HESSISCHES MINISTERIUM
DES INNERN UND FÜR SPORT

HESSEN

SOZIALE NETZ-WERKE

Nutzen und Risiken im Verhältnis zum Dienstbetreiber

Privatsphärenschutz zwischen Nutzern

Nutzer als Ziel professioneller Angreifer

Einflüsse auf Unternehmenssicherheit

Die Dienstbetreiber: Segen und Risiko zugleich

Viele Nutzer **übersehen**, dass sie mit dem Hochladen von Daten dem Dienstbetreiber Facebook umfangreiche, teilweise unwiderrufliche **Nutzungsrechte** für vielfältige **Anwendungszwecke** einräumen. Dieses Problem findet sich auch bei vielen anderen Diensten.

Im Jahr **2009** eröffnete die US-Handelsbehörde (Federal Trade Comission – FTC) **gegen Facebook ein Verfahren** wegen „möglicher unfairer Verhaltensweisen" gegenüber seinen Nutzern. Im Raum standen beispeilsweise Vorwürfe zu **irreführenden** Privatsphäre-Einstellungen, unfairen Änderungen dieser Funktionen, und Veröffentlichung von **Nutzerfotos** und -videos. 2011 schloß die FTC das Verfahren mit einem Vergleich gegen Auflagen ab.

Betreiber sozialer Netzwerk bieten umfangreiche Datenverarbeitungsdienste gebührenfrei an. Um diese Dienste finanzieren zu können versuchen die Betreiber aber gleichzeitig die Daten ihrer Nutzer gewinnbringend in Dienstleistungen für ihre Geschäftskunden einzusetzen, z. B. für gezielte Werbeschaltungen oder Markt- und Meinungsforschung. Die Betreiber präsentieren ihren Nutzern zudem häufig neue Informationsverknüpfungen und -sammlungen, um das Interesse der Nutzer an dem Dienst zu stärken, z. B. automatische Gesichtserkennung in Fotos und Funktionen zur Geolokalisierung. Wenngleich Nutzer eine gebührenfreie Dienstbereitstellung erwarten, bestärkt die Nutzung persönlicher Daten durch den Dienstbetreiber den Eindruck, dass dieser Privatsphärenbedürfnisse der Nutzer missachtet. Dieses Spannungsfeld lässt sich schwer auflösen. Nutzer sollten jedoch prüfen, ob sie optionale, problematische Funktionen deaktivieren können.

WIR RATEN IHNEN

- Achten Sie darauf, dass Sie nicht versehentlich Daten aus Adressbüchern und anderen E-Mail-Konten zum sozialen Netzwerk übermitteln.
- Prüfen Sie angebotene Konfigurationsmöglichkeiten für personalisierte Werbung.
- Verbieten Sie Drittanbieteranwendungen Ihrer Kontakte auf Ihre Daten zuzugreifen.

Privatsphärenschutz zwischen Nutzern

Herabwürdigende öffentlich sichtbare **Äußerungen** über den Arbeitgeber in sozialen Netzwerk können **ungewollte Folgen** haben: So verlor ein Mitarbeiter einer Basketball Mannschaft in Pittsburgh seinen Job, nachdem er sich auf Facebook öffentlich negativ über die Leistungen der Spieler geäußert hatte.

Durch **fehlerhafte Privatsphäreeinstellungen** bei Facebook wurde aus einer Einladung zu einer privaten Geburtstagsfeier einer Jugendlichen aus Hamburg **ungewollt** eine **öffentliche** Veranstaltung. Mehr als tausend **Partygäste zogen** zum Haus der Eltern des Mädchens; welches von einem Aufgebot an Polizisten vor Randalierern geschützt werden musste.

Soziale Netzwerke erweitern die Interaktionsmöglichkeiten zwischen Menschen um neue Formen, die unabhängig von räumlichen und zeitlichen Einschränkungen sind. Insbesondere die Möglichkeit mit entfernteren Bekannten (sog. weak ties) in Verbindung zu stehen, als auch das unmittelbare Teilen von Informationen mit engeren Freunden machen den Reiz dieser Dienste aus. Trotz dieser Vorteile haben Nutzer auch negative Erlebnisse; so werden gelegentlich Informationen versehentlich und ungewollt mit zu vielen Personen geteilt, werden durch Verknüpfungen von Informationen in den Diensten, z. B. Fotos und Markierungen von Gesichtern, ungewollt Informationen offengelegt, oder Nutzer werden Opfer von Online-Schikanierungen. Umgangsformen für soziale Netzwerke müssen sich vielfach erst zwischen den Nutzern entwickeln.

WIR RATEN IHNEN

- Legen Sie mit ihren Privatsphären-Einstellungen fest wer persönliche Informationen zu Ihrer Person sehen darf. Konfigurieren Sie dabei Ihr Profil lieber restriktiv.
- Überlegen Sie sich genau, wen Sie als Kontakt hinzufügen möchten. Wenn Sie die Arbeit nicht scheuen, können Sie Ihre Kontakte auch gruppieren, um bestimmten Personenkreisen bewusst Informationen vorzuenthalten.
- Prüfen Sie besonders kritisch Funktionen, die Ihren Freunden erlauben, Informationen zu Ihrer Person einzugeben, z. B. durch das Markieren Ihres Gesichtes in Fotos, oder durch Kommentieren von Einträgen auf Ihrer Nachrichtenseite.
- Vergewissern Sie sich bevor Sie Bilder hochladen, Personen in Bildern markieren, oder Nachrichten auf Pinnwänden hinterlassen, dass Sie andere Personen nicht verletzen oder beleidigen.

Professionelle Angreifer und sonstige Risiken

Mit seiner Software **Firesheep** demonstrierte der Softwareentwickler Eric Butler, wie leicht sich Datenverbindungen mit sozialen Netzwerken in ungeschützten **WLANs** kapern lassen. Sein Rechner, auf dem er das Programm Firesheep installierte, schnitt den Netzwerkverkehr mit und entwendete die **Sitzungscookies** von anderen Nutzern, die im gleichen WLAN Facebook und Co. nutzten. In einem von Butler weiterentwickeltem Internetbrowser reichten **wenige Mausklicks**, um als ein anderer Nutzer aus dem WLAN bei Facebook eingeloggt zu sein. Butler konnte so testweise fremde **Nachrichten lesen** und mit „fremden Freunden" interagieren.

2012 starteten die **Schufa** und das Hasso-Plattner-Institut (HPI) ein gemeinsames **Forschungsprojekt** um u. a. Daten aus sozialen Netzwerken zur **Bonitätsprüfung** zu nutzen. Nach heftigen Protesten von **Datenschützern** kündigte das HPI den Forschungsvertrag und stellte das Projekt ein. Es gibt aber auch andere Ideen von veröffentlichten Nutzerdaten zu profitieren: In den USA setzen besispielsweise **Versicherungsfirmen** Daten der Nutzer als **Beweismittel** in Gerichtsprozessen ein.

In und um soziale Netzwerke tummeln sich Personen und Gruppen, welche den Nutzern schaden zufügen wollen, indem sie sich beispielweise Zugang zu vertraulichen, privaten Daten verschaffen, Spam-Nachrichten versenden, oder Viren und Würmer verbreiten. Solche Angreifer können einerseits selbst in den Plattformen als Nutzer aktiv sein, andererseits aber auch klassische Angriffe wie z. B. Abhören von Netzwerkverbindungen mit Spezialisierung auf soziale Netzwerke durchführen.

WIR RATEN IHNEN

- Achten Sie auf Verschlüsselung der Verbindung zum Dienstanbieter (HTTPS), insbesondere in öffentlichen WLAN-Netzwerken, Internetcafés oder Hotels.
- Aktualisieren Sie regelmäßig Ihren Webbrowser und andere Software auf Ihrem Rechner.
- Wählen Sie sichere, ausreichend lange Passwörter für Ihren Dienstzugang.

Unternehmenssicherheit

Bei einem **Angriff** auf die Sicherheitsfirma RSA im Jahre 2011 nutzten Hacker Daten aus sozialen Netzwerken für sogenannte **Spear Phishing-Attacken**, also gezielte Angriffe mit **gefälschten E-Mails** auf ausgewählte Mitarbeiter des Unternehmens. Ihnen gelang es damit, **Schadsoftware** in die Firma **einzuschleusen** und anschließend **hochvertrauliche** Unternehmensinformationen zu stehlen.

2010 konnte der Sicherheitsberater **Thomas Ryan** mittels gefälschter Facebook- und **LinkedIn-Profile** einer fiktiven Cybersecurity-Spezialistin annähernd **300 »virtuelle« Kontakte** zu Pentagon-Mitarbeitern aufbauen. Einige dieser Mitarbeiter vertrauten ihm **sensible** persönliche und dienstliche **Informationen** an. Das **Pentagon** musste nach Bekanntwerden einräumen, dass interne **Richtlinien** unzureichend waren, um den Informationsabfluss zu **verhindern**.

Unternehmen begreifen soziale Netzwerke als Chance zur Gewinnung neuer Kunden und Mitarbeiter. Gleichzeitig können Mitarbeiter, welche soziale Netzwerke nutzen, ein großer Risikofaktor für die Unternehmensicherheit sein, wenn sie vertrauliche Informationen – meist ungewollt – preisgeben oder durch ungeschickte Aktionen den Ruf des Unternehmens schädigen. Die unbemerkte Vermischung von Privatem und Dienstlichem spielt dabei eine besondere Rolle. So erkennen Mitarbeiter manchmal nicht, dass sie dienstlich agieren, z. B. wenn sie sich mit anderen Mitarbeitern des Unternehmens in einer eigenen Mitarbeitergruppe in einem sozialen Netzwerk zu dienstnahen Themen austauschen.

WIR RATEN IHNEN

- Bieten Sie Ihren Mitarbeitern Ansprechpartner für alle Fragen im Umgang mit sozialen Netzwerken und anderen Social Media-Diensten.
- Entwickeln Sie Social Media-Richtlinien, die Ihren Mitarbeitern erläutern, was das Unternehmen von ihnen beim Umgang mit den Diensten erwartet. Unterstützen Sie Ihre Mitarbeiter, richtig mit sozialen Netzwerken umzugehen, anstatt willkürlich Verbote auszusprechen.
- Berücksichtigen Sie im Risikomanagement mögliche Schadensfälle durch soziale Netzwerke.

HESSEN

Hessisches Ministerium des Innern und für Sport

Viktor Jurk
Leiter der Abteilung eGovernment und Verwaltungsinformatik
Friedrich-Ebert-Allee 12
65185 Wiesbaden
Telefon +49 (0611) 353 1900
www.hmdis.hessen.de

KONTAKT

Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75,
64295 Darmstadt
Telefon 06151 869-213
Telefax 06151 869-224
E-Mail info@sit.fraunhofer.de
URL www.sit.fraunhofer.de

Download der Studie:
www.sit.fraunhofer.de/SozialeNetzwerke2013