

Inhalt

1	Der Faktor Mensch in der Informationssicherheit	1
1.1	Der Mensch als Lösung	2
1.2	Wer bin ich – und wenn ja, wie viele?	7
1.3	Informationssicherheit	12
2	Der Mensch als Bedrohung	19
2.1	It's me, hi, I'm the problem, it's me	19
2.1.1	Typische Szenarien – (un)sicheres Verhalten	20
2.1.2	Gründe für unsicheres Verhalten	24
2.2	Enemy Mine – Malicious Insider	30
2.2.1	Insider	31
2.2.2	Insider Threats	33
2.2.3	Typen von Malicious Insidern	34
2.2.4	Maßnahmen gegen Malicious Insider	38
3	Der Mensch als Opfer	43
3.1	Die Kunst des No-Tech-Hackings	44
3.1.1	Social Engineering	44
3.1.2	Social Engineering Attack Cycle	45
3.1.3	Social Engineering-Ontologie	49
3.2	Die Methoden der Social Engineers	51
3.2.1	Phishing	51
3.2.2	Watering Hole Attack	56
3.2.3	Impersonating/Pretexting	57
3.2.4	Reverse Social Engineering	59
3.3	Menschen manipulieren	60
3.3.1	Thinking, Fast and Slow	60
3.3.2	Autorität	61
3.3.3	Soziale Bewährtheit	63
3.3.4	Sympathie, Ähnlichkeit und Täuschung	65
3.3.5	Verpflichtung, Gegenseitigkeit & Konsistenz	66
3.3.6	Ablenkung	68
4	Information Security Awareness	71
4.1	Grundlagen Information Security Awareness	72

4.1.1	Awareness im Kontext Informationssicherheit	72
4.1.2	Erkenntnisse aus der Verhaltenspsychologie	77
4.1.3	Individualisierung	83
4.2	Vorgehensmodell zur zielgerichteten Sensibilisierung	90
4.2.1	Das Vorgehensmodell im Überblick	91
4.2.2	Analysephase	93
4.2.3	Umsetzungsphase	98
5	Information Security Awareness fördern	103
5.1	Wissen erhöhen und Fähigkeiten fördern	104
5.1.1	Wissen	105
5.1.2	Lernen	106
5.1.3	Gestaltung didaktischer Szenarien	111
5.1.4	Mediendidaktik	113
5.2	Verhaltensabsicht fördern und beeinflussen	114
5.2.1	Einstellungen	116
5.2.2	Wahrgenommene Norm	120
5.2.3	Persönliche Handlungsfähigkeit	125
5.3	Salienz fördern	133
5.3.1	Begriff und Konzepte zur Salienz	133
5.3.2	Förderung der Salienz	136
5.4	Gewohnheiten fördern	140
5.4.1	Merkmale von Gewohnheiten	141
5.4.2	Gewohnheitsmäßiges Verhalten	142
5.4.3	Faktoren zur Förderung von Gewohnheiten	143
5.4.4	Überführung von alten in neue Gewohnheiten	148
6	Messen von Information Security Awareness	151
6.1	Hintergrund – warum, was und wie messen	151
6.2	Messen von Wissen und Fähigkeiten	155
6.3	Messen der Verhaltensabsicht	160
6.3.1	Einstellungen bewerten	161
6.3.2	Bewertung wahrgenommener Normen	164
6.3.3	Bewerten der persönlichen Handlungsfähigkeit	167
6.4	Messen von Salienz	171
6.4.1	Salienz personenbezogen messen	172
6.4.2	Salienz unternehmensbezogen messen	174
6.5	Messen der Gewohnheitsstärke	178
7	Zukunft Mensch	181
	Literaturverzeichnis	185
	Stichwortverzeichnis	195