Bastian Braun, Patrick Gemein, Benedikt Höfling, Michael Marc Maisch, Alexander Seidl

Angriffe auf OpenID und ihre strafrechtliche Bewertung

Cross-Site-Request-Forgery, Phishing und Clickjacking im Fokus

Die Vision, nach einer einmaligen Authentifikation alle Benutzerkonten im Internet ohne wiederholte Anmeldung nutzen zu können, rückt mit OpenID ein Stück näher. Als erstes Single-Sign-On-System hat es OpenID zu ansehnlicher Verbreitung im World Wide Web gebracht. Doch die neue Rollenverteilung, in der sich viele Nutzer bei einem Anbieter für zahlreiche Anwendungen anmelden können, ist nicht hinreichend untersucht. Dieser Beitrag analysiert das technische Angriffspotenzial und nimmt eine strafrechtliche Bewertung ausgewählter Angriffe auf OpenID-Verfahren vor.

1 Überblick

Das Single-Sign-On-Verfahren OpenID hat sich unter den Authentifikationsverfahren etabliert. Beim Login zu einer Webanwendung kommt OpenID nicht mehr nur bei Blogs, Content Management Systemen oder kleinen Webseiten zum Einsatz. Mittlerweile werben auch große Webseitenbetreiber wie Google, Microsoft, Yahoo oder Facebook mit der Unterstützung von OpenID.[1]

OpenID ist ein Single-Sign-On-Verfahren, das nicht das Erfordernis der Registrierung eines Benutzerkontos ersetzt, sondern den Login-Vorgang erleichtert. Der Benutzer kann über die einmalige Authentifikation bei seinem OpenID-Provider auf alle Webanwendungen zugreifen, ohne wiederholt seine jeweiligen Benutzerdaten (Benutzername und Passwort) eingeben zu müssen.[2]

OpenID kann damit vor Risiken für die IT-Sicherheit schützen, die durch die Mehrfachverwendung desselben Passworts drohen. Darüber hinaus verleitet der wachsende Verwaltungsaufwand bei Passwörtern dazu, Zeichenketten zu verwenden, die leicht erraten oder via Brute-Force-Attacken kompromittiert werden können.

2 OpenID

Um eine OpenID-Identität zu erhalten, wird vom Benutzer ein OpenID-Provider als Aussteller frei ausgewählt.[3] Der Benutzer registriert ein Benutzerkonto bei dem OpenID-Provider (sog. Identity Provider, IdP), in der Regel unter Angabe von Namen, Passwort und E-Mailadresse. Mit Abschluss der Registrierung teilt der IdP dem Benutzer eine OpenID-Identität (auch sog. Identifier) zu, die sich in einer OpenID URL (sog. Uniform Resource Identifier[4]) manifestiert, bei der der Benutzername in einer Subdomain angelegt ist, z.B. *benutzername.idp.com*. Diese Spezifikation ist eine Besonderheit von OpenID, bei der sich Benutzer wie andere IT-Ressourcen über eine URL ausweisen.[5]

Die OpenID-Identität wird vom Benutzer im Rahmen des Login-Verfahrens bei einer Webanwendung angegeben, bei der er ein bereits registriertes Konto besitzt. Dazu werden ein bestimmtes Feld zur Eingabe der URL und ein Submit-Button bereitgehalten.

Mit der Angabe der OpenID-Identität ermittelt die Webapplikation, die auf die Authentifikation des Benutzers durch den IdP vertraut und deshalb als Relying Party (RP) bezeichnet wird, den richtigen IdP. Dieser ergibt sich aus der URL. Die RP und der IdP handeln einen Schlüssel aus, um eine vertrauliche TLS-Verbindung aufzubauen.

Im nächsten Schritt wird der Benutzer an seinen IdP weitergeleitet (sog. Redirect), indem die Webseite des IdP im selben oder in einem neuen Browserfenster angezeigt wird.[6]

Beim IdP gibt der Nutzer seinen OpenID-Benutzernamen und sein OpenID-Passwort ein.[7] Der IdP nimmt für die RP die Authentifikation des Nutzers vor und sendet das Ergebnis an die RP, indem der Nutzer an die Web-Applikation zurückgeleitet wird. Das Ergebnis wird mittels einer Zeichenkette in der URL an die RP übermittelt. Die RP erlaubt nunmehr dem Benutzer den Zugriff auf sein Benutzerkonto bzw. auf die Webanwendung.

Beim IdP kann der Benutzer veranlassen, eingeloggt zu bleiben, sodass die wiederholte Eingabe seiner OpenID-Daten nicht erforderlich ist. Der Benutzer muss bei einer RP lediglich seine OpenID-Identität angeben. Der IdP eröffnet dazu eine serverseitige Session[8], die den Benutzer anhand eines Cookies identifiziert. Mit Beendigung des Browsers – nicht nur eines Browsertabs - wird die Session gelöscht.

[1] Arrington, TechCrunch v. 07.02.2008, http://techcrunch.com/2008/02/07/openid-welcomes-microsoft-google-verisign-and-ibm.

[2] Ausführlich zur Entstehungsgeschichte von OpenID, Raepple, DuD 2009, 174 ff.

[3] http://openid.net/get-an-openid/.

[4] RFC 3986.

[5] Raepple, DuD 2009, 174, 175.

[6] Alle hier beschriebenen Vorgänge sind von der Implementierung im Einzelfall abhängig; zum Ablauf vgl. Raepple, DuD 2009, 174, 175 f.

[7] Ein höheres Sicherheitsniveau an dieser Stelle verspricht die Verwendung clientseitiger Zertifikate, die eine vertrauenswürdige Stelle ausgestellt hat.

[8] Eine Session ist eine Sitzung, die mit einer sog. SessionID, die z.B. über Cookies oder URIs übertragen wird, einer Person zugeordnet werden kann. Die SessionID überbrückt damit die Zustandslosigkeit des HTTP-Protokolls.

2.1 Identity Provider (IdP)

OpenID beschreibt ein dezentralisiertes Protokoll, bei dem jedermann einen OpenID-Provider betreiben kann.[9] Dem IdP kommt unter den Akteuren des OpenID-Verfahrens eine besondere Stellung - mit Missbrauchspotential - zu.

Er versichert der RP, dass der Benutzer sich ordnungsgemäß authentifiziert hat. Das ermöglicht dem IdP zum einen, sich selbst als jeder seiner Nutzer auszugeben, indem er sich selbst eine gültige Authentifikation attestiert. Zum anderen sind seine Sicherheitsmaßnahmen maßgeblich dafür verantwortlich, ob bzw. wie leicht ein Angreifer sich als einer der Benutzer ausgeben oder in den Besitz der Benutzerpasswörtern gelangen kann.

Eine Vertrauensbeziehung besteht daher nicht nur zwischen dem Benutzer und dem IdP, sondern auch zwischen der RP und dem IdP.

2.2 Relying Party (RP)

Die RPs sind in der Regel Webseitenbetreiber, die z.B. Informationsdiente, E-Commerce-Plattformen oder soziale Netzwerke anbieten und die Authentifikation beim Login von registrierten Benutzern an einen IdP auslagern.

3 Angriffe

Beim OpenID-Verfahren werden bekannte Gefährdungslagen um neue Angriffsvektoren erweitert. Die Angriffsmöglichkeiten des IdP wurden bereits angedeutet. In diesem Kapitel wird das Angriffspotenzial bösartiger oder kompromittierter RPs näher beleuchtet.

3.1 Phishing-Angriff

Im Phishing-Szenario delegiert eine bösartige RP evil.com den Authentifikationsvorgang des Nutzers an einen bösartigen IdP, der der Benutzeroberfläche eines originalen IdP nachempfunden ist. Das Opfer wird entsprechend getäuscht und zur Eingabe seiner Login-Daten verleitet.

Ein Angreifer könnte diese OpenID-Daten verwenden, um sich bei dem echten IdP als sein Opfer auszugeben und sich somit bei beliebig vielen RPs zu authentifizieren. Dieser Angriff gilt derzeit als eine der gefährlichsten Bedrohungen für die Single-Sign-On-Infrastruktur (SSO).[10]

3.2 Cross-Site-Request-Forgery-Angriff

Cross-Site-Request-Forgery (CSRF) bezeichnet einen Angriff auf ein IT-System, der mit Hilfe eines ahnungslosen Opfers durchgeführt wird. Der Angreifer schiebt seinem Opfer, das bereits bei einer Webapplikation angemeldet ist und daher über eine gültige Session verfügt, einen HTTP-Request[11] unter.[12] Dies kann im Wege einer manipulierten URL auf einer Webseite oder einer elektronischen Nachricht erfolgen.[13]

Für einen erfolgreichen CSRF-Angriff ohne OpenID-Verfahren sind folgende Schritte notwendig:

- Das Opfer authentifiziert sich bei einer Webseite (z.B. example.com).
- Ohne die Session bei example.com zu beenden (z.B. durch Logout), besucht das Opfer eine weitere Webseite (z.B. evil.com).
- Die Webseite evil.com veranlasst den Browser des Opfers einen HTTP-Request auf example.com auszuführen.[14]
- Dieser Request wird im noch gültigen Session-Kontext des Opfers ausgeführt.
- Der Request erfolgt ohne Kenntnis des Opfers und ermöglicht dem Angreifer, die Rechte und Rollen des Opfers bei example.com auszunutzen.

Im Rahmen von Cross-Site-Request-Forgery ist es grundsätzlich unerheblich, ob das Opfer über ein OpenID-Verfahren authentifiziert worden ist.

Es ergibt sich allerdings ein erhöhtes Angriffspotenzial durch die OpenID-Architektur und die Implementierung des IdP. Ein erfolgreicher Angriff im Kontext von OpenID könnte folgendermaßen ablaufen (s. Abb. XSRF-Angriff.png):

- Das Opfer meldet sich via OpenID bei der RP an. Die RP wird von einem Angreifer betrieben (evil.com).
- Mit der OpenID-Authentifikation existiert eine gültige Session zwischen dem Opfer und evil.com und zwischen dem Opfer und dem IdP, der die Authentifikation durchgeführt hat.
- Die RP evil.com hat nun Kenntnis der OpenID-Identität des Opfers.
- Sodann veranlasst die RP evil.com das Opfer, einen Login-Request bei einer dritten Webanwendung (csrf-anfaellig.com) auszuführen (bspw. in einem Frame oder IFrame). evil.com nutzt folglich die bestehende Session des Opfers zum IdP dazu aus, um den Nutzer ohne dessen Wissen auf einer weiteren OpenID-basierten Webanwendung einzuloggen.

Ein unmittelbarer (Vermögens-) Schaden entsteht nicht. Das Opfer wird in diesem Szenario lediglich bei einer Webseite angemeldet, ohne diesen Vorgang und die Authentifikation selbst aktiv angestoßen zu haben. Möglich ist aber, dass der Angreifer in Folge dessen weitere CSRF-Angriffe im Session-Kontext des Opfers auf der Webanwendung csrf-anfaellig.com ausführt. Der Angreifer kann dazu alle Rechte des Opfers ausnutzen, über die es im Rahmen seines Benutzerkontos verfügt, bspw. Kauf einer Sache, Hinzufügen eines Kontakts, Löschen einer Information etc.

Zum Schutz vor CSRF-Angriffen kann das Zeitfenster einer IdP-Session begrenzt werden (Session-Timeout). Unachtsame Benutzer, die eine Authentifikation beispielsweise durch im Browser gespeicherte Zugangsdaten zu schnell durchführen, schützt auch ein kurzer Session-Timeout nicht. Desweiteren werden Sicherheitstoken (Nonces) in Kombination mit Cookies verwendet, die verhindern, dass der Angreifer selbstständig einen Login-Request im Namen des Opfers vorbereiten kann.

Ein besonderer Angriffsvektor besteht durch neue Zugriffsmöglichkeiten bei JavaScript, ActionScript (Flash) und Silverlight. Ursprünglich ist JavaScript ein Zugriff auf Objekte einer anderen Webseite nur dann gestattet, wenn diese aus derselben Quelle stammen, sog. Same-Origin-Policy. Dieses Sicherheitskonzept wird im Wege von Cross-Origin Ressource-Sharing teilweise aufgehoben,

[9] Vgl. http://openid.net/developers/.

[10] Tsyrklevich/Tsyrklevich, Single-Sign-On for the Internet: A Security Story, Black Hat, USA 2007.

[11] Ein HTTP-Request ist eine Anfrage, die ein Browser, der auf einem Client betrieben wird, an einen Server richtet. Das Protokoll HTTP verfügt über Methoden wie z.B. GET oder POST, um die Modalitäten der Kommunikation zu definieren.

[12] Open Web Application Security Project, Cross-Site Request Forgery (CSRF) – OWASP, https://www.owasp.org/index.php/Cross-Site_Request_Forgery_%28CSRF%29, April 2010.

[13] Häufig werden Requests mit Schädigungsabsicht in ein HTML Image Element, bspw. <img src="http://host/?command">, oder in ein JavaScript Image Object eingebettet, vgl. http://www.cgisecurity.com/csrf-faq.html.

[14] Vgl. Fn. 11.

sodass für verschiedene Webseiten keine Einschränkungen bestehen. Entscheidend ist daher, dass jede Webseite eine adäquate Policy zum Cross-Origin-Resource-Sharing einführt. Diese soll bspw. keine Universalerlaubnis „*“ enthalten, sondern muss die erlaubten Quellen ausdrücklich benennen.[15] Die Verwendung von Sicherheitstoken (Nonces) ist hier nicht ausreichend, da diese von JavaScript u.a. gelesen werden können.

3.3 Clickjacking-Angriff

Ein Clickjacking-Angriff zielt darauf ab, die Darstellung einer Webseite im Browser des Opfers so zu manipulieren, dass sie von einer anderen Darstellung überlagert wird. Das Opfer kann den tatsächlichen Kontext der sichtbaren Objekte nicht erkennen. Hierzu bereitet der Angreifer eine Webseite vor, die sein Opfer dazu verleitet, Aktionen (Clicks) auf einer Ziel-Webseite durchzuführen, ohne dass das Opfer Kenntnis von den wirklichen Folgen seiner Clicks hat.[16] Auch innerhalb von Webanwendungen können Clickjacking-Angriffe vorgenommen werden.[17]

Ein Clickjacking-Angriff könnte sich wie folgt abspielen:

- Das Opfer besucht die bösartige RP evil.com.
- Das Opfer will sich authentifizieren und gibt evil.com seine OpenID-Identität preis.
- Nach Erhebung der OpenID-Identität wendet sich die bösartige RP evil.com der RP example.com zu und gibt vor, der Browser des Opfers zu sein.
- Mit der Eingabe des Benutzernamens des Opfers bei der RP example.com erhält die bösartige RP eine Weiterleitung zum IdP des Opfers.
- Die RP evil.com veranlasst den Browser des Opfers, die Weiterleitung zum IdP in einem präparierten IFrame[18] zu laden.
- Ist das Opfer bereits beim IdP eingeloggt und besitzt bereits eine gültige Session, dann erfolgt automatisch die Weiterleitung des Opfers zu example.com. Die Anmeldung ist dadurch vollzogen.
- Ist das Opfer noch nicht beim IdP eingeloggt, kann die Login-Seite mit den Eingabefeldern eines IdP in einem IFrame aufgerufen und von einem unsichtbaren IFrame mit identischen Eingabefeldern (Benutzername, Passwort, Submit-Button) derart überlagert werden, dass das Opfer nun seine Daten nicht beim IdP, sondern in die gefälschten Eingabefelder der RP evil.com eingibt. Der Angreifer kann auf diese Weise die OpenID-Daten des Opfers beim IdP erhalten und kann sich somit jederzeit als das Opfer beim IdP ausgeben.

In der klassischen Variante eines erfolgreichen Clickjacking-Angriffs auf eine Webseite mit Benutzername- und Passwortauthentifizierung sind die Auswirkungen auf diese eine Webseite beschränkt, wenn der Benutzer für jede Webseite ein individuelles Passwort vergeben hat. Diese Gefährdungslage verändert sich durch den Einsatz von OpenID. Ein Angreifer kann die Login-Daten durch einen Clickjacking-Angriff nicht mehr bei der RP abgreifen, da diese dort nie eingegeben werden, sondern aufgrund des überlagernden IFrames bei der Eingabe der OpenID-Daten durch den Benutzer beim IdP.

Indem der Angreifer durch Clickjacking die OpenID-Daten des Benutzers erheben kann, handelt es sich bei dem Angriff – in gleicher Weise wie beim Phishing-Angriff – um eine erhebliche Gefährdungslage für die Sicherheit der Identitäten. Hat der Angreifer die OpenID-Daten erhoben, ist er nicht weiter an die Gültigkeit einer Session gebunden, sondern kann sich selbst als der Benutzer bei Webanwendungen ausgeben.

Eine simplere Variante des Angriffs ist möglich, wenn der Benutzer seinen (OpenID-) Benutzernamen und Passwort für den IdP im Browser gespeichert hat. Dann genügt das Einbinden des Submit-Buttons des IdP in einen IFrame. Der Browser füllt daraufhin die entsprechenden Felder mit Benutzername und Passwort, und das Opfer meldet sich an, wenn es dem Angreifer gelingt, das Opfer zum Klick auf den Submit-Button zu bewegen.

Ein häufig anzutreffender Schutz vor Clickjacking ist die Implementierung von Frame Busting.[19] Es handelt sich dabei um JavaScript, das in den HTML-Quellcode eines IdP oder einer RP integriert wird. Diese Schutzmaßnahme dient dazu, zu verhindern, dass eine Webseite innerhalb (in einem IFrame) einer anderen Webseite (von einem potentiellen Angreifer) geladen werden kann. Gleiches bewirkt eine Anweisung des Servers, die mit der Seite als sog. HTTP-Header ausgeliefert wird.[20] Letztere Möglichkeit funktioniert zuverlässiger, sofern der verwendete Browser diese Option unterstützt.

Mit browserspezifischen Add-Ons[21] können Benutzer Maßnahmen zum Selbstschutz vor Clickjacking vornehmen.

3.4 Session Hijacking und Session Fixation

Darüber hinaus sind noch weitere Angriffe denkbar, wie bspw. Session Hijacking und Session Fixation, die jedoch hier nicht vertieft untersucht werden können.[22]

Bei einem Session Fixation-Angriff versucht der Angreifer, dem Opfer eine dem Angreifer vorher bekannte SessionID (SID) unterzuschieben.[23] Bei einem Session Hijacking-Angriff geht es dem Angreifer darum, eine gültige Session des Opfers zu übernehmen.

Beide Angriffe zielen darauf ab, dass der Angreifer die gültige Session eines Opfers verwenden kann. Bei diesen Angriffen ist es zunächst unerheblich, ob die Authentifikation über OpenID läuft oder über eine herkömmliche Passwort-Eingabe. Bei der Verwendung von OpenID kommt jedoch ein weiterer Angriffsvektor hinzu. Aufgrund der Tatsache, dass durch die SSO-Architektur eine neue Partei (IdP) hinzutritt, erhöht sich das Risiko durch eine Kompromittierung der Session zwischen Benutzer und IdP. Dies ermöglicht dem Angreifer, sich nahezu unbegrenzt bei

---

[15] Bspw. „Access-Control-Allow-Origin: http://website.com:8080 “.

[16] Hansen/Grossman, Clickjacking. http://www.sectheory.com/clickjacking.htm.

[17] Bei Facebook häufen sich Clickjacking-Angriffe, die die Funktionalität des Like-Buttons missbrauchen und die Nutzer zu Spam-Versendern machen.

[18] Ein InlineFrame (IFrame) ist ein HTML-Element, das dazu dient, andere Webinhalte als selbstständige HTML-Dokumente, z.B. Werbung, in einem definierten Bereich des Browsers anzuzeigen. In der Browserzeile wird nur die Adresse der den IFrame umgebenden HTML-Seite angezeigt. Die Adresse der Seite im IFrame bleibt so dem Benutzer verborgen. Dieser Umstand wird für Clickjacking-Attacken ausgenutzt.

[19] Ausführlich zu der Umgehung von Frame Busting und sicheren Schutzmaßnahmen, Rydstedt/Bursztein/Boneh/Jackson, Busting frame busting: A study of clickjacking vulnerabilities at popular sites, IEEE Oakland Web, 2010.

[20] https://developer.mozilla.org/en/The_X-FRAME-OPTIONS_response_header.

[21] http://noscript.net/faq#qa7_3.

[22] Zur Vertiefung vgl. Schrank/Braun/Johns/Posegga, Session Fixation - the Forgotten Vulnerability? Lecture Notes in Informatics, Proceedings of Sicherheit 2010, Sicherheit, Schutz und Zuverlässigkeit, 2010.

[23] Vgl. Fn. 22.

beliebigen RPs zu authentifizieren, solange die Session ihre Gültigkeit nicht verliert oder der IdP eine erneute Authentifizierung verlangt.

4 Strafrechtliche Würdigung[24]

4.1 Phishing-Angriff

Bei der Beurteilung der Strafbarkeit des Phishing-Angriffs[25] ist zunächst zwischen der Datenbeschaffung und der anschließenden Verwendung der erlangten Daten zu unterscheiden.

4.1.1 Strafbarkeit der Datenbeschaffung

§ 202a StGB

Zunächst kommt eine Strafbarkeit nach § 202a StGB in Betracht. Diese Vorschrift stellt das Ausspähen von Daten unter Strafe. Geschützt werden dabei nur solche Daten, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden (§ 202a Abs. 2 StGB).

Zum Teil wird schon daran gezweifelt, ob es sich bei Benutzername und Passwort um taugliche Tatobjekte i.S.d. § 202a Abs. 2 StGB handelt. Die Zugangsdaten, die das irregeführte Opfer zunächst in seinen Rechner eingibt, um sie sogleich weiterzusenden, seien zwar nicht mehr „unmittelbar wahrnehmbar", doch befänden sie sich lediglich vorübergehend im Arbeitsspeicher und dies reiche für eine „Speicherung" i.S.v. § 202a Abs. 2 Alt. 1 StGB nicht aus.[26] Auch § 202a Abs. 2 Alt. 2 StGB („übermitteln") sei nicht erfüllt, denn Daten, die der Berechtigte selbst gezielt an den Täter übermittelt, seien hiervon nicht erfasst.

Ungeachtet dessen scheitert die Strafbarkeit nach § 202a StGB aber jedenfalls am Tatbestandsmerkmal „unter Überwindung der Zugangssicherung", denn das Opfer gibt die Daten gerade freiwillig an den Täter heraus.[27]

§ 202b StGB

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2 StGB) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, macht sich gem. § 202b StGB strafbar.

Beim Phishing-Angriff fehlt es am „Verschaffen aus einer nichtöffentlichen Datenübermittlung", denn die Daten sind bei einer Übermittlung infolge einer auf Täuschung ausgelegten Phishing-Webseite von Anfang an Teil einer Datenübermittlung zwischen Täter und Opfer, werden somit also nicht „abgefangen".[28]

§ 269 StGB

Im Hinblick auf die Phishing-Webseite (die Nachbildung der Webseite des originalen IdP) ist umstritten, ob eine Strafbarkeit wegen Fälschung beweiserheblicher Daten anzunehmen ist. Voraussetzung hierfür ist eine Gedankenerklärung, deren Inhalt nicht von ihrem angeblichen Aussteller herrührt. Geht man davon aus, dass unter den spezifischen Bedingungen des Internets allein die IP-Adresse für den „Aussteller" der Webseite steht, weil er nur durch sie eindeutig namentlich identifiziert werden kann, so fehlt es an der Beeinträchtigung der Garantiefunktion. Denn die angegebene IP-Adresse ist richtig, gefälscht wird allein der auf der Benutzerebene verwendete Domainname.[29]

Diese Ansicht überzeugt jedoch nicht. Die Webseite stellt eine unechte Datenurkunde dar. Sie enthält die beweiserhebliche Aufforderung, im Rahmen des Anmeldevorgangs Daten einzugeben und die Tatsache, dass sich versteckt auf der Webseite die richtige, vom Täter verwendete IP-Adresse befindet, steht dem Merkmal der Unechtheit nicht entgegen. Hierfür reicht aus, wenn für einen durchschnittlichen Empfänger in ausreichendem Maße eine falsche Herkunft vorgespiegelt wird, was aufgrund des auf der Webseite enthaltenen Textes und des falschen IdP-Logos der Fall ist. Das Erstellen der Phishing-Webseite erfüllt damit den Tatbestand des § 269 StGB.

§ 263a Abs. 3 StGB

Mit der Einrichtung der Phishing-Webseite könnte eine Vorbereitungshandlung zum Computerbetrug gem. § 263a Abs. 3 StGB verwirklicht sein. Die Vorschrift untersagt bestimmte Vorbereitungshandlungen, die im Zusammenhang mit Computerprogrammen stehen, deren Zweck die Begehung eines Computerbetrugs ist. Computerprogramme sind aber nur lauffähige Applikationen, sodass die Einordnung von Webseiten umstritten ist.[30] Aber auch durch die Einrichtung der Phishing-Webseite wird § 263a Abs. 3 StGB – selbst dann, wenn man sie als Computerprogramm einstufen würde – nicht verwirklicht, da sie nicht unmittelbar der Durchführung des späteren Computerbetrugs dient. Da die Webseite nur auf die Erlangung der Daten abzielt, während die eigentliche Tat nach § 263a Abs. 1 StGB erst in einem weiteren Schritt durch die unbefugte Verwendung dieser Daten verwirklicht wird, dient die Webseite ihrerseits nur der Vorbereitung und nicht der „Begehung" eines Computerbetrugs.[31]

4.1.2 Strafbarkeit der Datenverwendung

§ 202a StGB

Indem der Täter die durch Phishing erlangten OpenID-Daten für eine Anmeldung beim IdP nutzt, könnte er sich nach § 202a StGB strafbar machen. Mit den erlangten Daten (Benutzername und Passwort) verschafft sich der Täter Zugang zum IdP-Konto bzw. zu den verschiedenen Webanwendungen des Opfers, welche Daten enthalten, die nur für das Opfer bestimmt sowie durch die vorgeschaltete Abfrage der Zugangsdaten besonders gesichert sind, sodass er den Tatbestand des § 202a StGB folglich verwirklicht.

Nach anderer Ansicht scheidet eine Strafbarkeit des Angreifers dagegen mangels Vorliegen einer besonderen Zugangssicherung aus. Denn durch die Weitergabe von Benutzername und Passwort an den Angreifer werde die Zugangsbeschränkung faktisch aufgehoben, woran auch der Umstand, dass das Phishing-Opfer durch Täuschung zur Herausgabe der Informationen veranlasst wird, nichts ändere.[32]

Diese Argumentation überzeugt jedoch nicht. Mit der vorgeschalteten Zugangsdatenabfrage wird eine Vorkehrung getroffen, die objektiv geeignet und subjektiv nach dem Willen des Berech-

[24] Die strafrechtliche Bewertung beschränkt sich auf das StGB.

[25] Zur Strafbarkeit des „klassischen" Phishing-Angriffs beim Online-Banking vgl. Seidl/Fuchs, HRRS 2010, 85 ff.

[26] Vgl. zum Phishing beim Online-Banking, Popp, MMR 2006, 84, 85.

[27] Seidl/Fuchs, HRRS 2010, 85, 86.

[28] Goeckenjan, wistra 2009, 47, 51.

[29] Popp, MMR 2006, 84, 85.

[30] Zustimmend vgl. Borges/Stuckenberg/Wegener, DuD 2007, 275, 278.

[31] Cramer/Perron, in: Schönke/Schröder, StGB, 28. Aufl. 2010, § 263a, Rn. 33a.

[32] Zum Phishing beim Online-Banking, Graf, NStZ 2007, 129, 131.

tigten dazu bestimmt ist, den Zugriff auf die Daten auszuschließen, sodass de facto ursprünglich eine „besondere Sicherung“ i.S.d. § 202a StGB vorlag. Dass diese Sicherung letztlich durch die Mithilfe des Opfers ausgehebelt wird, ändert nichts an der Tatsache, dass sie anfänglich objektiv bestand.[33] Die Auswirkung der Mitwirkungshandlung des Opfers auf die Strafbarkeit des Angreifers nach § 202a StGB ist vielmehr erst beim Tatbestandsmerkmal „unter Überwindung der Zugangssicherung“ zu diskutieren. Da § 202a StGB auf die Frage, wie der Zugangsschutz letztlich überwunden wird, aber nicht eingeht, steht das „selbstschädigende“ Verhalten des Opfers einer Strafbarkeit des Täters nicht entgegen.

§§ 263, 263a bzw. 269, 270 StGB

Je nach weiterer Verwendung der gephishten Benutzernamen und Passwörter kommen die Delikte des Betrugs (§ 263 StGB), des Computerbetrugs (§ 263a StGB) bzw. der Fälschung beweiserheblicher Daten (§§ 269, 270 StGB) in Betracht.

Nutzt der Täter beispielsweise die Daten zur Authentifikation bei Online-Auktionshäusern, um im Namen des Opfers Waren zu bestellen, kommt eine Strafbarkeit nach § 263 StGB in Betracht. § 263a StGB in der Handlungsvariante der unrichtigen Gestaltung eines Programms kommt in Frage, wenn der Täter ein Online-Spiel in vom Systembetreiber nicht vorgesehener Weise manipuliert, um sich z.B. einen fremden virtuellen Gegenstand zu verschaffen.[34] Das Merkmal „unbefugt“ ist dabei nach h.M. betrugsspezifisch auszulegen, d.h. die Handlung des Angreifers muss täuschungsäquivalent sein. Die IdPs vergeben Benutzername und Passwort, um ihren Kunden damit den Nachweis ihrer Identität zu ermöglichen, weshalb die Verwendung dieser Daten mit der Vorlage eines Ausweises bei persönlichem Geschäftskontakt verglichen werden kann.

Indem der Angreifer die Zugangsdaten des Opfers verwendet und damit weitere Anwendungen ausführt, stellt er u.U. Datensätze her, die die RP speichert und deren Erklärungsinhalt z.B. ein Kaufvertrag ist. Durch die Verwendung von Benutzername und Passwort erklärt er, Verfügungsberechtigter über das IdP- bzw. das Webanwendungs-Konto zu sein.[35] Damit speichert der Täter beweiserhebliche Daten so, dass bei ihrer Wahrnehmung eine unechte Urkunde vorliegen würde, vgl. §§ 269, 270 StGB.

4.1.3 Strafbarkeit von Vorbereitungshandlungen nach § 202c StGB

Handlungen, die die Datenerlangung vorbereiten, erfüllen den Tatbestand des § 202c StGB nicht, da diese nicht nach §§ 202a, b StGB strafbar ist. Was Vorbereitungshandlungen zur Datenverwendung betrifft, so ist § 202c StGB zwar einschlägig, aber gegenüber dem vom Angreifer verwirklichten § 202a StGB subsidiär.

4.2 Cross-Site-Request-Forgery

Bei einem CSRF-Angriff im Kontext von OpenID veranlasst der Täter das Opfer zum Login bei seinem IdP und zur Ausführung eines HTTP-Requests, um das Opfer bei einer weiteren Webanwendung csrf-anfaellig.com einzuloggen.

Für die strafrechtliche Bewertung ist zwischen der Vorbereitung eines CSRF-Angriffs und seiner Ausführung zu unterscheiden.

4.2.1 Vorbereitung

§§ 202a, 202b und 202c StGB

Indem der Angreifer mit seiner Webseite evil.com eine Nutzerauthentifikation beim IdP herbeiführt und im Zuge des Verfahrens die OpenID-Identität und die SessionID erfährt, könnte er sich gem. §§ 202a, 202b StGB strafbar machen. Gemäß § 202a StGB macht sich strafbar, wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft (Ausspähen von Daten).

Als Daten, die nicht für den Täter bestimmt sind, kommen die OpenID-Identität und die SessionID in Betracht. Da das Opfer sich aber gerade bei der RP evil.com anmeldet, sind diese Daten für den Angreifer bestimmt - selbst wenn das Opfer eine missbräuchliche Verwendung seiner OpenID-Daten nicht wünscht.

Ferner müsste der Täter die OpenID-Daten unter Überwindung einer Zugangssicherung erlangt haben. Eine solche Sicherung ist im OpenID-Verfahren nicht ersichtlich, da der IdP die Daten an die bösartige RP übermittelt. Der Täter nutzt lediglich das Vertrauen des Opfers in die RP aus. Eine Zugangssicherung zu den OpenID-Daten wird jedoch nicht überwunden. Der Tatbestand des § 202a StGB ist folglich nicht erfüllt.

Eine Strafbarkeit wegen des Abfangens von Daten gem. § 202b StGB kommt für den Täter in Frage, der unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft.

Die OpenID-Daten erlangt der Täter, indem er eine Webseite mit OpenID-Unterstützung herstellt und betreibt. Ob dies ein technisches Mittel ist, kann jedoch offen bleiben, da eine „nichtöffentlichen Datenübermittlung“ hier fernliegend ist. Bei der Nichtöffentlichkeit kommt es nicht auf Art oder Inhalt der übertragenen Daten oder eine etwaige Verschlüsselung an.[36] Nichtöffentlich ist eine Datenübermittlung, die objektiv erkennbar für einen beschränkten Nutzerkreis bestimmt ist, ohne dass es auf die Wahrnehmbarkeit durch Unberechtigte ankommt.[37] Die OpenID-Daten werden vom IdP an die RP gesendet, die eine Weiterleitung veranlasst hatte. Die RP gehört damit zu dem Empfängerkreis. Das Motiv der RP, die OpenID-Daten zu CSRF-Angriffen nutzen zu wollen, spielt für § 202b StGB keine Rolle.

Die Erhebung der OpenID-Daten des Opfers könnte jedoch gem. § 202c StGB strafbar sein. Danach macht sich strafbar, wer zur Vorbereitung eines Ausspähens oder Abfangens von Daten Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten ermöglichen, oder Computerprogramme, deren Zweck die Begehung einer Tat nach § 202a oder § 202b StGB ist, herstellt oder sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht.

Ein Passwort ist eine Zeichenkombination, die bei einer Sicherungsabfrage

[33] Vgl. Seidl/Fuchs, HRRS 2010, 85, 88.

[34] Heckmann, in: Heckmann (Hrsg.), jurisPK-Internetrecht, 3. Aufl. 2011, Kapitel 8 Rn. 264.

[35] Dazu KG Berlin, Beschl. v. 22.07.2009 - (4) 1 Ss 181/09 (130/09), m. Anm. Maisch/Seidl, jurisPR-ITR 22/2009 Anm. 3.

[36] Vgl. Weidemann, in: v. Heintschel-Heinegg (Hrsg.), BeckOK, StGB, Ed. 18, § 202b, Rn. 6.

[37] LG Wuppertal, Beschl. v. 19.10.2010 - 25 Qs 10 Js 1977/08 - 177/10, MMR 2011, 65, 66.

den Zugang zu Daten ermöglicht.[38] Bei einem CSRF-Angriff erhält der Täter die OpenID-Identität eines Opfers. Es handelt sich dabei nicht um ein Passwort, da bei einer SSO-Architektur die Authentifikation an einen IdP ausgelagert wird und das Opfer dort einmalig sein OpenID-Passwort eingibt. Die OpenID-Identität könnte ein „sonstiger Sicherungscode" sein. Darunter werden informationstechnische Sicherungen verstanden, die Passwörtern ähnlich sind und „die den Zugang zu einem Computersystem als Ganzem oder zu einem Teil davon ermöglichen".[39] Die OpenID-Identität allein ermöglicht keinen Zugang zu einem Computersystem. Das Ziel eines CSRF-Angriffs, der Login bei csrf-anfaellig.com oder die Ausführung anderer Aktionen, verwirklicht sich nur, wenn ein Session-Kontext zwischen dem Opfer und seinem IdP vorhanden ist oder begründet wird.

Der Session-Kontext ist ferner kein Sicherungscode, der allein zur Vornahme einer Authentifikation genügt.

Die Implementierung einer Webseite, die der bösartigen RP nur dazu dient, die OpenID-Identität des Opfers zu erheben und einen Session-Kontext des Opfers mit seinem IdP zu begründen oder nutzbar zu machen, könnte jedoch die Herstellung eines Computerprogramms gem. § 202c Abs. 1 Nr. 2 StGB sein. Ob eine Webseite als ein Computerprogramm bewertet werden kann, ist umstritten.[40] Da es sich bei einem HTML-Quelltext aber um Anweisungen an den Browser bzw. an die dahinterliegende Datenverarbeitungsanlage handelt, dürfte es sich um ein Computerprogramm im Sinne des Tatbestandes handeln.

Die Herstellung einer Webseite, die als bösartige RP OpenID-Daten erhebt und einen entsprechenden Session-Kontext veranlasst, die Begehung von CSRF-Angriffen als strafbare Handlungen gem. §§ 202a, 202b StGB vorzubereiten, ist demnach gem. § 202c StGB strafbar.

4.2.2 CSRF-Angriff

§ 202a StGB

Die Herbeiführung eines heimlichen Logins des Opfers bei csrf-anfaellig.com könnte ein Ausspähen von Daten gem. § 202a StGB sein.

Als Daten im Sinne von § 202a StGB kommen das Benutzerkonto und die darin gespeicherten Informationen in Betracht, die nur für das Opfer bestimmt sowie durch die vorgeschaltete Abfrage der Zugangsdaten besonders gesichert sind.

Eine Zugangssicherung ist gegeben, wenn Vorkehrungen getroffen sind, den Zugriff auf Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren.[41] Eine solche Vorkehrung ist der passwortgestützte Zugriffsschutz.[42] Als technische Gestaltungsalternative zu einer Passwortabfrage bildet das OpenID-Verfahren eine besondere Zugangssicherung. Die Daten, die bei der Webanwendung csrf-anfaellig.com gespeichert sind, werden daher besonders gesichert.

Der Täter müsste sich Zugang zu diesen gesicherten Daten unter Überwindung der Zugangssicherung verschaffen. Mit dem CSRF-Angriff zielt der Täter nicht auf den ggf. vorhandenen Passwortschutz einer Webanwendung, sondern auf die OpenID-Authentifikation ab. Indem der Täter die OpenID-Daten des Opfers erhoben und einen Session Kontext geschaffen hat, kann er mittels eines Requests des Opfers einen Login bei der Webanwendung ohne Wissen und Wollen des Opfers herbeiführen und so die Zugangssicherung überwinden. Der Tatbestand des § 202a StGB ist damit erfüllt.

Mit dem Login des Opfers in die Webanwendung kann der Täter die Rechte des Benutzerkontos ausnutzen und ggf. mittels weiterer CSRF-Angriffe auf gespeicherte Daten Zugriff nehmen oder Transaktionen veranlassen.

§ 263a Abs. 3 StGB bzw. § 303a StGB

Das Unterschieben eines HTTP-Requests könnte ferner als strafbare Vorbereitungshandlung eines Computerbetrugs gewertet werden. Selbst wenn das Unterschieben eines Requests im Rahmen einer bösartigen RP-Webseite als Computerprogramm bewertet werden würde,[43] fehlt es an der Unmittelbarkeit des Computerbetrugs. Der CSRF-Angriff müsste unmittelbar zu einem Vermögensschaden führen. Die bösartige RP und das Unterschieben von Requests dient hier jedoch nur dazu, einen Login bei example.com vorzunehmen. Die eigentliche Tat gem. § 263a Abs. 1 StGB würde erst in einem weiteren Schritt verwirklicht. Eine Vorverlagerung des Computerbetrugs auf Webseiten, mit denen OpenID-Daten erlangt oder Logins herbeigeführt werden können, wird abgelehnt.[44]

Darüber hinaus werden bei dem hier skizzierten CSRF-Angriff keine Daten rechtswidrig verändert, sodass der Tatbestand der Datenveränderung gem. § 303a StGB nicht erfüllt ist. Etwas anderes gilt dann, wenn ein CSRF-Angriff genutzt wird, um Daten innerhalb eines eingeloggten Benutzerkontos zu löschen, oder das Konto in seiner Gebrauchsfähigkeit beeinträchtigt wird.[45]

4.3 Clickjacking-Angriff

Ein Clickjacking-Angriff zeichnet sich im Unterschied zum CSRF- und Phishing-Angriff dadurch aus, dass z.B. mittels eines IFrames die Login-Eingabefelder eines IdP derart überlagert werden, dass das Opfer seine OpenID-Daten in die gefälschten Felder des Angreifers eingibt. Diese Überlagerung könnte eine Datenveränderung gem. § 303a StGB darstellen.

Danach macht sich strafbar, wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert. Die Überlagerung der Eingabefelder mittels eines IFrames könnte eine Veränderungen oder Unterdrückung von Daten sein. Als Daten kommt die Webseite des IdP als HTML-Dokument mit ihren Inhalten in Betracht.

Daten werden verändert, wenn sie inhaltlich umgestaltet werden und deshalb einen anderen Informationsgehalt aufweisen. Zwar wird die Darstellung einer Webseite im Browserfenster verändert, eine Veränderung von Dateninhalten wird dadurch jedoch nicht bewirkt.

Ein Unterdrücken von Daten ist gegeben, wenn diese vorübergehend oder auf Dauer dem Zugriff des Berechtigten entzogen werden und dieser sie daher nicht mehr nutzen kann.[46] Indem die originalen Eingabefelder durch einen passgenauen IFrame überlagert werden, wird der Zugang zu diesen Webseiten-Elementen temporär verhindert. Darin ist ein Unterdrücken zu sehen.

Der bisher von der Rechtswissenschaft kaum erforschte Angriff des Clickjackings erfüllt damit als Unterdrücken

[38] Weidemann, in: v. Heintschel-Heinegg (Hrsg.), BeckOK, StGB, Ed. 18, § 202c, Rn.4.

[39] Vgl. Art. 6 Abs. 1, lit. a Nr. ii Übereinkommen über Computerkriminalität

[40] S.o. Fn. 30.

[41] BGH, Beschl. v. 06.07.2010 - 4 StR 555/09, MMR 2010, 711.

[42] Fischer, StGB, 59. Aufl. 2012, § 202a, Rn. 8a.

[43] S.o. Fn. 30.

[44] Cramer/Perron, in: Schönke/Schröder, StGB, 28. Aufl. 2010, § 263a, Rn. 33a.

[45] Dazu im Kontext von (D)DoS-Angriffen, Heckmann, in: Heckmann (Hrsg.), jurisPK-Internetrecht, 3. Aufl. 2011, Kap. 8, Rn. 20.

[46] Weidemann, in: v. Heintschel-Heinegg (Hrsg.), BeckOK, StGB, Lfg. 18, § 303a, Rn.9.

von Daten den Tatbestand des § 303a StGB.

Je nach Ausgestaltung der IFrames könnte auch § 269 StGB verwirklicht sein.

5. Ausblick

OpenID bringt neben der herausragenden Eigenschaft, endlich ein einziges, sicheres, einprägsames Passwort haben zu können, eine Reihe unüberschaubarer Risiken mit sich. Insgesamt zeigt sich, dass sowohl IdPs als auch RPs ein erhebliches Risiko für Angriffe in sich bergen.

In der Rechtswissenschaft, insbesondere im Strafrecht, sind z.B. die Angriffe Cross-Site-Request-Forgery und Clickjacking bisher weitgehend unbekannt.

Wer keinem IdP sein Vertrauen schenken möchte, dem steht die Möglichkeit offen, einen privaten oder Unternehmens-IdP zu betreiben.

Ferner können RPs in Vertrauensklassen unterteilt werden, wobei für jede Klasse eine eigene OpenID-Identität eingerichtet wird, z.B. je eine Klasse für E-Commerce, soziale Netzwerke und weitere Webanwendungen. Je mehr Klassen definiert werden, desto weiter nähert man sich allerdings dem bisherigen Authentifikationsmodell mit einem Passwort je Webanwendung.

Die Zukunft gehört einfach benutzbaren, session-unabhängigen Authentifikationsverfahren und alternativen Session-Konzepten, die für mehr Sicherheit bei der Verwendung von OpenID sorgen.