Security versus Usability

Sicherheit ist nach Ansicht der Händler nach wie vor der wichtigste Faktor für den Erfolg eines Zahlungssystems, das geht aus der EHI-Studie „Kartengestützte Zahlungssysteme im Einzelhandel 2014" klar hervor. Auf der anderen Seite mag der Kunde es schnell und unkompliziert, Express-Checkout-Verfahren liegen beim Bezahlen des Onlinekaufs ganz vorne. Laut „EHI Online-Payment-Studie 2014" zahlen Kunden in Deutschland am liebsten mit Rechnung (25,4 %), PayPal (19,9 %) und Lastschrift (19,3 %), weil diese Methoden schnell und ohne große Dateneingabe funktionieren. Auch in dieser Studie wird deutlich, wie relevant die Sicherheit ist – 77,1 Prozent der befragten Online-Händler glauben, dass Sicherheit für die Kunden das wichtigste Kriterium eines Zahlungsverfahrens ist. Allerdings meinen auch 94,3 Prozent, dass die Usability, also die einfache Bedienung eines Verfahrens, für den Kunden entscheidend ist.

Authentifikation mit Maß

Die Empfehlungen von SecuRe Pay beinhalten die Forderung, dass Kunden ihre Authentizität durch mindestens zwei der drei folgenden Kriterien belegen:

a) etwas, das nur der Kunde weiß (z.B. Passwort)
b) etwas, das nur im Besitz des Kunden ist (z.B. Smartphone)
c) etwas, das elementar zum Kunden gehört (z.B. Fingerabdruck)

Fast alle Händler äußerten in der Online-Payment-Befragung, dass sie Software-basierte Authentifizierungsmöglichkeiten für praxistauglich halten. Zwei Drittel sehen dies auch bei Handy-basierten Möglichkeiten. Hardware- und Biometrie-basierte Verfahren beurteilen sie in der Mehrzahl allerdings nicht als praxistauglich.

Die SecuRe-Pay-Empfehlungen sind nach dem „Comply or Explain"-Prinzip entworfen. Man kann als betroffenes Unternehmen die Anforderungen annehmen bzw. erfüllen oder erläutern, warum man die geforderten Ziele auch ohne die Erfüllung der Anforderungen erreicht. Letzteres hat beispielsweise PayPal in seiner Stellungnahme benutzt. Das System sei durch Backend-Prozesse (Risikoeinschätzung und Authentifizierung) durchaus in der Lage, den Anspruch an starke Kunden-Authentifikation auch ohne die geforderten zwei von drei Kriterien zu erfüllen. „Dies zeigt, dass eine alternative ganzheitliche Betrachtung des Themas mit Backend und Frontend nötig ist, „ so Tim Kiesewetter: „Wir als EHI favorisieren Software-basierte Lösungen und einen gesunden Trade-off zwischen Sicherheit, Kundennutzung und Kosten."

Bestellmöglichkeit für die „Online-Payment-Studie 2014": *http://www.ehi-shop.de/de/handelsthemen/zahlungssysteme/studie-online-payment-studie-2014*

Passwort-Hack: Das Problem sind die Webseiten

Eine TeleTrusT-Position

Zu den jüngsten Berichten der „New York Times" und des US-Unternehmens Hold Security über den Diebstahl von 1,2 Milliarden Benutzernamen und zugehöriger Passwörter sowie mehr als 500 Millionen E-Mail-Adressen ist festzuhalten, dass die Daten nach aktuellem Kenntnisstand nicht von den privaten Rechnern der Nutzer, sondern offenbar von den Webseiten bzw. aus Datenbanken mehrerer Online-Anbieter stammen. Zwar ist es richtig, in diesem Zusammenhang erneut auf die Wichtigkeit starker Passwörter und die Vorteile zum Beispiel einer Zwei-Faktor-Authentifizierung hinzuweisen. Im vorliegenden Fall scheinen aber nicht die Passwörter an sich, sondern eher deren Speicherung bzw. die Art der Speicherung in den Webservern der Seitenanbieter das Problem zu sein.

Passwörter können in dieser monströsen Größenordnung nur gestohlen werden, wenn sie unverschlüsselt gespeichert sind oder die Verschlüsselung unsicher ist. Das Bundesamt für Sicherheit in der Informationstechnik ruft deshalb die Anbieter von Online-Diensten zu Recht dazu auf, mehr für die Sicherheit ihrer Systeme und die Sicherheit der Kundendaten zu tun.

Oliver Dehning, Leiter der TeleTrusT-AG „Cloud Security": „Eine bessere Schutzvorkehrung ist es, das Passwort selbst gar nicht zu speichern, sondern nur Passwort-Hashes, aus denen das Passwort nicht zurückberechnet werden kann. Dafür zuständig ist die Seite, in die man sich einloggen will."

Ein weiteres Problem, das Hackern den aktuellen Diebstahl offensichtlich erleichtert hat, sind Botnetze. Diese basieren maßgeblich darauf, dass viele Rechner mindestens teilweise ungeschützt am Internet hängen. Zumeist, aber nicht nur, sind dies Rechner von Privatpersonen und kleineren Unternehmen und Organisationen. Diese Rechner werden von den Kriminellen zur Ausführung ihrer Taten genutzt – ob es nun der Versand von Spams ist (z.B. um weitere Rechner zu kapern) oder das Ausspähen von Websites. Die Täter verfügen dadurch über immense Rechenleistung und Bandbreite und sind auch noch anonym, während der scheinbare Angreifer in Wahrheit unschuldig ist (man könnte ihm höchstens vorhalten, dass er seinen Rechner nicht ausreichend gesichert hat).

Was muss man tun, um solche Diebstähle zu verhindern?

1. Den eigenen Rechner sichern: aktuelle Patches installieren, Virenscanner aktiv und aktuell halten.
2. Webserver-Betreiber sollten die Server mit aktueller Software betreiben (Content Management-Systeme) und Passwörter nicht speichern (nur Hashes) oder doch mindestens sicher verschlüsseln.

Es ist angesichts der berichteten großen Zahl gestohlener Zugangsdaten naheliegend, dass sehr viele Internetnutzer, mutmaßlich auch deutsche, betroffen sind. Welche Sites genau und wie wichtig die Zugänge sind, ist bei der derzeitigen Nachrichtenlage unklar. Vermutlich werden insbesondere Webshops im Fokus sein. Wer sichergehen will, sollte seine Passwörter für Zugänge zu wichtigen Shopping Websites ändern. Die Anbieter dieser Art von Webseiten sind gut beraten, aus dem Vorgang Schlüsse zu ziehen und in mehr IT-Sicherheit zu investieren. Hackerangriffe auf Kundendaten haben Einfluss auf die künftige Akzeptanz der Kunden und deren Neigung, die betroffenen Einkaufsportale zu nutzen.

Universität des Saarlandes: Studiengang „Cybersicherheit"

Über die US-amerikanischen Überwachungsprogramme dringen immer mehr Details an die Öffentlichkeit. Doch nicht nur Geheimdienste, auch Unternehmen und Kriminelle betreiben Datenspionage. Wie man die eigenen Daten vor solchen Angriffen schützen kann, können Abiturienten ab Oktober im neuen Bachelor-Studiengang „Cybersicherheit" an der Universität des Saarlandes studieren.

Direkt vom ersten Vorlesungstag an erforschen die Studenten selbst die digitalen Bedrohungen im weltweiten Netz. Auf diese Weise lernen sie die notwendigen Fähigkeiten für den Ernstfall, ver-