DEUTSCHER PRÄVENTIONSTAG

„Soziale Netzwerke - mehr als eine Kommunikationsplattform. Gefahren bei Facebook, Twitter und Co.“

von

Andrew Noack

Dokument aus der Internetdokumentation
des Deutschen Präventionstages www.praeventionstag.de
Herausgegeben von Hans-Jürgen Kerner und Erich Marks im Auftrag der
Deutschen Stiftung für Verbrechensverhütung und Straffälligenhilfe (DVS)

Zur Zitation:
Andrew Noack: Soziale Netzwerke - mehr als eine Kommunikationsplattform. Gefahren bei Facebook, Twitter und Co., in: Kerner, Hans-Jürgen u. Marks, Erich (Hrsg.), Internetdokumentation des Deutschen Präventionstages. Hannover 2011, www.praeventionstag.de/Dokumentation.cms/1691

Vortrags zum 16. Präventionstag am 30.und 31.Mai 2011 in Oldenburg:
Soziale Netzwerke im Internet - mehr als eine Kommunikationsplattform
Gefahren bei Facebook, Twitter und Co.

Der Vortrag beschäftigt sich einführend mit der der Nutzung und dem Nutzen von sozialen Netzwerken im Internet. Erst wenn man versteht welche Bedürfnisse hier erfüllt werden sollen und welche Geschäftsmodelle hinter einigen bekannten sozialen Netzwerken liegen, werden die Risiken transparent. Neben den technischen Gefahren, die im Vortrag aufgezeigt werden, gegen die man technische Maßnahmen treffen kann, wird erläutert welche Möglichkeiten des „Social Engineering" genutzt werden können. Vorfälle aus der Praxis machen die oft als abstrakt eingeschätzten Gefahren anschaulich. Der Vortrag gibt Anregungen wie sich jeder einzelne den Risiken bewusst werden kann und welche Maßnahmen zur Minimierung der Risiken ergriffen werden sollten. Der Referent versucht die oft technisch geprägte Diskussion mit Beispielen plastisch darzustellen. Der Zuhörer wird in die Welt der neuen Medien, mit Bezug auf das echte Leben, mitgenommen.

1.
Vorletzte Woche gab es die Themenwoche in der ARD, der mobile Mensch.
Genauso wie Busse, Bahnen, Automobile oder Zweiräder genutzt werden, genauso selbstverständlich werden Elektronische Medien täglich von vielen Menschen in Deutschland so verwendet.

Das Telefon ist wohl das erste elektronische Kommunikationsmedium, das bewusst von Kindern verwendet wird.
Fernsehen ist das erste Informations-Medium was ein Kind eigenständig nutzt und bedienen kann. Dieses „klassische" elektronische Informations-Medium verweist aber immer häufiger auf weitere Informationen im Internet. Damit ist die Brücke zum PC geschlagen.

Bevor aber das Kind oder der Jugendliche den PC eigeninitiativ nutzt, werden schon MP3-Player und Spielkonsolen verwendet. Z.B. sind iPod und Nintendo DS bereits WLAN fähig. Somit beginnt der Besuch des Internets schon über diese Geräte sehr schnell und sehr leicht.

Danach ist die Nutzung von sozialen Netzwerken im Internet nur noch ein kleiner Schritt.

2.

Was versteht man unter einem sozialen Netzwerk im Internet?

Soziale Netzwerke im Sinne der Informatik sind Web-basierende Dienste und Netzgemeinschaften auch social network services genannt.

Typische Funktionen dieser Dienste umfasst das Eintragen und Verwalten von Persönliche Profilen, pflegen von Kontaktliste oder Adressbuch, Austausch von Nachrichten über Postings (plakatierte Meldungen) oder oder Blogs. Und selbstverständlich auch Suchfunktionen, die auf umfassende Datenbestände zugreifen können.

Soziale Netzwerke finanzieren sich durch Mitgliedsbeiträge sowie verschiedene Formen von Werbung und Sponsoring. Da die Zahlungsbereitschaft der Nutzer zumeist gering ist, setzen die meisten Betreiber auf Anzeigenerlöse.

Da die Dienstebetreiber den vollen Zugriff auf jeden Einzelnen dieser Netzgemeinschaft hat, wissen sie also, welches Mitglied mit welchen anderen Mitgliedern wie in Relation steht. Somit verfügen sie über eine kommerziell interessante Informationsbasis, etwa für zielgruppengerichtete Werbung. Aus der Nutzung dieser Erkenntnisse machen die Anbieter auch kein Hehl.

Viele verwenden soziale Medien nicht nur privat sondern auch beruflich:

- um Geschäftspartner kontaktieren
- Produkte zu vermarkten
- um selbst Werbung zu schalten
- um neue Kontakte schließen

In den letzten Jahren konnte ein massives Wachstum im Bereich sozialer Medien beobachtet werden – eine in 2009 von Cisco initiierte Studie kam zu dem Ergebnis, dass fast 2% aller Online-Klicks auf Social-Networking-Websites getätigt werden, zwei Drittel hiervon auf Facebook.

3.

Das Internet ist weltumspannend wie die Ozeane.

Häufig glauben wir, die See ist sehr ruhig und die Gefahren betreffen ja wohl nur die Anderen.

Wir selbst bewegen uns machmal im Netz, als ob wir unverwundbar wären.

4.
Im April wurden in Bielefeld die diesjährigen "Preisträger" gekürt: In der Kategorie Kommunikation bekamen das soziale Netzwerk Facebook und die Apple GmbH in München den Negativpreis.
Facebook verdiene mit systematischen Datenschutzverstößen Milliarden, hieß es in der Begründung.
(dpa/tc)
Auch der **Bundesdatenschutzbeauftragte Peter Schaar sagte anläßlich des** fünften Europäischen Datenschutztag am 28. Januar 2011: „Der Datenschutz muss europaweit gestärkt werden. Die Debatte über den Datenschutz im Internet zeigt, dass nationale Regelungen allein nicht ausreichen.
So vertreten globale Internetunternehmen wie Google und Facebook die Auffassung, nicht an das europäische Recht oder die Datenschutzgesetze der Mitgliedsstaaten gebunden zu sein.
Die anstehenden Änderungen des europäischen Rechtsrahmens müssen gewährleisten, dass sich alle in Europa aktiven Unternehmen an die gleichen Standards zu halten haben.“
Insbesondere ein funktionierender Schutz vor Profilbildung sei ein wichtiges Element.

5. Machen Sie sich mit den Regeln vertraut

In einer von Sophos durchgefürhrten Umfrage wurde Facebook als das Sozaile Netzwerk mit dem höchsten Sicherheitsrisiko benannt.
Eine Sophos Umfrage im Juni 2010 deckte auf, dass 95 % aller Befragten sich von Facebook ein schärferes Vorgehen gegen so genannte Likejacking-Attacken wünschten (Clickjacking mittels Klicken des „Gefällt mir“-Buttons auf Facebook).

Was macht Soziale Netzwerke im Internet so erfolgreich?
Sie bieten eine Plattform der Kommunikation über soziale- und Ländergrenzen hinweg.

Die politischen Ereignisse der letzen Monate haben uns allen gezeigt, welche Möglichkeiten sich durch soziale Netzwerke eröffnen.
Früher hat man sich als Schüler, zur Planung weiterer Freitzeitaktivitäten nach der Schule, persönlich verabredet für, später hieß es, lass uns telefonieren, heute verabredet man sich über das soziale Netzwerk im Internet.

Smartphones und PC sind heute fester Bestandteil der familiären Infrastruktur. Der Nutzen ist vielfach offensichtlich, Vorteile werden schnell verinnerlicht, aber die objektive Einschätzung von Risiken oder gar Gefahren, werden nur unzureichend beleuchtet und berücksichtigt.
Auf was sollten wir als Nutzer achten:

6.

So weißt die Facebook – Datenschutzrichtiline vom 22.12.2010 hin:

Geltungsbereich. Diese Datenschutzrichtlinien gelten für alle Aspekte von Facebook. Sie haben jedoch keine Gültigkeit für Körperschaften, die nicht Eigentum von Facebook sind oder von Facebook kontrolliert werden, wie Anwendungen und Webseiten, welche die Plattform verwenden.

Transaktionsdaten. Gegebenenfalls speichern wir die Daten der von dir auf Facebook getätigten Transaktionen oder Zahlungen.

Wenn du nicht möchtest, dass wir die Kontonummer deiner Zahlungsquelle speichern, kannst du diese auf deiner Zahlungsseite entfernen.

Zugriff auf Informationen von Zugangsgeräten und Browsern. Wenn du über einen Computer, ein Handy oder ein anderes Gerät auf Facebook zugreifst, sammeln wir u. U. von diesem Gerät Informationen über deinen Browsertyp, deinen Standort, deine IP-Adresse und die Seiten, die du besuchst.

Informationen von anderen Webseiten. Es ist uns gestattet, zusammen mit Werbepartnern und anderen Webseiten Programme einzurichten, mit denen diese uns Informationen mitteilen:

- So bitten wir beispielsweise u. U. Werber, uns mitzuteilen, wie unsere Nutzer auf die Werbeanzeigen reagiert haben, die sie bei uns gesehen haben (und zu Vergleichszwecken auch, welche Vorgänge andere Nutzer, welche die Werbeanzeigen nicht gesehen haben, auf der Webseite des Werbers durchgeführt haben). Durch die Weitergabe dieser Daten, gemeinhin als „Besuchsaktionsauswertung“ oder „Conversion Tracking“ bezeichnet, können wir unsere Werbewirksamkeit besser einschätzen und die Qualität der Werbeanzeigen verbessern, die du siehst.
- Wir erhalten dabei ggf. Informationen darüber, ob du bestimmte Werbeanzeigen auf anderen Webseiten gesehen und mit diesen interagiert hast, und können so die Wirksamkeit solcher Werbeanzeigen ermitteln.

Sollten wir in einem solchen Fall Daten erhalten, über die wir noch nicht verfügen, werden wir diese innerhalb von 180 Tagen „anonymisieren“, sie also nicht mehr mit einem bestimmten Nutzer in Verbindung bringen. Im Rahmen dieser Programme nutzen wir die Informationen ausschließlich so wie im untenstehenden Abschnitt „Verwendung deiner Informationen durch uns“ beschrieben.

Damit wir auf rechtlich begründete Aufforderungen reagieren und Schäden verhindern können. Aufgrund von Vorladungen, Gerichtsentscheidungen oder anderen Anfragen (einschließlich Straf- und Zivilrechtsangelegenheiten) dürfen wir Informationen offenlegen, wenn wir in gutem Glauben der Meinung sind, dass ihre Offenlegung gesetzlich notwendig ist. Dazu zählt u. a. die Beantwortung von Anfragen von Stellen außerhalb der USA, wenn wir in gutem Glauben der Meinung sind, dass ihre Beantwortung nach den lokalen gesetzlichen Bestimmungen des betreffenden Landes, dessen Rechtsprechung der Nutzer unterliegt,

notwendig ist, und dass diese Anfragen im Einklang mit international anerkannten Standards stehen. Wir dürfen auch Informationen weitergeben, wenn wir in gutem Glauben der Meinung sind, dass ihre Offenlegung zur Vermeidung von betrügerischen oder anderen rechtswidrigen Handlungen, zur Vermeidung einer drohenden Körperverletzung oder zu unserem eigenen und zu deinem Schutz vor Personen notwendig ist, die gegen die in unserer Erklärung der Rechte und Pflichten verankerten Nutzungsbedingungen verstoßen. Dazu zählt u. a. die Weitergabe von Informationen an andere Unternehmen, Rechtsanwälte, Gerichte oder sonstige Behörden.

Übertragung beim Verkauf oder bei einer Änderung der Eigentumsverhältnisse. Bei einer Änderung der Eigentumsverhältnisse, d. h. einem Übergang des Eigentums am gesamten oder nahezu gesamten Unternehmen, dürfen wir deine Informationen an den neuen Eigentümer übertragen, damit der Betrieb des Dienstes fortgesetzt werden kann.

Inhärente Risiken beim Informationsaustausch. Obwohl wir dir die Möglichkeit bieten, den Zugriff auf deine Informationen über die Privatsphäre-Einstellungen einzuschränken, solltest du dir darüber im Klaren sein, dass keine Sicherheitsmaßnahme perfekt oder unüberwindbar ist. Wir haben keine Kontrolle über die Handlungen von anderen Nutzern, mit denen du deine Informationen austauschst. Wir können nicht garantieren, dass nur befugte Personen deine Informationen ansehen. Wir können nicht gewährleisten, dass Informationen, die du auf Facebook austauschst, nicht öffentlich zugänglich werden. Wir übernehmen keine Haftung, wenn Dritte Privatsphäre-Einstellungen oder Sicherheitsmechanismen auf Facebook umgehen. Du kannst diese Risiken allerdings durch gängige Sicherheitsverfahren verringern, indem du ein starkes, nicht leicht zu entschlüsselndes Passwort festlegst und unterschiedliche Passwörter für verschiedene Dienste und eine aktuelle Virenschutzsoftware verwendest.

7. Nutzen Sie sichere Kennwörter

8.
41 Prozent der Bundesbürger verändern aus eigener Initiative niemals ihre Zugangscodes für Online-Konten, E-Mail-Postfächer, Auktionsplattformen, PCs oder das Handy.

Das ergab eine repräsentative Forsa-Umfrage im Auftrag des Branchenverbands Bitkom. Nur jeder Sechste (17 Prozent) ändert seine wichtigsten Geheimzahlen und Passwörter wenigstens einmal im Quartal. "Bei Passwörtern zahlt sich Treue nicht aus – die wichtigsten Passwörter sollten alle drei Monate geändert werden", kommentiert Dieter Kempf vom Präsidium des Bitkom die Umfrage.

9.
Institut für Internetsicherheit (IF IS) in Gelsenkirchen hat eine Befragung durchgeführt über die Passwort-Qualität:
Sonne und Sonne123

10.

Gawker-Einbruch: Beliebtestes Passwort ist 123456

Die Sicherheitsexperten von Duo Security haben die gestohlenen Nutzerdaten des US-Blogbetreibers Gawker analysiert und dabei auch etwa 400.000 der ungefähr 1,3 Millionen DES-verschlüsselten Passwörter geknackt. Dabei kam heraus, dass 123456 auch hier das am häufigsten gewählte Passwort ist. Es wurde über 2500 Mal eingesetzt. Kurz darauf folgt password, dass fast 2200 Anwender als Passwort wählten. Für 12345678 haben sich immerhin über 1200 Anwender entschieden. Darauf folgen qwerty, abc123, 12345, monkey, 111111, consumer, letmein und 1234.

(rei)

11.
Über 45% der Nutzer verwenden dasselbe Passwort für alle genutzten Anwendungen

12.
13.
14. Überprüfen Sie die Standardeinstellung
15.
Facebook – Datenschutzrichtiline vom 22.12.2010

Zur Ergänzung deines Profils. Wir dürfen Informationen über dich, die wir von anderen Facebook-Nutzern erfassen, zur Ergänzung deines Profils verwenden (wenn du beispielsweise auf einem Foto markiert oder in einer Statusmeldung erwähnt wirst). In diesen Fällen geben wir dir im Allgemeinen die Möglichkeit, den Inhalt zu entfernen (zum Beispiel kannst du eine Fotomarkierung von dir entfernen) oder die Sichtbarkeit des Inhalts in deinem Profil einzuschränken.

6. Weitergabe von Informationen durch uns

Wir geben deine Informationen an Dritte weiter, wenn wir der Auffassung sind, dass du uns die Weitergabe gestattet hast, damit wir unsere Dienste im Bedarfsfall anbieten können oder wenn wir aus rechtlichen Gründen dazu gezwungen sind. Zum Beispiel: Dann sind einige Beispiele genannt.

Zum Anbieten von gemeinsamen Diensten. Wir können Dienstleistungen, wie beispielsweise Kleinanzeigen im Marktplatz auf Facebook, gemeinsam mit anderen Unternehmen anbieten. Bei Inanspruchnahme dieser Dienstleistungen durch dich dürfen wir deine Informationen zur leichteren Erbringung dieser Dienstleistung weitergeben. Bevor du diesen Dienst verwendest, geben wir jedoch die Identität des Partners und die Datenschutzrichtlinien des gemeinsamen Dienstleisters bekannt.

16.

Vorsicht bei Fotos

17.
Quelle Süddeutsche Zeitung, Februar 2010:
Sie erinnern sich sicher an die Tragödie, als eine junge Frau im Juni 2009 in Teheran bei einer Demonstration ums leben kam. Ihre Bilder wurden über YouTube ins Netz gestellt.
Auf der Suche nach der Identität stiessen Redakteure auf den Namen Neda und in Facebook auf den Nachnamen Soltan. Studentin an der Islamic Anzad Universität in Teheran. Sie selbst ist auch an der Unitversität in Teheran angestellt.

Auch Neda Soltani unterhielt eine Seite in Facebook.

Die Inhalte ihrs Profil war nur für Ihre Freunde freigegeben, allerdings konnte man auf Ihr Foto zugreifen. Da sie der getöteten Frau ähnlich sah verbreitete sich Ihr Bild in windeseile übe soziale Netzwerke, Blogs und Portale so dass auch CNN, BBC, CBS, ARD und ZDF sendet.

Nun wollten auf einmal unzählige Menschen auf Ihrer Facebook Seite registrieren. Nach und nach erfuhr sie, dass es sich um eine Verwechselung handelte. Sie schrieb die einzelnen Sender an und sende zum Vergleich ein zweites Foto. Dieses zweite Foto wurde ebenfalls verbreitet.

Nachdem Sie aus Ihrem Facebook-Profil ihr Foto entfernt hat, wähnte man Zensur.
Auch nachem durch Angehörige der Toten ein echtes Foto der Toten freigegeben wurde, liess sich das fälschliche Foto nicht mehr in den Medien eliminiern.

Ihre Klarstellung im Netz wurde von der Gemeinschaft der Nutzer als Betrug abgetan und sie wurde nun persönlich angefeindet. Sie wurde bedroht und geriet im Iran immer mehr unter Druck. Nachdem auch Freunde und Verwandte diesem Druck ausgesetzt waren, entschloss Sie sich ihre Familie, ihre Freunde, ihren Arbeitsplatz ja sogar ihr Land zu verlassen.

Heute lebt sie in der Nähe von Frankfurt.

Ihr Bild gehört nicht mehr ihr. Es gehört CNN und den anderen.

Nehmen wir dieses unglaubliche Beispiel als Mahnung für unser tägliches Handeln mit unseren eigenen persönlichen Daten und denen anderer Menschen sorgfältig und verantwortungsbewusst umzugehen.

18. Big Brother is Watching you
19.
Auf Social Networking-Diensten gepostete Informationen können u.U. wertvolle Ressourcen darstellen, da gezielte Phishing- Attacken validierte Informationen aus dem Internet sowie Identitätsprüfungen seriöser Websites gezielt nutzen.

Welche Gefahren eine Veröffentlichung persönlicher Informationen gerade auf Social Networking Sites mit sich bringen kann, wurde auf erschreckende Weise deutlich, als die Frau des britischen Geheimdienstchefs hoch brisante Details zum Wohnort des Ehepaars und seiner Freunde auf Facebook postete.

Beispiel: Transparenz
Da werden durch einzelne Person oder Familienmitglieder im sozialen Netzwerk Informationen ausgetauscht über:

- Arbeitgeber
- Dienstreisen
- Gemeinsame geschäftliche Freunde
- Vielleicht auch über Projekte

Da stellt sich die Frage als Arbeitgeber:
Erlaube ich es den Nutzern von dienstlichen PC ins soziale Netzwerk zu gehen.
Ich kann nicht vermeiden, dass soziale Netzwerke genutzt werden.

Beispiel: Bewerbungen
Sie kennen die Warnungen an die jungen Leute, keine kompromittierenden Fotos oder Aussagen ins Netz zu stellen.
Aber was heute ein 17 Jähriger noch für unproblematisch hält, sowohl Fotos von der Abi-Abschlussfeier, oder vom Apree-Ski mit Freunden, als auch Meinungsäusserungen in irgendwelchen Blogs, wird er als 35 jähriger vielleicht ganz anders sehen. Nur dann gibt es keine Chance mehr diese Veröffentlichungen zurückzunehmen.

Beispiel: Einbruch-Diebstahl
Einer der Familienangehörigen verbreitet im Netz den Zeitraum indem die ganze Familie in Urlaub fährt. So werden die eigenen vier Wände eine lohnendes Ziel für Langfinger.
Oder welche tolle neue Anschaffung im Haus nur darauf wartet abgeholt zu werden.

Wie wir alle wissen, ergibt sich bei der Recherche nach Informationen im Netz, erst durch die Zusammenführung der vielen Einzelinformationen (auch über Facebook-Freunde) ein umfassendes Bild.

20.
Schützen Sie Ihre Computer

21.
Soziale Netzwerke haben sich zur lukrativen und ressourcentechnisch bestens geeigneten Plattform für die Verbreitung von Malware entwickelt.

Neben der aufmerksamen Nutzung von eMails, und sozialen Netzwerken ist es wichtig auf seinem PC-Arbeitsplatz aktuelle Anti-Malware uns Anti-Spam Lösung zu betreiben.

Dies gilt sowohl für die privaten als auch für beruflich genutzte PC-Arbeitsplätze.
Gerade im deutschen Mittelstand erkennen wir hier immensen Nachholbedarf.

Um sich ein Bild über den aktuellen IT-Sicherheitsstandard zu machen, stellt der Verein Deutschland sicher im Netz einen IT-Sicherheitscheck zur Verfügung.

Aus diesem anonymen Sicherheitscheck lässt sich eine Bedrohungsanalyse erstellen und Handlungsempfehlungen ableiten.

22.
In diesem Beispiel sehen wir eine Koobface-Nachricht und ein Klick auf den Link führt uns zu einer „lustigen“ Grafik. Koobface hält jedoch viele böse Überraschungen bereit …

23.
Der Koobface-Wurm geht mit äußerster Geschicklichkeit vor. Er kann nicht nur Facebook-Accounts erstellen und diese mittels einer an Gmail gesendeten E-Mail bestätigen, sondern auch Freundschaften zu Fremden schließen und wahllos Facebook- Gruppen beitreten.

Außerdem kann der Wurm Nachrichten auf den Pinnwänden seiner Facebook-Freunde hinterlassen (oft vermeintliche Links zu Videos, bei denen es sich aber tatsächlich um Malware handelt). Um nicht zu viel Aufmerksamkeit zu erregen, werden die maximale Anzahl neuer Freundschaften pro Tag begrenzt.
Aber er versucht genauso abgespeicherte Passworte herunterzuladen.

Koobface weitete seinen Angriffsradius aus, treibe in 18 Sprachen sein Unwesen und greift inzwischen nicht mehr ausschließlich das Netzwerk Facebook an, welches dem Wurm seinen Namen verlieh.

Seit 2008 zählen auch Social Networking Sites wie MySpace und Bebo sowie seit Anfang 2009 Tagged und Friendster zu den Opfern des Wurms.

Erst kürzlich wurde der Code des Schädlings außerdem erweitert, um im Rahmen neuer Angriffswellen auch Twitter attackieren zu können.

Es ist äußerst wahrscheinlich, dass weitere Malware- Schädlinge in die Fußstapfen von Koobface treten. Diese werden genauso Web 2.0- Botnets zum Diebstahl von Daten aufbauen und vermeintliche Anti-Virus-Meldungen anzeigen, welche Hacking-Gangs ein lukratives Einkommen bescheren.

24.

Schalten Sie Ihr Gehirn ein vor jedem Klick

25.
Malware oder Schadsoftware kann zahlreiche Effekten haben. Die Bandbreite reicht von der Anzeige irritierender Nachrichten auf dem Bildschirm über Datendiebstahl bis hin zur Fremdkontrolle von Computern.

In ihrem Streben, Computer mit Malware zu infizieren, haben Cyberkriminelle gefälschte Accounts auf Websites wie LinkedIn erstellt. Hier zwei Profile berühmter Persönlichkeiten, deren Links jedoch zu gefährlichen Websites führen. Durch ein Klicken der Links werden Sie auf Websites weitergeleitet, die Sie mit Malware infizieren können.

26.
Ein häufig auf Facebook anzutreffender Angriffstyp ist das so genannte „Clickjacking“. Bei dieser Art von Attacke kommen Schad- Webseiten zum Einsatz, auf denen sich die tatsächliche Funktion eines Buttons unter einer harmlos anmutenden, jedoch undurchsichtigen Ebene verbirgt. Sobald der Benutzer den entsprechenden Inhalt mit seinen Facebook-Freunden teilt bzw. „Gefällt mir“ klickt, wird die Attacke über Newsfeeds und Statusupdates an sämtliche Kontakte gesendet und der Scam somit maximal verbreitet.

Clickjacking setzt auf ein Standard-Arsenal perfider Social-Engineering-Tricks, um Benutzer dazu zu verführen, auf maskierte Links zu klicken. Neben den üblichen Lockmitteln wie Humor, manipulierten Promi-Fotos und großen Nachrichten- und Entertainment-Events mussten wir einen Anstieg zunehmend bizarrer und oft grausiger Inhalte beobachten.

27.

- **Betrüger locken mit vermeintlichen Fotos von Bin Ladens Tod**
- Cyberkriminelle nutzen ihre Chancen, um Schadsoftware zu verbreiten. Derzeit kursieren etwa E-Mails im Netz, die vermeintliche Fotos von Osama Bin Ladens Tötung enthalten sollen. Wird der E-Mail-Anhang ausgeführt, installiert sich ein Trojaner auf dem PC , der Online-Banking-Daten ausspioniert

Quelle: http://www.buerger-cert.de/newsletter_archiv.aspx?param=Zxo7YT%2f0plcmMIv0aUV7mQ%253d%253d#anchor1

28. Bedrohliche Unbekannte
29. SPAM

    67% der Nutzer Sozialer Netzwerke berichten, dass sie auf diesem Weg SPAM bekommen haben. Das sind doppelt so viele wie in 2009

30. PHISHING

43% der Nutzer Sozialer Netzwerke berichten von Phishing-Angriffen auf diesem Weg Das sind mehr als doppelt so viele wie in 2009.

31. Malware

    40% der Nutzer Sozialer Netzwerke berichten von Malware-Angriffen über diesen Kanal. Das sind fast doppelt so viele wie in 2009.

Diese Zahlen sollen nur unterstreichen, wie wichtig es ist, aktuelle Anti-Viren, Anti-Spam-Produkte auf Ihrem Rechner zu haben.

32.
Security Threat Report

33.
Toolkit

34.

Machen Sie sich bewusst, welche Information Sie der Wolke Internet anvertrauen.
Denken Sie darüber nach, was diese Meldung auf dem Bildschirm von Ihnen möchte und was Sie nach dem Klick erwarten wird.

Schauen Sie sich den Rechner an, auf dem Sie gerade Arbeiten, - ist er durch aktuelle Sicherheitssoftware geschützt!

Nur durch technische Sicherheitsvorkehrungen und den bewussten Umgang mit neuen Medien machen Sie sich Ihre Cloud ein wenig sicherer.

35 Ende