Micha Borrmann, Daniel Bachfeld

Zechpreller

Unsicheres Bezahlsystem ermöglicht kostenloses Einkaufen in vielen Webshops

Durch die unvollständige Verarbeitung von Transaktionsparametern in Webshops ist es möglich, ohne Bezahlung Waren zu erhalten. Betroffen sind unter anderem führende Shop-Systeme.

Wer einen Webshop betreibt, muss seinen Kunden verschiedene Zahlungsarten anbieten können. Eine der beliebtesten Methoden ist die Bezahlung per Kreditkarte, bei der der Kunde seine Daten nebst Sicherheitsnummer übermitteln muss. Für die Verarbeitung und Aufbewahrung solcher Daten in Online-Shops haben die Kartenherausgeber das Regelwerk Payment Card Industry Data Security Standard (PCI DSS) veröffentlicht. Darin wird den Händlern in 12 Regeln vorgeschrieben, wie sie mit Daten umzugehen haben und was für Sicherheitsmaßnahmen auf dem Server erforderlich sind (siehe Kasten PCI-DSS-Richtlinien).

Je nach Umsatzvolumen werden bei Zuwiderhandlung Strafen verhängt, Einschränkungen ausgesprochen oder einem Shop sogar die weitere Annahme von Kreditkarten untersagt. Größere Shops und Dienstleister mit mehr als sechs Millionen Kreditkartentransaktionen pro Jahr müssen die Sicherheit ihrer Netzwerke zudem alle drei Monate extern prüfen lassen. Die hohen Hürden schrecken viele kleine Online-Shops ab, die deshalb statt einer eigenen PCI-Zertifizierung lieber auf einen externen zertifizierten Dienstleister zurückgreifen, um gar nicht erst mit Kreditkartendaten in Berührung zu kommen. Zu den Anbietern solcher Dienste gehören unter anderem 1&1 mit seinem Produkt ipayment und die Bank für Zahlungsverkehrsdienstleistungen (VÖB-ZVD) mit DirectPOS. Diese bieten den Shops eine spezielle Schnittstelle zur Abwicklung an.

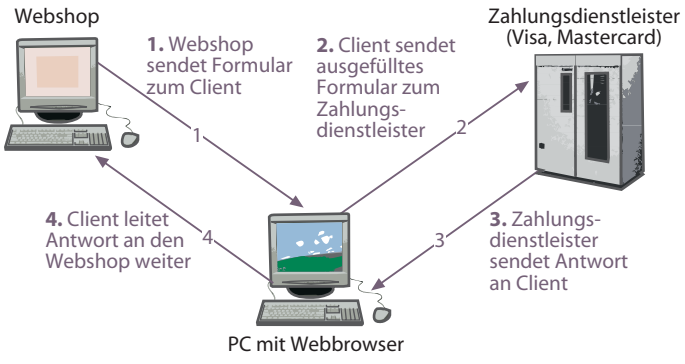
Über Bande

Damit ein Webshop keine Kreditkartendaten verarbeiten muss, benutzt er den Browser des Kunden quasi als Relaisstation. Der Shop liefert an diesen ein Formular zur Eingabe der Kreditkartendaten aus, das beim Abschicken durch den Kunden nicht im Shop, sondern beim Zahlungsdienstleister landet (siehe Bild unten). Die Antwort des Zahlungsdienstleisters, ob der Bezahlvorgang erfolgreich war oder nicht, landet zunächst im Browser des Kunden (Schritt 3). Diese Antwort des Zahlungsdienstleisters ist häufig eine statische URL des Webshops, die etwa als Redirect übermittelt und vom Browser aufgerufen wird (Schritt 4). Doch allein der Aufruf der richtigen statischen URL genügt in einigen Fällen, um dem Webshop vorzugaukeln, man hätte etwa an ipayment gültige Kreditkartendaten für die Bezahlung übermittelt.

Landet der Kunde nach der Eingabe falscher Daten beispielsweise auf www.example.com/error.php (Bild Seite 96 rechts oben), so kann er anschließend durch den Aufruf der URL www.example.com/order_ok.php (Bild Seite 96 rechts unten) die Bestellung trotzdem abschließen. Die Ursache für diese gravierende und einfach auszunutzende Lücke liegt in der fehlenden Überprüfung der vom Zahlungsdienstleister zurückgelieferten Signalisierungsparameter im Webshop. Die Schnittstelle von ipayment lässt sich nämlich auf verschiedene Arten in Shop-Systeme einbinden, um Betreibern eine größtmögliche Flexibilität zu bieten.

Dazu gehören die beschriebene unsichere Methode über statische URLs und die Methode mit „Security-Hash zur Absicherung der Aufruf-Parameter". Bei Letzterer wird zwischen dem Webshop und ipayment ein MD5-Hash übertragen, den das System aus einem vereinbarten Kennwort und anderen Parametern wie dem zu bezahlenden Preis abgeleitet hat. Dadurch genügt es nicht mehr, einfach nur eine URL aufzurufen, um dem Shop eine gültige Transaktion vorzuspielen. Derzeit nutzen offenbar viele Shops diese sicherere Schnittstelle nicht. Außerdem ist das beschriebene Verfahren auch nicht hundertprozentig sicher, da sich der Hash bei weiteren Transaktionen wiederverwenden lässt, sofern keine variablen Parameter in den Hash einfließen.

Dass ein Kunde durch einfaches Ändern der URLs ohne Bezahlung im Webshops eingekauft hat, wird der Betreiber erst nach dem Versenden der Ware bemerken. Möglich ist es zwar, noch zu versuchen, die Ware zurückzufordern. Im Falle versandloser Bestellungen wie Handy-Klingeltöne, Software-Lizenzkeys, eBooks und MP3 ist der



Um keine Kreditkartendaten verarbeiten zu müssen, nutzen Webshops externe Zahlungsdienstleister.

PCI-DSS-Richtlinien

Anforderung 1:	Installation und Verwaltung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten
Anforderung 2:	keine Verwendung der Standardwerte des Herstellers für Systemkennwörter und andere Sicherheitsparameter
Anforderung 3:	Schutz von gespeicherten Karteninhaberdaten
Anforderung 4:	Verschlüsselung der Übertragung von Karteninhaberdaten über offene, öffentliche Netzwerke
Anforderung 5:	Verwendung und regelmäßige Aktualisierung von Antivirusprogrammen
Anforderung 6:	Entwicklung und Verwaltung sicherer Systeme und Anwendungen
Anforderung 7:	Beschränkung des Zugriffs auf Karteninhaberdaten auf die geschäftlich erforderlichen Daten
Anforderung 8:	Zuweisung einer eindeutigen ID zu jeder Person mit Computerzugriff
Anforderung 9:	Beschränkung des physischen Zugriffs auf Karteninhaberdaten
Anforderung 10:	Verfolgung und Überwachung sämtlicher Zugriffe auf Netzwerkressourcen und Karteninhaberdaten
Anforderung 11:	regelmäßiger Test von Sicherheitssystemen und -prozessen
Anforderung 12:	Verwaltung einer Richtlinie zur Informationssicherheit

Aufwand für den Shop-Betreiber aber erheblich und sehr wahrscheinlich mit weiteren Kosten verbunden.

Was war

Konkret weisen die Shop-Software osCommerce und die davon abstammende Lösung xt:commerce diese Schwachstelle auf. Sie wurde während eines Penetrationtests des Online-Shops eshoppen.de vom Sicherheitsdienstleister SySS entdeckt und recht schnell von den betreuenden Webentwicklern von Phoenix Medien beseitigt. Da andere Shops auf derselben Software beruhen und beide Shop-Systeme weltweit verbreitet sind, dürften zahlreiche Betreiber ebenfalls von diesem Problem betroffen sein. Schätzungen zufolge kommen die Systeme zusammengenommen auf 25 Prozent Marktanteil – allein xt:commerce soll auf rund 100 000 Servern seine Arbeit verrichten.

Zwar wurde die Schwachstelle durch die Analyse aufgedeckt, allerdings war das Problem damit noch längst nicht gelöst, da ein Patch erforderlich ist, um es aus der Welt zu schaffen. Längere Zeit war nicht klar, wer für den Fehler verantwortlich ist und wer ihn behebt. Ursprünglich soll das Kreditkartenmodul zur Anbindung von osCommerce an ipayment im Jahr 2002 aus der Open-Source-Gemeinde übernommen worden sein. Dieses offensichtlich unsichere Modul wurde später von den xt:commerce-Entwicklern in ihren Fork integriert.

Hat der Kunde keine gültigen Kreditkartendaten eingegeben, bekommt er eine Fehlermeldung vom Webshop zu sehen, die eigentlich vom Zahlungsdienstleister stammt.

Da osCommerce von ipayment offiziell unterstützt wird, hat 1&1 nach eigenen Angaben schon vor einiger Zeit einen externen Dienstleister beauftragt, ein sicheres Zahlungsmodul zu entwickeln. Damit wird laut 1&1 unter anderem ein Hidden-Trigger-Mechanismus zur Authentifizierung einer Bestellung implementiert. Dabei soll es sich im Wesentlichen um eine zusätzliche direkte Kommunikation zwischen Zahlungsdienstleister und Webshop handeln, die nicht manipulierbar sei. Der alternative Anbieter DirectPos setzt ebenfalls seit längerem auf die direkte Rückmeldung zu den Shops, ohne den Client zu involvieren. Dies setzt aber voraus, dass die Shop-Software die Rückmeldung vom Zahlungsdienstleister auch korrekt auswertet. Mindestens eine in Eigenregie entwickelte Shop-Lösung ist den Autoren bekannt, bei denen die Shop-Software die Rückmeldung von DirectPos nicht korrekt auswertete.

Für xt:commerce war ein überarbeitetes Modul bei 1&1 jedoch zunächst nicht geplant, hieß es auf Anfrage von heise Security. Die Entwickler von xt:commerce sahen sich selbst nicht in der Lage, in einem überschaubaren Zeitraum ein Sicherheitsupdate zu liefern.

Auf Anregung von heise Security sprangen die Entwickler von Phoenix Medien in die Bresche, die als Betreuer von eshoppen.de ja ohnehin bereits einen Interims-Fix entwickelt hatten. Innerhalb weniger Tage bauten sie einen vollständigen Patch für xt:commerce 3.04 SP2.1, der nicht nur die Sicherheitslücke durch Einbau eines Transaktions-Security-Keys schließt, sondern darüber hinaus dafür sorgt, dass die Shops nun wirklich PCI-DSS-konform werden. Bei der Analyse des ursprünglichen Fehlers stellte sich nämlich heraus, dass die Software die Kreditkartendaten doch temporär im Shop verarbeitete – was laut PCI-DSS eigentlich eine Zertifizierung erfordert.

Was wird

Das Update für osCommerce wird auf den Seiten von osCommerce zum Download angeboten, das xt:commerce-Update ist auf den Seiten von xt:commerce zu finden (siehe Soft-Link). Für beide Produkte stehen Anleitungen zum Installieren der Patches bereit. Shop-Betreiber sollten die Software so schnell wie möglich installieren, um zu verhindern, dass böswillige Kunden mit den im Artikel geschilderten Informationen kostenlos im Shop einkaufen können.

Der Sicherheitsdienstleister SySS wird zudem auf dem Heise Forum '08 – Sicherheit und IT-Recht (Halle 5, Stand E38) jeweils Mittwoch, Freitag und Sonntag um 14 Uhr das Live-Hacking eines eigens dafür aufgesetzten verwundbaren Webshops zeigen. Interessierte können sich dort ein Bild verschaffen, wie einfach es ist, ohne Bezahlung exemplarische eBooks in Form von PDF-Dokumenten herunterzuladen.

Das Problem trat in einem Bereich auf, für den sich zunächst niemand so recht verantwortlich fühlte – insbesondere weil es sich um die Schnittstelle zwischen verschiedenen Systemen und Verantwortlichkeiten handelte. Der Fall zeigt aber deutlich, dass das Verständnis der Webentwickler für die Kommunikationsprozesse der Schnittstellen und deren Manipulationsmöglichkeiten verbessert werden muss. (dab)

Durch das simple Ändern der URL gaukelt man dem Webshop eine gültige Bezahlung vor und schließt somit den Bestellvorgang ab.

Soft-Link 0806094 c't