# Frontiere future e futuribili della Social Media Security

RELATORI:
**Simone Bonavita**, Professore a contratto in Trattamento Dati Sensibili, Università degli Studi di Milano, anno accademico 2013/2014.

**Carlo Bernardi**, Dottore in Sicurezza dei Sistemi e delle Reti Informatiche, Università degli Studi di Milano.

**Mattia Reggiani**, Dottore in Informatica, perfezionato in Cyber Warfare, Università degli Studi di Milano.

# Di cosa parleremo:

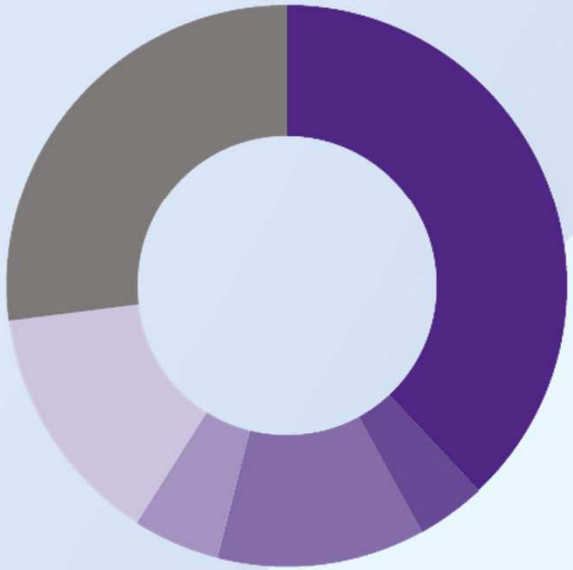
- Aziende 2.0: che ruolo avranno in futuro i Social Media all'interno delle realtà aziendali;
- Social Media e aziende: policy, reputazione, marchio, informazioni sensibili, privacy, furto di identità, attacchi informatici;
- Casi concreti: frode informatica nel profilo Facebook di Alpitour S.p.A. e furto di informazioni dal sito web di Matteo Renzi;
- Definizione di Social Media Security;
- La nostra soluzione: contratti, policy e software di sicurezza;
- Limiti incontrati;
- La privacy che verrà.

# Aziende 2.0 (USA)

Grafici tratti dal report «Social media risks and rewards» di Grant Thornton, Settembre 2013.

**Figure 1: How companies use social media**

- Brand awareness **38%**
- Crowd sourcing **4%**
- Customer care **12%**
- Fulfillment **5%**
- Identity participants/customer profiling and identification **14%**
- Recruiting **27%**



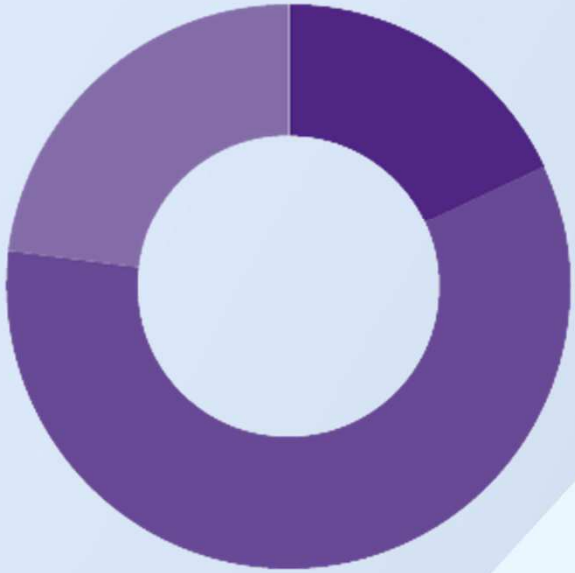
# Aziende 2.0 (USA)

**Figure 5: Concern about potential risks**

# Aziende 2.0 (USA)

**Figure 7: Company performs social media risk assessment**

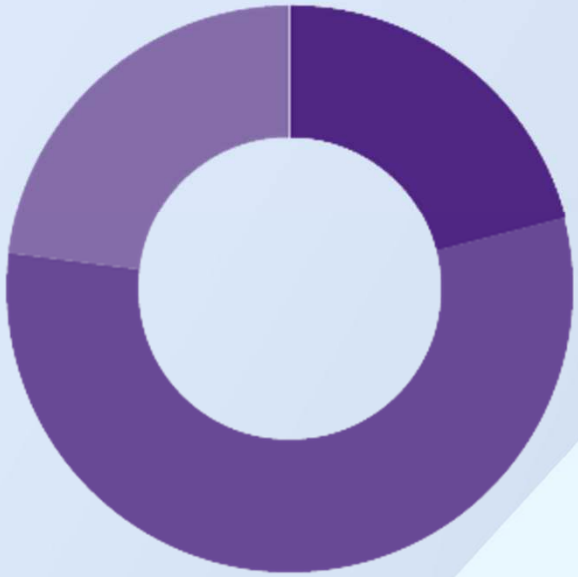
- Yes **18%**
- No **59%**
- I do not know/unsure **23%**



# Aziende 2.0 (USA)

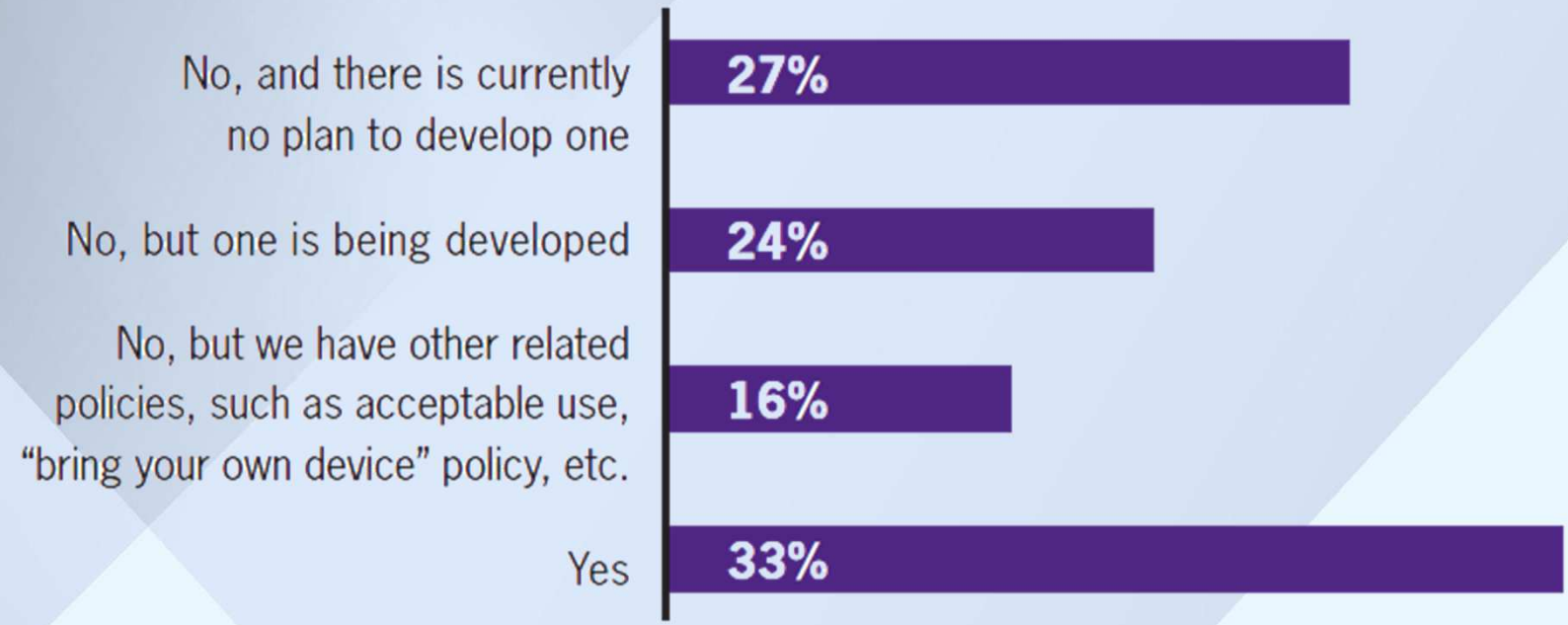
**Figure 10: Company has incident management plan**

- Yes **21%**
- No **56%**
- I do not know/unsure **23%**



# Aziende 2.0 (USA)

**Figure 13: Company has social media policy**



# Aziende 2.0

Ricerca effettuata analizzando un campione di dirigenti di livello senior delle aziende presenti negli USA

Se l'USA è in questa situazione

L'Italia ?

# Social Media e aziende

Riassumiamo:

- i Social Network rappresenteranno una vera e propria estensione dell'azienda al di fuori del suo perimetro;
- I Social Network saranno il reale punto di contatto tra azienda e clienti;
- L'utilizzo dei social network in ambito aziendale è destinato a crescere.

Ma attenzione:

# Social Media e aziende

Social Media e management aziendale:

- Esistono delle policy aziendali che definiscano una linea di condotta o un piano di azione da applicare all'interno del Social Network?
- C' è un team delegato alla gestione dei Social Media?
- La gestione dei Social Media è affidato totalmente ad una web Agency?
- C'è un piano di Incident Management per un attacco social?
- Quanto si investe nella sicurezza aziendale? E in quella Social?
- Ci sono degli standard che definiscono le policy da attuare per la sicurezza in ambiente Social?

# Social Media e aziende

Quali sono i rischi associati?

- Danno alla reputazione aziendale e al marchio;
- Esposizione di informazioni confidenziali;
- Violazioni della Privacy dei clienti;
- Furto di identità;
- Attacchi informatici (hacking, phishing, frodi informatiche).

# Casi concreti: Alpitour S.p.A. (09/2013)

Tratto da lastampa.it:

«[…]sono state rubate le credenziali degli amministratori dei profili Facebook dell'azienda e quindi sono stati postati annunci in italiano che pubblicizzavano viaggi inesistenti. Cliccando sugli annunci, link apparentemente innocui indirizzavano su pagine web che contenevano programmi pericolosi, progettati per impadronirsi delle coordinate bancarie di chi fa acquisti online. […]»

- Perdita di informazioni aziendali (furto password profili Facebook);
- Attacco Phishing con finalità di frode informatica;
- Furto di dati sensibili degli utenti (coordinate bancarie) e violazione della Privacy;
- Reputazione e web identity danneggiati.

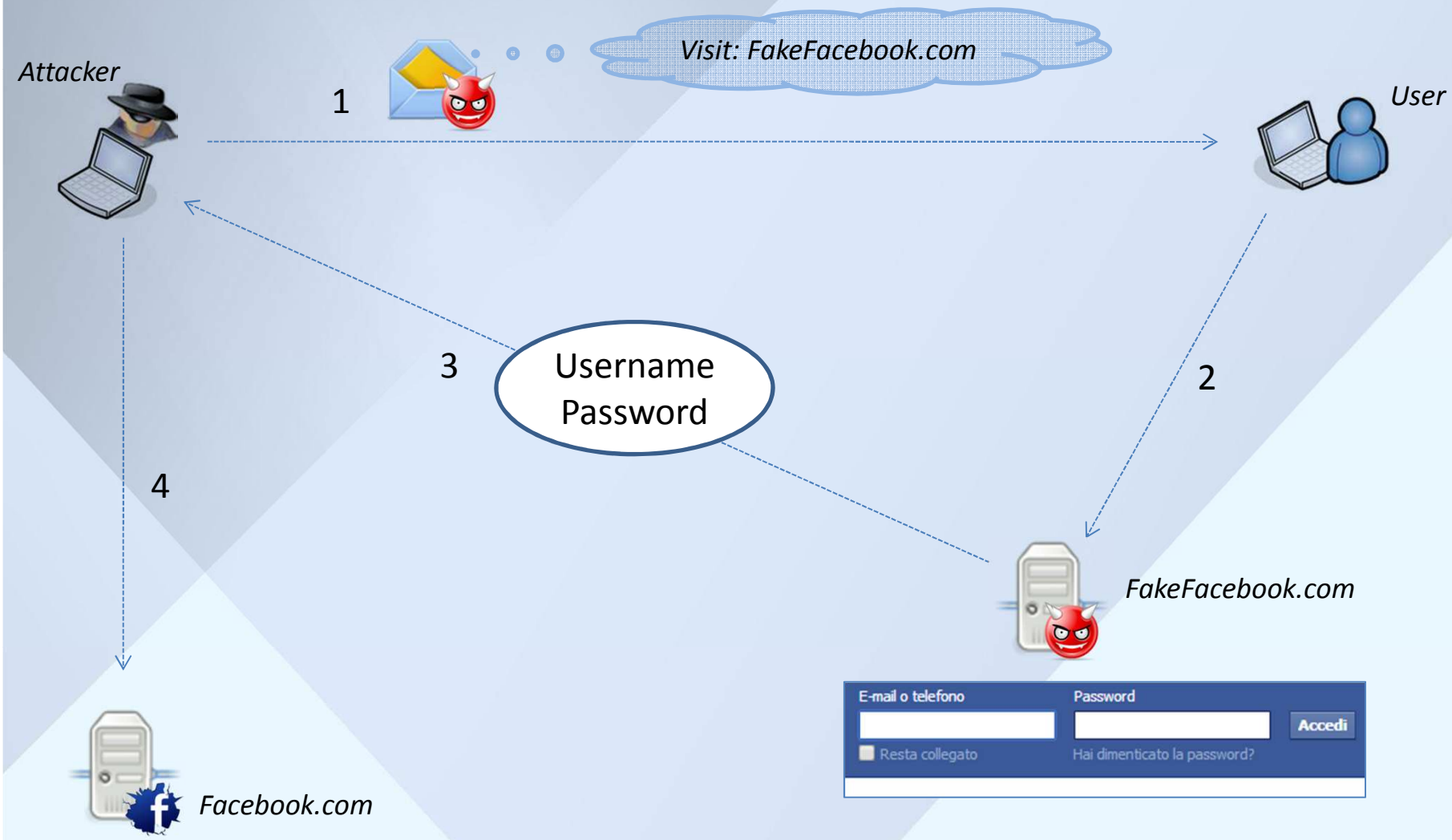
# Casi concreti: Matteo Renzi (12/2013)

Tratto da ilpost.it:

«[…] A seguito di un grave attacco informatico alla piattaforma dei siti web di Matteo Renzi, sono stati violati e pubblicati alcuni dati degli utenti registrati sul sito social.matteorenzi.it o che avevano contribuito alla campagna donando on line. […] Essendo state pubblicate le password di accesso alla piattaforma social.matteorenzi.it, nel caso in cui utilizzaste la medesima password per altri servizi vi consigliamo di cambiarla per una maggiore sicurezza. […] »

- Furto di dati sensibili degli utenti (password, orientamento politico) e violazione della Privacy;
- Sistema di sicurezza non idoneo (password salvate in chiaro);
- Reputazione e web identity danneggiati.

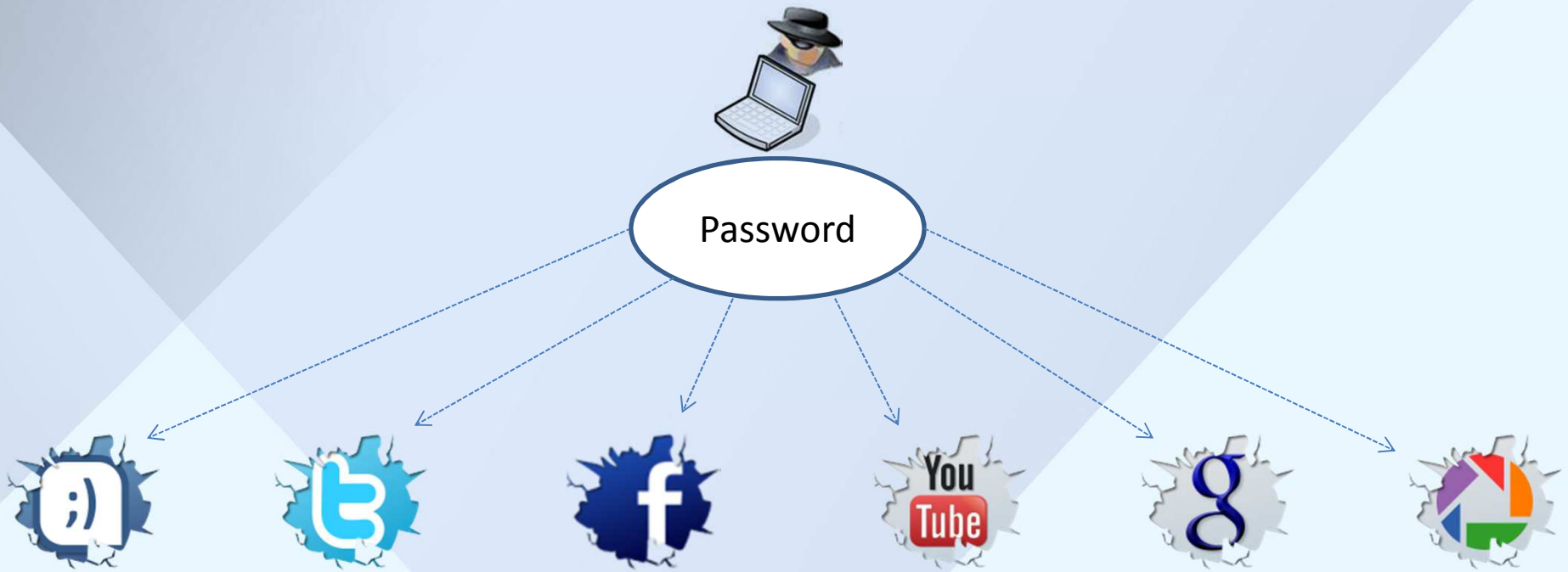
# Tipologie attacco: Social Engineering



# Tipologie attacco: 1 password → N profili

1. L' utente usa le stesse credenziali per più account
2. L' attaccante riesce ad ottenere la password (es. social engineering)

3. Ha accesso a tutti gli account

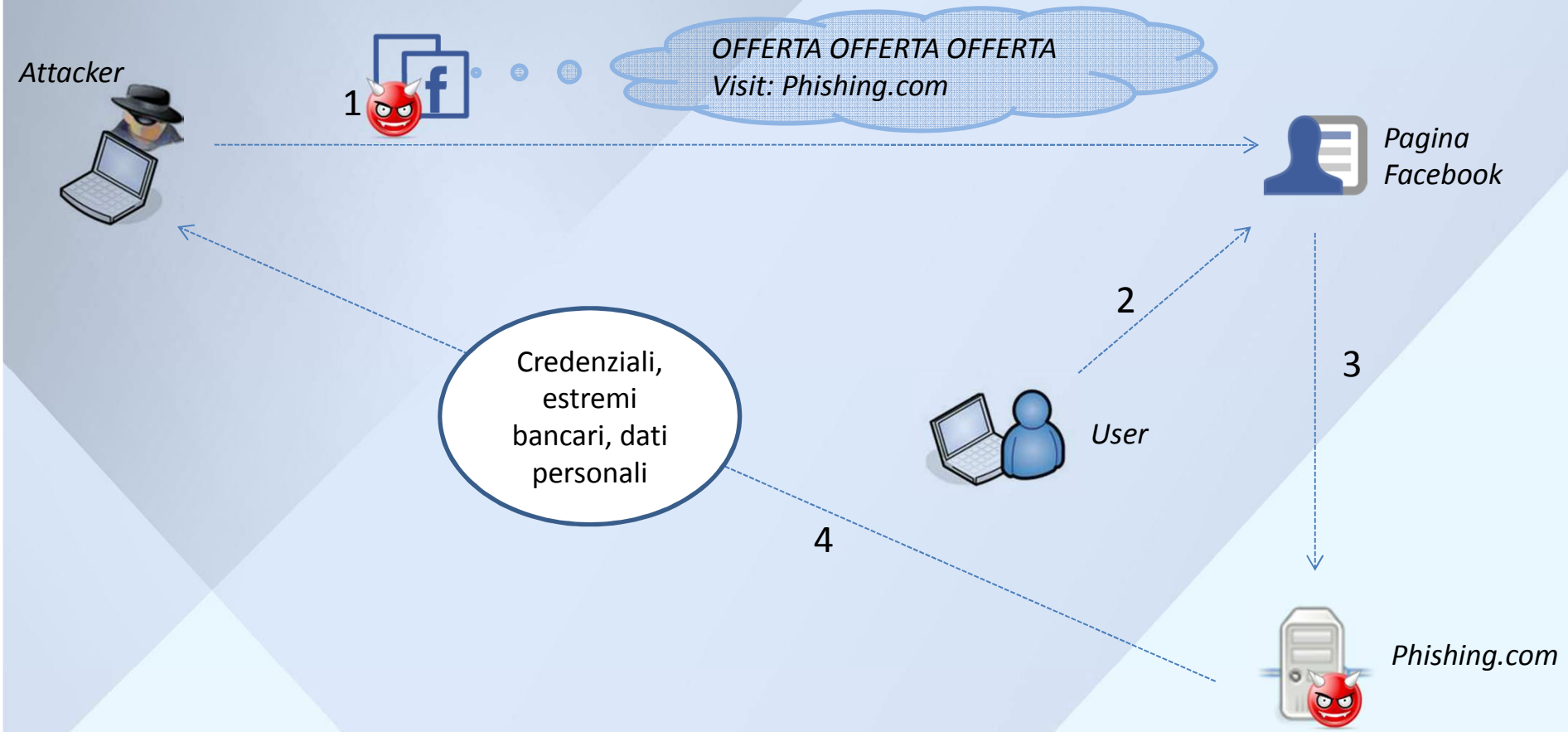


# Tipologie attacco: password riconducibili

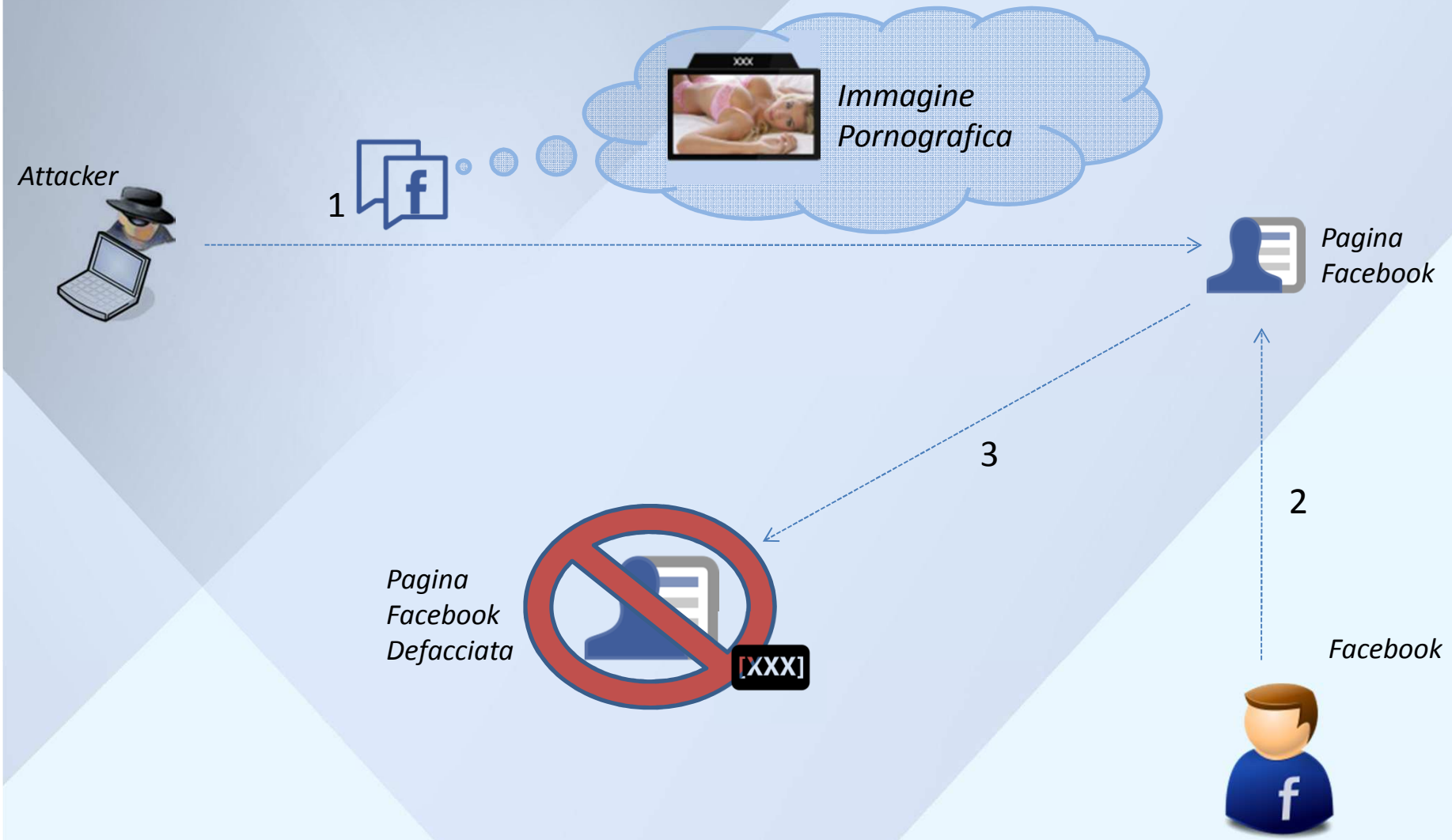
Caso concreto Casaleggio (02/2014): la password usata è l'indirizzo della sede legale


*Fonti: http://espresso.repubblica.it/attualita/2014/02/27/news/e-un-hacker-buca-anche-casaleggio-1.155130*
*http://www.tuttoindirizzi.it/a-casaleggio_associati_srl_via_santorsola_4_milano_mi_20123_0272093741-3219463.html*

# Tipologie attacco: Social Phishing



# Tipologie attacco: Social Defacing



# Social Media Security

*un ramo della sicurezza informatica che applica i principi classici di* ***confidenzialità****,* ***integrità****,* ***disponibilità*** *e* ***autenticità*** *al mondo dei social network, fondendo aspetti* ***informatico-giuridici*** *ad un* ***framework tecnologico****, con lo scopo di mitigare i rischi, presidiare le informazioni e tutelare la privacy*.

# La nostra soluzione:


Obiettivi:

- Tutela della privacy;
- Tutela del marchio e delle reputazione;
- Protezione delle informazioni sensibili;
- Presidio delle informazioni e della identità digitale;
- Prevenzione e mitigazione di attacchi informatici.

# La nostra soluzione: policy

Definizione dei ruoli e delle linee guida per l'utilizzo responsabile dei servizi social, regolamentando in particolare la sicurezza e la privacy.

Aspetti:

- Creazione di un Social Specialist Team;
- Individuazione dei ruoli e delle responsabilità;
- Gestione della sicurezza delle informazioni;
- Gestione dei flussi comunicativi e decisionali;
- Definizione di un processo di Incident Response;
- Gestione dei dati personali degli utenti;
- Gestione della Pagina Social: impostazioni, privilegi e ruoli;
- Gestione dei Contenuti: approvazione, pubblicazione e moderazione;
- Gestione delle Password;
- Trattamento dei dati sensibili;
- Tutela dell'immagine aziendale.

# La nostra soluzione: contratto

Col contratto «Social» vengono regolamentati i ruoli, le responsabilità e gli obblighi delle parti che sono stati precedentemente definiti nella policy.

Le parti:

- Azienda
- Web Agency

Gli aspetti critici/innovativi:

- Inserimento di Contenuti (origine, proprietà intellettuale, tempi e modalità);
- Inserimento di risposte standard;
- Moderazione di Contenuti;
- Gestione degli utenti (amministratori, moderatori, creatori di contenuto);
- Gestione delle credenziali (password idonee e rinnovo frequente);
- Facebook Law e rispetto della normativa vigente;
- Indisponibilità del Social Network;

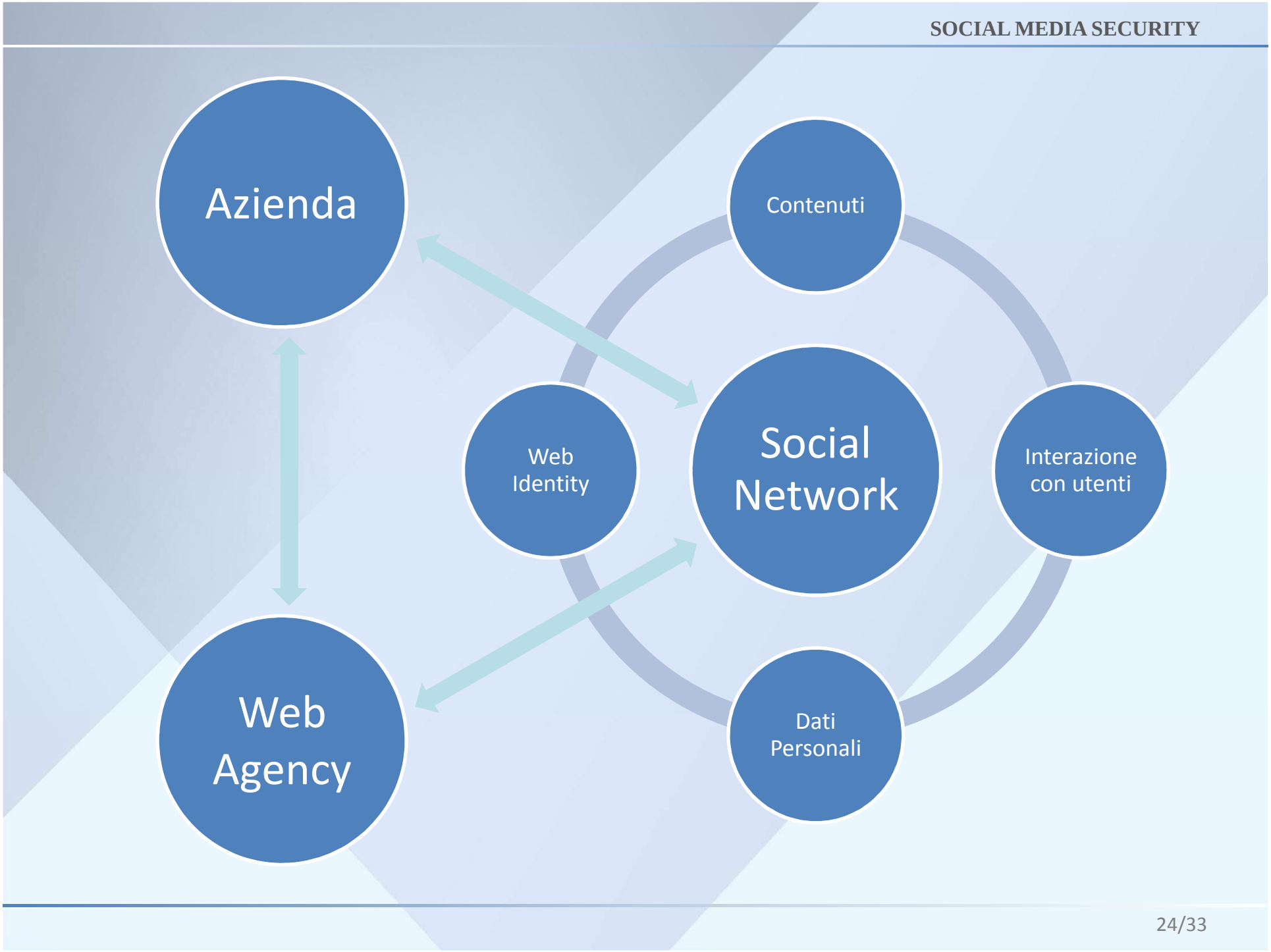
# La nostra soluzione: contratto

Gli aspetti critici/innovativi [Continua]:

- Security breach;
- Trattamento dei dati;
- Uso del Marchio;
- Diritti di proprietà intellettuale ed industriale sui Contenuti;
- Cooling off e disattivazione e consegna delle credenziali (rimozione dei contenuti ammessi, responsabilità della Web Agency).

Sono tutti aspetti che nei contratti software o di cloud computing non compaiono: perché?

I Social Network hanno una natura diversa e più complessa rispetto ad un comune software o ad un servizio di cloud; sono intrinsecamente legati a: contenuti, web identity, dati personali, interazione con utenti terzi.


Azienda
Contenuti
Web
Identity
Social
Network
Interazione
con utenti
Web
Agency
Dati
Personali

# La nostra soluzione: software

Requisiti:

- Gestione Contenuti (pubblicazione post/immagini);
- Funzionalità di sicurezza e privacy:
  - Monitoraggio Pagina Social;
  - Parsing contenuti;
  - Protezione del marchio.

Caratteristiche:

- Web-based;
- Multi-user;
- Lato server: PHP, MySQL, Facebook Graph API;
- Lato client: HTML, CSS, Javascript, Ajax, Jquery;
- Servizi esterni: geo-localizzazione.

# Software: gestione del Social Network

- Inserimento di contenuti

Insert (post)

| Post ID | Content | … |
|---|---|---|
| 231027697 | “Post 1” | … |
| … | … | … |
| 231028127 | “New Post” | … |

| Post ID | Content | … |
|---|---|---|
| 231027697 | “Post 1” | … |
| … | … | … |
| 231028127 | “New Post” | … |

- Cancellazione di contenuti

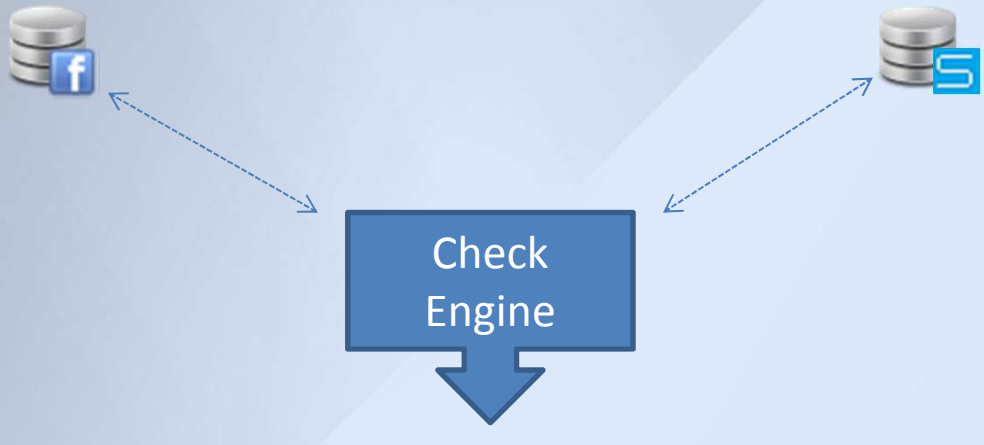
Delete (post)

| Post ID | Content | … |
|---|---|---|
| 231027697 | “Post 1” | … |
| ~~233142658~~ | ~~“Post 2”~~ | ~~…~~ |
| … | … | … |

| Post ID | Content | … |
|---|---|---|
| 231027697 | “Post 1” | … |
| ~~233142658~~ | ~~“Post 2”~~ | ~~…~~ |
| … | … | … |

# Software: Funzionalità di sicurezza

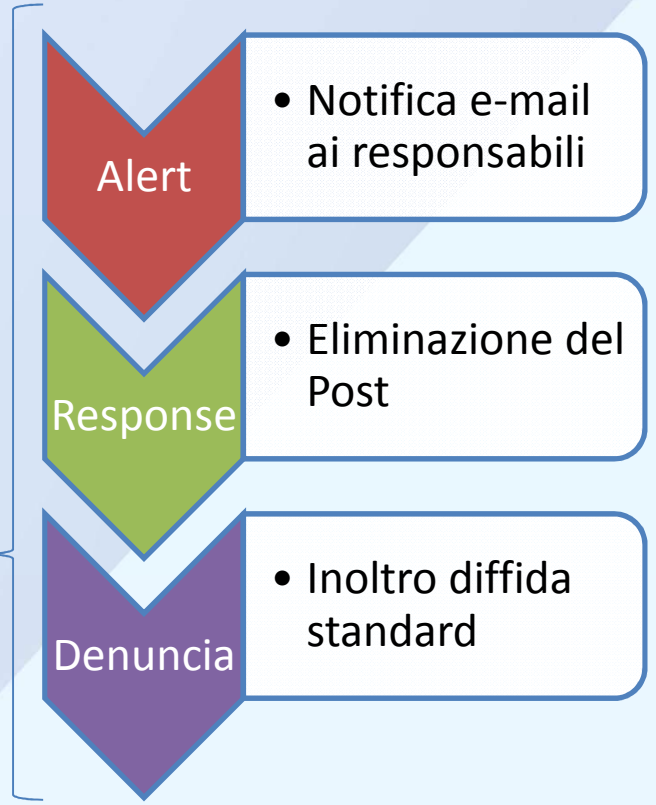
- Monitoraggio della Pagina Social




| Post ID | Content | ... |
|---|---|---|
| 111111111 | “Post 1” | ... |
| 222222222 | “Post 1” | ... |
| 999999999 | “Post Not Auth” | ... |
| ... | ... | ... |

=
=
≠
=

| Post ID | Content | ... |
|---|---|---|
| 111111111 | “Post 1” | ... |
| 222222222 | “Post 1” | ... |
| 333333333 | “Post 3” | ... |
| ... | ... | ... |



# Software: Funzionalità di sicurezza

- Parsing del contenuto

Check Engine

| Post ID | Comment | From | … |
|---|---|---|---|
| 845316874 | “Hello word” | User 1 | … |
| 963485219 | “Sex” | User 2 | … |
| … | … | | … |

- **Alert**
  - Notifica e-mail ai responsabili
- **Response**
  - Eliminazione del Commento
- **Blocco**
  - Disabilitazione utente

# Software: Funzionalità di sicurezza

- Protezione del marchio

# Problemi incontrati: API

Le API di Facebook sono orientate alla gestione dei contenuti e non alla gestione degli utenti, della sicurezza e della privacy.

Non è attualmente possibile:

- Gestire le Password;
- Modificare i privilegi degli Utenti;
- Bloccare la pagina che si gestisce.

# La privacy che verrà

- Il ruolo dei Social Network all'interno della aziende sarà sempre più determinante;
- È necessario estendere le policy e la governance aziendale anche ai Social Network;
- Vi è quindi necessità da parte delle aziende di investire sulla sicurezza nel mondo social al fine di tutelare la privacy;
- Le API devono estendersi dai servizi di base per offrire maggiore sicurezza e privacy.
- Il concetto alla base delle API deve cambiare: sono state concepite per migliorare l'esperienza dell'utente in un sito esterno al Social Network, non per gestire il Social Network stesso.

# La privacy che verrà: cosa fare in azienda

Cosa devono adottare le aziende per poter garantire la privacy delle proprie informazioni, ma soprattutto la privacy degli utenti che visitano la pagina social?

- Sensibilizzarsi al problema (la sicurezza non è solo interna al perimetro aziendale);
- Avere una policy ed un contratto che definiscano le linee guida, i ruoli e le responsabilità per una corretta gestione dei Social Media;
- Avere un piano di Incident Response per porre rimedio e limitare i danni;
- Presidiare continuamente il proprio spazio social e intraprendere le azioni necessarie ad evitare furto di dati ed attacchi informatici;
- Utilizzare un software automatico per rendere più efficace ed efficiente il presidio.

# Grazie per l'attenzione

Per qualsiasi informazione:

info@mediasocialsecurity.com
339 3128439

Simone Bonavita - Carlo Bernardi - Mattia Reggiani