

Social Engineering

-

Der Mensch als Exploit

Marko Rogge

Haking – Security – Journalismus
<http://www.marko-rogge.de>

2. SLAC // Heinlein Support
Berlin 2007

Grundsätzlich

- Jeder Mensch hat seinen Preis, käuflich ist zu 99% jeder Angestellte
- Schlechte Motivation der Mitarbeiter/Arbeitnehmer
- Mangelnde Teambildung um die Gemeinschaft zu fördern
- Administratoren sind oftmals „Heilige“, dennoch Alleinstellung
- Finanzsituation einzelner Mitarbeiter schlecht
- Wettbewerbsdruck am freien Markt
- Aufstiegschancen gering – persönliche Entwicklung gebremst
- Persönliche Situation unbefriedigend - Profilierung
- Unwissenheit



Social Network: Einfallstor im Web 2.0

The image displays two web pages side-by-side. On the left is the XING website, featuring a search bar with the text 'Suche: [Name, Firma oder andere Suchwörter] Finden' and a navigation menu with links like 'Guided Tour', 'Kontakt', 'Hilfe', 'Über uns', 'Jobs', and 'Sprache'. Below the search bar, there's a section titled 'Einzigartige Suchfunktionen' (Unique search functions) with a list of bullet points: 'Finden Sie neue Vertriebskanäle, Mitarbeiter und Jobs', 'Finden Sie schnell die richtigen Entscheidungsträger', and 'Erreichen Sie Ansprechpartner tausender Unternehmen'. There are also sections for 'Professionelles Kontakt-Management' and 'Business-Beschleuniger'. At the bottom, it says 'XING in der Presse:' followed by logos of various media outlets like DIE ZEIT, Frankfurter Allgemeine, WELT, SONNTAG, FOCUS, DER SPIEGEL, BUSINESS 2.0, Capital, and Wirtschafts Woche.

On the right is the iLove website, which has a search bar with the text 'Suche: [Name, Firma oder andere Suchwörter] Finden' and a navigation menu with links like 'SUCHE', 'GALERIE', 'CHAT', 'MAGAZIN', 'HILFE?', and 'ANMELDEN und LOSFLIRTEN!'. Below the search bar, there's a section titled 'Jetzt kostenlos anmelden!' (Sign up for free now!) with a list of bullet points: 'Finden Sie neue Vertriebskanäle, Mitarbeiter und Jobs', 'Finden Sie schnell die richtigen Entscheidungsträger', and 'Erreichen Sie Ansprechpartner tausender Unternehmen'. There are also sections for 'Professionelles Kontakt-Management' and 'Business-Beschleuniger'. At the bottom, it says 'XING in der Presse:' followed by logos of various media outlets like DIE ZEIT, Frankfurter Allgemeine, WELT, SONNTAG, FOCUS, DER SPIEGEL, BUSINESS 2.0, Capital, and Wirtschafts Woche.

Below the screenshots, there is a list of social networks and services: XING, iLove, Friendscout24, Parship, LinkindIn, Elitepartner.de, Neu.de, Blogs, Podcasts uvm.

At the bottom of the image, there is a section titled 'Die moderne Form des Exhibitionismus!' (The modern form of exhibitionism!) and a list of services: Datensammlung für Spione, Hacker, Angreifer, Staat, Geheimdienste ...

XING, iLove, Friendscout24, Parship
LinkindIn, Elitepartner.de, Neu.de,
Blogs, Podcasts uvm.

Die moderne Form des Exhibitionismus !

Datensammlung für Spione, Hacker, Angreifer, Staat, Geheimdienste ...

XING – Das perfekte Werkzeug

Wirtschaftsspionage
leicht gemacht.

Mitglieder – Das Potential:

- Selbständige / Freiberufler
- Geschäftsführer
- Entscheidungsebene
- Administratoren
- Mitarbeiter / Vertriebler

Vermeintliche
Erfolgsaussichten

XING 18.719 Mitglieder online

Suche: **Finden**

+ Kontakte einladen 0 0

Start Mitglieder Nachrichten Adressbuch Gruppen Termine Marketplace PremiumWorld

Meine Startseite Mein Profil Profil bearbeiten Einstellungen Mitgliedschaft

Marko Rogge

Marko Rogge
Marko Rogge
Frankfurt/Main, Deutschland

Options:
Businessdaten bearbeiten
Kontaktdaten bearbeiten
Web-Daten bearbeiten
"Über mich"-Seite bearbeiten

Meine Einladungen
gesamt:
erfolgreich:
Premium-Mitglieder:

Empfehlen Sie XING!
» Für jeweils 10 erfolgreiche Einladungen erhalten Sie einen Monat Premium-Mitgliedschaft gratis.

Statistiken von Marko Rogge:
2 Gruppenmoderator
2 Premium-Mitglied
Mitglied seit: 05/2004
Seitenaufrufe: 13.395
Direkte Kontakte: 361
Aktivitäts-Index: 100%

Aufrufe meines Profils
» Mitglieder, die mein Profil kürzlich aufgerufen haben
» Mitglieder, deren Profil ich kürzlich aufgerufen habe
» Mitglieder, die kürzlich meine Firmen-Homepage angeklickt haben
» Mitglieder, die kürzlich eine meiner vorherigen Firmen-Homepages angeklickt haben

Businessdaten Kontaktdaten Web Über mich Gästebuch

Status Freiberufler

Ich suche Verlage, Branchenkontakte, IT-Sicherheit, Datenschutz, Hacking, Security, Kollegen, Journalisten, Beratern EDV-Sicherheit und Datenschutz, EDV Verlage, für die Verbreitung von Publikationen aus meiner "Feder", Veranstalter, Vorträge, Hacking, Security, Mobile Security, und, Hacking, interessante Kontakte, Linux Anwender

Ich biete Penetrationstests, Security Analysen, IT-Sicherheits-Tests, Scans, Analysen, Netzwerkberatung, IT-Sicherheitsberatung, Schulungen, Vorträge Security & Hacking, Moderation von EDV Veranstaltungen, Bluetooth Hacking, Mobile Hacking, Linuxinstallation, Support, Linux Integration, Debian Linux, Ubuntu Linux, Fedora Linux

Firma Marko Rogge: Marko Rogge

Branche IT-Grundschutz, IT-Sicherheit, Vorträge Hacking, Security, Unternehmensberatung, IT-Journalismus, Security-Analysen, Moderation von EDV Veranstaltungen

Weitere derzeitige Firmen

• Hakin9: Autor		(03/2007 -)
• F-Secure: freie Kooperation, Referent		(2006 -)
• Penton Median GmbH: Moderator, Referent		(2005 -)
• Datenschutz-Berater / Handelsblatt		(2004 -)

XING - Authentisch?

Wer mit wem und wer bin ich?

- Wie echt sind die Daten, die eingestellt sind?
- Ist die Person existent?
- Stellt die Google-Suche ein Kriterium der Recherche dar?
- Sind Querverbindungen zuverlässig? Personen daraus bekannt?
- Profildaten sind aussagekräftig?

- Kein Post-ID Verfahren bei der Anmeldung oder dergleichen !

Sind Sie sicher?



XING - Möglichkeiten

Horst Schlämmer.

- Horst Schlämmer und Stromberg waren Mitglieder.
- Falsch aber offensichtlich. Aber ist das auch sicher?
- Marko Rogge - https://www.xing.com/profile/Marko_Rogge/
- Dr. Stephan Weiershausen?

- Falsche Identitäten bewusst erstellen um Schaden zu erreichen
- Echte Identitäten erstellen (Marko Rogge) mit falschen Inhalten
- Mobbing, Denunzierung

Identitätsdiebstahl ist eine Straftat.



XING - Vertrauen?

Aufbau von Vertrauen für gezielte Eingriffe.

- Einbringen einer Backdoor/Trojaner/Spyware in das Netzwerk über Zugriff
- Zusenden von „wichtigen“ Informationen per Mail
(Ich habe Ihnen was „wichtiges“ zugeschickt, schauen Sie mal rein!)
- Sicherheitsanalyse ist auch eine Analyse?
- gezieltes Abwerben von Mitarbeitern dient als Vorwand
- zeitlich unbegrenztes Aufbauen von Vertrauen



XING – Die Jobmaschine

XING Marketplace:
Die Job & „Spionagebörse“

Was verraten Jobangebote?

- Eingesetzte Sicherheitssysteme
- Betriebssysteme Desktop/Server
- Eingesetzte Anwendungen
- Programmiersprachen
- Netzwerkstrukturen

Probearbeiten: Backdoor einschleusen.

Vorstellungsgespräch: Informationsbeschaffung.



The screenshot shows the XING Marketplace website interface. At the top, there is a navigation bar with a green 'Marketplace' button and a dark green 'PremiumWorld' button with a red 'NEU!' badge. Below the navigation bar, there are links for 'Angebot erstellen' and 'Meine Angebote'. The main content area features a blurred image of a person's face on the left and a text box on the right. The text box contains the heading 'Auf XING Marketplace anbieten', a paragraph describing the service: 'Ihr Stellenangebot an Millionen qualifizierte Fach- und Führungskräfte aus allen Branchen und Regionen. Erstellen Sie Ihre Stellenanzeige in wenigen Schritten und stellen Sie sie sofort online.', and a green button labeled 'Auf Marketplace anbieten'.

Fazit

Nichts ist wie es scheint ...

Flirten, Chatten, Daten ...Datendiebstahl

Zwanglose Kontakte
Erfüllung von Wünschen
Eingehen auf Sehnsüchte

Mehr als 2 Millionen
Mitglieder in iLove*

Große Flirtportale buhlen
um Mitglieder.

Frauen kostenlos.
Männer ca. 5,- € je Woche

*Angabe iLove

The screenshot shows the iLove website interface. At the top left is the iLove logo with the tagline "Dating, Flirten, Freunde finden". To the right is a login section with fields for "Login:" and "Passwort:" and a "Los" button. Below the login fields are checkboxes for "Automatisch einloggen" and "Passwort vergessen?". A navigation bar contains links for HOME, SUCHE, GALERIE, CHAT, MAGAZIN, HILFE ?, and ANMELDEN und LOSFLIRTEN!. The main content area is divided into several sections:

- Schnellsuche:** Search filters including "Ich bin:" (Mann), "und suche:" (Frauen), "zwischen:" (18-30), "Land:" (Deutschland), "Ort / PLZ:", and "Umkreis*:" (20 km). A "Suchen" button and "Weitere Suchkriterien..." link are present.
- Gerade Online:** A table showing 6089 users online:

Frauen	2808
Männer	3281
- Jetzt kostenlos anmelden!** A large banner with a photo of a couple and a "GO!" button.
- Aktuell bei iLove:** A section with three featured items:
 - Lovestories:** "Der erste Heiratsantrag über iLove! Mehr" with a photo of a couple.
 - TV Casting:** "iLove Casting ab ins Fernsehen! Mehr" with a photo of a TV set.
 - Online Flirten:** "11 erfolgreiche Tipps zum Online flirten!" with a photo of a woman.
- TOP SINGLES:** A carousel of five profile pictures with names: aipir..., hotpam8, hereisme, kreta198..., and ge.

At the bottom, there is a footer with links for Impressum, AGB, Partnerprogramm, Presse, Jobs, and Regional Katalog, and a "powered by Jamba!" logo.

Flirtbörsen – Date(n) per Klick

- Millionenschäden durch privates Surfen am Arbeitsplatz
- Plauderlaune von Angestellten in nicht hohen Positionen
- Erschleichen von Vertrauen ohne die Person zu kennen
(Auch hier: Identitätsdiebstahl, Ausnutzen von Unwissenheit)
- Verlagerung der Kommunikation vom Portal zu E-Mail direkt
(ilove.de nach m.rogge@musterfirma.de)
- Angabe des Berufes, Stellung in der Firma
- Empfänglichkeiten von Frauen und Männern
- definierte Erfüllung der Wünsche, Träume, Sehnsüchte
- Informationsweitergabe an den Wettbewerb

Einfallsvektoren - Weiterführend

- Unwissenheit über die Brisanz von Informationen: Der Mensch
- CDs überreichen: Inhalt ist nicht bekannt, auch wenn der Aufdruck echt scheint
- USB Devices: mechanische Sperren kaum gegeben
- Instant Messenger: Informationen verlassen via Chat das Unternehmen
- Ego: fehlendes Feedback für die Arbeit, daher schneller Vertrauen in Fremde
- Smalltalk im Café, in öffentlichen Verkehrsmitteln, Bars, Clubs
- Bestechung, Hilfsbereitschaft, Vertrauensmißbrauch



Fazit und Abhilfe

- Bewusstsein schärfen (Persönlichkeiten ausgrenzen)
- Unternehmerisches Denken fördern
- Definierte Information über Weitergabe von Daten und Informationen
- Sensibel mit Informationen und Daten umgehen
(2x Fragen kostet nichts, nicht fragen kann aber den Arbeitsplatz kosten)
- Management muss handeln – Vorbildfunktion
- Datenschutz Regeln aufstellen, aktiv weiterführen



Danke für die Aufmerksamkeit

Sie haben Fragen?

Marko Rogge

<http://www.marko-rogge.de>

Marko Rogge ist als Autor und freier Journalist in der DV-Branche groß geworden und hat bereits diverse Publikationen für Printmedien abgeliefert.

Tätigkeitsschwerpunkte der Unternehmensberatung sind die Bereiche IT-Grundschutz und IT-Security in Unternehmen sowie die aktive Unterstützung bei der Einführung von Unternehmensdatenschutz. Hierfür stehen fachlich kompetente Partner zur Seite.

Als Moderator und Referent beteiligt sich Marko Rogge aktiv an der effektiven Informationsverbreitung zur Verbesserung von IT-Grundschutz und Zertifizierungen in Unternehmen.

Darüber hinaus engagiert er sich in freien Projekten, die sich gegen die Internetzensur richten.

