

Dies ist eine Zusammenfassung längerer Beobachtungen des sozialen Netzwerkes SchülerVZ.de.



Das SchülerVZ unter der Lupe

SchülerVZ - ein soziales Netzwerk, von vielen Jugendlichen benutzt, die sich nicht allzu viele Gedanken um ihre Sicherheit machen. Jugendliche, die noch unbeschwert im Internetz umherirren, und denken, dies sei nur ein Treffpunkt und ein Ort zum Spaß haben (was es ja unter anderem auch ist). Solche, die eben nicht die Schattenseiten kennen.

Dieser Bericht möchte auf eben diese Punkte eingehen.

1. Sicherheit der persönlichen Daten
2. Speicherdauer und Beeinflussbarkeit der persönlichen Daten
3. Darf's noch eine Sicherheitslücke sein?
4. ~~Wie SchülerVZ gegen „Freidenker“ vorgeht~~ (Kapitel entfernt - Wir möchten anonym bleiben)

Es liegt nahe, dass sich all die hier genannten Fakten auch auf das StudiVZ und MeinVZ anwenden lassen.

1. Sicherheit der persönlichen Daten

Stichwort „Crawling“.

In der Vergangenheit gab es immer wieder Fälle, wo von „Crawling“ die Rede war. Schon Ende 2006 wurde das gesamte StudiVZ Opfer eines gezielten Auswertens von Daten, nachzulesen auf studivz.irgendwo.org.

Doch seitdem hat sich doch sicher einiges getan? SchülerVZ wird doch gewisse Maßnahmen ergriffen haben, um dem präventiv entgegenzuwirken? Denn neuerdings wirbt es immerhin mit allerlei [Datenschutzversprechen](#). So heißt es, die Daten auf den SchülerVZ-Servern seien bestmöglich gesichert. Doch das ist leider eine glatte Lüge.

Denn es gibt Schlupflöcher: Zum Beispiel die Suchfunktion. Du wirst feststellen, dass diese auch nach dem tausendsten Benutzen keinen „Captcha“-Schutz hat. Nein, die Suchfunktion ist eine solche Funktion, mit der es ein leichtes ist, große Datenbanken von Jugendlichen zu erstellen. Datenbanken, die sich nach Alter, nach Wohngebiet, nach Beziehungsstatus oder nach Geschlecht richten können. Große Datenbanken, mit Bildern, mit Namen, mit Schulen, mit Altern, mit politischen Interessen - große Datenbanken mit eben wieder alledem, was sich über die „[Supersuche](#)“ alles finden lässt. Und das sind Daten, die sicher auch für die Schober-Group interessant wären. Also nicht unbedingt so harmlos. Und faktisch gesehen immerhin *nicht* „sicher auf den Servern“ - diese Lüge ist eine Frechheit.

Wir haben dies zu Testzwecken einmal ausprobiert. Das Ergebnis lies sich sehen - in wenigen Stunden etwa eine Millionen Personen, mit Schule, Name, Bild, Alter, Geschlecht und so weiter.*

* (1) Auch automatisiert kein Problem: Man benötigt nur ~ 30 Zeilen Code und 10 Minuten Aufwand.

* (2) Anmerkung 21.09.09: Die erstellte Datenbank wurde von uns **nicht** veröffentlicht! Einziger Empfänger war die Redaktion von Netzpolitik.org, die die Daten umgehend gelöscht haben. Auch wir haben dies getan. Mit dem in den Medien genannten 20-jährigen Mann, welcher selbstständig Daten in böser Absicht sammelte und verkaufen wollte standen wir nie in Verbindung. Unsere Absicht bestand einzig und allein darin, auf diese Problematik aufmerksam machen zu wollen, da SchülerVZ auf unsere Hinweise hin nicht gehandelt hat.



Ein Ordner voll von "gecrawlt" Daten...

Arno Nühm

ID:	506c8f4cc56c067d
Schul-ID:	19315
Geburtstag:	06.12.1993
Geschlecht:	männlich

... und ein einzelnes Profil...

2. Speicherdauer und Beeinflussbarkeit der persönlichen Daten

Ein Recht auf Informationelle Selbstbestimmung?

2.1 Das Profil

SchülerVZ bietet jedem Mitglied an, sich auf seiner eigenen Profilseite (eine Art Visitenkarte) vorzustellen. Hierbei kann man von Geschlecht bis zur politischen Richtung alles mögliche angeben. Dass diese Informationen nicht ausreichend durch SchülerVZ geschützt werden, wurde bereits in Kapitel 1 "Deine Daten sind sicher?" behandelt und wird hier außer Acht gelassen.

Kritisieren wollen wir an dieser Stelle, dass man sein Profil nicht genügend vor den Augen Dritter und Unbekannter verbergen kann. Es ist durch die Betreiber von SchülerVZ unmöglich, sein Profilbild, seinen Namen und seine Schule unkenntlich zu machen. Die Angabe dieser Daten ist bei der Anmeldung verpflichtend (abgesehen Profilbild, dazu unten mehr). Weiterhin ist es durch §§7.4 der SchülerVZ AGB untersagt, sich durch die Angabe falscher Daten vor dem automatisiertem Auslesen seiner Daten zu schützen. (Siehe 1.).

In Bezug auf das Bild eines Profils sind uns noch weitere bedenklich erscheinende Fakten aufgefallen. Entscheidet man sich einmal dafür, ein Profilbild zu erstellen, lässt sich dies nicht mehr rückgängig machen.

„Wenn du etwas löschst, ist es auch weg. Und das komplett!“

So heißt es auf der vereinfachten Datenschutzseite vom Schülerverzeichnis. Doch abgesehen von der rhetorischen Meisterleistung dieses Satzes stimmt da noch etwas nicht.

Zwar ist es möglich, sein aktuelles Profilbild zu ändern oder gar zu „löschen“, doch Vorsicht - „Löschen“ ist hier nicht gleich Löschen. Das Bild bleibt weiterhin bestehen und für jeden aufrufbar, der die Adresse besitzt. Probiere es aus: Bild [hochgeladen](#), die Bildadresse kopiert, anschließend das gute Stück mit einem Klick auf „[löschen]“ wieder entfernt und dann schließlich das Aufrufen der Bildadresse - Du wirst überrascht sein.

Das Problem hierbei ist einfach der schlichte Verrat - denn wenn man etwas löscht, so bleibt es doch bestehen, „und das komplett“. Alle Bits und Bytes des Bildes bleiben über die 750 Servern VZnet Netzwerke Ltd. erreichbar. Der Satz oben: Eine üble Lüge.

Auch nach Löschung des Accounts bleiben alle hoch geladenen Profilbilder weiterhin auf den Servern von SchülerVZ erhalten. Es ist zu vermuten, dass dieses Vorgehen auch auf die restlichen Teile des Profils zutrifft, denn auch wenn ein Nutzer gesperrt oder „gelöscht“ wird, so lässt sich auf diese Art weiterhin das Bild aufrufen. Es liegt nahe, dass auch die Reste des Profils in gesperrter Form auf den Servern liegen bleibt, nur zugänglich für Mitarbeiter oder eventuelle Kunden des Netzwerkes.

Der Nutzer hat folglich nur noch beschränkte Kontrolle auf seine von ihm SchülerVZ anvertrauen Daten. Zwar kann er sie visuell unzugänglich machen, doch was im Netz ist, bleibt im Netz. Das Netzwerk bietet kein Recht auf Informationelle Selbstbestimmung.

Bevor wir zum nächsten Punkt voranschreiten, möchten wir hier nochmal die AGB zitieren.

SchülerVZ AGB §§7

7.1 Soweit der Nutzer die von ihm gemachten Angaben ändert oder berichtigt und dabei alte Einträge löscht, werden diese von ihm vormals eingegebenen Daten automatisch vollständig gelöscht. Ein Antrag auf Berichtigung oder Löschung ist nicht erforderlich.

7.3Soweit der Nutzer sein Profil endgültig löscht und damit seine Mitgliedschaft bei SchülerVZ beendet, werden alle von ihm vormals eingegebenen Daten automatisch vollständig gelöscht. Ein Antrag auf Löschung ist nicht erforderlich.

2.2. Fotoalben

SchülerVZ bietet unter anderem auch an, Fotos von sich oder anderen zu veröffentlichen. Nun kann man sich aber vorstellen, dass es Menschen gibt, die nicht mit der Veröffentlichung eigener Bilder oder Fotos, auf denen diese Menschen abgebildet sind einverstanden sind. Von einer Plattform dieser Größe sollte man eigentlich erwarten können, diesen Wunsch zu akzeptieren. Wir, die Autoren dieses Textes haben SchülerVZ auf diesen Aspekt getestet. Hierzu forderten wir unabhängig voneinander SchülerVZ per E-Mail dazu auf, einzelne Bilder zu entfernen.

Sehr geehrte Damen und Herren,

soeben musste ich feststellen, dass ihr Unternehmen Bildnisse meinerseits öffentlich zur Schau stellt.

Ich habe ihnen zu keinem Zeitpunkt meine Einwilligung für die Veröffentlichung und für die Anbietung erteilt (§§22 KunstUrhG). Zwar kann ein Teil der Bildnisse, auf welchen ich nach denen in §23 Abschnitt 1 KunstUrhG genannten Eigenschaften abgebildet bin ohne meine Einwilligung veröffentlicht werden, doch möchte ich mit diesem Schreiben mein Interesse an der Löschung der Bilder bekräftigen, was die Befugnis außer Kraft setzt.

Ich verlange gemäß §37 des KunstUrhG eine sofortige Vernichtung jeglicher Bildnisse, auf welchen ich abgebildet bin, die sie auf ihren Servern öffentlich zur Schau stellen. Mit Bezug auf §43 und §44 des KunstUrhG bin ich über den Verlauf der Vernichtung zu informieren. Einen Großteil der entsprechenden Bildnisse können sie über folgenden Hyperlink erreichen:

<http://www.schuelervz.net/PhotoAlbums/Tags/zensiert>

Hochachtungsvoll, Ano nym.

Der im letzten Satz genannte Link verwies auf alle uns (damals) bekannten Bilder, auf denen einer der Autoren abgebildet war. Die E-Mail beinhaltet im Grunde genommen alle nötigen Informationen, die erforderlich sind, um einer solchen Forderung nachzukommen. Dennoch erhielten wir folgende Antwort:

Hi Ano,

Ohne zu wissen wie du aussiehst bzw. eine genaue Beschreibung von den unerwünschten Bildern, können wir gar nichts für dich tun. Bitte teile uns doch genau mit (am besten in Form von Links direkt zu den Bildern), welche Fotos du gelöscht wünschst, und wir werden der Sache nachgehen. Solltest du jemanden

kennen, der ein Profil bei uns hat, lasse denjenigen doch bitte die Fotos über unsere Meldenfunktion melden und wir können sie anschließend sofort entfernen.

Liebe Grüße,

Dein Support-Team

Nun folgte noch weiterer E-Mail-Verkehr, die Bilder wurden aber nie gelöscht. Wir haben diesen Versuch mehrfach durchgeführt, eine Löschung der Bilder konnten wir per E-Mail allerdings nie erreichen.

SchülerVZ ermöglicht dies nur über die 'Melde-Funktion', welche aber nur für Mitglieder verfügbar ist. Dies ist definitiv nicht ausreichend, da der Aufwand enorm erhöht wird und Personen über 21 Jahren nicht berechtigt sind im SchülerVZ angemeldet zu sein.

3. Darfs noch eine Sicherheitslücke sein?

Diese Lücke ist kritisch.* SchülerVZ benutzt bei seinen Formularen Formularschlüssel und einen „iv“-Schlüssel, beides sehr kryptische Folgen an Zahlen und Worten. Doch offensichtlich beides ohne jeden Sinn und Zweck. Man baue - oder kopiere - ein beliebiges Formular der Seite (beispielsweise den Buschfunk), nehme von dort auch die Werte „formkey“ und „iv“, schreibe all das in eine HTML-Datei, realisiere mit Javascript ein automatisches Abschicken des Formulars und binde die Datei versteckt - beispielsweise mittels einem iFrame - in eine Heimseite seiner Wahl ein. Das Ergebnis lässt sich sehen - jeder, der nun diese Seite besucht, schickt automatisch das Formular versteckt in seinem „Web-Browser“ ab, und schickt so zum Beispiel eine vorgefertigte Buschfunknachricht ins SchülerVZ. Das könnte Werbung sein, oder Beleidigungen - und alles, obwohl man es gar nicht möchte.

Hier mal ein kleines Beispiel eines solchen Codes:

```
<body onload="document.form.submit();">
<form method="post" action="http://www.schuelervz.net/Profile/EditPersonal" name="form">
<input type="text" name="userNotLike" value="Das SchülerVZ!" />
<input type="hidden" name="formkey" value="8b08[...]2ea" />
<input type="hidden" name="iv" value="7396d3f9d[...]fd84ee5ea6" />
<input type="submit" />
</form>
</body>
```

Wie genau man die beiden Werte berechnet und wie lange sie gültig sind, lässt sich nur schwer erraten. Fakt ist aber, dass die eigenen, persönlichen Werte auch bei anderen Nutzern von SchülerVZ funktionieren.

Wichtig ist auch, dass man die Werte stets vom jeweiligen Formular nimmt. So könnte man beispielsweise keine Werte aus dem Buschfunkformular entnehmen, und diese anschließend benutzen, um Profildaten zu verändern.

Weiterhin scheint es wichtig zu sein, dass die Werte stets aktuell bleiben. Das heißt, mittels eines Programms ist wieder ein automatisiertes Auslesen gefragt, beispielsweise jede halbe Stunde.

Kritisch wird die Lücke, wenn sie beispielsweise für Werbung missbraucht wird, um Rufmord zu begehen oder um einen Menschen zu beleidigen. Man kann die Lücke auch ausnutzen, um Einstellungen zu verändern, zum Beispiel, wer Deine Seite besichtigen darf, auf welche Schule Du gehst, oder - besonders schlimm - man kann Deine E-Mail-Adresse verändern. Hier muss dann nochmals das Ganze mittels Bestätigungscode verifiziert werden. Um dann das Benutzerkonto eines „Opfers“ zu übernehmen, müsste dieses wieder auf eine präparierte Seite gelangen, welche wieder genau diese Lücke ausnutzt. Auf diese Art kann ganze Benutzerkonten übernehmen - und wenn die Zielperson nicht nochmals auf einen Link Deinerseits klickt, bekommst Du immer noch dessen ursprüngliche E-Mail-Adresse 'raus. Automatisiert bedeutet das: Viele E-Mail-Adressen. E-Mail-Adressen von Jugendlichen im Alter von 10-20. Das ist eine viel gefragte Zielgruppe. Eine Zielgruppe, für die sich der Kauf dieser Adressen lohnt.

Die Sicherheit Deiner Daten? Spätestens jetzt sollte diese Lüge widerlegt sein.

* (1) Diese Art von Sicherheitslücke nennt sich übrigens Cross Site Request Forgery. Bis vor kurzem wies auch Wer-kennt-wen.de diese Lücke auf. Dort wurde die Lücke aber bereits nach 9 Stunden behoben.

Nachwort vom 21. Oktober 2009

Dass dieser kurze Bericht ein solches Presseecho erzeugt, hätten wir nie erwartet. Leider wurden jedoch einige Dinge verdreht, die wir hier klarstellen möchten.

Gerücht 1: *„Der Informant von Netzpolitik.org hat millionenfach Daten weitergegeben“*

Es ist wohl ein dummer Zufall, dass zur Entstehungszeit dieses Berichtes ein 20-jähriger Mann aus Erlangen Daten aus MeinVZ, StudiVZ und SchülerVZ gesammelt und auch weitergegeben hat. Zu diesem haben wir allerdings keinerlei Verbindung. Unsere Absicht bestand ausschließlich darin, auf die Problematik aufmerksam zu machen, da SchülerVZ auf unsere Hinweise hin nicht gehandelt hat. Wir hoffen, dass Taten, die denen des 20-jährigen Erlangers ähnlich kommen in Zukunft verhindert werden können.

Gerücht 2: *Ein Datenleck hat nie bestanden und alle Sicherheitsvorkehrungen haben gegriffen*

Hätte kein Datenleck bestanden, wäre es auch nicht möglich gewesen mit nur einem PC, einem SchülerVZ-Account und so wenig Zeit eine so große Menge an Daten auszulesen. Das alle existierenden Sicherheitsvorkehrungen gegriffen haben stimmt zwar, was aber daran lag, dass es gar keine gab. Der Captchaschutz schaltete sich bis vor einigen Tagen nur beim Aufrufen ganzer Profilseiten ein. Unser Testprogramm las die Daten allerdings aus der Suchfunktion aus, weshalb es nicht nötig war, die Profile selbst aufzurufen. Das dies nicht die einzige Datenschutzlücke ist, haben wir ja im Bericht gezeigt. (siehe Kapitel 1 und 2)

Wir haben SchülerVZ auf die Datenschutzlücken bereits im September hingewiesen. Nun, im Oktober 09 wurden endlich Maßnahmen ergriffen.

Wir danken der Netzpolitik.org Redaktion für die Kooperation und SchülerVZ für Behebung und Neueinführung von Datenschutzvorkehrungen.

Für Kommentare, Anfragen, usw.: svzbericht@yahoo.de