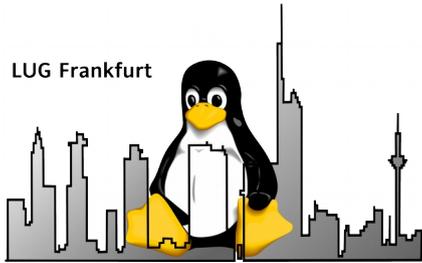


SOCIAL ENGINEERING

Dr. Christoph Zimmermann

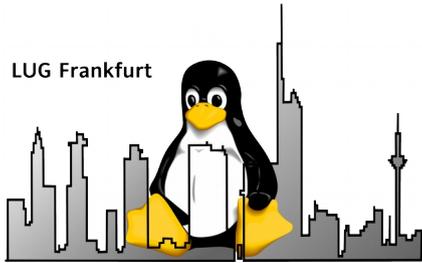
FraLUG

25. August 2015



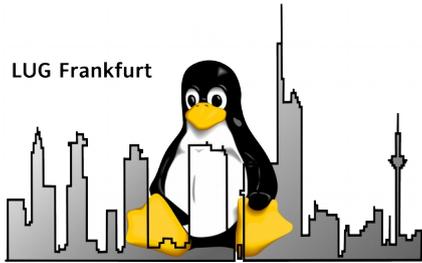
Übersicht

1. Einführung
2. Ablauf
3. Hintergründe
4. Vorbeugung
5. Weiterführendes

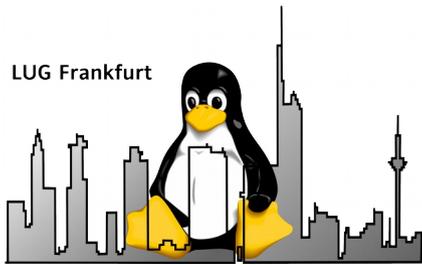


Einführung

- „Cyberattacke: Computernetz des Bundestags droht Totalschaden“ (Spiegel Online, 10. 6. 2015)
- „ISIS Hacker übernehmen Kontrolle über TV5Monde Gruppe während eines noch nie dagewesenen Angriffs“ (The Telegraph, 9. April 2015)
- „Angriff auf Firmennetz: Hacker stellen Sony-Mitarbeiter bloß“ (Spiegel Online, 4. 12. 2014)
- „Kassen der US-Handelskette Target über Hausmeisterzugang gehackt“ (Heise online, 8. 2. 2014)

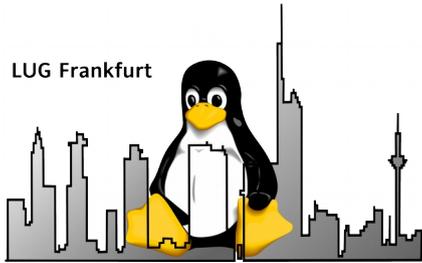


- Social Engineering:
„Zwischenmenschliche
Beeinflussungen mit dem Ziel, bei
Personen bestimmte Verhalten
hervorzurufen.“ (Wikipedia)



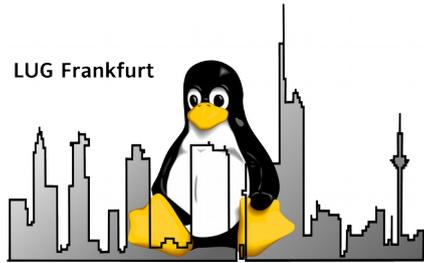
Bundestagsangriff

- Emails mit Merkels Büro als vermeintlichem Absender
- Infizierung einzelner Rechner via Email-Anhang bzw. Links in Emails („Terminverschiebung einer Ausschußsitzung“)
- Ausspähung größerer Teiler der Infrastruktur inkl. mehrerer Domänenstrukturen
- Infizierung immer größerer Teile der Desktops + Server-Landschaft
- Möglich: komplette Übernahme der Kontrolle via C+C



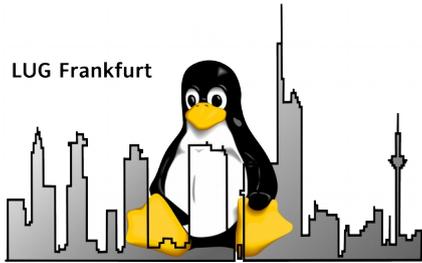
Bundestagsangriff II

- Merkmale:
 - Vermeintliche Autorität als Absender
 - Schrittweises Vorgehen
 - Zwiebel-Taktik bei Überwachung / Übernahme
 - Längerer Zeitraum
 - Aktuelle Malware-Technologie bzw. wahrscheinlich veraltete Sicherheits-Produkte



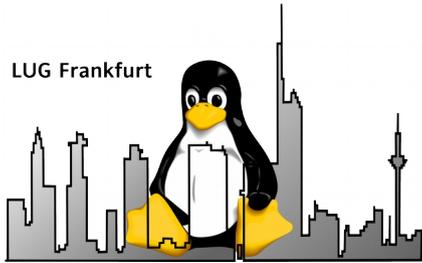
Ablauf

- Z. B. Pen-Testing (*SE-Teile*):
 - *Informationsbeschaffung*
 - *Informationsextraktion*
 - *Angriff:*
 - Weiterführende Aktionen
 - Abschluß / Bericht



Beschaffung

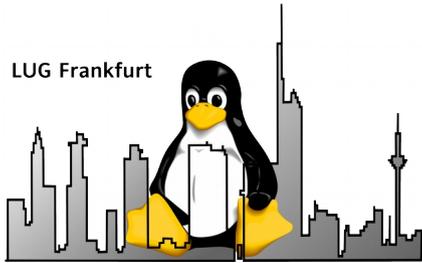
- Öffentlich zugängliche Quellen:
 - Soziale Netzwerke
 - Websites (inkl. Firmenauftritte)
 - Automatisierungs-Tools (z. B. maltego)
- Dumpster Diving
- Maschinelle Untersützung:
 - Z. B. (Spear) Fishing Kampagnen (Emails)
 - Aber auch: USB-Speicher mit infizierten PDF-Dateien



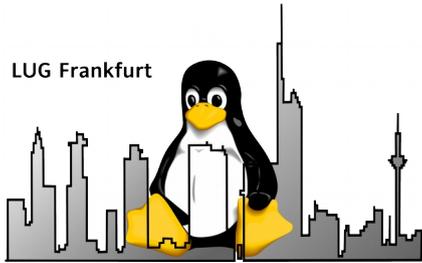
Extraktion

- Interaktion mit Zielperson(en)
- Ziel: maximale Informationsgewinnung
- Mechanismen u. a.:
 - Geistige Einstellung (Preloading)
 - Rapport-Bildung
 - Wahl des Egos (Pretexting)
 - Fragetechniken
 - Wahrnehmungsmanipulation (Framing)

Angriff

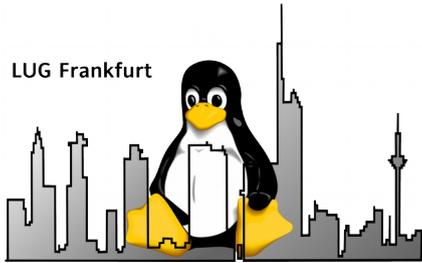


- Kombination aus
 - Social Engineering Techniken
 - Maschinellen / Automatisierungs-Werkzeugen:
 - Metasploit
 - Effektive Verknüpfung basierend auf Aufgabenstellung



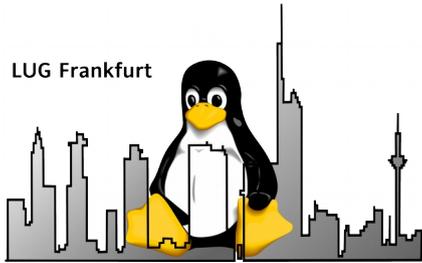
Hintergründe

- Evolutionsbiologie:
 - Helfer-Syndrom
 - Südkurve am Samstag
- Gruppendynamik:
 - Inklusion
 - Tailgating
- Kognitive Psychologie:
 - Bewusste / unbewusste Wahrnehmung



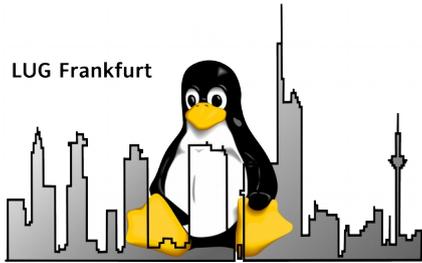
Hintergründe II

- Neurolinguistische Programmierung (NLP):
 - Rapport-Bildung
 - Reframing
- Kommunikationstheorie:
 - Fragetechniken, z. B. offen / geschlossen
 - Körpersprache



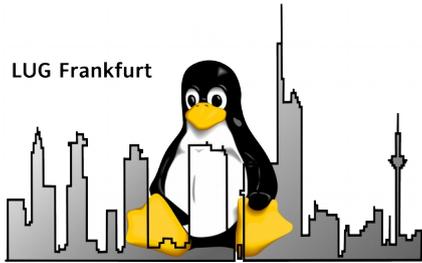
Vorbeugung

„Wenn Du Deine Feinde und Dich selbst kennst, brauchst Du die Folgen von hundert Schlachten nicht zu fürchten“ (Sun Tzu, Die Kunst des Krieges, ca. 500 B.C.)



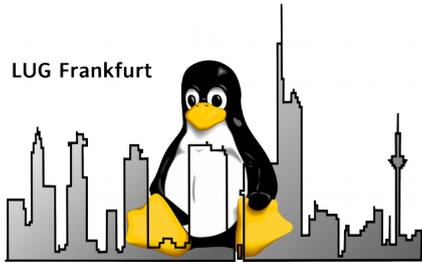
Vorbeugung II

- Analyse
- Risiko-Bewertung
- Festlegung von Richtlinien:
 - Kommunikation (PR, soziale Medien, etc.)
 - IT
 - (Physische) Sicherheit (inkl. Autorisierung, Authentifizierung, etc.)



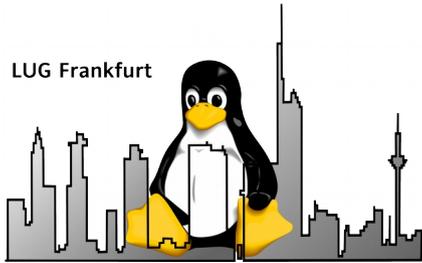
Vorbeugung III

- Schulung:
 - Erkennen von Vektoren
 - Umsetzung und Einhaltung von Richtlinien
 - Vermeidung von Angriffen
- Audits (regelmäßig + extern!):
 - Umfang
 - Dauer
 - Kosten
 - Ergebnis / Kommunikation



Vorbeugung IV

- Audit-Regeln:
 - Klare Definition von Zielen und Dauer
 - Keine Entlassung von Mitarbeitern!
 - Ergebnisse sollten aufgrund von Vorgaben reproduzierbar sein
 - NDAs (!) / Referenzen



Weiterführendes

- social-engineer.org (inkl. Podcast)
- Kevin Mitnick:
 - Die Kunst der Täuschung
 - Das Phantom im Netz
- Chris Hadnagy:
 - Die Kunst des Human Hacking
 - Social Engineering enttarnt