SOCIAL ENGINEERING

The art of hacking humans

Christoph

28. Januar 2016

Übersicht

OWASP
The Open Web Application Security Project

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

Einführung

OWASP
The Open Web Application Security Project

„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)

„ Attacke 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

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

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

Ablauf

OWASP
The Open Web Application Security Project

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

Beschaffung

OWASP
The Open Web Application Security Project

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

Extraktion

OWASP
The Open Web Application Security Project

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

Angriff

OWASP
The Open Web Application Security Project

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

Hintergründe

OWASP
The Open Web Application Security Project

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

Hintergründe II

OWASP
The Open Web Application Security Project

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

Vorbeugung

OWASP
The Open Web Application Security Project

„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

OWASP
The Open Web Application Security Project

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

Vorbeugung III

OWASP
The Open Web Application Security Project

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

Vorbeugung IV

OWASP
The Open Web Application Security Project

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

Weiterführendes

OWASP
The Open Web Application Security Project

- 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

Weiterführendes II

OWASP
The Open Web Application Security Project

- Kognitive Psychologie:
  - Paul Ekman: Gefühle lesen; Ich weiss, daß Du lügst,
  - Joe Navarro: Menschen lesen
- NLP:
  - Robin Dreeke: It's not all about me
- Phishing:
  - Chris Hadnagy: Phishing dark waters

OWASP
The Open Web Application Security Project

Diskussion