

M8 - MEMORY

- Druckt dieses Dokument auf festes Papier,
- schneidet die Kärtchen aus und
- übt die Begriffe gemeinsam im Memory-Spiel!

Kontrollblatt:

Malware = Überbegriff für unerwünschte, schädliche Software

Backup = Datensicherung

Social Engineering = „Datendiebstahl“ durch zwischenmenschliche Beeinflussung

Phishing = „Datendiebstahl“ durch falsche E-Mails

Shoulder Surfing = Beobachtung bei der Eingabe von Daten (Bankomat,...)

Information Diving = Diebstahl von Daten, die unachtsam einfach weggeworfen wurden

Pretexting = Daten eines Dritten (unter Vorgabe einer fremden Identität) besorgen

Computerwurm = Virus, der sich direkt über Netze (Internet) verbreitet

Makroviren = Viren, die als Programm in ein Dokument eingebettet sind

Trojaner = versteckt in einem scheinbar nützlichen Programm

Rootkit = Programm, das Viren im Betriebssystem versteckt

Keylogger = Programme, die Tastatureingaben mitprotokollieren

Backdoor = „Hintertür“ für Dritte über einen Computer Spams zu verteilen

Spyware und Adware = forschen das Nutzerverhalten aus und senden die Daten an Hersteller

Pharming = Betrugsmethode, bei der der User auf gefälschte Webseiten umgeleitet wird

Cookies = Dateien, die am Computer abgespeichert werden (z.B. Anmeldeinformationen)

Cyber-Mobbing = Mobbing mit Hilfe von elektronischen Medien

Cyber-Grooming = gezieltes Ansprechen von Minderjährigen im Internet mit dem Ziel der Anbahnung sexueller Kontakte

Digitale Signatur = stellt sicher, dass die E-Mail vom angegebenen Absender stammt und unverändert übermittelt wurde

Spam und Junk E-Mails = unerwünschte Werbemails

Instant Messaging = chatten

Malware	Backup	Social Engineering
Überbegriff für unerwünschte, schädliche Software	Datensicherung	„Datendiebstahl“ durch zwischenmenschliche Beeinflussung
Phishing	Shoulder Surfing	Information Diving
„Datendiebstahl“ durch falsche E-Mails	Beobachtung bei der Eingabe von Daten (Bankomat,...)	Diebstahl von Daten, die unachtsam einfach weggeworfen wurden

Pretexting	Computerwurm	Makroviren
Daten eines Dritten (unter Vorgabe einer fremden Identität) besorgen	Virus, der sich direkt über Netze (Internet) verbreitet	Viren, die als Programm in ein Dokument eingebettet sind
Trojaner	Rootkit	Keylogger
versteckt in einem scheinbar nützlichen Programm	Programm, das Viren im Betriebssystem versteckt	Programme, die Tastatureingaben mitprotokollieren

Backdoor

Spyware
und
Adware

Pharming

„Hintertür“
für Dritte
über einen
Computer
Spams
zu verteilen

forschen das
Nutzerverhalten
aus und senden
die Daten
an Hersteller

Betrugsmethode,
bei der der User
auf gefälschte
Webseiten
umgeleitet wird

Cookies

Cyber-Mobbing

Cyber-Grooming

Dateien, die am
Computer
abgespeichert
werden (z.B.
Anmelde-
informationen)

Mobbing mit Hilfe
von elektronischen
Medien

gezieltes
Ansprechen von
Minderjährigen im
Internet mit dem
Ziel der Anbahnung
sexueller Kontakte

