, ebenfalls.

Gegenmaßnahmen

Soll der Nutzen des Web nicht auf Dauer Schaden leiden, so dürfen die aus den hier genannten Zusammenhängen resultierenden Probleme keineswegs als Probleme der Anwender abgetan werden. Die Website-Betreiber, die E-Business- oder E-Government-treibenden Institutionen müssen es als ihre Verantwortung annehmen, dass der Anwender nicht zu Schaden kommt. Denn seine Möglichkeiten, sich zu schützen, sind äußerst begrenzt.

Die 'Konditionierung' des Anwenders in der richtigen Weise und der Einschluss semantischer Gesichtspunkte in die Betrachtung der Sicherheit von Webanwendungen sind äußerst wichtige Bestandteile einer nachhaltig abgesicherten Nutzung des Mediums Web. Im „Maßnahmenkatalog und Best Practices zur Sicherheit von Webanwendungen"[i] des Bundesamts für Sicherheit in der Informationstechnik (BSI) sind weitere Bedrohungen genannt, die aus der Vernachlässigung der semantischen Ebene resultieren (insbesondere B100, B110, B260, B265).

Als konkrete Maßnahmen zur Verkleinerung der Angriffsfläche sind insbesondere das Minimalitätsprinzip (M250) und das Identitätsprinzip (M260) anzuwenden.

Fazit

Bei der Betrachtung der Web Application Security muss ein Website-Betreiber auch die Sicherheit auf der semantischen Ebene im Blick haben. Die Entscheidung über die Aufmachung der Website und die Ausprägung von Features, Geschäftsprozessen und Abläufen müssen unter Berücksichtigung der hier geschilderten Zusammenhänge getroffen werden. Dem Benutzer müssen Kriterien an die Hand gegeben werden, an denen er sich orientieren kann und die ihn befähigen, die missbräuchliche Ausnutzung des Vertrauens in eine Website zu erkennen.

[i] http://www.bsi.de/literat/studien/websec/WebSec.pdf

Thomas Schreiber, SecureNet GmbH

Impressum

DATAKONTEXT FACHVERLAG

Verlag: DATAKONTEXT-FACHVERLAG GmbH
Augustinusstr. 9d
50226 Frechen
Tel.: 02234/96610-0
Fax: 02234/96610-9
fachverlag@datakontext.com
www.datakontext.com

Redaktionelle Partner: