Soziale Netzwerke
Vielschichtige Gefahren eines neuen Zeitalters

Marc Ruef
www.scip.ch
)SCIP(

ISSS
Information Security Society Switzerland

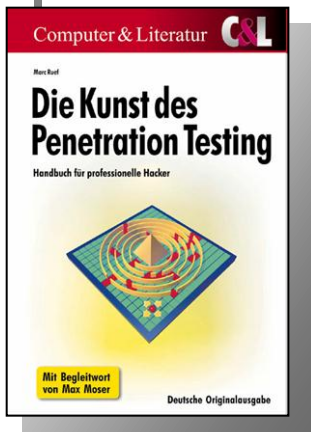
ISSS
08. Juni 2011
Zürich, Schweiz

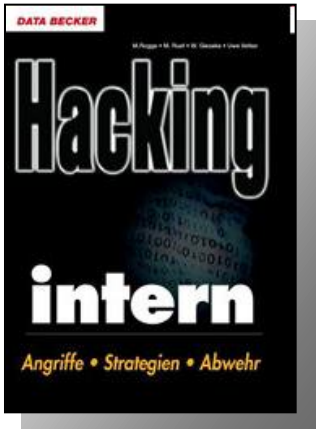
Agenda | Soziale Netze – Vielschichte Gefahren

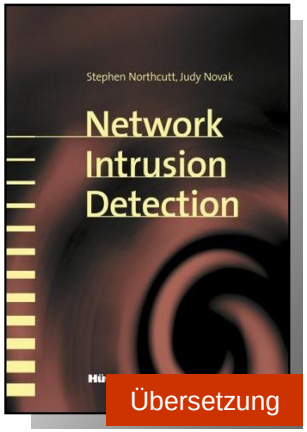
1. Intro	
Einführung	2 min
Was sind Soziale Netze?	3 min
2. Beispiele populärer Plattformen	
Facebook	2 min
Twitter	2 min
LinkedIn	2 min
3. Angriffsfläche Soziales Netzwerk	
Data Mining	5 min
Social Engineering	5 min
Malware	2 min
Massnahmen	4 min
4. Abschluss	
Zusammenfassung	3 min

Einführung | Wer bin ich

Name	Marc Ruef
Beruf	Mitinhaber / CTO, scip AG, Zürich
Private Webseite	http://www.computec.ch
Letztes Buch	„Die Kunst des Penetration Testing“, Computer & Literatur Böblingen, ISBN 3-936546-49-5







Intro
- Wer?
- Was?

Beispiele
- Facebook
- Twitter
- LinkedIn

Angriffsfläche
- Data Mining
- Social Engineering
- Malware
- Massnahmen

Abschluss
- Zusammenfassung
- Fragen

Einführung | Gefahren Sozialer Netze

Phishing sites that target social networks routinely receive the highest number of impressions per active phishing site […] but still only accounted for 4.2 percent of active sites in December, despite receiving 84.5 percent of impressions that month.

Microsoft Security Intelligence Report, Vol. 10 (2011)

Intro
- Wer?
- Was?

Beispiele
- Facebook
- Twitter
- LinkedIn

Angriffsfläche
- Data Mining
- Social Engineering
- Malware
- Massnahmen

Abschluss
- Zusammenfassung
- Fragen

Einführung | Was sind Soziale Netze?

- Webseiten mit der Möglichkeit, sich mit anderen Benutzern zu verbinden
- Aktivitäten dieser Freunde werden unmittelbar angezeigt
- Dadurch wird ein personalisierter Aktivitätsverlauf möglich

Intro
Wer?
Was?
Beispiele
Facebook
Twitter
LinkedIn
Angriffsfläche
Data Mining
Social Engineering
Malware
Massnahmen
Abschluss
Zusammenfassung
Fragen

INFO@SCIP.CH
SECURITY · CONSULTING · INFORMATION · PROCESS | T +41 44 404 13 13 | F +41 44 404 13 14
BADENERSTRASSE 551 | 8048 ZÜRICH
)SCIP(

Beispiele | Facebook – Persönlicher Kanal

Zielgruppe	
Privatpersonen, Firmen	
Verbindungen	
Freunde, Gruppen	
Zusätzliches	
Applikationen	
Gründung	
Februar 2004	Cambridge, UK
Mitarbeiter	
>2000	2011
User	
600 Millionen	Januar 2011
Ähnlich	
MySpace, Orkut, StudiVZ	

Intro
- Wer?
- Was?

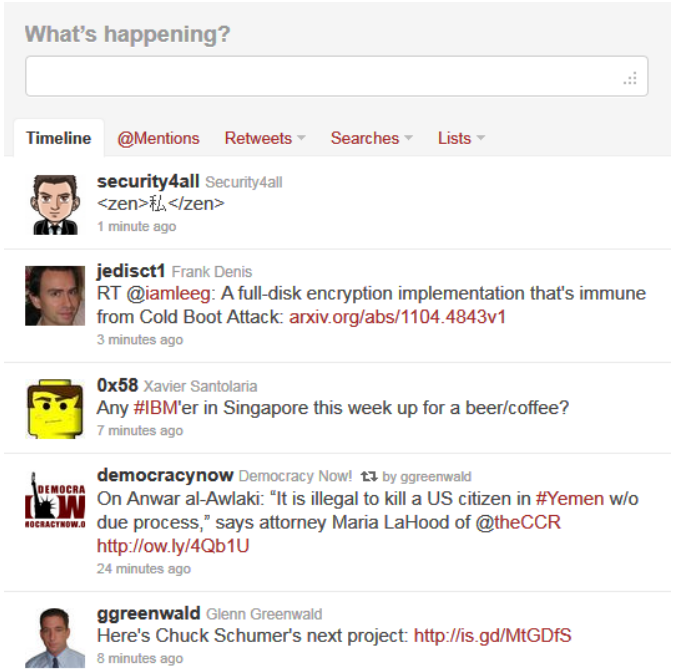
Beispiele
- Facebook
- Twitter
- LinkedIn

Angriffsfläche
- Data Mining
- Social Engineering
- Malware
- Massnahmen

Abschluss
- Zusammenfassung
- Fragen

Beispiele | Twitter – Kurznachrichten

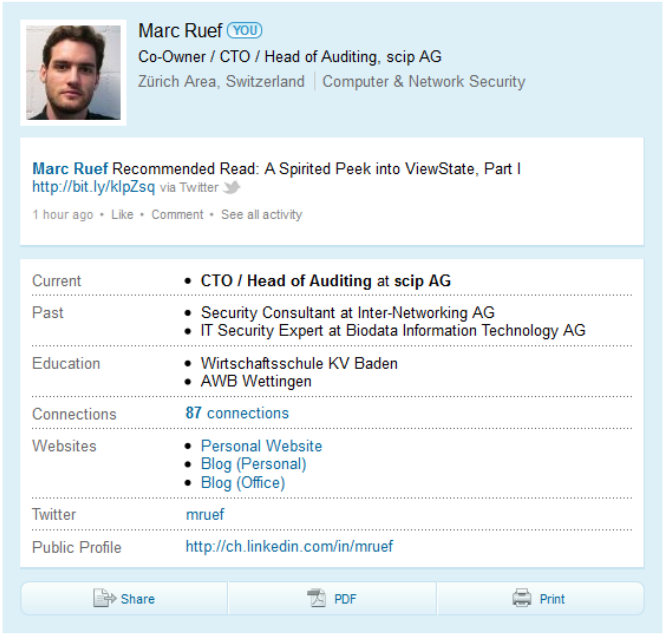
Zielgruppe	
Personen, Firmen, Bots	
Verbindungen	
Follower, Lists	
Zusätzliches	
Nachricht max. 140 Zeichen	
Gründung	
Juli 2006	Frisco, USA
Mitarbeiter	
>450	2011
User	
200 Millionen	März 2011
Ähnlich	
Google Buzz, FriendFeed	



Intro
Wer?
Was?
Beispiele
Facebook
Twitter
LinkedIn
Angriffsfläche
Data Mining
Social Engineering
Malware
Massnahmen
Abschluss
Zusammenfassung
Fragen

Beispiele | LinkedIn – Berufliches Portfolio

Zielgruppe	
Geschäftspartner, Firmen	
Verbindungen	
Connections, Groups	
Zusätzliches	
Applikationen, kommerziell	
Gründung	
Mai 2003	Santa Monica
Mitarbeiter	
>1'000	2010
User	
100 Millionen	März 2011
Ähnlich	
Xing, Plaxo, Hub Culture	



Intro
Wer?
Was?
Beispiele
Facebook
Twitter
LinkedIn
Angriffsfläche
Data Mining
Social Engineering
Malware
Massnahmen
Abschluss
Zusammenfassung
Fragen

Angriffsfläche | Data Mining – Möglichkeiten

- Veröffentlichte Informationen sammeln
  - Name, Anschrift
  - Mailadresse, Benutzerkonten, Benutzernamen
  - Fotos, Videos
  - Postings (Statusmeldungen, Kommentare)
- Verbindungen zu anderen Benutzern
  - Direkte Freunde
  - Indirekte Kontakte

Intro
- Wer?
- Was?

Beispiele
- Facebook
- Twitter
- LinkedIn

Angriffsfläche
- Data Mining
- Social Engineering
- Malware
- Massnahmen

Abschluss
- Zusammenfassung
- Fragen

Angriffsfläche | Datamining – Informationen

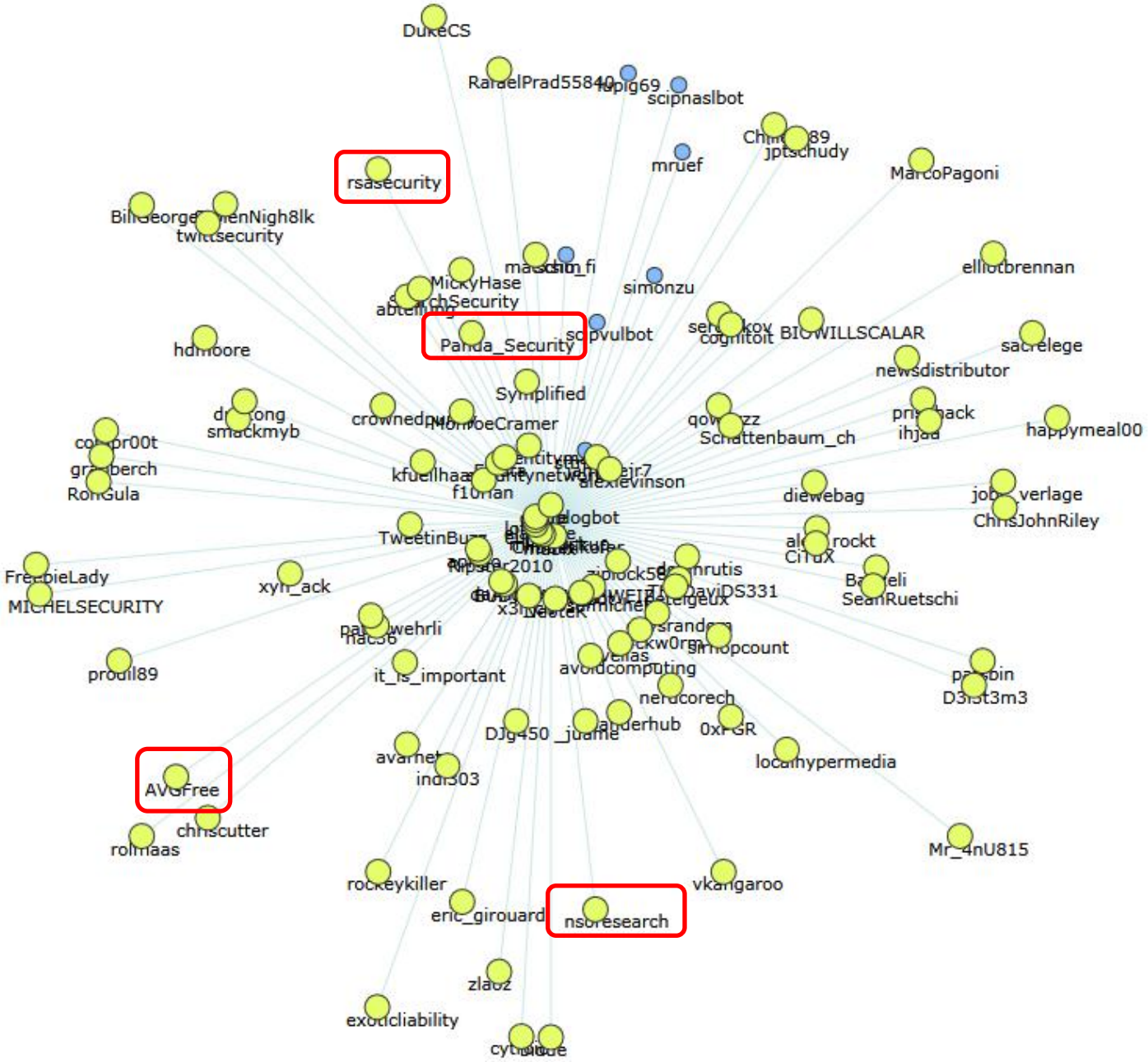
Intro
- Wer?
- Was?

Beispiele
- Facebook
- Twitter
- LinkedIn

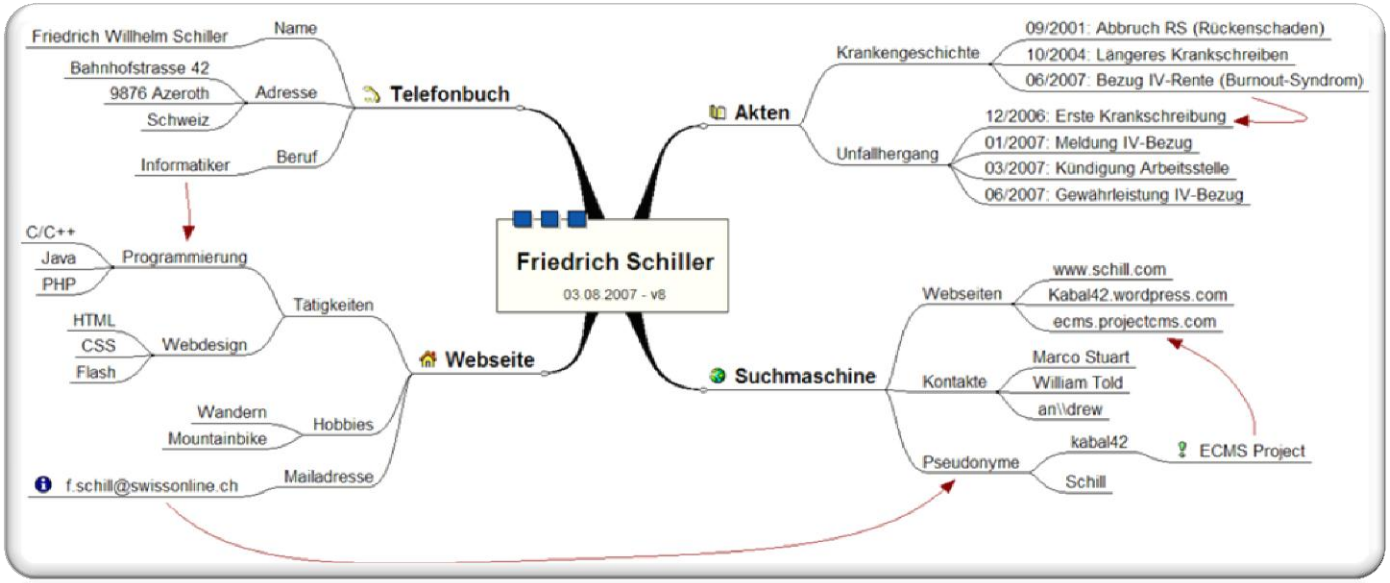
Angriffsfläche
- Data Mining
- Social Engineering
- Malware
- Massnahmen

Abschluss
- Zusammenfassung
- Fragen

Angriffsfläche | Data Mining - Verbindungen zu @scipag



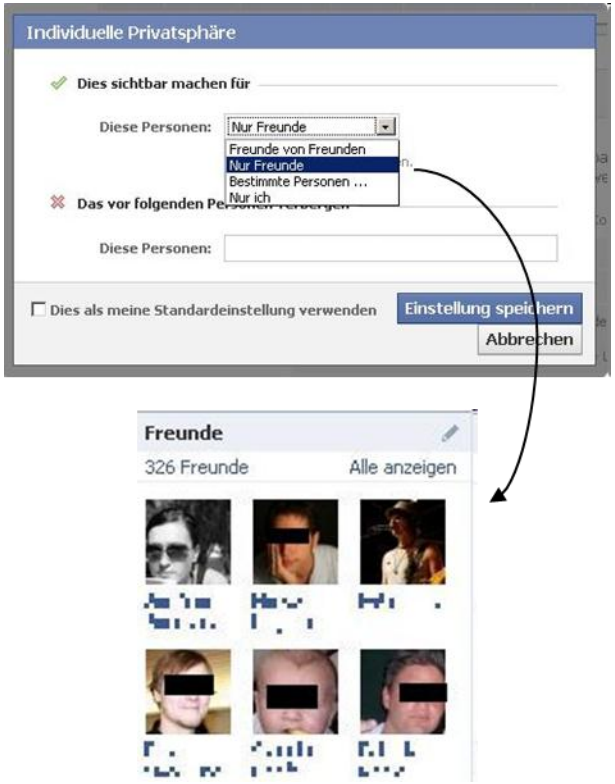
Angriffsfläche | Data Mining – Ergebnis



Intro
Wer?
Was?
Beispiele
Facebook
Twitter
LinkedIn
Angriffsfläche
Data Mining
Social Engineering
Malware
Massnahmen
Abschluss
Zusammenfassung
Fragen

Angriffsfläche | Social Engineering – Übersicht

- Ablauf
  - Kontaktaufnahme
  - Manipulation der Zielperson
  - Provokation einer kompromittierenden Handlung



Intro
Wer?
Was?
Beispiele
Facebook
Twitter
LinkedIn
Angriffsfläche
Data Mining
Social Engineering
Malware
Massnahmen
Abschluss
Zusammenfassung
Fragen

Angriffsfläche | Social Engineering – Hintergrund

- Mögliche Szenarien
  - Stalking, Mobbing
  - Informationsbeschaffung für Behörden/Versicherungen
  - Industriespionage durch Mitbewerber
  - Wirtschaftsspionage durch ausländische Dienste
  - Manipulation durch Kriminelle
- Beispiele
  - Preisgabe sensitiver Informationen
  - Herausgabe von Passwörtern
- Erfahrung
  - 84.1% unserer Zielpersonen unter 35 Jahren benutzen soziale Netze (vorwiegend Facebook)
  - 76.2% männlicher Benutzer antworten weiblichen Benutzer, trotz fehlendem Zusammenhang

Intro
- Wer?
- Was?

Beispiele
- Facebook
- Twitter
- LinkedIn

Angriffsfläche
- Data Mining
- Social Engineering
- Malware
- Massnahmen

Abschluss
- Zusammenfassung
- Fragen

Angriffsfläche | Social Engineering – Beispiel Versicherungsbetrug

Angriffsfläche | Malware – Übersicht

- Soziale Netze sind ein alternativer Kommunikationskanal
- Verbreiten von Malware ist möglich wie über Webseiten, Email und Instant Messenger
- Diverse Social Media Wurm-Epidemien schon passiert

Intro
Wer?
Was?
Beispiele
Facebook
Twitter
LinkedIn
Angriffsfläche
Data Mining
Social Engineering
Malware
Massnahmen
Abschluss
Zusammenfassung
Fragen

Angriffsfläche | Massnahmen Richtlinien Auswahl

Social Media Anbieter	Prio
Nur vertrauenswürdige Anbieter	2
Nur inländische Anbieter/Lokationen	2
Keine Zugriffe externer Anbieter/Firmen	1
Datenklassifizierung	
Nur öffentliche Daten freigeben	1
Keine Firmen-/Kundeninformationen freigeben	1
Keine Verbindungen zu Kunden (nur auf expl. Anfrage)	2
Zugriffsschutz	
Einsatz eines sicheren Passworts (mind. 6 Zeichen, ...)	1
Regelmässiges Ändern des Passworts (alle 90 Tage)	2
Zugriffe nur über gesicherte Endpunkte (Firmen-Laptops)	2
Verwaltung	
Nur unternehmensbezogene Aktivitäten	1
Nicht mehr benötigte Konten löschen	2

Intro
- Wer?
- Was?

Beispiele
- Facebook
- Twitter
- LinkedIn

Angriffsfläche
- Data Mining
- Social Engineering
- Malware
- Massnahmen

Abschluss
- Zusammenfassung
- Fragen

Angriffsfläche | Massnahmen Technisch Auswahl

Endpoint-Security (Workstation, mobile Geräte, ...)	Prio
Trennung von sensitiven und öffentlichen Bereichen	1
Hardening/Patching des Betriebssystems	1
Hardening/Patching der Software (z.B. Webbrowser)	1
Installieren einer aktualisierten Antiviren-Lösung	2
Installieren einer Personal Firewall und/oder HIPS	2
Zentraler Zugriffsschutz	
Einschränken der Zugriffe auf legitime Dienste	1
Verhindern des Downloads ausführbarer Dateien	1
Verhindern des Downloads aktiver Inhalte	2
Analysieren des Datenverkehrs mittels Antivirus	1
Verhindern des Uploads von sensitiven Daten (DLP)	1
Logging und Monitoring der Aktivitäten	2
...	

Intro
- Wer?
- Was?

Beispiele
- Facebook
- Twitter
- LinkedIn

Angriffsfläche
- Data Mining
- Social Engineering
- Malware
- Massnahmen

Abschluss
- Zusammenfassung
- Fragen

Zusammenfassung

- Einführung
  - Soziale Netze erlauben den effizienten Datenaustausch mit Gleichgesinnten
  - Durch das Verbinden mit anderen Benutzern lässt sich ein personalisierter Aktivitätsverlauf etablieren
- Beispiele
  - Es gibt verschiedene Soziale Netze, die sich bezüglich Zielgruppe und Struktur unterscheiden
  - Zu den populärsten gehören Facebook, Twitter und LinkedIn
- Angriffsfläche
  - Die grundsätzlichen Gefahren des Internets sind auch in Sozialen Netzen zu berücksichtigen
  - Sowohl Richtlinien als auch technische Massnahmen erlauben einen sicheren Umgang mit diesem Kommunikationskanal

Intro
Wer?
Was?
Beispiele
Facebook
Twitter
LinkedIn
Angriffsfläche
Data Mining
Social Engineering
Malware
Massnahmen
Abschluss
Zusammenfassung
Fragen

Quellen

- Microsoft Security Intelligence Report, Vol. 10 (2011), http://www.microsoft.com/security/sir/
- Schutzmassnahmen in Sozialen Netzen (2010), http://www.scip.ch/?labs.20100423

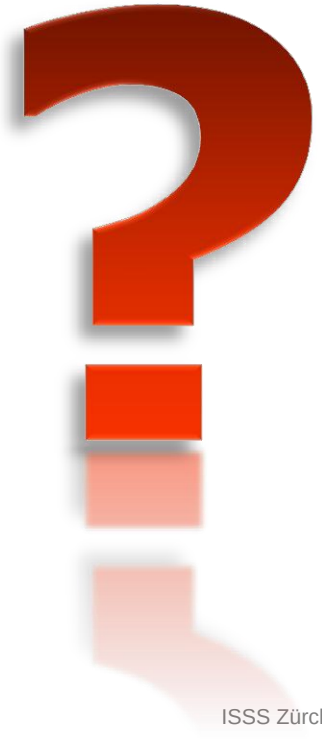
Intro
- Wer?
- Was?

Beispiele
- Facebook
- Twitter
- LinkedIn

Angriffsfläche
- Data Mining
- Social Engineering
- Malware
- Massnahmen

Abschluss
- Zusammenfassung
- Fragen

Fragen



Intro
- Wer?
- Was?

Beispiele
- Facebook
- Twitter
- LinkedIn

Angriffsfläche
- Data Mining
- Social Engineering
- Malware
- Massnahmen

Abschluss
- Zusammenfassung
- Fragen

Security is our Business!

scip AG
Badenerstrasse 551
CH-8048 Zürich

Tel +41 44 404 13 13
Fax +41 44 404 13 14
Mail info@scip.ch
Web http://www.scip.ch
Twitter http://twitter.com/scipag

)SCIP(

☑ Strategy | Consulting
☑ Auditing | Testing
☑ Forensics | Analysis