T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting 2011

Networking mit Nebenwirkungen - Risiken sozialer Medien

Sascha Dubbel
Palo Alto Networks Inc.
Systems Engineer Central Europe

Was sind soziale Netzwerke?

Definition von Facebook in Wikipedia:

- **Facebook** (englisch sinngemäß „Studenten-Jahrbuch“) ist eine Website zum Erstellen und Betreiben sozialer Netzwerke, die der Facebook Inc. mit Sitz im kalifornischen Menlo Park gehört.
- Die Plattform war im Februar 2004 erstmals zugänglich und erreichte im September 2011 rund 800 Millionen Mitglieder weltweit.[2][3]
- Facebook steht regelmäßig aufgrund seiner Datenschutzpraktiken[4] und zahlreicher Verstöße gegen das Datenschutzrecht der Bundesrepublik Deutschland und der Europäischen Union[5] in der Kritik

Der Gründer von Facebook, Mark Zuckerberg

Deutschlands beliebteste sozialen Netzwerke

Quelle: Google AdPlanner, Nutzerzahlen in Millionen

1	facebook.com	11
2	gmx.net	9,1
3	stayfriends.de	6,2
4	schuelervz.net	6,2
5	wer-kennt-wen.de	6,1
6	studivz.net	5,6
7	meinvz.net	4,2
8	myspace.com	3,8
9	xing.com	2,9
10	jappy.de	2,2
…		
13	www.odnoklassniki.ru	1,1

•Kennen Sie das?

Es ist weniger populär, wird aber bestimmt auch bei Ihnen genutzt und auch dort werden gerne Viren verteilt!

Vorteile für Unternehmen: das wünscht man sich…

- Positive Selbstdarstellung
- Gewinnung von „Fans“
- Sammeln von Feedback aus z.B. Kommentaren
- Mitteilungsplattform und Werbekanal
- Mitarbeiter-Akquisition
- „Viral Marketing“
- Dynamische Verknüpfung mit anderen Medien (z.B. YouTube, Twitter etc.)

Vorteile für private Benutzer: nicht nur in der Freizeit…

- immer erreichbar sein
- alte Bekannte wiederfinden
- seine „sozialen Wert“ messen und Selbstbestätigung erfahren
- Business-Nutzer finden Zugriff auf aktuelle Berufschancen
- man kann seine Meinungsfreiheit ausleben und
- Alles was man möchte preisgeben und
- nach Herzenslust Lästern und Verunglimpfen
- spontan Teilnehmer finden für Veranstaltungen und Partys etc…

manchmal mehr als man möchte…

Nachteile und Gefahren durch die Nutzung sozialer Medien… das bekommt man

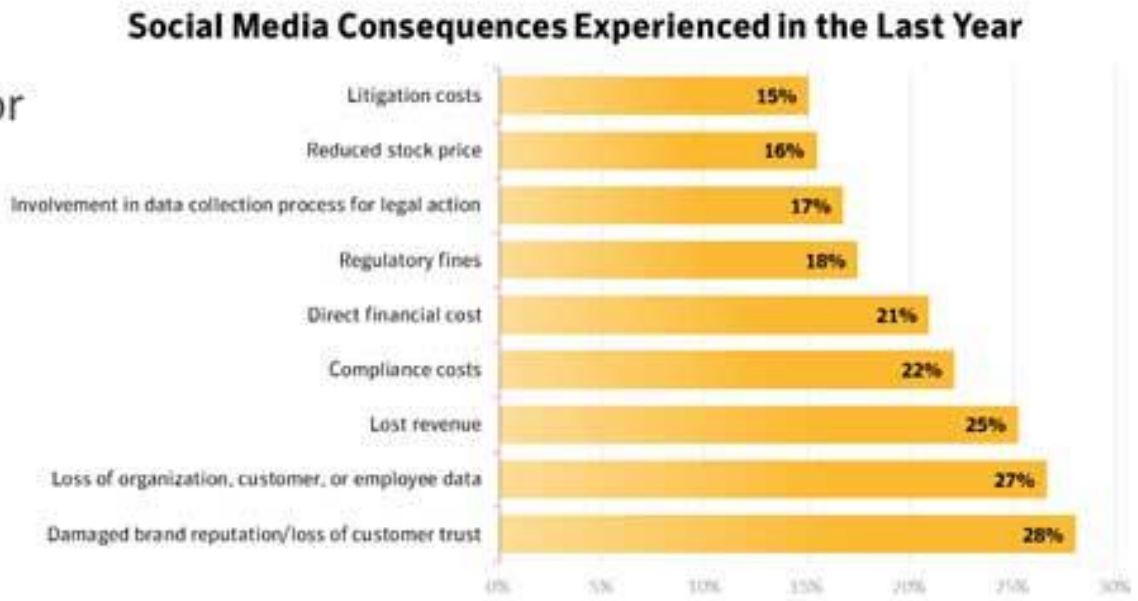
Die Gefahren und Folgen durch die Nutzung von Social Media treffen private Personen und Unternehmen meist gleichermaßen, da die Grenzen zwischen privater und geschäftlicher Nutzung fließend sind, und in den wenigsten Fällen überhaupt definiert wurden.

Erhebungen des Software-Unternehmens Symantec zufolge beziffern die befragten Unternehmen den Schaden der aus der ungeeigneten Nutzung von sozialen Medien entsteht im Jahr 2011 auf durchschnittlich 4 Millionen USD.

Nachteile und Gefahren durch die Nutzung sozialer Medien… das bekommt man

Mistakes Happen

- Typical: 9 social media incidents in past 12 months
- 94% experienced consequences due to incidents:
  - Damaged brand/trust (28%)
  - Loss of organization, customer or employee data (27%)
  - Lost revenue (25%)



Symantec.

Gefahren von Social Media: Sucht

Personen mit Sucht-Disposition können schnell abhängig werden

-Kontrollverlust über das eigene Leben, Zeitgefühl etc.

-Arbeitsplatzverlust

-Verwahrlosung

-Ausprägung schizoider Verhaltensmuster

-Bewegungsmangel mit allen Folgen

-Verlust realer sozialer Bindungen

Gefahren von Social Media: Malware

- Fast 12 Milliarden Stunden surften Facebook-Benutzer allein 2010 im sozialen Netz, dies ergibt ein Infektionspotenzial für Computer-Malware wie bei keinem anderen Medium dieser Zeit.

02.02.2011, 15:56

Trojan.Win32.Scar: Fiese Malware per

Fotostrecke: Die schlimmsten Facebook-Fettn

Der Sicherheits-Anbieter Emsisoft über einen neuen Schädling, der es auf unerfahrene Facebook-User abgesehen hat. Der Trojaner Win32.Scar verbreitet sich über den Chat des sozialen Netzwerks. Mit der Nachricht "hahahh Foto" lockt er gutgläubige User auf eine gefälschte Facebook-Seite.

Dort angekommen, erscheint die Meldung "Photo has been moved" (Foto wurde verschoben). Um das Bild dennoch anzuzeigen, soll der User auf "View Photo" klic nicht zum versprochenen Bild, sondern startet Bestätigt der User den Download, wird der Rec Worm.Win32.Yimfoca!A2 oder Trojan.Win32.Sc anschließend selbständig über die Nachricht m seine Freunde weiterverteilt.

16.05.2011, 17:30

Dislike-Button: Neue Malware auf Facebook

Facebook: Wurm zeigt angebliche Profilaufrufe an

Nachdem vor kurzem zahlreiche Facebook-User von einem Wurm betroffen waren, der ihnen versprach anzuzeigen wer das eigene Profil besucht hat, bahnt sich jetzt ähnliche geartete Malware den Weg durch das weltweit größte soziale Netzwerk: Diesmal kursiert eine Anleitung auf Facebook wie man angeblich einen Dislike-Button aktivieren kann.

Facebook: Auf dem sozialen Netzwerk verbreitet sich schon wieder Scam.

Blöde Kommentare, Meldungen oder ganze Pages würde man am Liebsten mit einem „Gefällt mir nicht"-Button abstrafen. Da es den aber nicht gibt, kommt eine Anleitung wie man den Dislike-Button aktiviert natürlich umso gelegener – aber Achtung, das ist eine Falle. Wer den Button installieren will, lädt sich Malware auf sein Facebook-Profil, die sich automatisch an alle Freunde weiterverteilt. Die Verbreitung des neusten Facebook-Scams funktioniert dabei ähnlich wie schon beim Profil-Wurm.

Quelle: Chip.de

Gefahren von Social Media: Verlust geheimer Informationen

Silicon.de, 25.5.2009: Als der Bundestagspräsident am Samstag die Wiederwahl von Horst Köhler zum Bundespräsidenten verkündete, war das Wahlergebnis schon längst via Twitter durchgesickert. Einige Abgeordnete hatten offenbar fleißig gezwitschert. Dabei kannte die Indiskretion keine Parteigrenzen.

Den Anfang machte der Bonner SPD-Parlamentarier Ulrich Kelber. Von seinem Handy schickte er Samstagnachmittag um 14.15 Uhr eine Mitteilung an den Kurznachrichtendienst Twitter: "Nachzählung bestätigt: 613 Stimmen. Köhler ist gewählt!" Erst eine Viertelstunde später gab Bundestagspräsident Norbert Lammert das Ergebnis offiziell bekannt.

Wenige Minuten zuvor hatte Kelber in 140 Zeichen erste Meldung gemacht: "Köhler hat 613 Stimmen. Das wäre genau die kleinste Mehrheit." Auch die CDU-Abgeordnete Julia Klöckner hatte per Handy eifrig ihren Twitter-Nachrichtenstrom bedient: "Müssen nachzählen – ah, jetzt stimmts. Umschläge werden geöffnet. Melde mich mal ab wg. Auszählgeheimnis."

Kurz danach meldete sie sich wieder, gut zehn Minuten vor Lammerts Bekanntgabe des Resultats. Mit der knappen Mitteilung: "Leute, ihr könnt in Ruhe Fußball gucken. Wahlgang hat geklappt!" Ähnlich salopp freute sie sich über die Antrittsrede des alten wie neuen Staatsoberhaupts: "Bundes-Hotte hält Dankes/Antrittsrede – toll!!!!"

Gefahren durch Social Media: Spionage

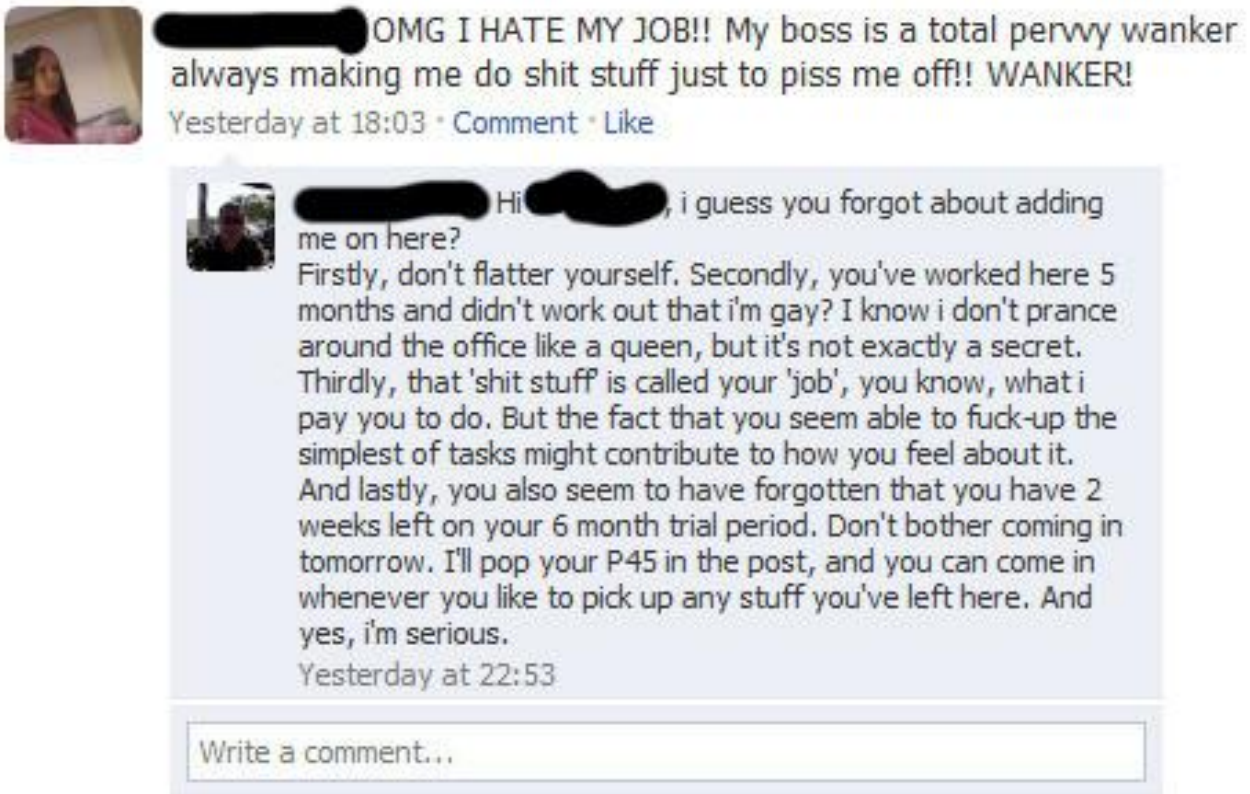
- Eine bezaubernde junge Frau freundet sich auf Facebook mit israelischen Militärs an – und entlockt ihnen Geheimnisse. Laut einem Pressebericht tappten 200 Elitesoldaten in die Falle. Dahinter steckt vermutlich die libanesische Schiitenmiliz Hisbollah. Über ein gefälschtes Facebook-Profil soll die Hisbollah eine israelische Eliteeinheit infiltriert haben. Mit dem Foto einer hübschen jungen Frau, die sich mit einem israelischen Namen einloggte, soll die libanesische Schiitenmiliz Kontakt zu Soldaten aufgebaut und sich so geheime Informationen beschafft haben. Das berichtet **das israelische Nachrichtenportal mySay.co.il** auf seiner Internetseite.

Quelle: afghanistan-blog.de

Gefahren durch Social Media: Reputationsschaden

- Schädigung der eigenen Reputation durch unbedachte Äußerungen, 2 Beispiele
- FR-Online.de: **Der irre Boss**

  Eine Mitarbeiterin eines Rettungsdienstes vergleicht ihren Chef in einer Facebook-Mitteilung mit einem psychiatrischen Patienten. Daraufhin bekam sie die Kündigung. Die Mitarbeiterin zieht nun vor Gericht.



Gefahren durch Social Media: Ressourcenverluste

- Arbeitnehmerzeit wird ungewollt für private Interessen auf z.B. Facebook verwendet. Die Produktivität der Mitarbeiter sinkt, die Rentabilität der Unternehmung wird gefährdet

- Internetbandbreite wird durch die Private Nutzung belegt, populäre Internetvideos verbreiten sich über private Netzwerke rasend schnell.
  - Somit steht die Internetanbindung für geschäftskritische Prozesse nicht mehr zur Verfügung.
  - Kosten entstehen durch Aufstockung der Kapazitäten (Leitung, Infrastrukturkosten

Organisatorische Gegenmaßnahmen

1. Mitarbeiter über Gefahren von Sozialen Netzwerken aufklären und sensibilisieren (Info-Event, Aushänge, Poster etc.)
2. Definieren Sie klare ethische Richtlinien für Mitarbeiter.
3. Für geschäftliche/betriebliche Zwecke eigene Firmen-Accounts anlegen und nur diese nutzen.
4. Geschäftskommunikation ausschließlich den dafür berechtigten Personen (Pressestelle, Marketing etc.) überlassen.
5. Haftung für Posts/Tweeds etc. klarstellen, ein Unternehmen haftet für seine Inhalte und hat hier Moderationspflichten
6. Regelmäßig prüfen, ob es zu Verstößen gekommen ist und unerwünschte Einträge löschen lassen. Aber Obacht: das Netz vergisst nicht und über Dienste wie Google Cache können auch längst vergessene Fehltritte und Ausrutscher wieder ans Tageslicht gelangen.

Organisatorische Gegenmaßnahmen

7. Kommunikationen in Chaträumen können einer Aufbewahrungspflicht unterliegen, hier müssen dann selbst kontrollierbare Medien genutzt werden.
8. Vorfälle an geeignete Stellen elden: Spionageabwehr der Innenministerien unterstützt, grade kleine und mittelständische Unternehmen sind die Innovationsmotoren und somit im Fadenkreuz von wirtschaftlich und politisch motivierten Angreifer-Organisationen/Staaten.
9. Private Internet-Nutzung klar reglementieren und regelmäßig geeignet kommunizieren (betrieblicher Übung vorbeugen!)
10. Prüfen Sie (ggf. gemeinsam mit dem Personalrat) ob sich in sozialen Netzen fremde Personen als Mitarbeiter Ihres Unternehmens/Institution ausgeben, auch Ihre Mitarbeiter sollten hier aufmerksam sein

Technische Gegenmaßnahmen

1. Machen Sie sich ein Bild zur derzeitigen Nutzung (anonymisiert!) Palo Alto Networks z.B. bietet hierzu einen Report im Rahmen einer kostenfreie Evaluierungen an.
2. Überlegen Sie, welche Personen/Benutzergruppen/Abteilungen Zugriff benötigen und nutzen Sie Zugriffskontrollmechanismen wie Firewalls der nächsten Generation (NGFW) um die Berechtigungen umzusetzen.
3. Sperren Sie das Risiko aus, indem Sie z.B. in Unternehmen mit geduldeter oder erlaubter Internet-Nutzung granular Funktionen der Sozialen Netzwerke sperren, von denen ein Risiko für Ihr Unternehmen ausgeht (z.B. Dateitransfers, Chat, Desktop Sharing), die gefahrlosen Bereiche oder Inhalte aber allen Usern zugänglich machen. Dies ist mit Applikations-basierten Firewalls sehr einfach umzusetzen, da Sie hier keine URLs, IP-Adressen oder Ports/Protokolle kennen müssen!

Technische Gegenmaßnahmen

4. Nutzen Sie einen Gateway Virenscanner der den erlaubten Datenverkehr auf Viren/Malware überprüft. Diese Funktion wird von führenden Firewall-Produkten in Echtzeit unter Nutzung von Hardware-Beschleunigung ermöglicht, sodass es nicht zu einer negativen Beeinträchtigung oder Proxy-typische Wartezeiten kommt.
5. Erzwingen Sie Bandbreitenrichtlinien um z.B. die maximal verfügbare Bandbreite für Soziale Netzwerke und Medienportale zu limitieren und für Geschäftskritische Prozesse die Verfügbarkeit zu garantieren.
6. Inline IPS (Intrusion Prevention) Systeme können Sie gleichzeitig vor der Ausnutzung von Schwachstellen auf Ihren Client-Systemen schützen und

Fragen, Wünsche Anregungen?

Wir sind für Sie da:

Sascha Dubbel, T.I.S.P.

Palo Alto Networks Deutschland

Wilhelm-Ruppert-Strasse 38

51147 Köln

sdubbel@paloaltonetworks.com

+49 151 127 05 241


paloalto
NETWORKS
the network security company™