Gefahren bei Facebook, Youtube, ICQ, Twitter, WhatsApp und YouNow

Gefahren bei Facebook

Oberflächlich bietet Facebook die Möglichkeit sich mit Freunden und Bekannten auszutauschen. Allerdings macht Facebook dies nicht aus sozialen Gründen, sondern will vor allem eines: Geld verdienen. Dafür ist Facebook auf die Daten der Mitglieder angewiesen.

Daten Sammeln:
Facebook archiviert alles, was die Mitglieder schreiben, die hochgeladenen Bilder, Kommentare, Freundschaften, jeden einzelnen „Like" Klick und vieles mehr und verbindet dieses zu einem Benutzerprofil. Viele Webseiten bieten diese sogenannten „Like" Symbole an. Wenn man den dort gelesenen Artikel gut findet, kann man diesen hiermit seinen Freunden mitteilen. Gleichzeitig weiß Facebook aber auch, wo und wann man diesen gelesen hat. Dieses ist vor allem für die Werbewirtschaft interessant. Facebook bietet solchen Firmen die Möglichkeit, personalisierte Werbung zu schalten. Dies bedeutet, dass diese Firmen die Werbung auf die jeweilige Person genau zuschneiden können. Was diese Firmen aber mit den Daten machen, kann der Benutzer nicht mehr kontrollieren.

Offenlegung von persönlichen Daten:
Das Facebook Profil ist darauf angelegt, dass man seine Daten öffentlich preisgibt. Dies öffnet natürlich die Möglichkeit des Missbrauchs durch dritte Personen. Telefonnummer, E-Mail Adressen, und andere Kontaktdaten sind für Kriminelle sehr interessant und auch sehr viel wert. Wenn ein User jetzt postet, dass er für eine gewisse Zeit nicht zuhause ist und er gleichzeitig seine Adressdaten angegeben hat, ist somit bekannt, wann sich z.B. ein Einbruch lohnen könnte. Ebenso können Fotos missbraucht werden, diese können in Bilderdatenbanken landen und von dort aus weiter verkauft und benutzt werden. Einmal im Netz gelandet ist es nahezu unmöglich diese wieder zu entfernen. Das auch Firmen zum Beispiel ihre Bewerber bei Facebook durchleuchten ist nichts Ungewöhnliches mehr. Ein falsches Party- oder Urlaubsfoto kann hier fatale Wirkung zeigen.

Spiele:
Spiele sind eine tolle Sache. Weniger schön ist es, dass die Spielehersteller es ebenfalls auf die Daten der Nutzer abgesehen haben. Nicht nur auf die eigenen, sondern auch auf die der Freunde, die eigentlich gar nichts mit dem Spiel zu tun haben. Wie das funktioniert ist einfach erklärt. In den Nutzungsbedingungen des Spieles steht, dass man dem Hersteller erlaubt das eigene Profil und auch die der Facebookfreunde auszuwerten. Ohne eine Zustimmung dazu ist das Spiel nicht spielbar. Ein weiterer Punkt ist, viele der Titel sind zwar sogenannte „Free 2 Play" Spiele, also in der Grundfunktion umsonst zu spielen, aber so aufgebaut, dass man Geld investieren muss, um mit anderen Spieler/innen mitzuhalten. Das mögen auf den ersten Blick nur geringe Beträge sein. Allerdings summieren sich diese sehr schnell zu stattlichen Summen, die weit über das übliche Taschengeld hinausgehen können.

Auch ohne Mitgliedschaft, Facebook kennt einen:
Facebook bietet die Möglichkeit, das man seine Adressdatenbanken (z.B. aus dem E-Mail Programm) importieren kann. Somit landen auch Kontaktdaten von Leuten bei Facebook, die dort nicht Mitglied sind. Facebook speichert auch diese Daten, angeblich um eine Liste von Leuten zu haben die keine Facebook e-Mails oder Einladungen wollen. Was sonst damit gemacht wird, kann der Betroffene nicht kontrollieren.

Account Missbrauch:
Nicht nur beim Online-Banking besteht die Gefahr, dass ein Fremder die Daten abgreift. Auch bei einem Facebook Account sind unerfahrene Nutzer betroffen. So genannte „Phishing" Mails machen die Runde. Dies sind angeblich „offizielle" Facebook E-Mails, wo der Benutzer aufgefordert wird auf einer Website

seinen Benutzernamen und das Passwort einzugeben. Diese Website ist natürlich nicht die echte Facebook Seite sondern die eines Kriminellen. Auch Schadsoftware kann man sich über einen unbedarften Klick auf einen Link in einem Facebookprofil einfangen. Dies können neben Viren auch Keylogger sein, diese protokollieren jeden Tastendruck und können so ebenfalls Passwörter und Benutzerdaten ausspähen.

Ein neueres Phänomen ist das sogenannte „Clickjacking". Dies funktioniert relativ simpel. In der „Neuigkeiten" Liste taucht ein neues Video, meist mit kuriosem oder schockierendem Vorschaubild. Da viele User sehr neugierig sind klicken sie so eines an. Einige Zeit später fällt dann auf das man dieses Video selbst mit seinen Freunden teilt, obwohl man dieses gar nicht wollte. Wie das passieren konnte ist schnell erklärt. Über dem Video bzw. der ganzen Seite lag ein unsichtbarer „Like Button" dieser lässt sich mit einigen programmiertechnischen Tricks nämlich beliebig vergrößern. Mit einer ähnlichen Methode lassen sich kleine Programme durch die Hintertür einschleusen. Diese spionieren oftmals den eigenen Computer aus.

Auch versuchen immer mehr Betrüger den Leuten sogenannte Apps unterzuschieben. Diese gaukeln vor nützlich zu sein, z.B. neue Smileys und Ähnliches. Diese nützen aber nur den Erstellern, nicht dem Benutzer. Diese posten dann ständig ihre Werbebotschaften auf die Pinnwand, verschicken im Namen des Benutzers private Nachrichten und vieles mehr.

Entfernen und Herausgabe von Daten:
Facebook macht es einem nicht gerade einfach den Account zu löschen, man darf sich 18 Tage nicht einloggen. Allerdings ist dieses sehr schwierig durchzuführen. Facebook schickt einem nicht nur Erinnerungsmails, sondern jegliches versehentliche „Like" klicken oder das kommentieren in einem Blog kann als Aktivität gewertet werden, welche die Löschung widerruft. Ob Facebook die Daten dann wirklich löscht ist zudem eher unwahrscheinlich, denn Personen, die ihre Daten bei Facebook anforderten, fanden dort auch wieder gelöschte Informationen.

Facebook ist nach den Gesetzen der Europäischen Union dazu verpflichtet den Usern ihre Daten auszuhändigen. Facebook kommt diesem auch nach. Dies funktioniert über die Kontoeinstellung unter „Lade eine Kopie deiner Facebook-Daten herunter". Hin und wieder versucht Facebook dies abzulehnen, eine Drohung mit einer Beschwerde bei der irischen Datenschutzzentrale genügt hier. Facebook hat seinen Firmensitz in Irland und ist daher der irischen Gesetzgebung unterworfen. Einige Tage später, Facebook hat bis zu 40 Tage Zeit, erhält man einen Downloadlink mit einer PDF Datei. Achtung, je nach Facebook Aktivität kann diese mehrere hundert Megabyte groß sein und mehrere tausend Seiten enthalten.

Facebook und Recht:
Facebook ist aber kein rechtsfreier Raum, auch hier gilt das deutsche und europäische Recht. Beleidigende Kommentare, Rassismus, Pornographie und Gewaltdarstellung sind auch bei Facebook strafbar und werden auch von den Staatsanwaltschaften verfolgt. Wer hier also z.B. irgendeinen Künstler, den er nicht mag, beleidigt oder Gewaltandrohung gegen unliebsame Personen betreibt, wird sehr schnell Post von der Staatsanwaltschaft bzw. von dem Anwalt dieser Person bekommen.

Auch „Mobbing" bei Facebook kann verfolgt werden. Da Facebook Mitgliedschaften nicht anonym sind kann der Täter sehr schnell ausfindig gemacht werden. Ebenfalls ist das Urheberrecht zu beachten, einfach fremde Texte oder Bilder zu verwenden ist auch bei Facebook nicht zulässig und kann sehr schnell zu teuren Abmahnungen führen.

Auch ein falscher Klick kann fatale Auswirkungen haben. Schnell ist eine Partyeinladung öffentlich gemacht. Statt nur Freunde, melden sich eine große Anzahl an unbekannten Personen an. Dieses Phänomen nennt man mittlerweile „Facebook-Party". Zwar ist rechtlich noch strittig wer eigentlich dafür haftet. Dass so etwas aber unangenehme Folgen haben kann, ist mehrfach belegt.

Facebook ist nicht grundsätzlich dem deutschen Datenschutzgesetz unterworfen, denn Facebook hat seinen Sitz in Irland. Irland hat zwar ein ähnliches Datenschutzgesetz wie Deutschland, aber der Klageweg ist teuer und zeitintensiv. Dazu kommt noch, dass viele Firmen mit denen Facebook zusammenarbeitet in Ländern wie den USA ihren Sitz haben und dort die Datenschutzgesetze viel lascher sind als in der Europäischen Union.

Gefahren bei Youtube

Youtube ist eine sogenannte „Web 2.0“ Plattform. User können hier eigene Videos hochladen und diese so der ganzen Welt oder auch nur ausgewählten Personen zugänglich machen. Dies kann bereits beim Hochladen des Videos eingestellt werden. Selbst große Firmen und Konzerne nutzen mittlerweile diese Videoplattform. Allerdings birgt so eine Plattform diverse Gefahren. Zusätzlich zu den Gefahren bei Facebook gibt es hier einige weitere.

Das Urheberrecht:
Natürlich bietet es sich an das Lieblingsmusikvideo auf den eigenen Account hochzuladen. Nur ist dieses nur erlaubt, wenn man selbst entweder der Urheber ist oder eine Lizenz hat dieses Video zu benutzen. Ansonsten verstößt man gegen das Urheberrecht. Die Youtube Filter erkennen so etwas mittlerweile zwar, aber trotzdem gibt es die Möglichkeit, dass die Urheber und Rechteinhaber den User abmahnen. Dies geschieht meist durch eine Anwaltskanzlei, was sehr schnell zu Kosten von mehreren Tausend Euro führen kann.

Radikales Gedankengut:
Youtube sperrt zwar gerne Musikvideos, um Klagen der Musikindustrie zu vermeiden, ganz anders sieht es aber bei rechtsradikalem Gedankengut aus. Dieses findet man in hoher Anzahl ebenfalls bei Youtube, von Ansprachen, über Propagandafilme bis hin zu rechtsradikaler Musik ist hier alles vertreten. Wer den Bandnamen einer beliebigen Naziband bei Youtube sucht, wird schnell fündig. Diese werden teilweise von den Bands selbst eingestellt, hier greifen die Urheberrechtsfilter nicht. Solche Videos fallen zwar nach deutschem Recht unter den Rechtsbegriff der Volksverhetzung, aber diese werden von ausländischen Accounts hochgeladen. Zum Beispiel in den USA wird rechtes Gedankengut als „Freie Meinungsäußerung“ bewertet.

Auch religiöse Vereinigungen und Sekten machen sich die größte Videoplattform zu nutze. Nicht nur Propaganda von Sekten findet sich hier, sondern auch Hassvideos gegen andere Religionen. Nach deutschem Recht ist dieses zwar strafbar, diese Videos werden ebenso oftmals von nicht deutschen Accounts und Mitgliedern hochgeladen. Aktuell führte solch ein Video zu Gewaltausbrüchen in islamisch geprägten Staaten.

Beleidigung, Gewalt:
Youtube besitzt keine Altersverifikation, jeder User kann sich jedes Video ansehen. Dies kann dazu führen, dass Kinder und Jugendliche für sie nicht geeignetes Material zu Gesicht bekommen. Youtube geht zwar gegen gewalttätige Videos vor, aber auch nur im Rahmen ihrer Nutzungsbedingungen. So finden sich Filmtrailer oder Ausschnitte zu Spielen, die in Deutschland indiziert oder beschlagnahmt sind, dort genauso wieder wie Gewalt gegen Tiere oder Menschen. Youtube wendet nämlich gerne das US Recht an, dieses ist bei Gewalt viel toleranter als das deutsche Recht. Zudem reagiert Youtube meist erst auf verstärkte Usermeldungen.

Videos entfernen lassen:
Ein unangemessenes Video entfernen zu lassen ist hingegen nicht so einfach. Erst einmal benötigt man hierfür einen Youtube Account. Erst dann kann man unangemessene Videos direkt melden. Dies geschieht indem man auf das „Als unangemessen Melden“ Symbol klickt, welches als eine kleine Fahne dargestellt wird. Youtube will dann einen Grund dafür haben, je ausführlicher man diesen angibt, desto größer ist die

Chance dass Youtube reagiert. Sollte man so nicht zu seinem Recht kommen, so muss man Youtube direkt über die Kontaktdetails kontaktieren, hier ist die „Abuse“ Abteilung der richtige Ansprechpartner. Sollte Youtube hier auch nicht reagieren, hilft nur der Weg über einen Anwalt.

Gefahren bei ICQ

ICQ gehört zu den „Live Messengern“, dies bedeutet dass Nachrichten die man seiner/m Gesprächspartner/in schickt, diese sofort dort ankommen und nicht etwa zeitversetzt wie bei E-Mails. Hier gibt es ebenfalls einige Besonderheiten.

Schadsoftware:
Die Benutzung von ICQ birgt die Gefahr sich Schadsoftware einzufangen, dies erfolgt nach dem gleichen Prinzip wie bei Facebook, der User wird aufgefordert einen Link anzuklicken der auf die Infizierte Website führt.

Anbahnen von Kontakten:
Ebenfalls könnten Sexualstraftäter mit diesen Daten weitere Informationen über ihr potentielles Opfer erhalten. Wenn man seine ICQ Nummer auf mehreren Internetseiten angegeben hat braucht man diese nur zu googlen, um mehr über den/die Benutzer/in zu erfahren.

Gefahren bei Twitter

Twitter ist ein Kurznachrichtendienst. Hier lassen sich ganz kurze Nachrichten unterbringen, mit maximal 140 Zeichen. Die Palette reicht hier von Dingen die man gerade tut vor hat zu machen bis hin zu kurzen Links. Andere Nutzer/innen können anderen „Followen“. Das bedeutet, dass man die sogenannten „Tweets“ dieser Personen automatisch auf seinen Account bekommt. Zudem bietet Twitter einige speziellere Gefahren:

Gefälschte Identitäten:
Bei Twitter ist es kein Problem, dass sich Leute als andere Person ausgeben. So kann man sich nicht sicher sein, dass der Musiker, dem man folgt, auch wirklich dieser ist und nicht jemand anderes. Bedingt dadurch ist es durchaus möglich, dass jemand falsche Gerüchte über bestimmte Personen in die Welt setzt. Dies kann durchaus zur Rufschädigung durch Konkurrenten benutzt werden.

Spam:
Vor unerwünschter Werbung ist man auch bei Twitter nicht verschont, so kann es durchaus sein das Freundschaftsanfragen von Werberobotern kommen. Diese preisen in ihrem Profil irgendein Produkt an. Sollte man diese Freundschaftsanfrage annehmen, taucht dieses Profil in der Liste der Freunde, der sogenannten Follower auf. Man spekuliert dann darauf, dass andere Freunde sich dieses Werbeprofil anschauen.

Short-URLs:
Da der Platz in den Twitter Nachrichten oft nicht für Links ausreicht werden diese per „Short URL“ verkürzt. Diese Dienste verpacken lange Links in kurze Versionen, die dann über ihre Website aus aufgerufen werden. Das Problem dabei ist, dass man nicht mehr erkennen kann, was sich hinter dieser URL verbirgt. Diese ist nur noch eine Zahlen und Buchstabenansammlung. So kann es passieren dass man auf einer schädlichen Website landet, die dann Schadsoftware installiert. Ebenso besteht die Gefahr, dass man auf pornographischen Internetseiten landet.

Drittanbieter:
Twitter bietet die Möglichkeit das Drittanbieter ihren Dienst nutzen, z.B. um Grafiken hochzuladen und diese mit einem „Short-URL“ auf dem Twitteraccount zu posten. Allerdings wollen einige dieser Dienste

den Benutzernamen und das Passwort haben, sollte hinter dieser Seite ein Krimineller stecken, ist der Account in großer Gefahr zweckentfremdet zu werden.

Gefahren bei WhatsApp

WhatsApp ist eine für Smartphones programmierte Messenger-Anwendung. Hierbei wird es dem Anwender ermöglicht, anderen WhatsApp-Nutzern über das Internet Textnachrichten sowie Bilder, Videos und Tondateien zu senden. Allerdings birgt die Benutzung einige Gefahren und Risiken.

Kritische Aspekte an WhatsApp:
WhatsApp gehört zu der Firma Facebook, weshalb für WhatsApp sehr ähnliche Allgemeine Geschäftsbedingungen gelten. So gilt auch hier, dass der Benutzer das Recht am eigenen Bild und am eigenen Text abtritt. Dies bedeutet, dass sobald man eine Nachricht verschickt , diese von WhatsApp, ohne Benachrichtigung darüber, verwendet und verkauft werden darf, sodass zum Beispiel private Bilder bei Werbeagenturen landen können.
Des Weiteren ist WhatsApp unsicher programmiert, es können zum einen also Mitteilungen leicht abgefangen und mitgelesen werden , zum anderen können über diese App unerwünschte Zugriffe auf das Smartphone getätigt werden. Über WhatsApp besteht somit eine Möglichkeit das Smartphone als Abhörgerät oder Ortungsgerät zu benutzen.

Sichere Alternativen zu WhatsApp
Recht sicherere Alternativen zu WhatsApp sind „Telegram“ „Plus Messanger“, „Signal – Sicherer Messanger“, „Viber“ „LIME“ „Kakao Talk“, „TextSecure“, und „Threema“.
Über diese Anwendungen ist es schwerer von außen auf Smartphone-Funktionen zuzugreifen. Zudem verzichtet der Nutzer bei diesen Angeboten nicht auf sein Recht am eigenen Bild/Text. Ebenfalls werden bei diesen Messengern Verschlüsselungen benutzt, was den Zugriff von Dritten auf gesendete Nachrichten erheblich erschwert.

Gefahren bei YouNow

YouNow – Eine Streamingplattform mit Potential und Gefahren

2011 in den USA gegründet, ist die Internetplattform YouNow mittlerweile auch in Deutschland populär geworden. YouNow bietet den Nutzern die Möglichkeit mit einfachen Mitteln wie Webcam oder Smartphone einen Video-Livestream zu starten, der für alle anderen Nutzer der Plattform zugänglich ist. Außerdem bietet es die Möglichkeiten während des Livestreams mit den Erstellern der Streams (den sogenannten Host's) zu chatten und Bewertungen zu vergeben. Jeder der einen Account bei YouNow eingerichtet hat, dieser wird benötigt um YouNow zu nutzen, hat ein für jeden anderen Nutzer zugängliches Profil, auf dem u.a. eine Zahl(Stufe) vermerkt ist. Diese Zahl erhöht sich, wenn andere Nutzer Streams dieses Accounts positiv bewertet haben. Desweiteren gibt es You-Coins, eine Art Punktzahl, die man erhält, wenn man mit anderen auf der Plattform chattet, oder Streams positiv bewertet.

Diese Art Plattform bietet Möglichkeiten, die sehr positiv sind. So können hier zum Beispiel noch nicht sehr bekannte Musiker mit einfachen Methoden ein Konzert live übertragen, oder sich durch eine Live-performance in ihrer Bekanntheit steigern und das sogar international. Generell ist eine solche Plattform ideal für Künstler, die sich hier mit sehr wenig Kosten einer breiten Masse zur Verfügung stellen und so ihre Bekanntheit steigern können.

Das Problem und die Gefahr an YouNow ist die häufige Fehlnutzung der Plattform von Kindern und Jugendlichen. Denn viele jener starten einen Livestream direkt aus dem Kinderzimmer, lassen unbekannte Menschen an ihrem Leben teilhaben, nur um im Bekanntheitsranking auf YouNow aufzusteigen.

Für positive Bewertungen ihrer Streams machen Kinder und Jugendliche auch viele Dinge, die sie besser nicht machen sollten. So landen Daten wie Telefonnummer und Wohnort schnell im Internet, es werden Szenen gestreamt, die auf sie oder Mitmenschen negativ zurückfallen, oder sie gehen auf sexuelle Belästigung ein. Letzteres zieht auch sehr viele Pädophile auf die Plattform, die diese gezielt nach Streams von Kindern und Jugendlichen durchsuchen

Die Firma YouNow selbst äußert sich hierzu und sagt ausdrücklich, dass dies nicht der Zweck der Plattform sei. Als Reaktion hat YouNow eine Selbstbeschränkung eingeführt, sodass Nutzer erst ab 13 Jahren sich anmelden dürfen. Diese Selbstbeschränkung bringt allerdings nicht viel, da sie zum einen leicht zu umgehen ist, zum anderen auch über 13 Jahre alte Personen häufig zu viele Informationen über sich preisgeben und Streams direkt aus dem Zimmer hosten. Auch die Moderatoren, die gezielt YouNow nach Streams Minderjähriger durchsuchen und unangemessene Streams sperren sollen, sind viel zu wenige, sodass die Überwachung kaum etwas bringt. Und die Sperrmöglichkeit, die ein jeder Nutzer selber hat um einen solchen Stream zu verhindern wird selten genutzt.

Informationen und Beratung zu diesem Thema finden sie bei:

Siegfried Wolff (Abteilung Jugend und Familie des Kreis Kleve)
Tel.: 02821/85454
E-Mail: siegfried.wollf@kreis-kleve.de

Fassung vom 24.01.2017