Wenig Sicherheit auf Web-2.0-Sites

MySpace, YourSpace, OurSpace

Christoph Puppe

Betreiber von großen Plattformen wie MySpace, YouTube oder Flickr tragen nicht nur in Sachen Sicherheit eine große Verantwortung gegenüber ihren Mitgliedern. Das Beispiel MySpace zeigt, dass sie der nicht immer gerecht werden.

Der gewaltige Erfolg von MySpace lockt nicht nur Firmen auf die Plattform, sondern auch Kriminelle in großer Zahl und mit den unterschiedlichsten Motiven. Der Ahnungslosigkeit der Teilnehmer des vorwiegend an Jugendliche und Kinder gerichteten Angebots ist es geschuldet, dass die Bemühungen der Cyberkriminellen leider viel zu oft von Erfolg gekrönt sind.

Ein besonders krasser Fall von erfolgreichem Phishing kam am 15. Januar 2007 zutage, als über die Sicherheitsmailingliste „Full Disclosure“ eine Mail verbreitet wurde, die einen Link enthielt. Wer diesem Link folgte, erhielt eine Textdatei mit über 56 000 Zeilen. Jede dieser Zeilen besteht aus einer E-Mail-Adresse nebst Passwort eines MySpace-Mitgliedes. Neben rund 30 000 realen Accounts finden sich in der Liste auch wüste Beschimpfungen von MySpace-Benutzern an den Phisher.

Nachdem diese Liste eine nicht unerhebliche Öffentlichkeit erreicht hatte und niemand etwas gegen ihre weitere Verbreitung unternahm, fühlten sich zwei Mitglieder von „Full Disclosure“ verpflichtet, sie mitsamt den Passwörtern als Anhang an die Mailingliste zu schicken. So war sie auch weiterhin verfügbar, nachdem der Original-Link längst vom Netz genommen war. Also ein schlechtes Beispiel für den verantwortungsvollen Umgang mit dem Veröffentlichen kritischer Informationen („Responsible Disclosure“). In Hackerkreisen wird ein solches Verhalten häufig angeprangert, etwa von FX von phenoelit.net am Beispiel einer anderen sogenannten Dropsite (dort legen Trojaner ihre Daten ab) eines auf Bankdaten spezialisierten Trojaners.

Vermeintlich harmlose Website

Gesammelt wurden die Anmeldeinformationen auf einer Webseite, die einen Werkzeugkasten zur Verschönerung des eigenen Profils auf MySpace anbot. Der Inhaber der Domain, Marc Olano, antwortete nicht auf Anfragen zu einem Interview, aber in einem Kommentar auf einer Blogseite behauptet ein Marc, dass er wohl kaum seine eigene Domain mit seinem richtigen Namen für so einen Angriff nutzen würde. Überdies hatte er sich in der Vergangenheit stark engagiert und für MySpace-Benutzer Dienste und mehr bereitgestellt. So gerieten nicht nur die realen Accounts ins Visier der Angreifer, sondern auch ein motivierter Anbieter von Inhalten.

Nach dem Kursieren des Quicktime-Wurms Ende des letzten Jahres, der ebenfalls zum Ausspähen von Passwörtern beitragen sollte, ist dies der zweite Vorfall, der an die Öffentlichkeit gelangte und mehrere Zehntausend Benutzer betraf. Viele weitere Phishing-Angriffe werden nie bemerkt und nie veröffentlicht, die Zahlen der Betroffenen lassen sich daher nicht einmal annähernd schätzen. Allerdings ist nach Aussage von MySpace-Benutzern jeder dort schon einmal Opfer einer Account-Übernahme geworden. So macht MySpace seinem Ruf als AOL des neuen Jahrtausends alle Ehre.

Nach dem Wurmangriff im vergangenen Dezember begannen verschiedene Personen, etwa Krypto-Guru Bruce Schneier oder Brian Krebs von der Washington Post, die Qualität der 34 000 gephishten Passwörter zu analysieren und statistisch auszuwerten, etwa hinsichtlich Zeichenlänge, Abwechslung von Buchstaben und Zahlen et cetera. Neben der insgesamt eher schlechten

Qualität der Passwörter gab es Ausnahmen, beispielsweise „1ancheste23-nite41ancheste23nite4“ mit 32 Zeichen oder die ebenfalls relativ langen Passwörter „fool2thinkfool2thinkol2think“ sowie „dokitty17darling7g7darling7“. Allerdings hilft den Benutzern dieses Dienstes ein sehr gutes Passwort nur bedingt. Denn selbst das komplizierteste Passwort schützt vor Social Engineering nicht und kann vom Benutzer auf einer Phishing-Seite eingegeben werden.

Unter den Betroffenen der jüngsten Phishing-Attacke führte der Autor eine Umfrage durch. Dazu schickte er an alle Adressen aus der Liste eine Mail. Von den 56 000 Zeilen waren nach Anwendung einer Regular Expression, Sortierung und Dublettenprüfung noch 39 000 Adressen übrig. Von ihnen konnten über 29 000 zugestellt werden – wie viele davon allerdings in Spamfiltern hängen blieben, ist ungewiss. Immerhin über 900 Benutzer antworteten, wenngleich nicht immer in einer Form, die sich maschinell auswerten ließ.

Platzierung von „Erwachsenen-Werbung“

Fast ein Drittel der Antwortenden gab an, dass sie erst durch die Befragung Kenntnis von der Veröffentlichung ihrer Nutzerdaten im Internet erlangt haben – ein durchaus erwünschter Nebeneffekt der Aktion. Die meisten hatten allerdings schon von Freunden davon gehört, dass ihre Accounts missbraucht wurden. In der Regel bemerkten diese es anhand von Rundschreiben an den gesamten Freundeskreis (sogenannte „Bulletins“), die Spam für diverse Produkte enthielten. Auch veränderte Profile mit Werbung für teilweise nicht jugendfreie Inhalte fielen den Betroffenen und ihren Freunden auf. Kaum jemand der Befragten gab an, von MySpace selbst informiert worden zu sein, 801 verneinten das – ein skandalöses Ergebnis.

Die Nutzer der Zugangsdaten waren anscheinend hauptsächlich daran interessiert, Werbung zu versenden, die Benutzer durch verunstaltete Profile zu ärgern oder auch nur mal ein bisschen in den privaten Daten zu schnüffeln. So wurden nur wenige Passwörter geändert und die Benutzer dadurch ausgesperrt. Kompromittierendes Material haben aber nur wenige MySpace-Benutzer in ihren Profilen, da sich viele wohl des Risikos bewusst sind und überdies die AGBs der Plattform die Eingabe von Telefonnummern, Adressen et cetera verbieten. Dennoch befürchtet fast die Hälfte der Antwortenden, dass die Daten aus den privaten Teilen der Profile gegen sie verwendet werden können. Teilweise herrscht aber auch ein humorvoller Umgang mit dem Identitätsdiebstahl. So antwortete einer, dass sein Kredit-Rating so schlecht sei, dass die Phisher seine Identität gerne haben können.

Ein zusätzliches Risiko für jeden Benutzer ist die weit verbreitete mehrfache Nutzung von Passwörtern. So berichteten mehrere Betroffene, dass auch der E-Mail-Account, der als Benutzername bei MySpace dient, missbraucht wurde. In mindestens zwei Fällen hat der Angreifer beide Passwörter geändert. In einem solchen Fall gibt es einen Weg, zumindest den MySpace-Account zurückzuerhalten. Dazu muss der Benutzer ein Foto von sich mit einem Schild seiner MySpace-Nummer an den Kundensupport schicken.

Kundenverlustrisiko für Betreiber

Für MySpace selbst sind die Phishing-Attacken und deren Folgen für die angemeldeten Kunden auch nicht ohne Geschäftsrisiken. Die oft jugendlichen Benutzer gelten als wenig „produkttreu“ und sollen schnell die Sites wechseln, wenn es ihnen irgendwo nicht mehr gefällt. Diese verbreitete Meinung konnte die Befragung nicht bestätigen, nur sieben gaben an, dass sie ihr Profil gelöscht haben. Die gleiche Anzahl hat sich nach der Zerstörung des ersten Profils gleich ein neues angelegt. MySpace hatte im Laufe seiner Entwicklung mit technischen Herausforderungen zu kämpfen, die oft in Fehlern und Unzulänglichkeiten in der Darstellung mündeten. Die Benutzer waren in den letzten Jahren bereit, das in Kauf zu nehmen und die Anstrengungen der Betreiber, in Zeiten eines exponentiellen Wachstums die Technik am Laufen zu halten, durch Treue zu honorieren. Die Probleme mit der Sicherheit ignorierten sie allerdings.

Eine interessante Darstellung der Mitgliederentwicklung – allein bis Mitte 2005 26 Millionen Accounts – und der technischen Hintergründe bietet der Artikel „Inside MySpace.com“ von David F. Carr (siehe Kasten „Quellen im Internet“). Es ist, das muss man den Eigentümern zugute halten, sicher keine leichte Aufgabe, eine Plattform zu betreiben, die rund 40 Milliarden Page Views im Monat zu verzeichnen hat.

Bemühungen um den Kundenschutz

Derzeit sieht sich MySpace mehreren Klagen ausgesetzt. Kinder wurden auf der Plattform von Männern angesprochen und zu realen Treffen bewegt, bei denen es zu sexuellen Übergriffen kam. Die Klagen gehen von der Prämisse aus,

Benutzerauskünfte nach dem Passwort-Phishing

	ja	nein
Ich habe mein Passwort geändert:	818	23
Mein Passwort wurde von jemand anderem geändert:	50	704
Ich wurde von MySpace über den Vorfall informiert:	39	801
Ich habe davon über andere Wege erfahren:	319	504
Dass mein Passwort veröffentlicht ist, habe ich erst durch diese E-Mail erfahren:	293	463
Ich habe gemerkt, dass sich jemand in meinen Account eingeloggt hat:	573	234
Ich befürchte, dass diese Daten gegen mich benutzt werden können:	216	248

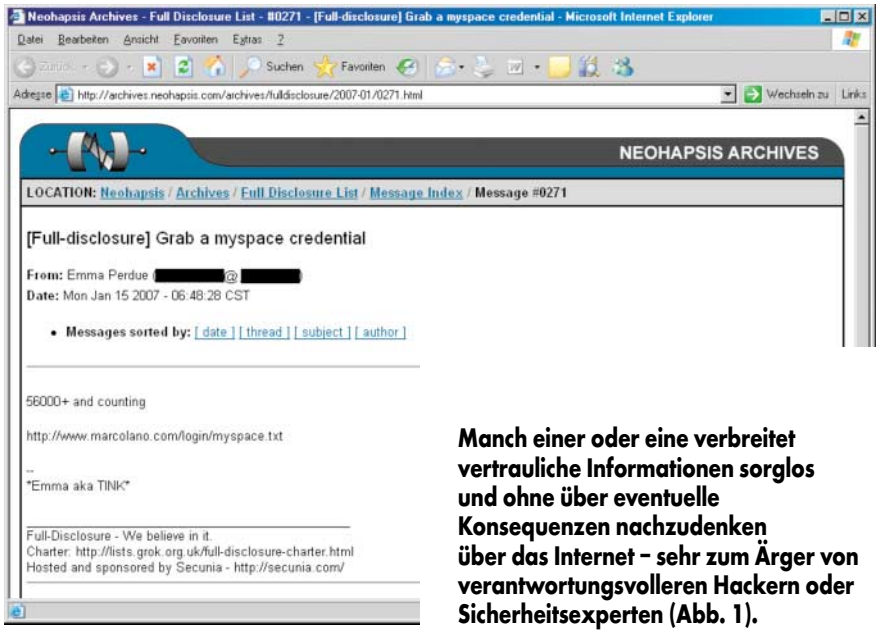
Quellen im Internet

Full Disclosure List:	www.security-express.com/archives/fulldisclosure
Kritik an „irresponsible disclosure“:	www.phenoelit.net/lablog/Irresponsible.sl
Kommentar Marc:	www.computerdefense.org/?p=193
Quicktime-Wurm-Attacke:	www.heise.de/newsticker/meldung/81924
Schneiers Passwortanalyse:	www.schneier.com/blog/archives/2006/12/realworld_passw.html
Analyse von Brian Krebs:	blog.washingtonpost.com/securityfix/2006/12/myspace_video_worm_pimps_adult_1.html
David Carr, Inside MySpace.com:	www.baselinemag.com/print_article2/0,1217,a=198614,00.asp

dass die Betreiber nicht alles dafür getan haben, die Sicherheit der Benutzer zu gewährleisten. MySpace ließ verlauten, dass der Schutz der Kinder im Internet Aufgabe der Eltern sei und nicht von einer Website geleistet werden könne. Mitte Februar hat nun ein texanischer Richter eine dieser Klagen mit dem Hinweis auf die Erziehungsverantwortung der Eltern abgewiesen. Im vergangenen Jahr hatte MySpace eine groß angelegte Sicherheitskampagne gestartet.

Auch technisch unternehmen die Betreiber einiges, um die Benutzer zu schützen. Beispielsweise wird Javascript in den Profilen vollständig ausgeschlossen und automatisiert herausgefiltert. Zur Individualisierung können die Benutzer externe Ressourcen einbinden, zum Beispiel Stylesheets, Bilder, Flash und Musik. Eine dieser Ressourcen, die Quick-Time-Videos, verteilte letztes Jahr durch eine Verwundbarkeit den oben erwähnten Wurm.

Kritikwürdig ist dagegen die spärliche Aufklärung der Benutzer. Der Link auf die Seiten mit den Sicherheitstipps ist ganz klein unten auf der Seite angebracht. Dort finden sich dann aber gut verständliche Tipps in Sachen Sicherheit. Allerdings fehlt hier der Hinweis, dass eine Anti-Phishing-Toolbar für Kids zur Minimalausstattung eines Browsers gehört – am Tag nach dem Posting in der Mailingliste war die Domain bereits in allen wichtigen Phishing-Toolbars registriert. Dagegen wird auf der Seite mit Tipps zur Internetsicherheit für Eltern auf die verfügbare Software zum Schutz der Kinder im Internet hingewiesen. Es fragt sich nur,



Manch einer oder eine verbreitet vertrauliche Informationen sorglos und ohne über eventuelle Konsequenzen nachzudenken über das Internet – sehr zum Ärger von verantwortungsvolleren Hackern oder Sicherheitsexperten (Abb. 1).

wie viele informierte Eltern es gibt, die sich mit dem Surfverhalten ihrer Kinder auseinandersetzen, und wie viele Kinder und Jugendliche die diesbezüglichen Ratschläge ihre Eltern annehmen.

Bessere Nutzeraufklärung erwünscht

Die Bulletins und Blog-Einträge des sogenannten Tom-Accounts (ein standardmäßig bei Neumitgliedern durch MySpace angelegter erster Freund namens Tom) haben einigen geholfen. Dort findet sich immerhin der Hinweis, dass man sein Passwort wechseln soll, wenn man Bulletins sieht, die man nicht selbst verschickt hat. Allerdings steht das nicht in der ersten Mail von Tom, die jeder neue Benutzer erhält. Überdies sind die wenigen Tipps, die die FAQ enthalten, kaum zu finden.

Aus Sicherheitssicht könnte MySpace mehr tun. Etwa wie Webmail-Anbieter alle externen Links durch einen zwischengeschalteten Link ersetzen, um die in der URL enthaltene Daten vor den Logfiles des externen Servers zu verstecken. So kann die Session des Benutzers nicht ausgenutzt werden. Ebenso könnte man auf diese Art verhindern, dass Angreifer Links zu bekannten Phishing-Sites in Profile setzen. Allerdings sind dieses Maßnahmen ziemlich aufwendig und zu guter Letzt ist die Sicherheit der Profile immer vom Verhalten des Benutzers abhängig.

Bei den Sicherheitsproblemen der Vergangenheit hat MySpace zum Teil sehr schnell reagiert. Die Betreiber schalteten etwa beim Grassieren des Samy-Wurms die gesamte Site ab und entfernten automatisiert den Schadcode aus den Profilen. Ähnlich verfuhren sie beim Quicktime-Wurm.

Beim aktuellen Vorfall kam die erste Reaktion von MySpace jedoch erst nach 10 Tagen. Ein Archiv der Mailingliste mit der gepostete Liste der Benutzerdaten wurde vom Netz genommen. Erreicht wurde das, indem MySpace den DNS-Provider aufforderte, die Domain nicht weiter aufzulösen. So war die Domain von Fyodor (www.seclists.org), Autor des Sicherheitsscanners *nmap*, für mehrere Stunden nicht erreichbar. Leider hat es MySpace versäumt, den Betreiber der Site zu kontaktieren und ihn aufzufordern, die Mails aus dem Archiv zu entfernen. Weitere Archive der Mailingliste sind noch aktiv und die Liste ist nach wie vor abrufbar.

Weder MySpace noch die Betreiber, Hoster oder DNS-Provider der Phishing-Site und der anderen Mailinglisten-Archive waren zu Auskünften über den Sicherheitsvorfall bereit. Angesichts der jetzt schon großen und weiterhin steigenden Anzahl von Benutzern solcher Plattformen ist es höchste Zeit, ein paar Gedanken mehr auf Warnhinweise und Sicherheitsmaßnahmen zu verwenden. (ur)

MySpace – Historie und Entwicklung eines Weberfolgs

MySpace ist heute das erfolgreichste Webangebot für private Profile zum Zwecke der Pflege und des Aufbaus von Freundschaften. Nach Schätzungen sind über 150 Millionen Profile registriert und es kommen jeden Tag cirka 230 000 hinzu. Laut Netcraft liegt MySpace auf Platz 65 der Zugriffe und laut Alexa.com auf Platz 6 des Traffics. Nach manchen Schätzungen hat MySpace doppelt so viele Pageviews wie Google. Mit diesen Traumwerten liegt das Portal um Größenordnungen vor seinem Vorbild Friendster (Netcraft: 278, Alexa: 36) und dem mit Google verbandelten Orkut (Netcraft: 267, Alexa: 8).

Initiiert wurde das Portal 2003 von Tom Anderson, Chris DeWolfe und einer kleinen Gruppe von Programmierern. Die beiden Gründer arbeiten schon seit 1999 zusammen, zuerst als Angestellte bei einem Angebot zum Speichern von Multimediadaten (xdrive) und seit 2001 in einer selbst gegründeten Firma zum Vertrieb von E-Mail-Listen für das Internet-Marketing (ResponseBase). Diese Firma nutzte die Mail-Adressen der auf xdrive registrierten Benutzer zum Verschicken von Spam, ein weiterer Geschäftszweck war ihr Verkauf an andere Versender unverlangter Werbemails. Teilweise wurden diese Mails bereits mit Absendern aus der Domain myspace.com verschickt, die Andersen und deWolfe von ihrem damaligen Inhaber gekauft hatten.

Sie verkauften ResponseBase 2003 an eUniverse und behielten nur wenige Anteile am Unternehmen, das heißt in der Folge auch an MySpace. eUniverse, das neben dem Versand von Spam auch das Installieren von Spyware als Einnahmequelle hatte, benannte sich 2004 in Intermix Media um. 2005 wurde dieser Vorwurf in einer Anklage des Staates New York gegen nun Intermix erhoben und endete in einem Vergleich, bei dem Intermix 7,5 Mio. US-$ zahlte. Im gleichen Jahr kaufte Rupert Murdochs News Corporation das Unternehmen für 580 Mio. US-$.

Mit Inkrafttreten des CAN-SPAM Act von 2003 wurde das Versenden von Spam zu einem riskanten Geschäft – was der Auslöser für Andersons und DeWolfes Verkauf von ResponseBase war. Auf der Suche nach einem neuen Geschäftsmodell stießen die beiden auf Friendster.com, das zu diesem Zeitpunkt viele neue Anmeldungen verzeichnete. Gerüchten zufolge wurde MySpace erst als Werbeplattform für Direktmarketing innerhalb von Friendster gestartet. Neben den technischen Problemen des Vorbilds war der große Gestaltungsspielraum, über den die Benutzer von MySpace verfügen, ein Motor des Erfolges. Auch heute noch sind die Profile auf MySpace bunter, personalisierter und individualisierter als auf allen anderen vergleichbaren Sites. Dass das nicht immer gut für die optische Qualität ist, kann man sich leicht vorstellen. Zumindest aber kann jeder, der CSS oder ein Werkzeug zu dessen Erzeugung benutzen kann, sein Profil nach eigenem Gusto verunstalten.

Diese große Freiheit der Gestaltung und die Zahl der Profile sind auch die Ursachen der immensen technischen Herausforderungen, denen sich MySpace seit der Gründung stellen musste. Wo ein normales Webangebot statische Inhalte präsentiert, die nur wenige Verantwortliche ändern, ist MySpace an dieser Stelle eine lupenreines Web-2.0-Angebot, denn jeder Inhaber eines Profils ist gleichzeitig Editor seines eigenen Angebots. So können klassische Methoden zur Lastverteilung in einer Farm von Webservern nicht genutzt werden. Beispielsweise ist das Cachen von Profilen kaum möglich, denn ein Benutzer erwartet, dass jede Änderung sofort für ihn und seine Besucher sichtbar ist. Bereits Verzögerungen von wenigen Minuten sorgen für Verstimmungen. Heute wird die Seite mit .Net betrieben und läuft seit Kurzem auch auf drei Rechenzentren verteilt. Besonders diese Verteilung aller Änderungen in kurzer Zeit war nicht einfach zu realisieren, aber nach einem Stromausfall im ersten Rechenzentrum dringend erforderlich geworden.

In bester Tradition der Gründer und von Intermix Media lebt MySpace von genau auf Zielgruppen ausgerichteter Werbung. Zu nennen sind hier die auf jeder Seite eingeblendeten Banner sowie das Marketing von Musikgruppen als Hauptquellen der Einnahmen. Ein immer wichtigerer Aspekt sind Webrepräsentanzen von Firmen, die sich und ihre Produkte in ihren Profilen promoten und zu allen aktuellen Trends Dienste anbieten. So kann ein Teilnehmer einfach seine Videos, Musik, Fotos oder Lebensbeichten in Blogs, Chaträumen und per Instant-Messaging verteilen. Auch Jobsuche oder Schulvergleiche finden sich im Angebot.