© compressor / Fotolia.com

Web 2.0 – schön, schnell und gefährlich

Erkenntnisse aus dem Forschungsprojekt Padiofire

Im Projekt Padiofire beschäftigen sich Forscher der Technischen Universität Cottbus (BTU), der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) und der genua mbh aus Kirchheim mit Methoden zur besseren Absicherung von Web-2.0-Anwendungen. Der Beitrag geht auf die Gefahren im Web 2.0 ein und betrachtet auf Basis erster Studienergebnisse, welche Schutzmechanismen existieren, ob diese ausreichend sind und an welchen Stellen man neue Wege zur Absicherung braucht.

Von Steffen Ullrich und Alexander von Gernler, Kirchheim

Im Gegensatz zum „alten Web“ mit seinen eher statischen Inhalten nutzen wir im modernen Web viele stark interaktive auf JavaScript beruhende Applikationen. Jeder Anwender hat hier außerdem die Möglichkeit, mit wenigen Klicks eigene Inhalte verfügbar zu machen. Hinzu kommt eine enge Integration von sozialen Netzwerken in die meisten großen Websites, ebenso wie die Integration von Anzeigen, die durch omnipräsente Tracking-Mechanismen bestmöglich auf den Nutzer zugeschnitten werden. Eine Vielfalt von Webbrowsern oder spezifischen mobilen Applikationen ermöglicht es uns, jederzeit und von fast überall auf diese Inhalte zuzugreifen. Der Komfort dieser Ubiquität führt zur Auslagerung von immer mehr privaten und geschäftlichen Daten und Aktivitäten in das Internet.

In diesem Artikel betrachten wir die dominanten Angriffsvektoren im heutigen Web sowie die Möglichkeiten des Schutzes im Detail. Wir nehmen dabei die Sicht eines Anwenders ein, welcher normalerweise nicht die Kontrolle über die Webapplikationen und Websites hat, die er besucht. Das Ziel des Anwenders ist es, in einer Umgebung, die keine hundertprozentige Sicherheit bietet, sich trotzdem sicher bewegen zu können und die persönlichen Folgen von Angriffen zu minimieren.

Grundschutz

Oft gesagt und doch immer noch gern ignoriert: Ein solider Grundschutz des Systems verringert die Wahrscheinlichkeit eines erfolgreichen Angriffes. Dazu gehört ein modernes Betriebssystem, inklusive aller Sicherheitsupdates, auf welchem keine überflüssigen Programme installiert sind. Diese sollten ebenfalls auf dem aktuellen Stand sein. Auch wenn das heute selbstverständlich scheint, so werden immer wieder uralte Bugs in Office-Applikationen, Flash-Playern oder dem Acrobat Reader erfolgreich ausgenutzt.

Viele Anwender verstehen noch, dass der Besuch der Grauzonen des Internets (z. B. Torrent Sites, Pornografieanbieter) unerwünschte Folgen haben kann und vermeiden solche Besuche. Meist verschwenden sie aber keinen Gedanken daran, ob das Netzwerk, in dem sie sich gerade befinden, vertrauenswürdig ist – egal ob es am Arbeitsplatz, zu Hause oder im Café ist. Dabei ist es für einen Angreifer in vielen Netzwerken ein leichtes, dem Webbrowser eines Opfers andere Daten als die angeforderten unterzuschieben. Sobald man sich also in einem Netzwerk befindet, dem man nicht voll vertrauen kann, sollte man einen anderen Rechner, ein VPN, einen anderen Nutzer

auf dem Rechner oder ein anderes Browser-Profil benutzen.

Auch ist es hilfreich, vor dem Öffnen von Anhängen in einer E-Mail, Klicken auf Links und Scannen von QR-Codes lieber einmal länger zu überlegen und sich nicht darauf zu verlassen, dass die installierte Sicherheitslösung etwaige Probleme abfängt.

Ebenso zum Grundschutz gehört ein vorsichtiger Umgang mit den eigenen Daten. Das beinhaltet die Weitergabe an Personen oder Firmen, bei denen man nicht sicher sein kann, dass diese die Informationen unerwünscht nutzen oder weitergeben. Bei Anbietern aus den USA sollte man im Zweifel den Zugriff von Regierungsbehörden, Gerichten und Geheimdiensten gleich mit einplanen. Zu den eigenen Daten gehören auch Zugangsdaten. Leider ist die Sicherheit bei der Ablage von Zugangsdaten bei vielen Anbietern eher schlecht und die Veröffentlichung von Unmengen geknackter Zugangsdaten ist keine Seltenheit mehr. Um zumindest einen weiterführenden Missbrauch dieser Daten zu verhindern, sollte man keine gleichen oder ähnlichen Zugangsdaten über mehrere Websites hinweg benutzen. Ein Fehler, den viele Nutzer aus Bequemlichkeit begehen.

Malware

Laut einer Studie von Sophos werden 80 Prozent der Malware über Websites verbreitet, deren Betreiber sich dessen nicht bewusst sind. Da moderne Betriebssysteme im Allgemeinen einen guten Schutz gegenüber den klassischen Buffer-Overflow-Techniken haben, nutzen Kriminelle hier zunehmend die Vielfalt alter, aber auch bisher unbekannter Lücken (Zero-Day-Exploits) in Adobe Flash, Acrobat Reader oder Java, um den Rechner des Nutzers zu infizieren.

Zum Schutz der Anwender untersuchen große Suchmaschinen-Provider wie Google oder Microsoft die von ihnen indizierten Websites auch auf Malware und stellen diese Informationen in sogenannten Blacklists zur Verfügung, welche in alle großen Browser eingebaut sind. Ähnlich versuchen die Hersteller von Virenscannern und anderen Sicherheitslösungen mittels Honeypots, Angriffsversuche zu entdecken und zu analysieren. Die Ergebnisse davon fließen dann zum Beispiel in die Aktualisierung der Virenscanner ein. Zusätzlich zum Nutzen dieser Sicherheitslösungen hilft es in den meisten Fällen schon weiter, Java von den eigenen Rechnern zu verbannen oder zumindest das Java Plugin im Browser zu deaktivieren. Ist man allerdings auf Java im Browser angewiesen, so sollten eingebundene Java-Applets zumindest nicht automatisch ausgeführt werden. Bei Chrome und Firefox ist das entweder standardmäßig bereits der Fall oder ist über eine Click-To-Play-Option beziehungsweise Erweiterung einstellbar. Ähnlich sollte man bei Adobe Flash vorgehen: Hier leistet die „FlashBlock"-Erweiterung für Chrome und Firefox gute Dienste.

Und auch wenn es eine unpopuläre Empfehlung sein mag: Da ein nicht unerheblicher Teil der Malware über oft undurchschaubare Anzeigennetzwerke mit ihren vielen „Affilates" kommt, ist ein Anzeigenblocker wie AdBlockPlus ebenfalls eine wichtige Sicherheitskomponente und nicht nur Komfort. Praktischer Nebeneffekt von AdBlockPlus ist, dass man beim Surfen Bandbreite spart, weil das Laden der vielen Anzeigengrafiken entfällt. Derartige Bilder machen laut Studien mehr als 25 Prozent des weltweiten Web-Traffics aus.

Einen zusätzlichen Schutz können bessere Perimeter-Firewalls bieten, indem sie ebenfalls Blacklists wie in den Browsern einsetzen und den durchfließenden Datenstrom mit einem Virenscanner untersuchen. Zumeist finden solche zentralen Lösungen aber tendenziell weniger Angriffe als ein lokaler Virenscanner, da lokale Scanner Malware auch noch über ihr Verhalten auf dem Client-Rechner und durch Beobachtung über einen längeren Zeitraum identifizieren können. Dagegen sind Firewalls über ihre zentrale Administration eventuell für den Einsatz in Firmen eine praktikablere Lösung. Client-seitige Sicherheitslösungen und Perimeter-Firewalls können sich aber auf jeden Fall sinnvoll ergänzen, besonders wenn durch Kombination von Blacklists und Virenscannern unterschiedlicher Hersteller die Wahrscheinlichkeit einer erfolgreichen Unterwanderung der Sicherheitsmechanismen sinkt.

Cross-Site-Scripting (XSS)

XSS ist eine weitere Angriffsform, die durch den intensiven Einsatz von JavaScript im Web 2.0 stark gestiegen ist. Die Grundidee ist, dass der Angreifer einer Website Skripte seiner Wahl unterschieben kann,

Website mit sozialen Plugins – bereits beim Laden wandern Daten an Facebook und Co. (Bild: genua)

welche dann der Anwender ausführt. Da das JavaScript im Kontext der aufgerufenen Website ausgeführt wird, kann es alles das tun, was auch der (evtl. eingeloggte) Anwender auf der Website tun kann.

Die bekannteste Form von XSS ist Reflected XSS, bei dem das schädliche Skript zum Beispiel in einen Link eingebettet wird, den das Opfer anklickt. Durch fehlerhafte Validierung aufseiten des Servers wird dieser Schadcode dann in die vom Server ausgelieferte Seite eingebettet und schließlich vom Anwender ausgeführt. Aktuelle Browser wie Chrome und Internet Explorer haben Heuristiken eingebaut, um diese Art von Angriffen zu erkennen. Diese arbeiten zwar recht gut, aber eben nicht perfekt. Firefox bietet einen solchen Schutz zum Beispiel über die sehr gute NoScript-Erweiterung, die auch gegen viele weitere Attacken hilft. Wegen der notwendigen Anpassung an das eigene Surfverhalten ist sie jedoch für einen unbedarften Anwender leider nicht praktikabel benutzbar.

Eine weitere Form von XSS ist Stored XSS, bei dem der Schadcode schon vor Längerem, etwa bei einem Angriff auf den Server, in die Website injiziert wurde. Einen effektiven Schutz davor bietet derzeit keine Sicherheitslösung. Allerdings kann man mit der NoScript-Erweiterung für Firefox und Chrome ein dem eigenen Surfverhalten angepasstes Profil erstellen und so die Menge an Websites, auf denen man JavaScript erlaubt, klein halten. Aber wie bereits gesagt, sind nur technisch versierte Anwender in der Lage, diese Erweiterung sinnvoll anzupassen.

Und schließlich macht der größte Teil der Websites eine Art von XSS selbst: durch die Einbindung von sozialen Netzwerken wie Facebook und Twitter, Anzeigennetzwerken und Tracking-Diensten. Denn obwohl die Websites im Allgemeinen keinen Einfluss auf die Inhalte oder die Sicherheit der eingebetteten Dienste haben, werden diese oft direkt als Skript eingebunden und bewegen sich daher im gleichen Sicherheitsbereich wie die eigentliche Website. Wer diese starke und unsichere Integration nicht benötigt, dem helfen Anzeigenblocker wie AdBlockPlus oder auch NoScript.

Einige wenige Perimeter-Firewalls haben auch Heuristiken für Reflected-XSS-Attacken. Diese sind tendenziell nicht schlechter als die im Browser eingebauten, da die Antwort vom Server nicht tief genug analysiert wird. Gegen Stored-XSS-Attacken gibt es derzeit keine Lösungen in Perimeter-Firewalls. Das Forschungsprojekt Padiofire soll diese Situation verbessern.

Cross-Site-Request-Forgery (CSRF)

Eine weitere Gefahr im Web 2.0 sind CSRF-Angriffe. Hier löst ein Angreifer einen Zugriff auf eine andere Website aus, verknüpft mit einer unerwünschten Aktion. Dieser Zugriff wird letztlich vom Browser des Anwenders ausgeführt. Der Angreifer hat damit alle vom Nutzer aus erreichbaren Systeme zu seiner Verfügung, also auch interne Router oder Drucker. Trotzdem ist der Angriff meist nicht zu bemerken: Bedingt durch das Design der Browser, werden beim Zugriff von diesen auch die für die attackierte Website gespeicherten Authentifizierungsdaten und Cookies mitgeschickt.

Diese Art von Angriff ist besonders verheerend gegen interne Systeme, da sie oft ohne Authentifizierung beziehungsweise mit Standardpasswörtern eingerichtet sind. Softwareaktualisieren bei Sicherheitsproblemen führen außerdem die meisten Nutzer nicht durch beziehungsweise bieten Hersteller diese nicht an.

Browser bieten gegen CSRF-Attacken keinen eingebauten Schutz, aber mithilfe der NoScript- oder CsFIRE-Plugins für Chrome oder Firefox kann man sich wappnen. Ein Anzeigenblocker kann auch hier Schutz bieten, indem er allgemein die Menge an potenziell bösartigen Websites verringert. In Perimeter-Firewalls gibt es ebenfalls derzeit keinen Schutz gegen diesen Angriff. Dazu kommt, dass Zugriffe auf lokale Systeme in den meisten Fällen auch nicht über die Perimeter-Firewall geleitet werden und damit dort prinzipiell keine Angriffserkennung möglich ist.

Angriffe auf lokale Systeme

Auch wenn wir in diesem Artikel den Fokus auf Angriffe aus Sicht des Anwenders legen und Lücken in den genutzten Websites selber nicht betrachten, so sind doch lokale Systeme oft unter der Verwaltung der Anwender selbst. Spätestens bei Attacken wie CSRF sollte klar geworden sein, dass keine Firewall das Intranet oder die internen Router einer Firma schützt. Selbst ein Schützen der Intranet-Website über Passwörter nutzt nichts, da der Browser bei einem CSRF einfach den aktuellen Session-Cookie des bereits eingeloggten Nutzers mitschickt. Es ist daher notwendig, die internen Systeme sicher zu halten und speziell auch gegen Attacken zu schützen, die leicht über CSRF ausgeführt werden können. Es gibt aber auch noch weitere Attacken wie DNS Rebinding, die einem Angreifer Zugriff auf interne Systeme ermöglichen.

Angriffe auf Websites

Da der Anwender auf die Sicherheit der Websites, die er besucht, praktisch keinen Einfluss nehmen kann, betrachten wir hier nur kurz die wesentlichen Probleme und die Qualität der existenten Lösungsansätze. Das Hauptproblem auf der Serverseite ist die mangelhafte Überprüfung von Nutzereingaben und die dadurch möglichen Attacken, wie

zum Beispiel SQL-Injections, Upload von Malware, Stored-XSS oder unautorisierter Zugriff auf sensitive Daten (z. B. Passwörter). Das wesentliche Problem bei der Validierung der Nutzerdaten ist jedoch weniger die fehlende Technik, sondern das mangelhafte Problembewusstsein bei Entwicklung und Management. Die meisten Entwickler fokussieren sich auf das reine Funktionieren der Website und haben die Sicherheit eher nicht im Hinterkopf. Dies ist zunächst auch wirtschaftlicher, immerhin funktioniert die Webapplikation ja auch ohne ernsthafte Validierung, und Implementierung oder intensives Testen kosten nur Zeit und Geld, bringen aber vordergründig keine spürbaren Vorteile.

Wenn Serverbetreiber überhaupt externe Tester mit der Überprüfung der Website beauftragen, ist das Ziel meist hauptsächlich das entsprechende Prüfsiegel oder Logo, um Vertrauen bei den Benutzern zu schaffen. Um das zu bekommen, reicht auch ein billiges Angebot. Die schlechtere Qualität der Tests führt zu einer weiteren Kostenersparnis, da keine oder weniger Probleme gefunden werden und die Betreiber sich damit teure Nacharbeit ersparen. Ähnliche Herangehensweisen sind bei der Absicherung der Serversysteme und Datenbanken zu finden, sodass ein Angreifer oft auf diesen Wegen einbrechen kann. Und selbst wenn Lösungen wie Web-Application-Firewalls (WAF) im Einsatz sind, dienen diese meist eher der Kaschierung und nicht der Lösung der Probleme – und sind zudem einem versierten Angreifer nicht gewachsen.

Fazit

Wir haben in diesem Artikel primär die dominanten und direkt gegen die Systeme des Anwenders gerichteten Angriffe betrachtet und bereits hier deutliche Mängel im standardmäßig enthaltenen Schutz entdeckt. An vielen Stellen kann man jedoch durch die Verwendung von Anzeigenblocker und ähnlichen Erweiterungen den Schutz signifikant verbessern. So können Nutzer das überbordende Vertrauen von Site-Betreibern in die Sicherheit von Anzeigen- und Tracking-Netzwerke einschränken. Und obwohl der korrekte Ort, die Probleme zu beseitigen, auf der Seite der Websites wäre, wird es wohl auf absehbare Zeit genug Site-Betreiber geben, die nicht genug Motivation oder Kenntnisse für die ausreichende Absicherung ihrer Systeme haben. Ebenso hält man wohl eher die Nutzer von AdBlockern fern, weil sie ein weitverbreitetes Geschäftsmodell gefährden, auf dessen Basis viele Webseiten arbeiten. Richtig wäre es jedoch, die zugrunde liegenden Sicherheitsprobleme zu beseitigen. ■

Alexander von Gernler ist Technischer Botschafter bei der genua mbh. Steffen Ullrich ist Software-Entwickler, ebenfalls bei der genua mbh.

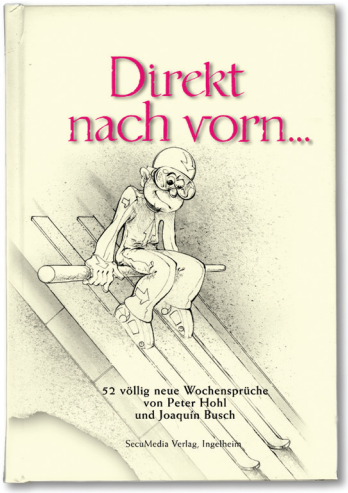
Abonnieren Sie Ihre IT-Sicherheit!

<kes> liefert alle relevanten Informationen zum Thema IT-Sicherheit – sorgfältig recherchiert von Fachredakteuren und Autoren aus der Praxis.

<kes>

- liefert Ihnen strategisches Know-how, damit Sie eine solide Grundlage zur Entscheidungsfindung haben
- berichtet über Trends und Neuentwicklungen
- gibt Hilfen zum Risikomanagement
- erläutert einschlägige Gesetze im Umfeld der IT und TK
- informiert über die wichtigsten Messen und Kongresse
- ermöglicht es Ihnen durch Anwenderberichte von den Erfahrungen anderer zu profitieren
- gibt mit Marktübersichten einen Überblick über ausgewählte Produkte und Dienstleistungen

Dankeschön für Ihre Bestellung



52 Wochensprüche zum Schmunzeln und Nachdenken.

ABONNEMENT-BESTELLUNG

☐ **Ich abonniere die Zeitschrift <kes> ab Ausgabe Nr . . . . .**

Als Dankeschön erhalte ich ein Aphorismen-Buch und das erste Heft des Abos gratis.

Das Abonnement enthält ein Passwort zur Nutzung des Abo-Bereichs auf www.kes.info mit allen aktuellen Beiträgen und dem **<kes>-Archiv** sowie dem Bezug des <kes>/SecuPedia Newsletters.

Ich kann das Abonnement bis 14 Tage nach Erhalt des ersten Exemplars formlos widerrufen. Nach Ablauf der Widerrufsfrist wird das Abonnement zu den regulären Bedingungen gültig:

Jahresbezugspreis (6 Ausgaben) € 129,00 inkl. MwSt. und Versandkosten (Schweiz SFr 247,00 / restl. Ausland € 153,41).

Der Jahresbezugspreis wird jeweils für ein Jahr im Voraus berechnet. Eine Kündigung des Abos ist dennoch jederzeit zur nächsten nicht gelieferten Ausgabe möglich. Überbezahlte Abogebühren werden rückerstattet.

Ich bin einverstanden, dass die Deutsche Post AG eine eventuell geänderte Anschrift weitergibt.

Datum | Zeichen | Unterschrift

Rechnung und Lieferung bitte an

Telefon Durchwahl

FAX an +49 6725 5994

SecuMedia Verlags-GmbH
Abonnenten-Service
Postfach 12 34
55205 Ingelheim