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

Hinweis: Die hier aufgeführten Fakten sind (glücklicherweise) veraltet.

Das SchülerVZ unter der Lupe

SchülerVZ – ein soziales Netzwerk, von vielen Jugendlichen benutzt, die sich nicht allzu so 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.

Und hier liegt auch schon das Problem – was, wenn SchülerVZ von vollkommen inkompetenten Leuten geführt wird? Und wenn von einer solchen Inkompetenz die Rede ist, dass *Sicherheitslücken* entstehen?

Dieser Bericht möchte auf eben diese Punkte eingehen.

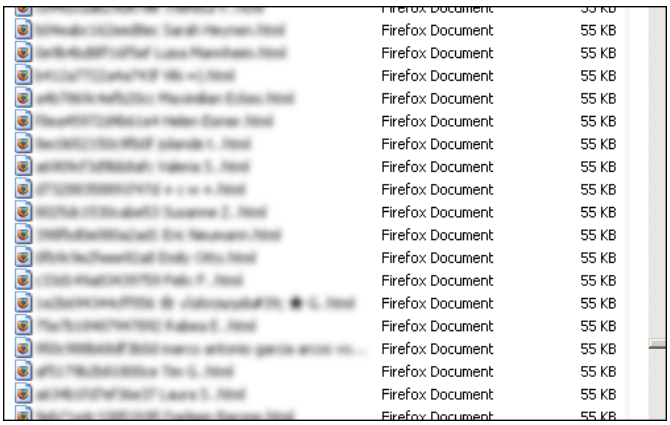
1. Sicherheit der persönlichen Daten
2. Speicherdauer und Beeinflussbarkeit der persönlichen Daten
3. Darf's noch eine Sicherheitslücke sein?
4. Wie SchülerVZ gegen „Freidenker“ vorgeht
5. Nachwort

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.



Ein Ordner voll von "gecrawlten" Daten...

Doch seitdem hat sich doch sicher einiges getan? SchülerVZ wird doch gewiss 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.

... und ein einzelnes Profil...

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 alldem, 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.

Jemand, eventuell wir, hat dies 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: Wir benötigten nur ~ 30 Zeilen Code und 10 Minuten Aufwand.

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.*
>
> 7.3 *Soweit 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, Arno N.*

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 Arno,*
>
> *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 seien, dass die Werte stets aktuell bleiben. Das heißt, mittels eines Programms ist wieder ein automatisiertes Auslesen gefragt, beispielsweise jede halbe Stunde.

Kritisch wird diese 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, deine Login E-Mail Adresse und sogar dein Passwort. Außerdem stellt dieses Sicherheitsproblem auch ein massives Datenleck dar. Über das 'Email-Adresse ändern'-Formular ist es ein leichtes, die E-Mail-Adresse von Nutzern an sein eigenes Postfach zusenden zu lassen. Abgesehen von Profildaten ist es also auch möglich, eigentlich nicht zugängliche Daten, wie die eben E-Mail-Adresse zu sammeln. E-Mail-Adressen von Jugendlichen im Alter von 10-20. Das ist eine viel gefragte Zielgruppe. Eine Zielgruppe, deren gekaufte E-Mail-Adresse sich für Spamverteiler lohnen würde.

Die Sicherheit Deiner Daten? Spätestens jetzt sollte man hier ernsthafte Bedenken haben.

* (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.

* (2) Die Wahl dieser Lücke als Beispiel geschah nicht ohne Grund. Es ist uns ein Fall der Ausnutzung bekannt, bei dem letztendlich die Polizei einen Schüler aus der Schule abgeführte, da dieser angeblich einen Amoklauf auf SchülerVZ angekündigt habe.

4. Wie SchülerVZ gegen „Freidenker“ vorgeht

Wir haben SchülerVZ auf die gesamte Problematik (teilweise sogar telefonisch) aufmerksam gemacht. Uns war die Beseitigung der oben genannten Datenlücken stets wichtig, da wir die Sicherheit unserer Daten und die der anderen Nutzer in Gefahr sahen. Man möchte meinen, SchülerVZ geht hier irgendwie subtil und professionell, freundlich und entgegenkommend vor.

Das können wir leider nicht behaupten, im Gegenteil!

Demonstrativ entwickelten wir ein Programm, welches automatisiert massenhaft Fotos downloadet. Als SchülerVZ Wind von der Sache bekam, bemühten sie sich keineswegs das Problem der vorhandenen Lücke, auf dem unser Programm basierte zu entfernen, sondern schickten ihre Anwälte los, um uns „mundtot“ zu machen. Nachdem wir SchülerVZ also bewiesen hatten, dass die Lücke existiert und sie aufforderten, das und weitere Probleme elementar und langfristig zu lösen, wurde uns folgendes entgegnet:

> *„Und sie glauben, wir sehen uns gezwungen, diese Methoden [das Beheben der Datenlücke] anzuwenden?“*
>
> - Vertreter des SchülerVZ, 09. September '09

Das Schülerverzeichnis kümmert sich also nicht um Probleme durch das Lösen, sondern durch das pure Unterdrücken. Ähnlich dem neuen Gesetz der Netzsperren („Sperren statt Löschen“): „Rumeiern statt Lösen“.

Aus dem restlichen Gesprächsverlauf konnten wir entnehmen, dass SchülerVZ sich nur zum Handeln verpflichtet sieht, wenn sie einen finanziellen Vorteil wittern.

5. Nachwort vom 24. Oktober 2009

Dass die SchülerVZ-Angelegenheit ein solches Presseecho erzeugt, hätten wir nie erwartet. Leider wurden jedoch einige Dinge verdreht, über- oder unterbewertet oder sonstig missverstanden. Wir möchten uns nun bemühen, diese Dinge klarzustellen.

Der Informant von Netzpolitik.org hat millionenfach Daten weitergegeben, so wurde immer wieder berichtet. Es war wohl ein dummer Zufall, dass zur Entstehungszeit unseres Gutachtens und während des Kontaktierens von netzpolitik.org ein 20-jähriger Mann aus Erlangen *auch* Daten aus MeinVZ, StudiVZ und SchülerVZ gesammelt und offensichtlich weitergegeben hat.
Zu unserer Verteidigung müssen wir sagen, dass wir hiervon nichts wussten, keinen Kontakt also zu ihm pflegten.

Unsere Absicht bestand ausschließlich darin, dass SchülerVZ *handelt*. Der SchülerVZ-Support hat es nicht so in sich, das merkt schon jeder, der per E-Mail Fotos gelöscht haben möchte, und dies sogar juristisch begründen kann (→ KunstUrhG). Diese schmerzliche Erfahrung mussten wir auch diesmal machen, wenngleich es hier um wesentlich brisantere Dinge als nur Fotos ging: Das Unternehmen zeigt da wenig Interesse und Beachtung – öffentlicher "Druck" wirkt hier wohl leider besser.
Wir hoffen, dass Taten wie jene des 20-jährigen Erlangers nun in Zukunft verhindert werden können.

Wir wünschten uns von SchülerVZ, dass sie mit technischer Kompetenz die Probleme lösen, und nicht mit Anwälten oder Ähnlichem antworten, wie es schon in der Vergangenheit hier und da der Fall war. Lieber „Löschen statt Sperren“, oder? Das lässt sich ganz gut auf diese Situation parallelisieren: Lieber „Lösen statt Verbieten“.

Dass *kein* Datenleck bestanden habe, wurde oftmals von SchülerVZ kommuniziert. Hier ist es Definitionssache, was man als Datenleck bezeichnet – wir finden, ein Datenleck ist eine solche Lücke, bei der keine Schutzmechanismen greifen, um große Mengen an Informationen einfach „abzusaugen“, sei dies nun eine kritische oder nur fahrlässige Sicherheitslücke.
Hätte also kein solches „Datenleck“ – nach unser Definition – bestanden, wäre es wohl nicht möglich gewesen, mit nur einem PC so viele Informationen auszulesen. Das Leck bestand darin, dass ein Captcha-Schutz zum Verhindern sogenannten „Crawlings“ schaltete – beziehungsweise nur bei Profilseiten. Die Suchfunktion hingegen lies sich locker-flockig benutzen, immer und immer wieder. Und auch diese Suchfunktion, die sogenannte Super-Suche, lässt schon einige Details zu: Name, Profilbild, Schule, Klasse, Wunschschule, Alter, Geschlecht, Einschulungsjahr, Schulstatus, Beziehungsstatus, politische Richtung.
Dass auch schon diese Informationen ausreichen, um beispielsweise dem späteren Arbeitgeber eine kleine Meinung über den Bewerber noch vor dem ersten Gespräch zu liefern, steht wohl außer Frage. Profilbild und politische Richtung sind hier beispielsweise schon recht interessante Daten.

Was uns bei der ganzen Geschichte weniger Gefallen hat, das war das ausschließliche Auge auf diese Datensätze. Das Datenleck war nur ein Teil unserer längerer Beobachtungen von SchülerVZ.
Ein anderer ist beispielsweise die Sache mit den Bildern: Wenn man das eigene Profilbild mit einem Klick auf "[löschen]" vermeintlich löscht, bleibt es weiterhin bestehen, man muss nur den Link hierzu kennen. Das bedeutet, die Bilder bleiben auf den Servern, was

wir höchst beunruhigend finden. Noch viel beunruhigender: Nach der ganzen Geschichte, all den Artikeln in der Presse und allen Berichten in den Medien hat sich daran nichts geändert: Noch immer werden und bleiben Bilder gespeichert. Und das gilt nicht etwa nur für Profilbilder, nein, auch für Fotoalben.
Und das, wo es doch so schön in den Datenschutzerklärungen heißt: „Wenn du etwas löschst, ist es auch weg. Und das komplett!“. Irgendwie widersprüchlich, beinahe heuchlerisch.
Wir stellen uns da als nächstes die naheliegende Frage, was noch alles vom Nutzer gespeichert wird und gespeichert *bleibt*, wenn es erst mal im VZ ist? Bilder sind viel größer als Zeichen, Sätze, Zahlen...

Wir danken an dieser Stelle besonders Herrn Markus Beckedahl von netzpolitik.org. Letztendlich ist es ihm zu verdanken, dass es dieses oben angesprochene große Pressecho gab – denn bis dahin haben wir auch vielen anderen Blogs, Zeitungen oder Magazinen unser Gutachten geschickt, worauf es aber keinerlei Reaktion gab. Als dann plötzlich dieser Artikel auf netzpolitik auftauchte, haben sich plötzlich alle dafür interessiert – auch jene, die wir schon zuvor erfolglos kontaktiert haben.