SSD 2011 - Merkblatt Social Networks
Versione italiana (B. Zumthor) / 04.02.2011

Opuscolo illustrativo

Corretto utilizzo delle Reti Sociali (Social Networks)

1. Scopo dell'opuscolo

L'importanza di applicazioni di Reti Sociali in Internet è continuamente cresciuta negli ultimi anni. Soltanto in Svizzera sono oggi attivi 2,48 milioni di utenti Facebook, mentre Facebook stessa e le altre offerte analoghe attirano sui loro siti Web ben più di 100 milioni di visitatori in tutto il mondo.
Le Reti Sociali e i profili (dati) personali che vi vengono depositati hanno oggi un valore importante, in quanto rappresentano le identità virtuali degli utenti in Internet. Qui si pone la domanda: come possono le Reti Sociali e i loro aspetti positivi essere utilizzati in modo ragionevole, mantenendo però un rapporto accettabile con la propria sfera privata?

2. Rischi per l'utente

Cosa succederebbe se il vostro (futuro) datore di lavoro vedesse le vostre fotografie scattate durante l'ultima festa in cui magari vi siete lasciati un po' andare? Come potrebbero dei malintenzionati utilizzare informazioni sul vostro lavoro o su vostri possibili soggiorni di vacanza? Dovreste porvi queste e altre domande del genere prima di inserire un vostro profilo in una Rete Sociale, risp. prima di pubblicarvi tutte le possibili informazioni su di voi.

Pubblicazione di informazioni private
Nelle Reti Sociali gli utenti possono inserire indirizzi e-mail, numeri telefonici, propri hobby, preferenze, ecc., in sostanza varie informazioni di tipo personale. Questi dati possono essere ad es. utilizzati da ditte interessate per bombardare gli utenti in modo mirato con messaggi pubblicitari. Purtroppo spesso all'apertura di un conto personale le impostazioni previste per la protezione della sfera privata non vengono tenute in debita considerazione, per cui tutti i dati inseriti sono automaticamente a disposizione di tutti gli utenti della Rete Sociale. Estratti dei profili sono in parte addirittura reperibili attraverso siti di ricerca (come Google) e quindi a disposizione degli utenti Internet di tutto il mondo.

Nelle procedure di assunzione i datori di lavoro utilizzano le Reti Sociali per ottenere informazioni sui potenziali collaboratori. Fotografie o espressioni compromettenti possono allora facilmente diventare un criterio di esclusione. Anche padroni di casa o assicurazioni potrebbero essere interessati a questo genere di informazioni di contorno.

Informazioni, testi e in particolare immagini vengono spesso archiviati dai privati anche al di fuori delle Reti Sociali, sul proprio computer collegato a Internet, e questo può portare a

ritrovare su altre pagine di Internet, o essere utilizzati in modo anomalo, dei dati che risultavano cancellati sulla Rete Sociale.

Furto d'identità

Dei criminali cercano sempre più spesso di penetrare in conti di utenti per utilizzarne l'identità a scopi illeciti. Spesso fingono poi una situazione di emergenza e chiedono degli aiuti finanziari agli amici dell'utente originario collegati in rete. Le informazioni ottenute in modo illecito dal profilo possono servire ad aumentare la fiducia e ingannare gli amici. Profili "non autentici" vengono spesso utilizzati per danneggiare le persone, ad es. spiando le possibili assenze per vacanza in cui l'abitazione è libera e quindi meno sorvegliata.

Diffusione di software nocivo (malware)

La fiducia degli utenti nelle Reti Sociali normalmente è grande. Truffatori hanno perciò trasferito su queste piattaforme una tecnica già sperimentata, cioè di inviare messaggi contenenti un link a pagine Web falsificate, attraverso le quali poi vengono diffusi programmi nocivi. Un esempio noto di questa tecnica è il verme informatico *Koobface* diffuso su Facebook. Da conti precedentemente infettati erano stati inviati ad altri utenti degli inviti a guardare un video. Se un utente cliccava sul link indicato, veniva dirottato su una pagina Facebook o YouTube falsificata, in cui veniva invitato a scaricare (download) il programma Flash Player. Dietro a questo download si nascondeva però il verme informatico *Koobface*, che poteva così diffondersi sempre più.

Alcune Reti Sociali offrono delle applicazioni supplementari che gli utenti possono aggiungere al loro profilo. Un esempio sono dei minigiochi, che gli utenti possono giocare anche in rete. L'aspetto problematico è che queste applicazioni provengono da terzi, i cui standard di sicurezza non corrispondono necessariamente a quelli delle Reti Sociali, per cui – volontariamente o meno – possono essere diffusi dei programmi nocivi.

Mobbing (aggressione)

Le Reti Sociali hanno portato il mobbing a un nuovo livello. Ad es. persone possono essere estromesse intenzionalmente da gruppi di amici, oppure i loro tabelloni digitali possono essere bombardati con ingiurie. Ciò può diventare molto pesante, soprattutto per degli adolescenti. In ogni caso il mobbing viene perseguito penalmente

Amicizie nelle Reti Sociali si stringono più velocemente che nel mondo reale, per cui certe informazioni arrivano a persone alle quali altrimenti forse non sarebbero state affidate. Chi ha cattive intenzioni può utilizzare queste informazioni per mettere a nudo qualcuno intenzionalmente oppure tessere intrighi contro di lui.

Stalking (persecuzione molesta)

Ci sono anche cosiddetti „cyberstalker", che preparano falsi profili nei quali si spacciano per persone diverse, reali o fittizie, che vengono poi utilizzate per molestare altre persone attraverso la Rete Sociale in modo del tutto anonimo.

3. Regole di comportamento per l'utilizzo delle Reti Sociali

Milioni di utenti Internet allacciano contatti e amicizie attraverso la rete, inserendo profili personali che contengono, oltre a informazioni di base su di sé (nome, cognome, ecc.), anche informazioni sui propri hobby, rapporti familiari, carriera professionale, ecc. Lo scopo delle Reti Sociali è quello di collegarsi in rete con degli amici e condividere dei contenuti. Affinché tutti gli utenti si trovino a loro agio nella rete è importante che si attengano ad alcune regole di comportamento – che poi valgono anche nella vita reale. Il collegamento in rete di tipo sociale dev'essere piacevole e divertente, e affinché ciò resti così va presupposto un trattamento reciproco gentile e rispettoso. Con le seguenti 12 regole di comportamento siete senz'altro ben preparati per la vita sociale in Internet.

1. **Siate prudenti nella rivelazione di informazioni personali!**
   Non tutto ciò che sapete su voi stessi deve anche essere messo a conoscenza di altre persone. Verificate criticamente quali dati volete rendere „pubblici". Pensate ad es. che sempre più datori di lavoro cercano su Internet informazioni su candidati. Anche ditte di selezione del personale, assicurazioni o padroni di casa possono essere interessati a tali informazioni complementari.

2. **Informatevi sulle condizioni generali e per la protezione dei dati della Rete Sociale che utilizzate o intendete utilizzare!**
   Su ambedue i tipi di condizioni dovreste essere bene in chiaro – già prima di inserire il vostro profilo. Applicate assolutamente le opzioni messe a disposizione dalla Rete Sociale per rendere accessibili solo in modo limitato le informazioni e immagini da voi inserite: devono avere accesso solo i vostri amici oppure tutti gli utenti?

3. **Siate prudenti e selettivi nel caso di richieste di contatto – dei criminali fanno spesso "raccolta" di amici per danneggiare le persone!**
   Nel caso di richieste da parte di persone che non conoscete dalla vita reale dovreste verificare criticamente se le volete effettivamente includere nella vostra lista di amici. Persone sconosciute potrebbero anche avere cattive intenzioni e voler ad es. spiare i vostri dati per sapere quando non siete in casa. Falsi profili vengono notoriamente utilizzati per danneggiare le persone – per vendetta, avidità o altre ragioni negative.

4. **Segnalate „cyberstalker" che vi contattano senza richiesta e in modo continuo attraverso la Rete Sociale!**
   Per questo genere di segnalazioni potete normalmente rivolgervi direttamente ai gestori della Rete Sociale che utilizzate. Questi potranno seguire il caso ed eventualmente cancellare il profilo sospetto. In casi più seri dovreste anche informare la Polizia e richiedere una procedura penale.

5. **Utilizzate per ogni applicazione Internet, in particolare se siete collegati a diverse Reti Sociali, una password diversa e sicura!**
   Rendetevi comunque conto che i vostri dati sono memorizzati su computer esterni, per cui la sicurezza di questi dati non dipende soltanto da voi, ma anche dai gestori delle Reti Sociali stesse: se i loro server vengono violati, anche i vostri dati non sono più al sicuro. In ogni caso, se viene scoperto un abuso, informate subito anche i vostri amici.

6. **Non pubblicate mai informazioni confidenziali sul vostro lavoro e i vostri datori di lavoro!**
   Informazioni di tipo professionale non vanno inserite nelle Reti Sociali. Anche spie commerciali e industriali hanno scoperto ormai le Reti Sociali ai loro scopi e tentano di carpirvi preziose informazioni. Ciò può costare alle vostre ditte del denaro e a voi stessi il posto di lavoro.

7. **Verificate criticamente quali diritti volete concedere ai gestori delle Reti Sociali per l'utilizzo dei vostri dati (testi, immagini, informazioni varie)!**
   Ogni prestazione ha un prezzo: l'entrata in una Rete Sociale vi costa la messa a disposizione di alcune informazioni. Molte ditte sono disposte a pagare per queste informazioni, per poter poi inviare in modo mirato dei messaggi pubblicitari. Se voi concedete alle Reti Sociali il diritto di disporre ad es. delle vostre immagini, i gestori potrebbero anche venderle a terzi. Controllate anche se eventualmente il diritto di utilizzo dei vostri dati resta valido anche se cancellate il vostro profilo.

8. **Se ricevete informazioni „dubbiose" da conoscenti, informatevi al di fuori delle Reti Sociali sull'affidabilità di queste notizie!**
   Il furto d'identità è un rischio dell'epoca digitale. Una persona sconosciuta può utilizzare un conto falsificato per assumere un'altra identità e così ingannare gli amici di quest'ultima. Truffatori possono ad es. inviare dei messaggi in cui simulano una situazione di emergenza e chiedono aiuto finanziario. Le informazioni d'identità carpite possono essere utilizzate per sostenere l'affidabilità della richiesta.

9. **Non cliccate a caso sui links che vi vengono presentati – le Reti Sociali vengono sempre più utilizzate per il "phishing"!**
   Il clic su un link è presto fatto. Ma attenzione: l'indirizzo indicato potrebbe corrispondere a una pagina Web falsificata che simula l'accesso a una Rete Sociale. Se immettete il vostro nome utente (user name) e la relativa password, questi dati vengono passati direttamente ai truffatori. Particolarmente in voga per tali attacchi informatici sono gli indirizzi URL (Uniform Resource Locator) cosiddetti brevi, che non permettono di riconoscere il vero indirizzo selezionato.

10. **Parlate con i vostri figli delle loro attività nelle Reti Sociali e informateli a fondo sui pericoli che nascondono!**
    Molti bambini e adolescenti non sono spesso consapevoli dei pericoli che si nascondono nelle Reti Sociali – il divertimento spesso prevale sulla sicurezza. Il rafforzamento della „competenza sui media" è un nuovo compito per i genitori nell'educazione dei figli. Ma anche gli altri membri della famiglia, nonché amici e conoscenti, dovrebbero essere coinvolti nelle discussioni su rischi e riflessioni di Sicurezza informatica.

11. **Datori di lavoro** che permettono l'uso di Reti Sociali come Facebook ecc. sul posto di lavoro, dovrebbero preparare una cosiddetta „Direttiva per l'utilizzo delle Reti Sociali" e sensibilizzare in proposito i propri collaboratori. Tale Direttiva dovrebbe par parte integrante del Contratto di lavoro ed essere firmata da ogni collaboratore.

12. **Se utilizzate Facebook su apparecchi mobili**, gli altri utenti di Facebook possono riconoscere la vostra posizione attuale, permettendo a potenziali ladri di sapere che al momento non siete in casa. Per cui è consigliabile disattivare o attivare solo in modo mirato tale funzione.

InfoSurance è un'Associazione per la promozione della Sicurezza informatica in Svizzera, fondata da grandi aziende e dalla Confederazione. Lo scopo è quello di sensibilizzare la popolazione svizzera sull'utilizzo delle nuove tecnologie.
(v 1.0, gennaio 2011)

Un'iniziativa di: sostenuta da: industria, amministrazione, formazione

InfoSurance
und Ihr Computer ist sicher.