

DIE KUNST DES HUMAN HACKING

CHRISTOPHER HADNAGY

Social Engineering – Deutsche Ausgabe



Inhaltsverzeichnis

	Vorwort	11
I	Ein Blick in die Welt des Social Engineering	19
1.1	Warum dieses Buch so wertvoll ist	21
	1.1.1 Das Layout	22
	1.1.2 Was zu erwarten ist	24
1.2	Social Engineering im Überblick	29
	1.2.1 Social Engineering und sein Platz in der Gesellschaft	34
	1.2.2 Verschiedene Typen von Social Engineers	39
	1.2.3 So nutzen Sie das Social Engineering-Framework ..	42
1.3	Zusammenfassung	44
2	Informationssammlung	45
2.1	Informationen sammeln	48
	2.1.1 Die Arbeit mit BasKet	49
	2.1.2 Die Arbeit mit Dradis	51
	2.1.3 Denken wie ein Social Engineer	53
2.2	Quellen zur Informationssammlung	58
	2.2.1 Informationen von Websites abgreifen	58
	2.2.2 Die Macht der Observation	64
	2.2.3 Den Müll durchwühlen	65
	2.2.4 Die Arbeit mit Profiling-Software	67
2.3	Kommunikationsmodellierung	69
	2.3.1 Das Kommunikationsmodell und seine Wurzeln	71
	2.3.2 Ein Kommunikationsmodell entwickeln	75
2.4	Die Macht der Kommunikationsmodelle	79
3	Elizitieren	81
3.1	Was ist Elizitieren?	82

3.2	Ziele des Elizitierens	85
3.2.1	Preloading	89
3.2.2	Elizitieren erfolgreich einsetzen	95
3.2.3	Intelligente Fragen stellen	101
3.3	Elizitieren meistern	106
3.4	Zusammenfassung	108
4	Pretexting – In eine andere Haut schlüpfen	109
4.1	Was ist Pretexting?	111
4.2	Prinzipien und Planungsphasen beim Pretexting	112
4.2.1	Je mehr Sie recherchieren, desto besser sind die Erfolgchancen	113
4.2.2	Der Einbau persönlicher Interessen steigert den Erfolg	114
4.2.3	Üben Sie bestimmte Dialekte und Redensarten.	117
4.2.4	Telefonnutzung sollte den Aufwand für den Social Engineer nicht reduzieren.	119
4.2.5	Je einfacher der Pretext, desto größer die Erfolgswahrscheinlichkeit	121
4.2.6	Der Pretext sollte spontan wirken	124
4.2.7	Liefern Sie der Zielperson einen logischen Schluss oder Anschlussauftrag	126
4.3	Erfolgreiches Pretexting	127
4.3.1	Beispiel 1: Stanley Mark Rifkin	127
4.3.2	Beispiel 2: Hewlett-Packard	130
4.3.3	Legal bleiben	133
4.3.4	Weitere Tools fürs Pretexting	134
4.4	Zusammenfassung	136
5	Gedankentricks – Psychologische Prinzipien im Social Engineering.	137
5.1	Formen des Denkens	139
5.1.1	Die Sinne	140
5.1.2	Die drei wichtigsten Denkmodi	141
5.2	Mikroexpressionen	147
5.2.1	Wut.	150
5.2.2	Ekel.	152

	5.2.3	Verachtung	154
	5.2.4	Angst	156
	5.2.5	Überraschung	159
	5.2.6	Traurigkeit	161
	5.2.7	Glück	164
	5.2.8	Mikroexpressionen selbst erkennen	166
	5.2.9	Wie Social Engineers Mikroexpressionen nutzen	169
5.3		Neurolinguistisches Programmieren	177
	5.3.1	Die Geschichte des neurolinguistischen Programmierens	178
	5.3.2	Die NLP-Codes	179
	5.3.3	NLP beim Social Engineering nutzen	180
5.4		Interviews und Vernehmungen	185
	5.4.1	Professionelle Befragungstaktiken	187
	5.4.2	Gestikulieren	198
	5.4.3	Die Haltung von Armen und Händen	201
	5.4.4	Den Weg zum Erfolg »erhören«	203
5.5		Schnell Rapport aufbauen	209
	5.5.1	Seien Sie authentisch bei dem Wunsch, Menschen kennenzulernen	210
	5.5.2	Achten Sie auf Ihre äußere Erscheinung	210
	5.5.3	Seien Sie ein guter Zuhörer	211
	5.5.4	Machen Sie sich Ihrer Wirkung auf andere bewusst	211
	5.5.5	Halten Sie sich bei Gesprächen heraus	212
	5.5.6	Denken Sie daran, dass Empathie der Schlüssel zum Rapport ist.	212
	5.5.7	Sorgen Sie für ein gutes Allgemeinwissen	214
	5.5.8	Entwickeln Sie Ihre neugierige Seite	214
	5.5.9	Finden Sie Wege, um die Bedürfnisse anderer zu erfüllen	215
	5.5.10	Weitere Techniken für Rapport	219
	5.5.11	Rapport testen	221
5.6		Der menschliche Pufferüberlauf	222
	5.6.1	Die Grundregeln	224
	5.6.2	Fuzzing des Betriebssystems Mensch	225

	5.6.3	Die Regeln eingebetteter Befehle	226
5.7		Zusammenfassung	229
6		Beeinflussung – Die Macht der Überredung	231
6.1		Die fünf Säulen von Beeinflussung und Überredung	232
	6.1.1	Ein klares Ziel im Kopf haben	233
	6.1.2	Rapport, Rapport, Rapport	234
	6.1.3	Beobachten Sie Ihre Umgebung	237
	6.1.4	Handeln Sie nicht verrückt, sondern flexibel	238
	6.1.5	Mit sich selbst in Kontakt sein	239
6.2		Taktiken der Beeinflussung	239
	6.2.1	Die Reziprozität	240
	6.2.2	Die Verpflichtung	244
	6.2.3	Das Zugeständnis	247
	6.2.4	Knappheit	249
	6.2.5	Autorität.	254
	6.2.6	Commitment und Konsistenz	258
	6.2.7	Gemocht werden	263
	6.2.8	Übereinstimmung oder Social Proof.	268
6.3		Die Realität verändern – Das Framing	273
	6.3.1	Politik.	274
	6.3.2	Framing im Alltag.	275
	6.3.3	Vier Arten der Rasterangleichung	280
	6.3.4	Framing für den Social Engineer	287
6.4		Manipulation – Kontrollieren Sie Ihr Ziel.	295
	6.4.1	Zurückrufen oder nicht?.	297
	6.4.2	Endlich geheilt – Angst	299
	6.4.3	Sie können mich nicht zwingen, das zu kaufen!	300
	6.4.4	Zielpersonen auf positive Reaktionen konditionieren.	305
	6.4.5	Anreize für Manipulation.	307
6.5		Manipulation beim Social Engineering	313
	6.5.1	Die Beeinflussbarkeit einer Zielperson erhöhen	313
	6.5.2	Die Umgebung der Zielperson kontrollieren	315
	6.5.3	Die Zielperson zur Neubewertung zwingen.	316
	6.5.4	Die Zielperson soll sich ohnmächtig fühlen.	317
	6.5.5	Immaterielle Strafen verteilen	318

6.5.6	Die Zielperson einschüchtern	318
6.5.7	Positive Manipulation	319
6.6	Zusammenfassung	323
7	Die Tools des Social Engineer	325
7.1	Werkzeuge und Instrumente	326
7.1.1	Öffnungswerkzeuge	326
7.1.2	Kameras und Aufzeichnungsgeräte.	335
7.1.3	Der GPS-Tracker	339
7.2	Online-Tools zur Informationsbeschaffung	347
7.2.1	Maltego	348
7.2.2	Das Social Engineer Toolkit	351
7.2.3	Telefonbasierte Tools	358
7.2.4	Passwort-Profiler	362
7.3	Zusammenfassung	368
8	Fallstudien: Social Engineering unter der Lupe	369
8.1	Mitnick-Fallstudie 1: Die Zulassungsstelle hacken.	370
8.1.1	Das Ziel	370
8.1.2	Die Story	371
8.1.3	Das SE-Framework auf den DMV-Hack anwenden.	374
8.2	Mitnick-Fallstudie 2: Die Sozialversicherungsbehörde hacken	378
8.2.1	Das Ziel	378
8.2.2	Die Story	378
8.2.3	Das SE-Framework auf den SSA-Hack anwenden.	381
8.3	Hadnagy-Fallstudie 1: Der viel zu selbstsichere CEO	383
8.3.1	Das Ziel	383
8.3.2	Die Story	384
8.3.3	Das SE-Framework beim Hack mit dem zu selbstsicheren CEO	391
8.4	Hadnagy-Fallstudie 2: Skandal im Vergnügungspark	393
8.4.1	Das Ziel	393
8.4.2	Die Story	394
8.4.3	Das SE-Framework auf den Park-Hack anwenden.	397

8.5	Fallstudie Top Secret 1: Mission not impossible	399
8.5.1	Das Ziel	399
8.5.2	Die Story	400
8.5.3	Das SE-Framework auf Top Secret 1 anwenden	406
8.6	Fallstudie Top Secret 2: Pentester als Social Engineer	408
8.6.1	Das Ziel	408
8.6.2	Die Story	409
8.6.3	Das SE-Framework auf Top Secret 2 anwenden.	415
8.7	Warum Fallstudien so wichtig sind	417
8.8	Zusammenfassung	418
9	Prävention und Schadensbegrenzung	419
9.1	Lernen Sie, Social Engineering-Angriffe zu identifizieren	420
9.2	Schaffen Sie eine persönliche Kultur des Sicherheitsbewusstseins	422
9.3	Seien Sie sich des Wertes der Informationen bewusst, nach denen Sie gefragt werden	425
9.4	Halten Sie Software aktualisiert.	429
9.5	Entwickeln Sie Handlungsabläufe	431
9.6	Lernen Sie aus Social Engineering-Audits	431
9.6.1	Das Social Engineering-Audit	432
9.6.2	Audit-Ziele festlegen.	432
9.6.3	Was zu einem Audit gehört und was nicht	434
9.6.4	Den besten Auditor wählen	436
9.7	Abschließende Bemerkungen	438
9.7.1	Social Engineering ist nicht immer negativ	439
9.7.2	Die Bedeutung der Sammlung und Organisation von Information	439
9.7.3	Wählen Sie Ihre Worte sorgfältig.	441
9.7.4	Sorgen Sie für einen guten Pretext	442
9.7.5	Üben Sie, Ausdrücke zu lesen	443
9.7.6	Manipulation und Beeinflussung	443
9.7.7	Achten Sie auf bössartige Taktiken	444
9.7.8	Nutzen Sie Ihre Angst	445
9.8	Zusammenfassung	447

Stichwortverzeichnis449