Cyber Security Teil 1
Faktor Mensch

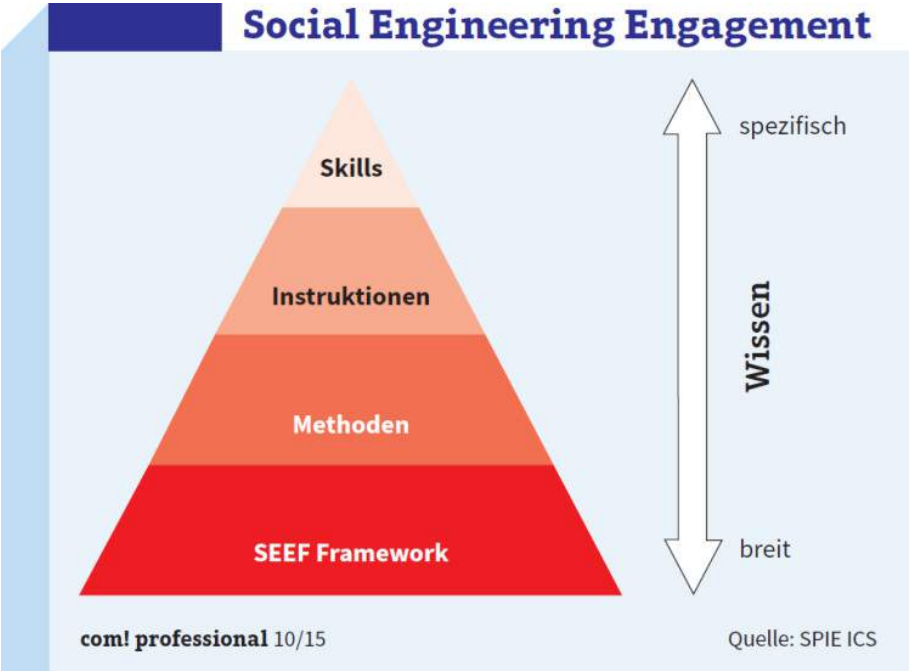
DI Gerald KORTSCHAK, BSc, CMC, CDC, CDISE
Hans Christian EINFALT

WIR NEHMEN **WISSEN** IN BETRIEB.

WKO Unternehmensberatung · Buchhaltung · IT STEIERMARK

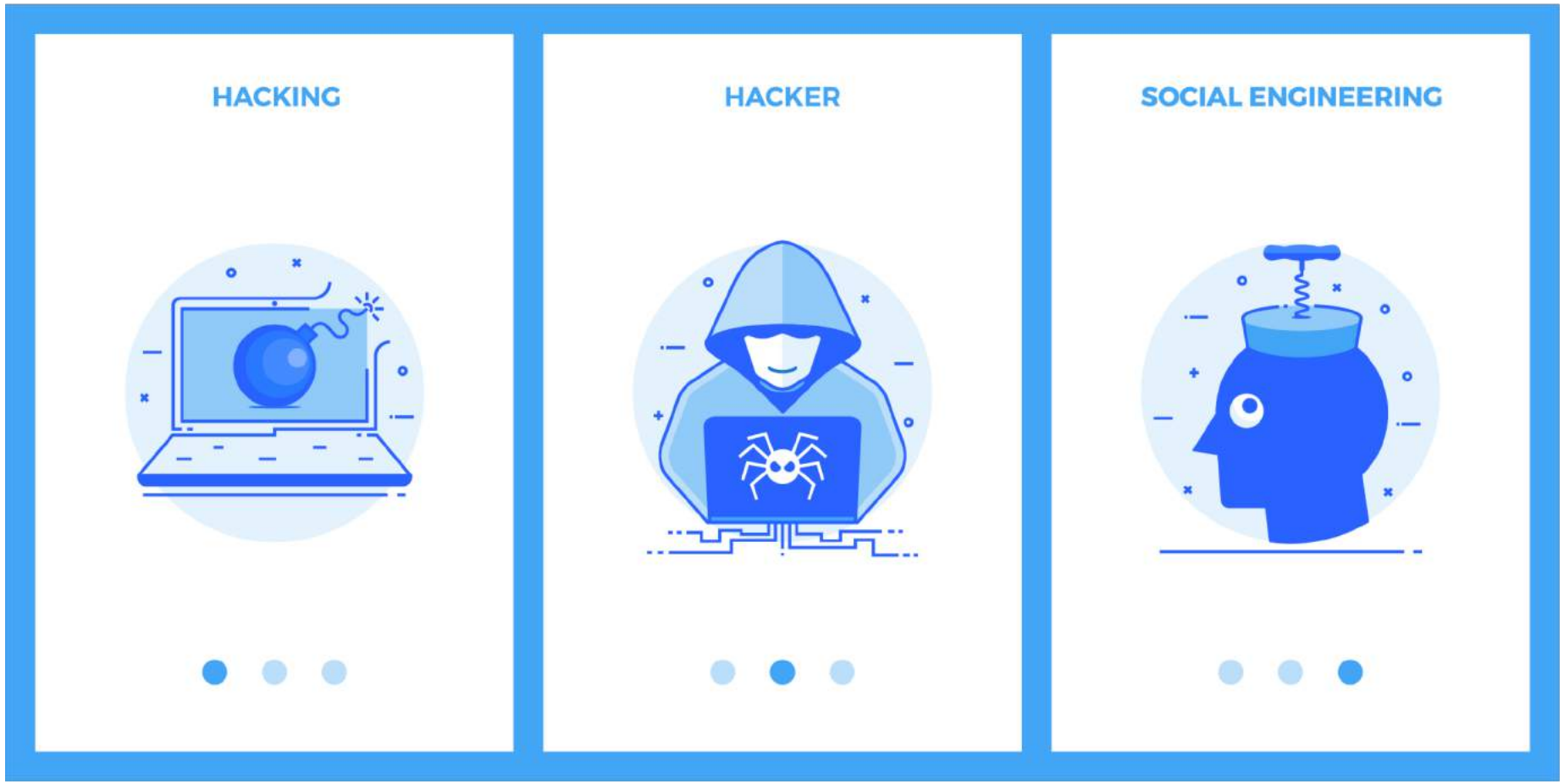
Präsentationsaufbau

- Themeneinführung
- Praktische Beispiele
- Psychologischer Aspekt
- Gegenmaßnahmen



https://fast.wistia.com/embed/iframe/ccefulfjpr

Differenzierung / Abgrenzung



Human Hacking

Social Engineering bezeichnet in der Informatik das Erlangen von Informationen durch Annäherung an Informationsträger mittels strukturierter Methoden (technisch oder interaktiv)

Social Hacking

Anteil an Angriffen?

- 66% aller Angriffe basieren auf SE

Blue Coat Security Lab 2014: Mobile-Malware-Bericht

Malvertising überholt Pornographie als führenden Bedrohungsvektor

Haupt-Bedrohungsvektoren

2013 übertraf **Malvertising** Pornographie als Nummer eins der mobilen Inhalte, die mit Malware infiziert waren, und hat sich mehr als verdreifacht.

Dreifach höhere Bedrohung als letztes Jahr.

2013	
Pornographie	22,16%
Verdächtige Aktionen	14,09%
Rechner/Internet	7,26%
Web-Anzeigen	5,69%
Unterhaltung	4,99%
Unbewertet	4,38%
Suchmaschinen/-portale	3,69%
Unternehmen/Wirtschaft	3,38%
Nachrichten/Medien	3,29%
Newsgroups/Foren	3,10%

2014	
Web-Anzeigen/-Analysen	19,69%
Verdächtige Aktionen	16,56%
Pornographie	16,55%
Gemischte Inhalte/wd. für Erwachsene	4,19%
Unkategorisiert	4,10%
Audio-/Video-Clips	3,79%
Unterhaltung	3,43%
Suchmaschinen/-portale	3,13%
Nachrichten/Medien	3,13%
Sport/Hobbies	2,62%
Newsgroups/Foren	0,94%

Definition Malvertising

"malicious" + "advertising"
(böswillig) (Werbung)

Malvertising: - Web-Anzeigen, die über legitime Ad-Netzwerke zur Verfügung gestellt werden und die Nutzer direkt auf bedrohliche Websites führen oder schädigenden Code enthalten.

BLUE COAT

Alte Tricks führen mobile Anwender hinters Licht

Anstelle der Sicherheits-Konzepte der Geräte, werden deren Benutzer überlistet. Die mobilen Bedrohungen von heute setzen auf Social Engineering und verleiten die Verbraucher, von sich aus Cyberkriminellen die Kontrolle zu überlassen.

Populäre mobile Bedrohungen

Die Benutzer werden bereits beim Herunterladen einer App überlistet. Was sich häufig als Porno-App tarnt, entpuppt sich später als Betrug, denn das Konto des Besitzers wird ohne Einverständnis mit einer Gebühr belastet.

Tipps

- Überprüfen Sie, ob Ihr Anbieter die Blockierung von SMS-Zahlungen ermöglicht.
- Seien Sie als Android-User misstrauisch. Überprüfen Sie Ihre Mobilfunk-Rechnungen.
- Seien Sie skeptisch bei mobilen Porno-Apps.

Links, die scheinbar von Freunden auf Social-Networking-Sites kommen, können zu Malware führen.

Tipps

- Klicken Sie nie auf verdächtige Inhalte, auch nicht von Freunden.
- Vermeiden Sie es, in Ihrem mobilen Gerät auf Werbeanzeigen zu klicken.
- Laden Sie niemals unbekannte Apps oder Anhänge herunter.

Apps zeigen riskante Verhaltensweisen, wie Zugriff auf Kontaktinformationen, Aufenthaltsort und Gewohnheiten, Interessen oder Suchvorgängen der Benutzer von mobilen Geräten.

Tipps

- Deaktivieren Sie niemals Ihre Sicherheitseinstellungen.
- Laden Sie niemals eine App außerhalb der offiziellen Märkte herunter (d.h. App Store, Google Play oder die Märkte der Hersteller selbst).
- Seien Sie misstrauisch bei „Anti-Malware"- und Porno-Apps.
- Unternehmen sollten App-Risikoprofile abonnieren.

Das Verhalten mobiler Anwender ändert sich

Verbraucher verlagern Ihre Aktivitäten zunehmend auf mobile Geräte und es liegt nahe, dass Cyberkriminelle folgen und beliebte Anlaufpunkte infizieren. Freizeit-Kategorien, wie Online-Shopping, sind am stärksten bedroht, wenn Verbraucher mobiler werden.

Nutzung auf PCs von **25%** auf **8,42 %** gesunken

Social networking

Heute mit **13%** dritthäufigste Aktivität auf mobilen Geräten

Verantwortlich für **4.12%** der Aktivitäten auf PCs im letzten Jahr

Online shopping

Um **68%** auf **7,48%** der Aktivitäten und damit auf Platz fünf der populärsten mobilen Aufgaben

Drive-by-Downloads aus Web-Anzeigen häufiger auf dem PC als bei mobilen Anzeigen

Web Anzeigen

Web-Anzeigen 2013 um **56%** gestiegen; ein Fünftel aller Weiterleitungen zu Malware erfolgt über mobile Anzeigen

7% der Online-Nutzung entfällt auf Audio/Video (Steigerung um 25 % seit 2012)

Unterhaltung

Nur **1%** der Videos werden browserbasiert betrachtet, bevorzugt werden Video-Apps wie YouTube und Hulu

Deutschland sicher im Netz

BLEIBEN SIE ACHTSAM!

Es gibt nur einen einzigen wirksamen Schutz vor Social Engineering: gesundes Misstrauen, verbunden mit dem strikten Einhalten vereinbarter Regeln zur Datenweitergabe! **Behalten Sie deshalb die Risiken immer im Blick!**

RISIKO **SOCIAL NETWORKS**

Ihr Profil und andere Daten in sozialen Netzwerken bieten Social Engineers vielfältige Angriffsmöglichkeiten!

RISIKO **LAUSCHANGRIFF**

Lauschangriffe finden überall statt! Ob im Büro am PC, unterwegs am mobilen Endgerät oder durch Mithören eines Gesprächs!

RISIKO **TELEFON**

Anrufer können mit falschen Angaben versuchen, an interne Informationen zu gelangen!

RISIKO **USB-STICK**

Fremde USB-Sticks bieten Kriminellen eine Möglichkeit, Ihre Daten auszulesen oder sogar Ihren PC fernzusteuern!

RISIKO **INNENTÄTER**

Sensible Daten dürfen selbst unter Kollegen nur an autorisierte Personen weitergegeben werden!

DATEV

Mehr zum Thema Social Engineering finden Sie unter: **www.datev.de/sicherheitsleitfaden** und **www.sicher-im-netz.de**

TOP 3 CYBER THREATS

facing organizations in 2016:

52%
Social Engineering

40%
Insider Threats

39%
Advanced Persistent Threat

SOURCE:
ISACA'S JANUARY 2016 CYBERSECURITY SNAPSHOT, GLOBAL DATA,
WWW.ISACA.ORG/2016-CYBERSECURITY-SNAPSHOT

CSX™ CYBERSECURITY NEXUS

ISACA®
Trust in, and value from, information systems

Statistik SE.org

- 90% of the people we ask will provide not just the spelling of their names but their email addresses without confirming our identity
- 67% of the people we ask will give out social security numbers, birth dates or employee numbers
- We have a 100% success ratio in physical breaches

SOCIAL ENGINEERING TACTICS

YOUR DATA IS AT RISK EVERYDAY THROUGH SOCIAL ENGINEERING ATTACKS.

WHY SOCIAL ENGINEERING?

HACKING A HUMAN IS **MUCH EASIER** THAN HACKING A BUSINESS.

laziness
ignorance
haste
fear
attitude
trust

ATTACKERS PREY ON YOUR HUMAN WEAKNESS

carelessness
sympathy
ego
ability
greed
desire

28%

Likelihood your business will experience a data breach in the next 2 years

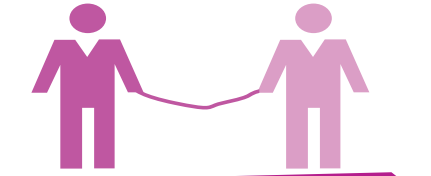
$3.8 M

The average cost of a single data breach in 2015

SOCIAL ENGINEERING: SCHWACHSTELLE MENSCH

AUTORITÄT

Vorsicht vor ...
E-Mails einer Bank



HILFSBEREITSCHAFT

Vorsicht vor ...
Nigerianischem Spam

VERTRAUEN

Vorsicht vor ...
falschen Facebook-Freunden

NEUGIERDE

Vorsicht vor ...
dem Öffnen von Anhängen und Klicken auf Links

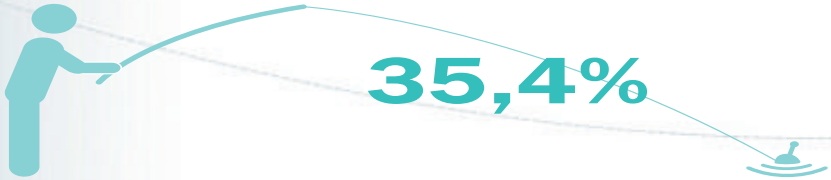
ZUGEHÖRIGKEIT

Vorsicht vor ...
Social-Media Account-Daten-Abfragen

„Für **Social Engineering** greifen Cyberkriminelle auf grundlegende Muster der menschlichen Psyche zurück und nutzen althergebrachte Schwächen aus.“ – Dr. Astrid Carolus, Medienpsychologin an der Universität Würzburg

PHISHING UND FINANZIELLE FOLGEN

TOP-3 DER PHISHING-OPFER*



35,4% Nutzer Sozialer Medien

31,5% Nutzer von Banken, E-Shops und Bezahldiensten

23,3% Nutzer von E-Mail-Diensten

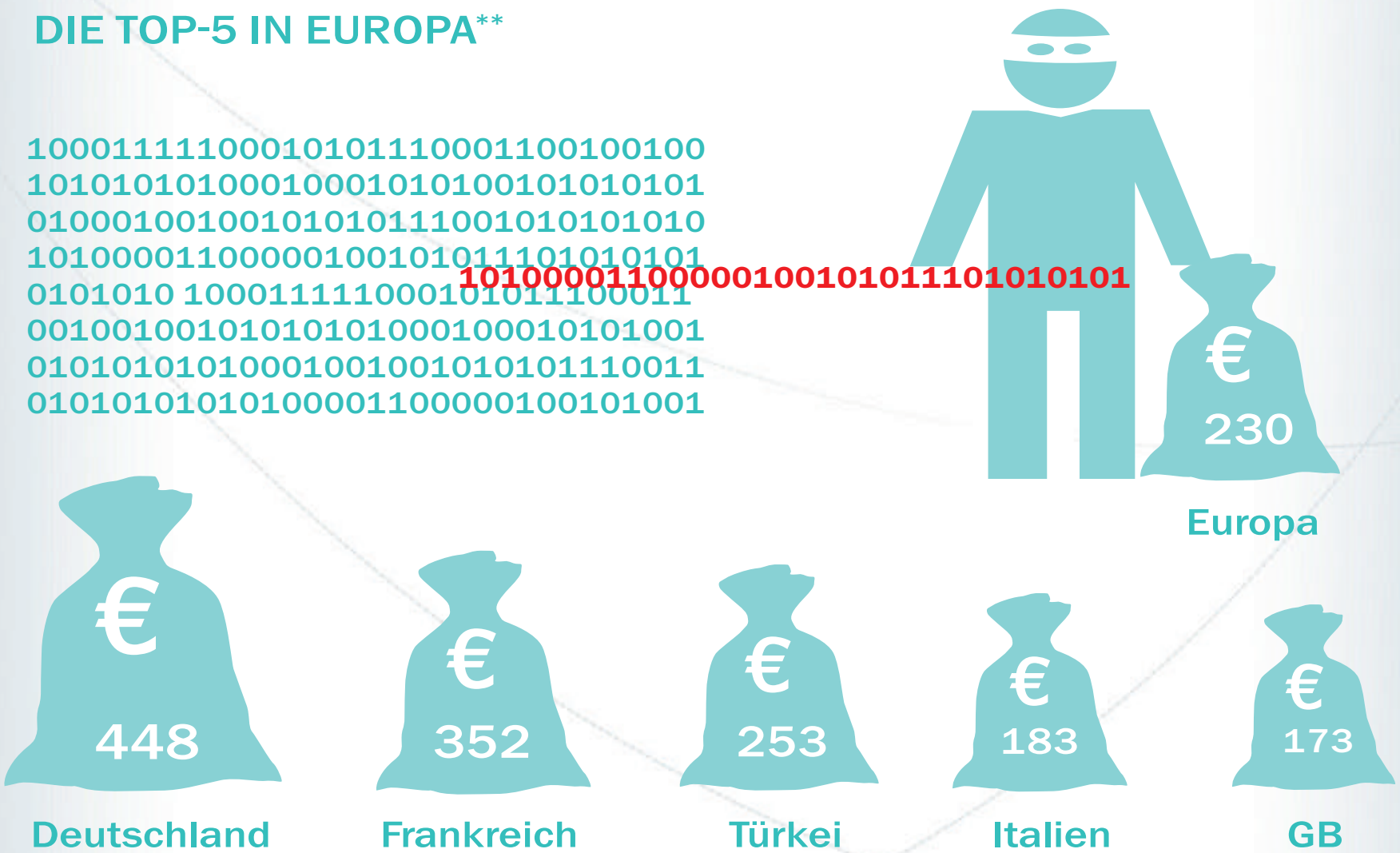
FINANZDATENKLAU IN EUROPA**

Passwort

41,0%

41% der Befragten haben E-Mails von Banken erhalten, in denen sensible Informationen wie Passwörter abgefragt wurden.

GELDVERLUST NACH DATENKLAU – DIE TOP-5 IN EUROPA**



Quellen:
* Von Kaspersky Lab für 2013 identifzierte finanzmotivierte Phishing-Attacken.
** Kaspersky Lab & B2B International. Befragt wurden 2,821 Nutzer in Europa.

Social Engineering: Wie man anderen mit Schokolade das Passwort entlocken kann

3. August 2016, 14:01

68 POSTINGS

Wissenschafter belegen erschreckend leichtfertigen Umgang mit vertraulichen Daten

Fast die Hälfte tauschte Passwort gegen Schokolade

So verriet fast jeder zweite Proband (47,9 Prozent) einer Umfrage mit 1.200 Teilnehmern sein persönliches Passwort, wenn er unmittelbar vor der Bitte eine Tafel Schokolade bekommen hatte. Wenn es das Geschenk direkt zu Beginn gab und bis zur Bitte einige Zeit verging, waren es immer noch 39,9 Prozent. Aus der Kontrollgruppe, deren Teilnehmer die Schokolade erst nach der Umfrage bekamen, gaben immerhin noch 29,8 Prozent ihr Passwort heraus.

Psychologische Aspekte

basierend auf Kevin Mitnick, The Art of Intrusion, 2006

Hauptaspekte

Zuneigung

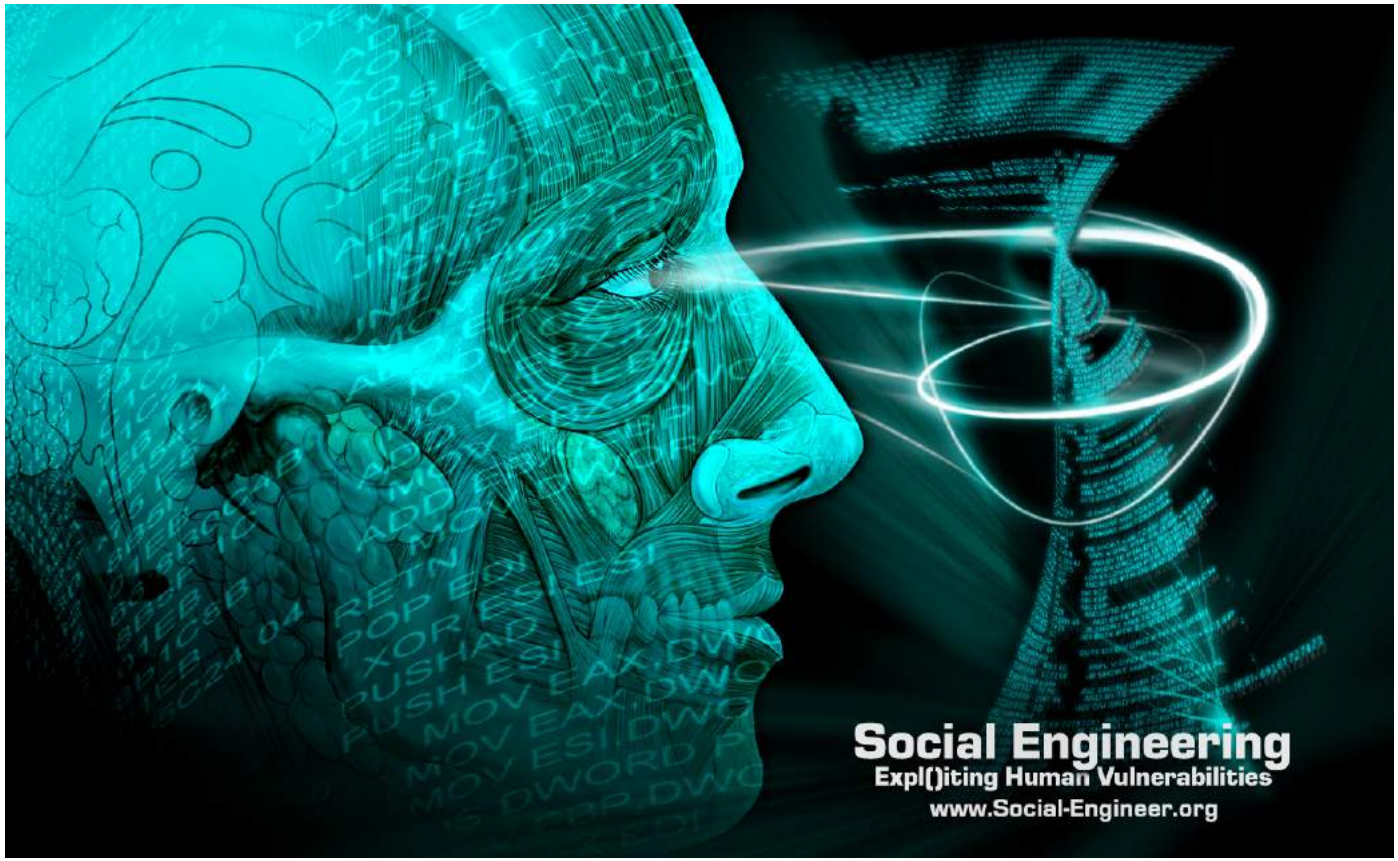
Furcht

Attribuierung

6 Zwischenmenschliche Verhaltenstendenzen

Psychologie

- Flirt
- Verkauf
- Bewerbung
- Prüfung



Grundlagen der Manipulation

- Faustregeln & Stereotype = Zeitersparnis
- Auslösemerkmale: Automatisches Verhalten
- Reaktion: Kontrolliertes Verhalten

Soziale Bewährtheit

- Superlative
- Early Adaptor
- Passive Bystander Effect
- Werther-Effekt

Autorität

- Titel
- Uniformen
- Luxus

Knappheit

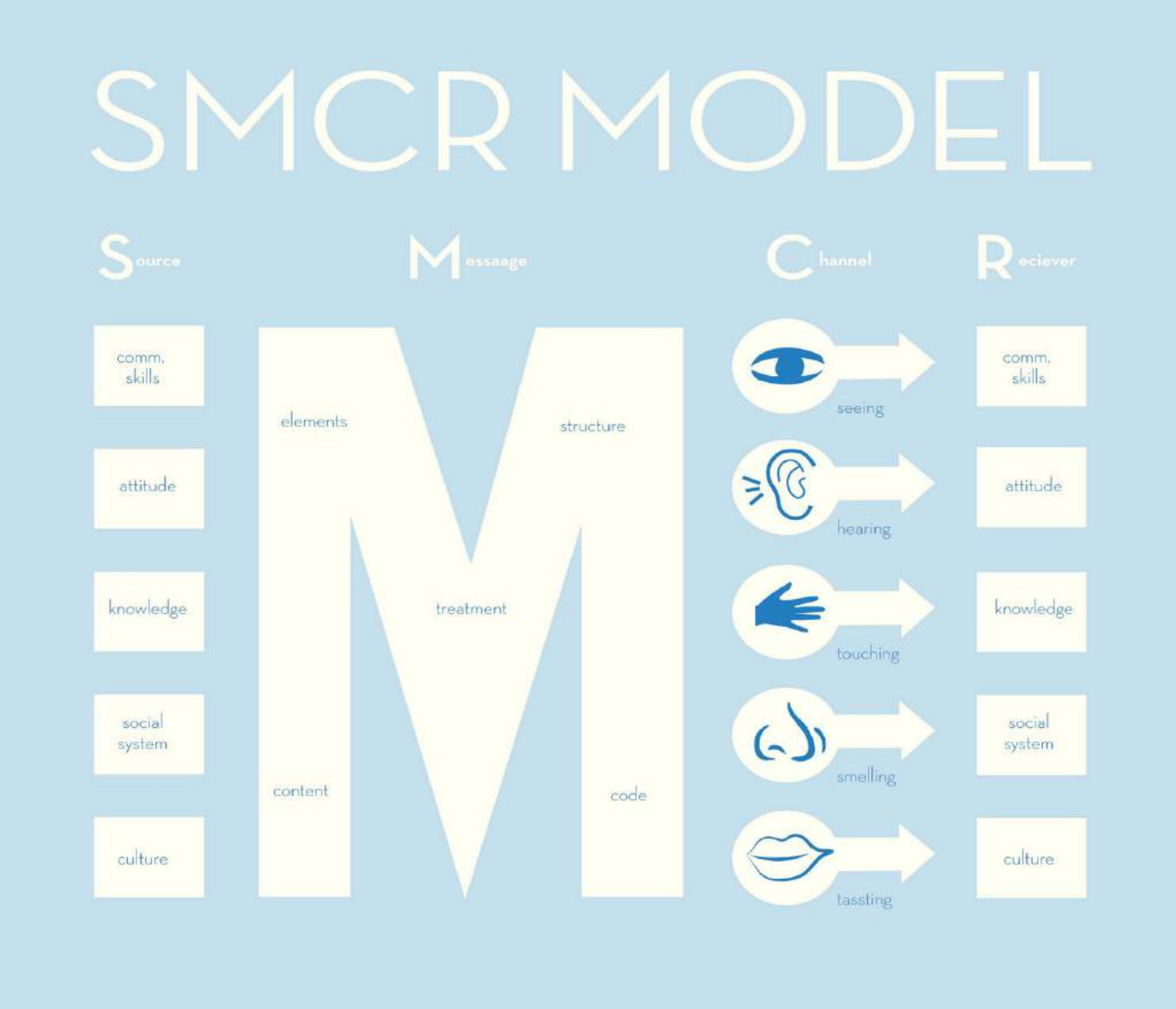
- Knappes Gut
  = wertvollere Ware

- Vorenthaltung von Information

Neuropsychologie & Biochemie

- Emotion
- Triebverhalten
- Endorphine
- Oxytocin

Sender - Empfänger



Sender – Empfängermodell nach Berlo

DIE 7 GRUNDEMOTIONEN
FREUDE
WUT
ANGST
EKEL
TRAUER
ÜBERRASCHUNG
VERACHTUNG

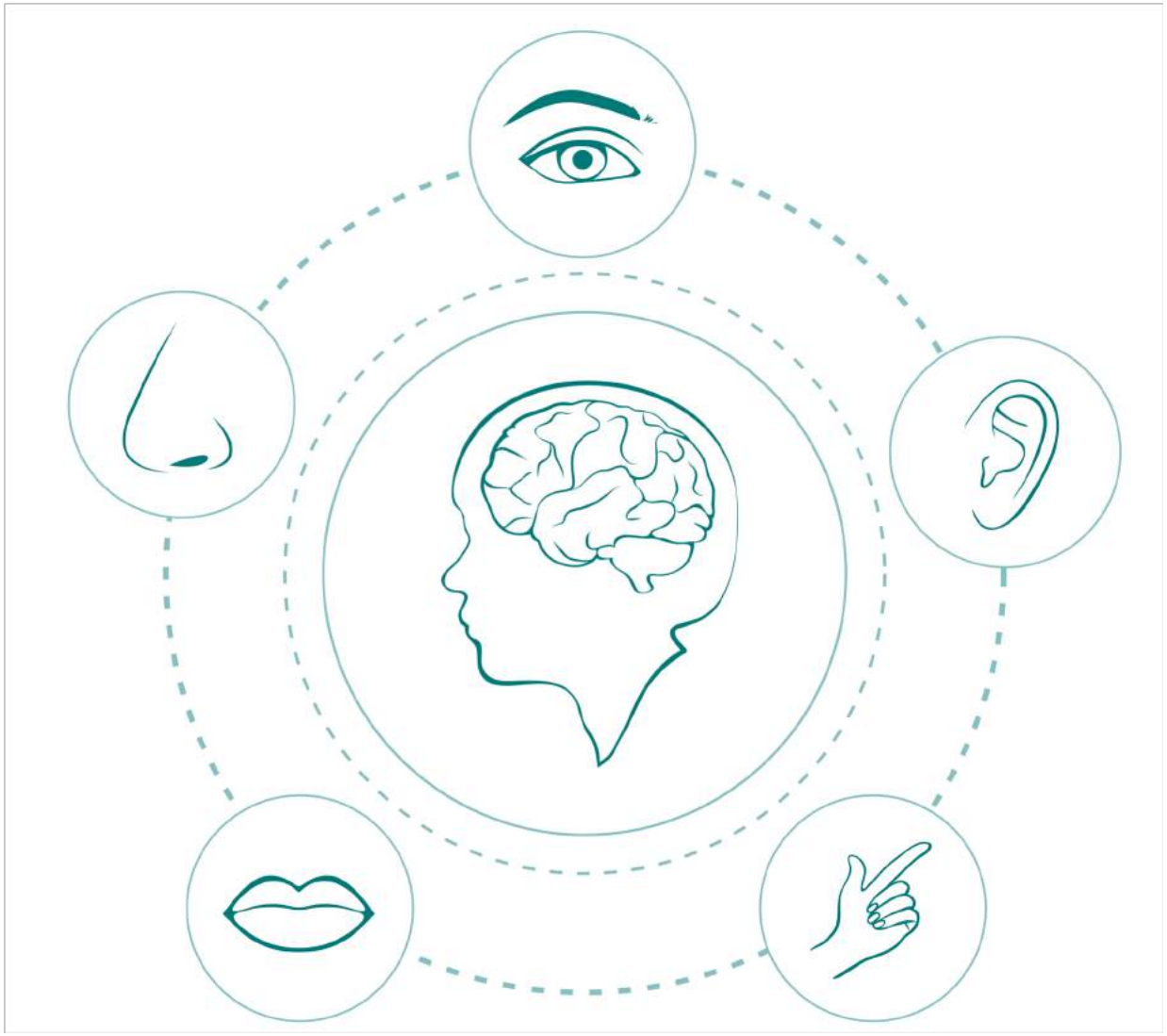
Art des Gegenübers

- Optisch, bzw. visueller Denker
- Gehör, bzw. auditiver Denker
- Gefühl, bzw. kinästhetischer Denker

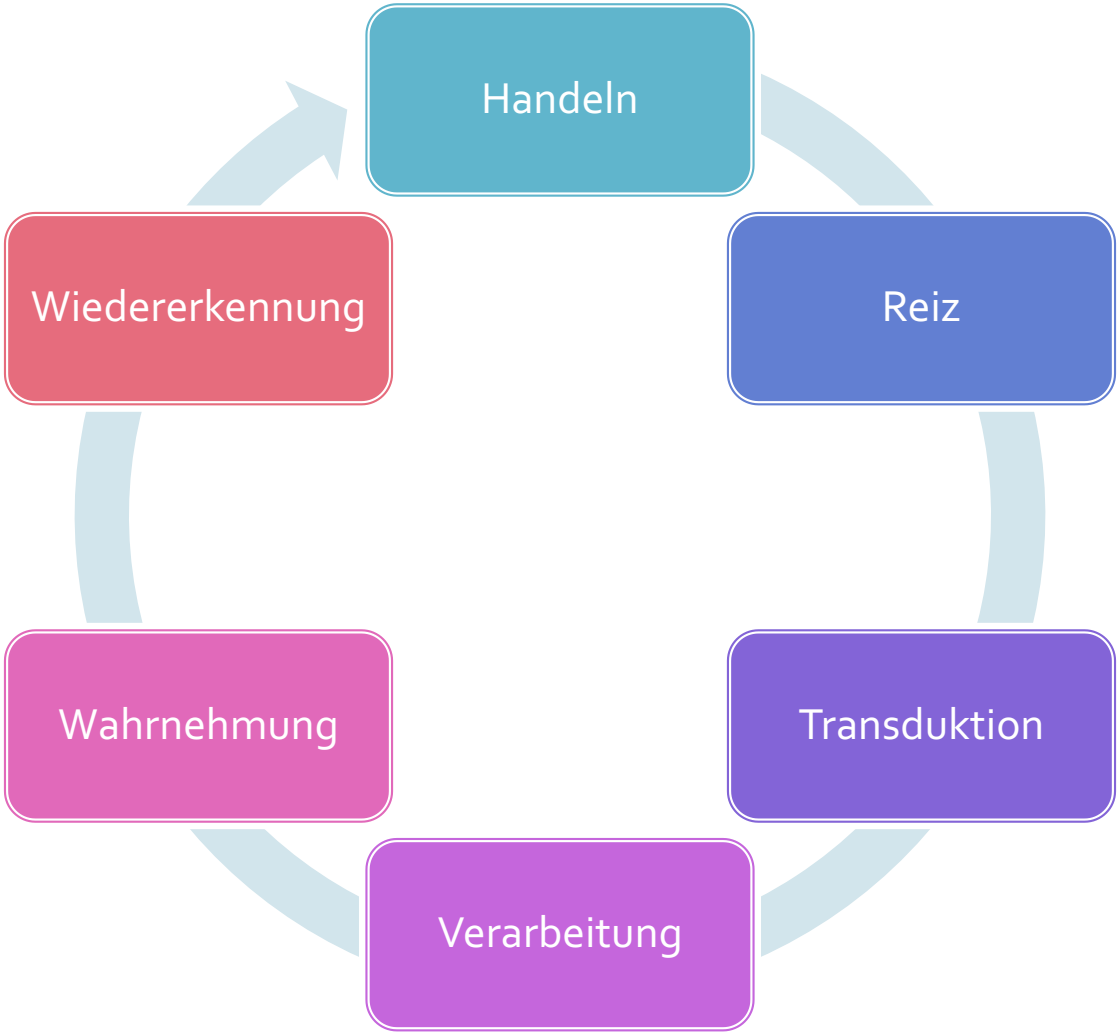
DENK-ARTEN

Ivan Pavlov, www.ivanpavlov.com

5 Sinne des Menschen



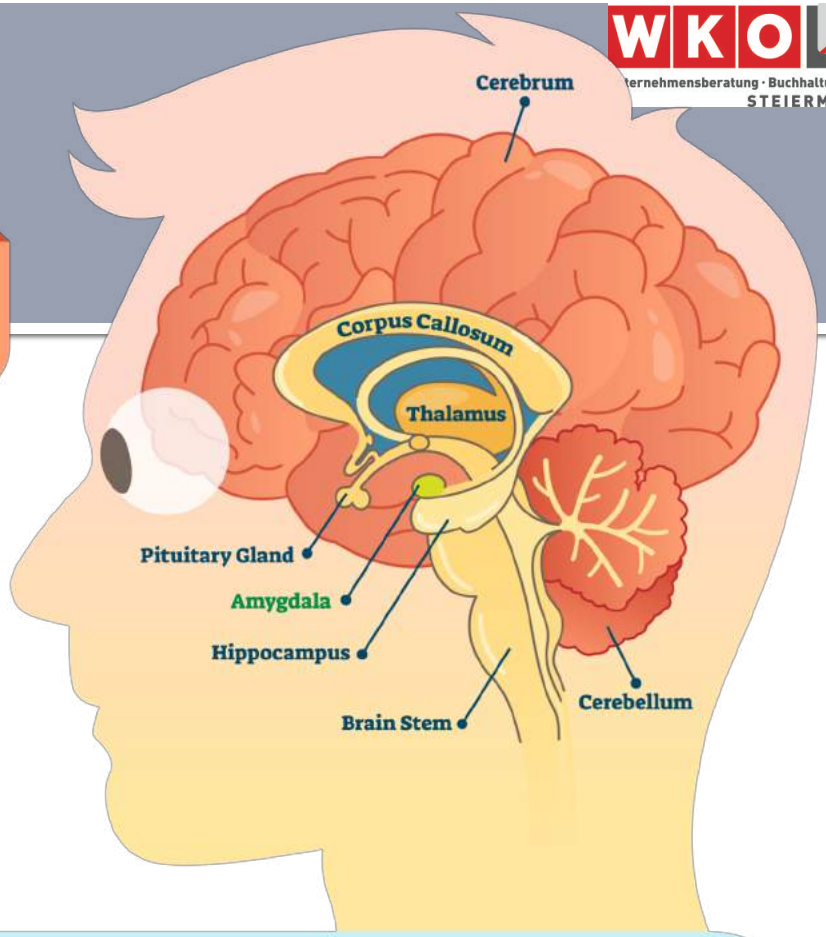
Auslösende Faktoren

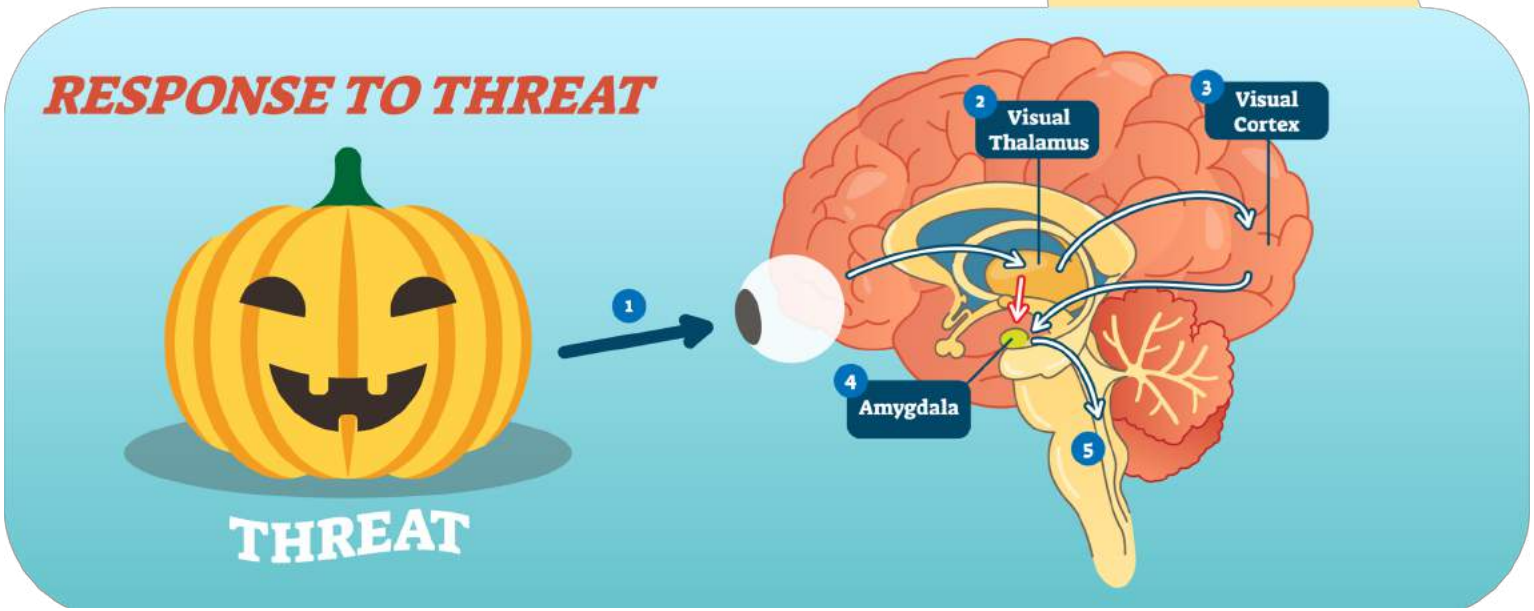


Hijacking

AMYGDALA

Responsible for the response and memory of emotions, especially fear.





Kontrollphrasen „visuell"

- Ich sehe, was Sie meinen.
- Für mich sieht das gut aus.
- Nun sehe ich das Gesamtbild.

- Helligkeit
- Grösse
- Farbe
- Bewegung
- Fokus

Kontrollphrasen „auditiv"

- Klar und deutlich.
- Etwas sagt mir, dass …
- Für mich klingt das gut/plausibel …

- Lautstärke
- Klangfarbe
- Tonhöhe
- Geschwindigkeit
- Entfernung

Kontrollphrasen „kinästhetisch“

- Ich habe die Idee erfasst.
- Inwiefern berührt das Thema Sie?
- Wie fühlt sich das an?
- Ich werde mit Ihnen in Kontakt treten.

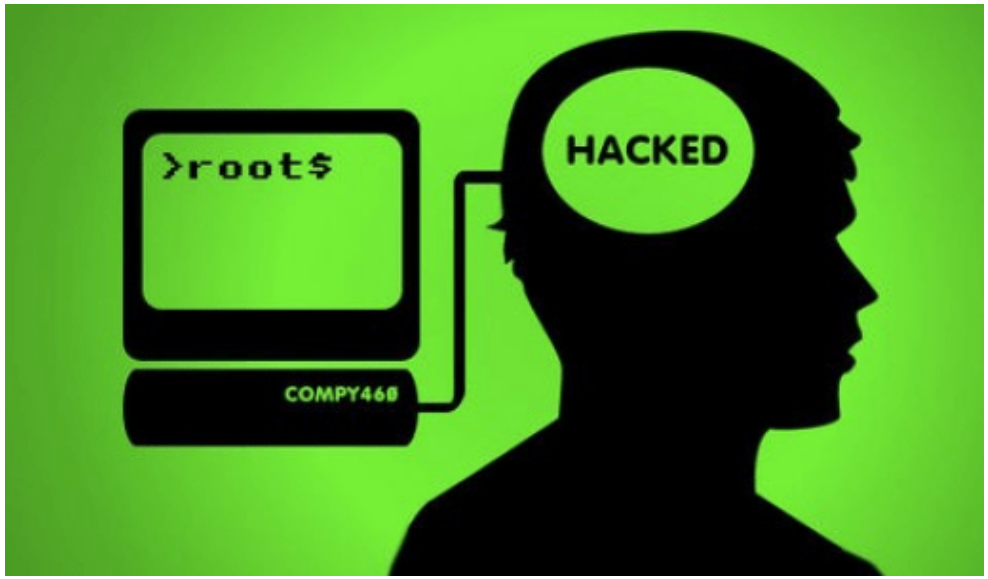
- Intensität
- Ausdehnung
- Oberfläche
- Temperatur
- Gewicht

Manipulations-Muster (Bsp.)

- Reziprozität
- Door in the Face
- Konsistenz
- Foot in the Door

Human Brain Hacking

- shellcode +=Gesetz der Erwartungshaltung
- shellcode +=Mentales Überladen
- shellcode +=Code einschleusen



Human Buffer Overflow

ByPass-Injection durch „Annahmen"

Da Joe meinte ich krieg die Lizenzen kostenfrei

Erwartungshaltung

Human Buffer Overflow

Grün Rot Blau Schwarz Violett Gelb Rot
Grün Rot Blau Schwarz Violett Gelb Rot
Grün Rot Blau Schwarz Violett Gelb Rot
Grün Rot Blau Schwarz Violett Gelb Rot
Grün Rot Blau Schwarz Violett Gelb Rot
Grün Rot Blau Schwarz Violett Gelb Rot

Die Farbe des Wortes, nicht das Wort!

Human Buffer Overflow

- 150 Wörter / Min => sprechen
- 500 – 600 Wörter / Min => denken
- Unterbewusstsein entscheidet 7sec vorab

Mentales Überladen (Mental Padding)

Human Buffer Overflow

Code Embedding

WENN SIE so ein **TOLLES** Produkt von jemandem wie **MIR KAUFEN** würden, was wären dann die wichtigsten Funktionen?

Weiss

- Sauberkeit
- Leicht
- Reinheit

- Sicherheitsgefühl
- Neutralitätsgefühl

- Güte und Vertrauen

Rot

- Erregung
- Glück

- Feier, Aktion, Energie

- Gute Gesundheit, Geschwindigkeit, Leidenschaft, Verlangen, Liebe

- Erzeugt Aufmerksamkeit und Emotionen

Lebenszyklus von Daten

- Entstehung
- Bearbeitung
- Übertragung / Übermittlung
- Speicherung / Archivierung
- Entsorgung / Löschung

vgl. Königs, 2005

Du UNGLAUBLICH Süßer! Wie hast du es bloß geschafft, die Probleme bei der Entwicklung von eurem TOLLEN Produkt zu überwinden?
Tja, für mich war das gar nicht so schwer. Ich habe zum Beispiel...
Wahnsinn!
Wie toll!
Unglaublich!
© 2005, 2015 by E-SEC GmbH, All rigths reserved, www.e-sec.com

Psychologische Hebel in Mails

sychologischer Hebel der Datendiebe	Beispiel
Methode „Herdentrieb“: Alle machen dies, Du musst dies auch tun.	Angebliche E-Mail des Administrators: Alle anderen Mitarbeiter haben fristgerecht ihr Passwort geändert. Machen Sie dies nun auch (endlich)!
Methode „Autorität“: Du musst gehorchen. Dabei setzen die Angreifer auch entsprechende Logos und Bilder ein.	Angebliches Fax der Bank: Es gibt ein Problem mit einer Überweisung. Rufen Sie eine (gefälschte) Nummer an und wiederholen Sie den Zahlungsvorgang.
Methode „Attraktivität“: Ich mag Dich, vertrau mir.	Angebliche E-Mail einer Verehrerin: Ich habe Dein Facebook-Profil gesehen und will Dich heiraten. Aber ich brauche Deine Hilfe …

Psychologische Hebel in Mails

sychologischer Hebel der Datendiebe	Beispiel
Methode „Pflichtbewusstsein": Als guter Bürger musst Du dies tun.	Angeblicher Brief der Stadtverwaltung: Jeder Bürger muss auf Bankeinzug umstellen, faxen Sie uns die Bankverbindung mit diesem Formular.
Methode „Keine Zeit": Du musst sofort reagieren.	Angebliche Gewinn-Benachrichtigung: Melden Sie sich sofort als Gewinner zurück, sonst ist es zu spät.
Methode „In der Schuld sein": Ich habe Dir geholfen, nun bist Du dran.	Angebliche Nachricht des Schulkameraden: Ich habe Dir in der Schule geholfen, jetzt brauche ich Deine Hilfe.

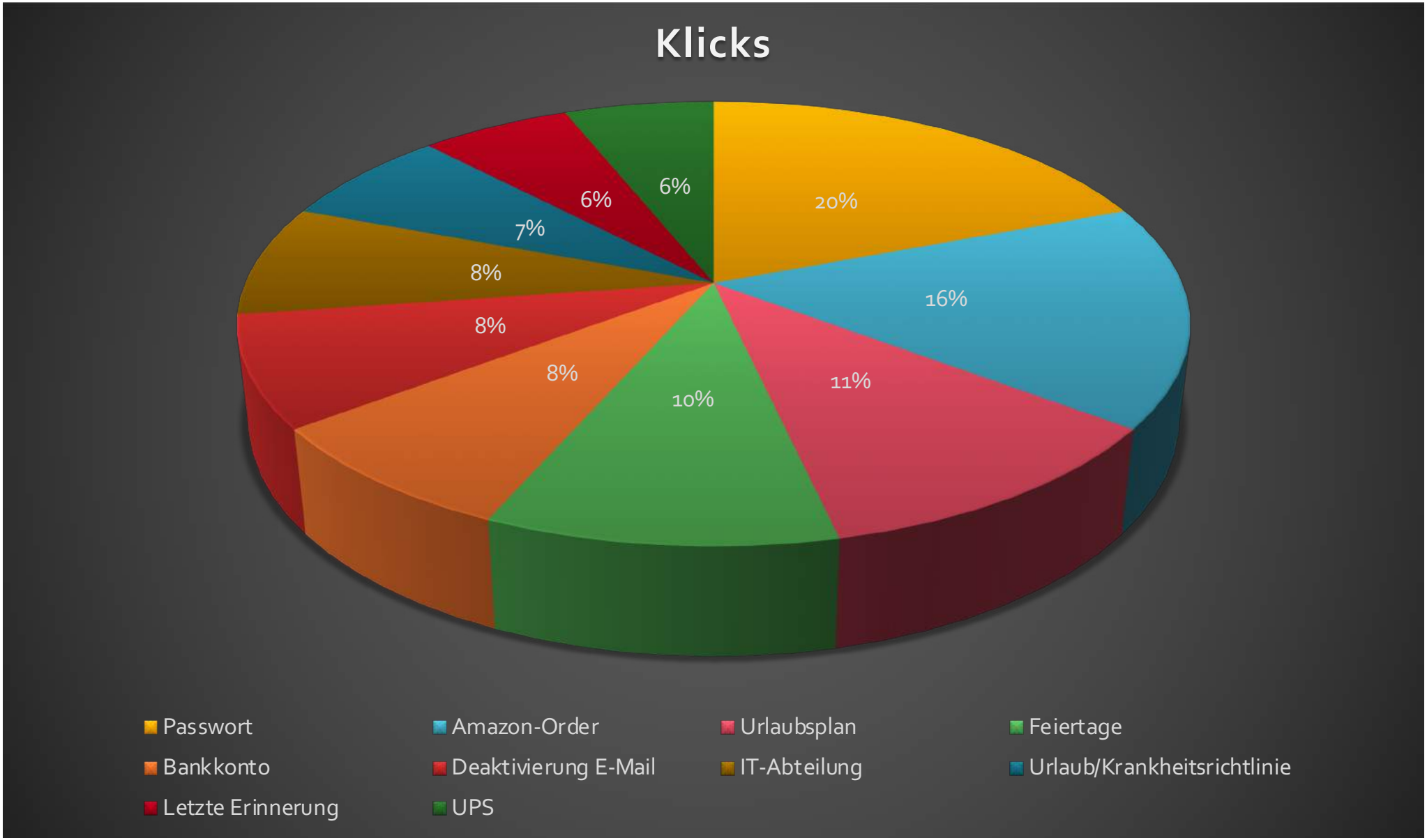
Psychologische Hebel in Mails

sychologischer Hebel der Datendiebe	Beispiel
Methode „Drohung“: Ich veröffentliche Vertrauliches über Dich.	Nachricht des Angreifers, dass er vertrauliche Daten über das Opfer verbreiten werde, wenn es nicht dieses oder jenes tut (Online-Erpressung).
Methode „Hilfsbereitschaft“: Mache das, ich zeige Dir, wie es geht.	Nachricht des Angreifers, die eine genaue Anleitung und sogar eine FAQ-Liste enthält, die es dem Opfer leichter machen soll.

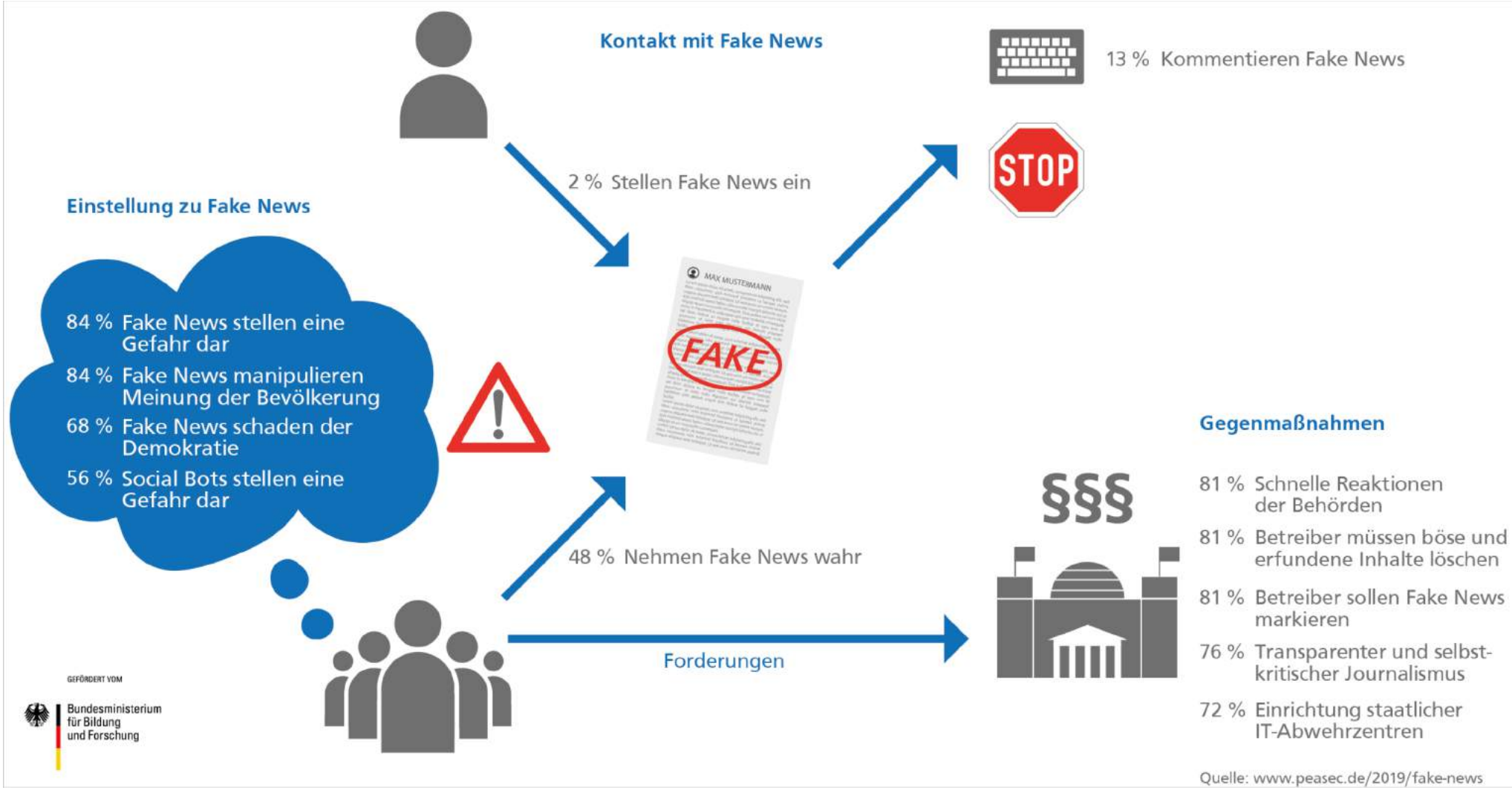
Top fünf Kategorien E-Mail Q4/2018

- Lieferungen
- Passwörter
- Unternehmens-Richtlinien
- Urlaub
- IT-Abteilung

Top-10-E-Mail-Betreffzeilen Q4/2018

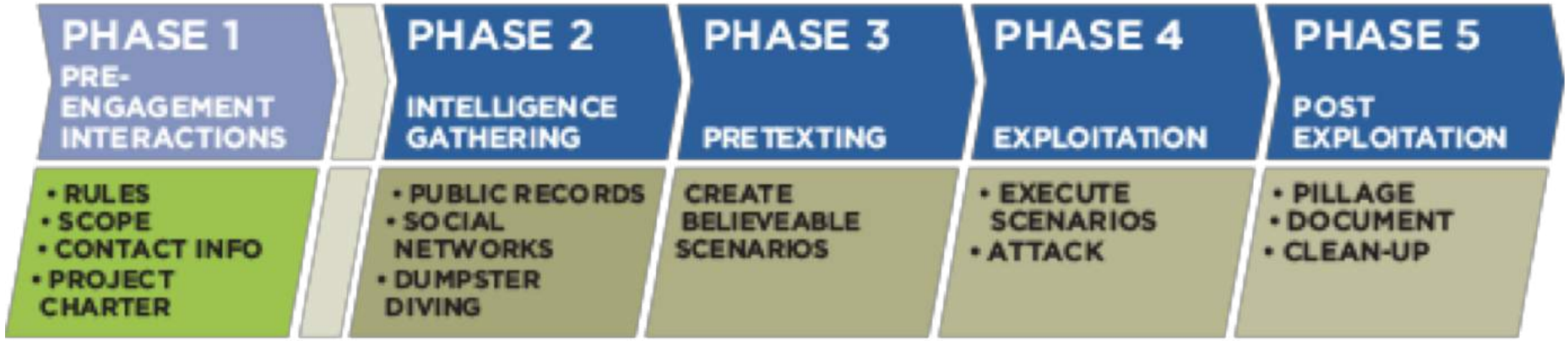


Fake-News


Kontakt mit Fake News
13 % Kommentieren Fake News
2 % Stellen Fake News ein
STOP
Einstellung zu Fake News
84 % Fake News stellen eine Gefahr dar
84 % Fake News manipulieren Meinung der Bevölkerung
68 % Fake News schaden der Demokratie
56 % Social Bots stellen eine Gefahr dar
MAX MUSTERMANN
FAKE
48 % Nehmen Fake News wahr
Forderungen
§§§
Gegenmaßnahmen
81 % Schnelle Reaktionen der Behörden
81 % Betreiber müssen böse und erfundene Inhalte löschen
81 % Betreiber sollen Fake News markieren
76 % Transparenter und selbstkritischer Journalismus
72 % Einrichtung staatlicher IT-Abwehrzentren
Quelle: www.peasec.de/2019/fake-news
GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

5 Phasen

SOCIAL ENGINEERING

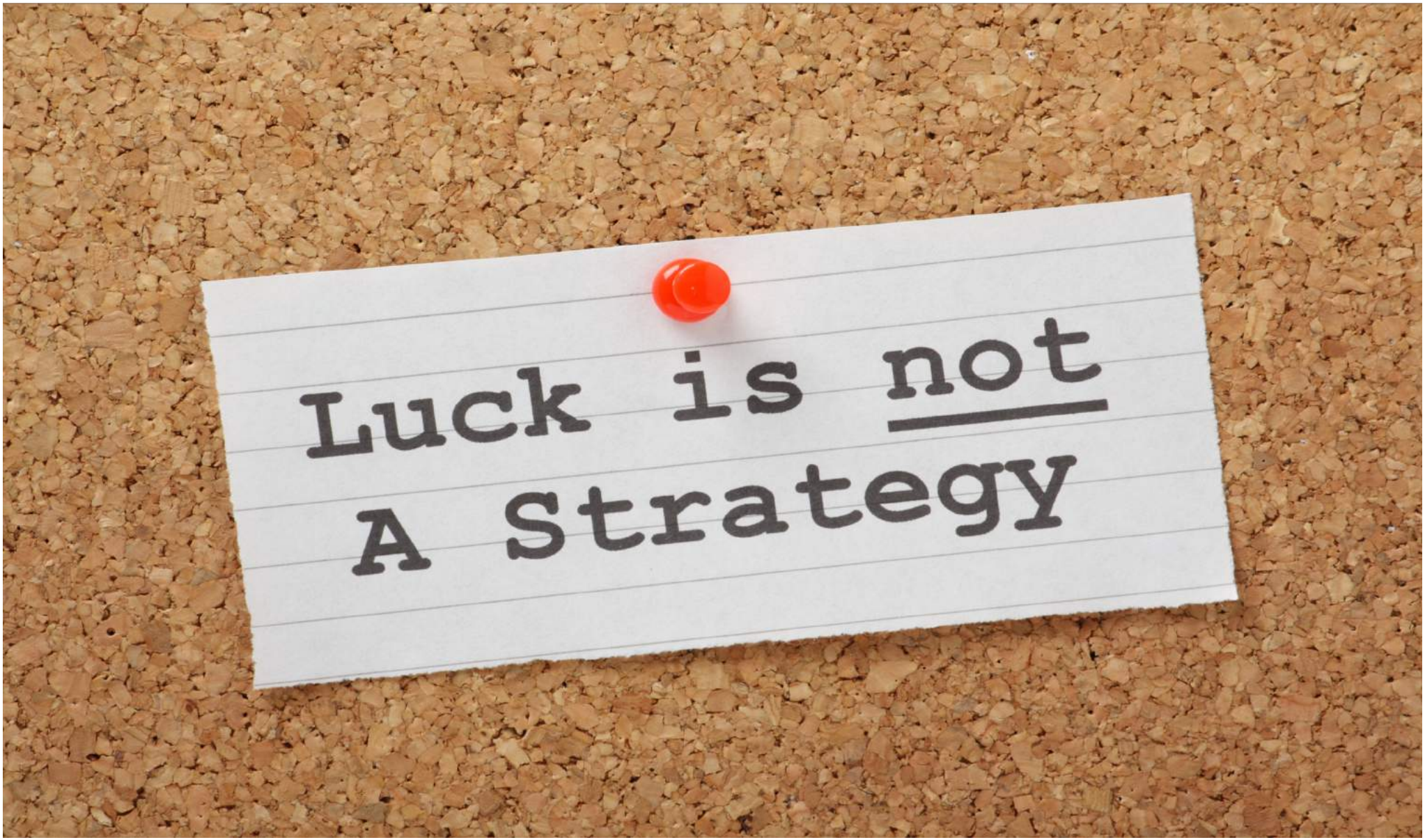


Angriffstechniken

- Dumpster Diving
- Tailgating
- Shoulder Surfing
- Physical Security
- Google
- Helpline
- P2P Hacking
- Kiosks / HotSpots
- Vehicle Surveillance
- Badge Surveillance
- whois
- Social Media

Hilfsmittel

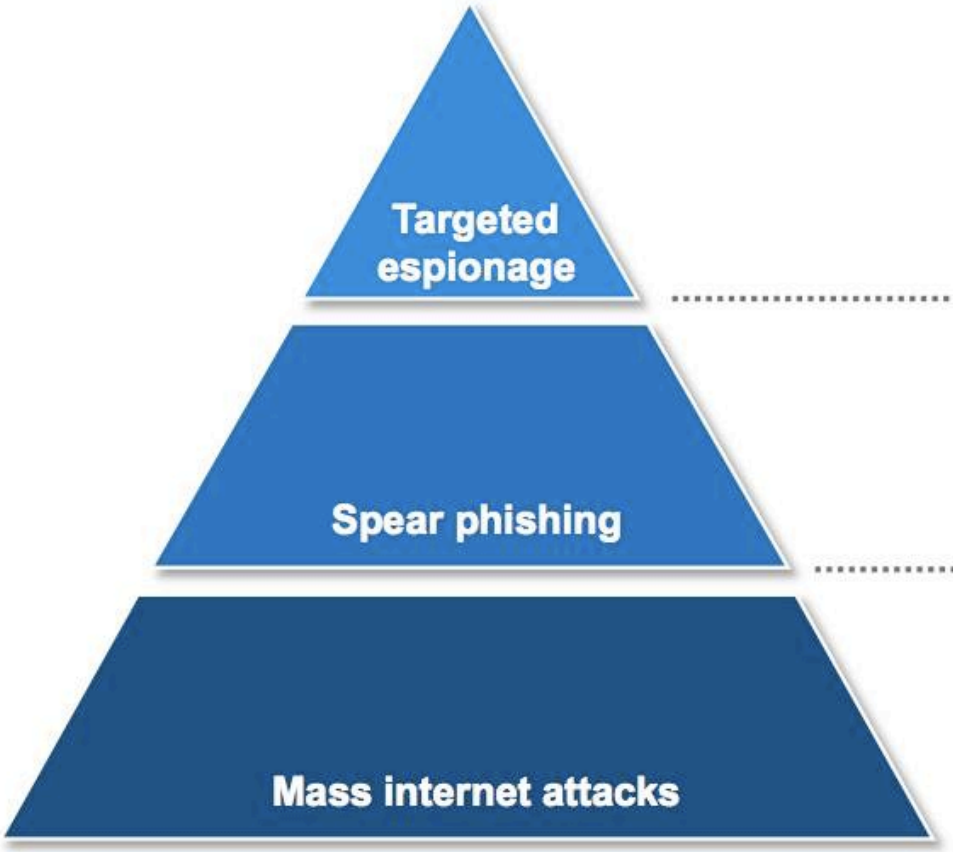
GREIFEN SIE AN!



Strategie

IDEA
CONNECTION
CREATIVITY
20%
20%
60%
CONTENT
PEOPLE
LIKE
SHARE
WEB
SOCIAL
FRIENDS
RESEARCH
INFORMATION
TECHNOLOGY
ANALYSIS
NETWORK
GROWTH
ACCESS
MANAGEMENT
GROUP
COMMUNITY
FEEDBACK
STRATEGY
WHO
WHEN
SOLUTION
SECURITY
TEAMWORK
PLANNING
WHAT
WHY
SUCCESS
MARKETING
INNOVATION
VISION
TARGET
WHERE
HOW
GOAL
SKILLS

Abwehr



- Target is *intellectual property* or *operational data*
- Warrant specific exploit research
- High potential revenue per unit

- *Ability to act* is targeted
- Medium revenue per unit
- **BBB/IRS/DOJ spear phishing**

- *Computing power* or *ability to act* is targeted
- Low revenue per unit
- **Drive by exploits**

Preparing the ground for the attack:

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).

Closing the interaction,
ideally without arousing suspicion:

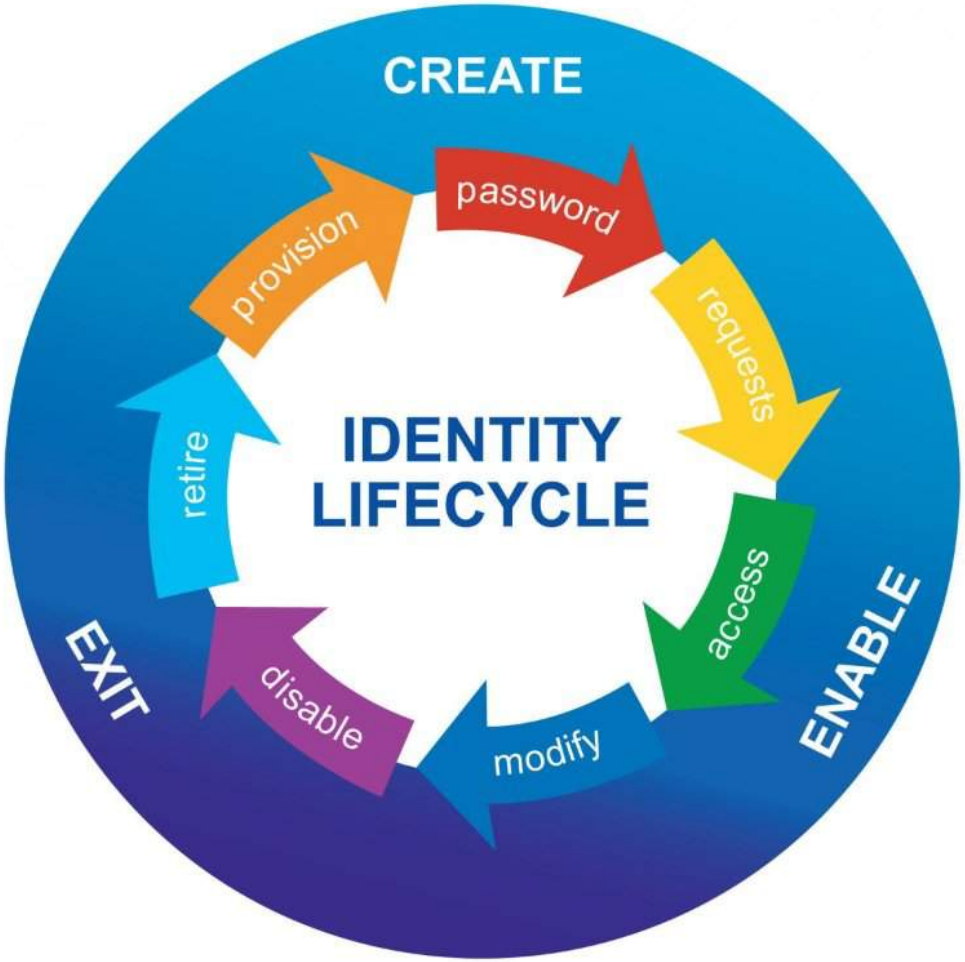
- Bringing the charade to a natural end.
- Removing all traces of malware.
- Covering tracks.

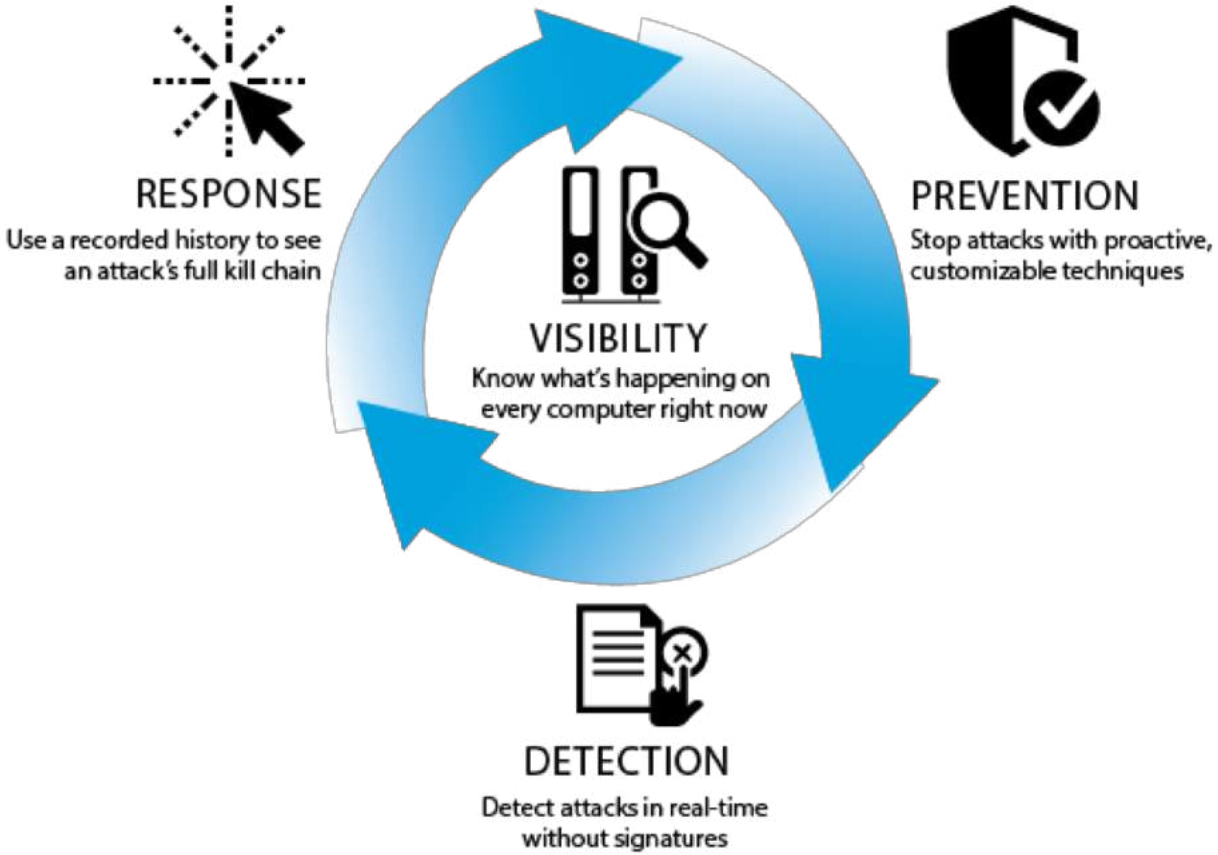
Deceiving the victim(s) to gain a foothold:

- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.


CREATE
password
requests
ENABLE
access
modify
disable
EXIT
retire
provision
IDENTITY
LIFECYCLE


RESPONSE
Use a recorded history to see an attack's full kill chain
PREVENTION
Stop attacks with proactive, customizable techniques
VISIBILITY
Know what's happening on every computer right now
DETECTION
Detect attacks in real-time without signatures

Tipps gegen Phishing

(Benutzernamen, Passwörter, TANs etc.) per E-Mail, via Link oder telefonisch übermitteln.

Seriöse Unternehmen erfragen keine persönlichen Daten per E-Mail oder Chat.

Verdächtige E-Mails löschen und keine darin enthaltenen Links klicken.

Nie unbekannte Dateianhänge in E-Mails öffnen (Achtung: Schadsoftware!).

Tips for avoiding a Social Engineering Attack

LIMIT PUBLIC INFORMATION:

Limit the amount of personal information that you share online.

BE SKEPTICAL:

Always question requests for sensitive information.

TRUST BUT VERIFY:

Don't share information with people you don't know unless you can verify their identity.

CALL THEM BACK:

Through the main switchboard if possible.

NO PASSWORDS OVER THE PHONE:

Never share your password with anyone over the phone.

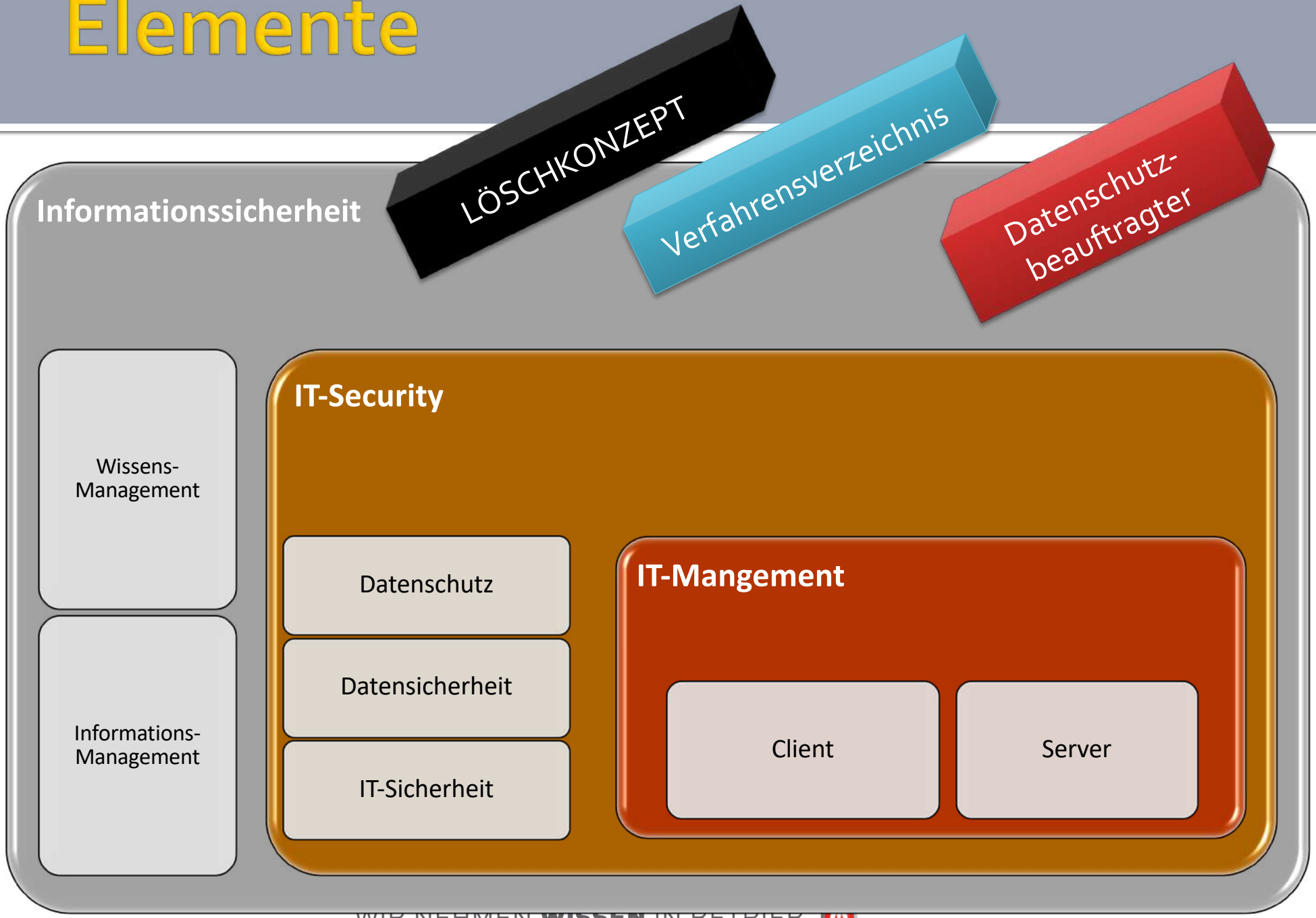
Wordfence™

wordfence.com/learn

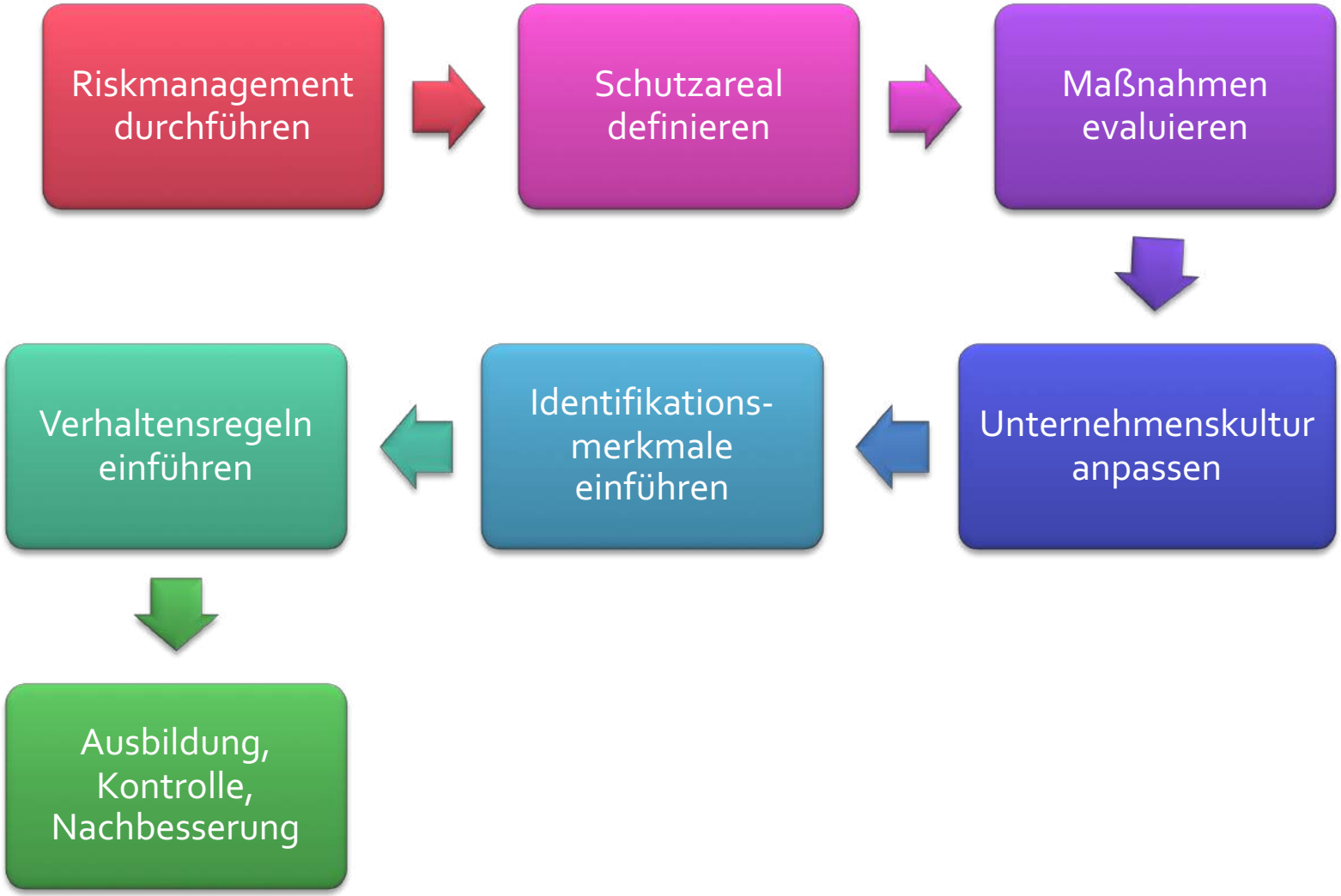
WIR NEHMEN **WISSEN** IN BETRIEB.

Informationssicherheit

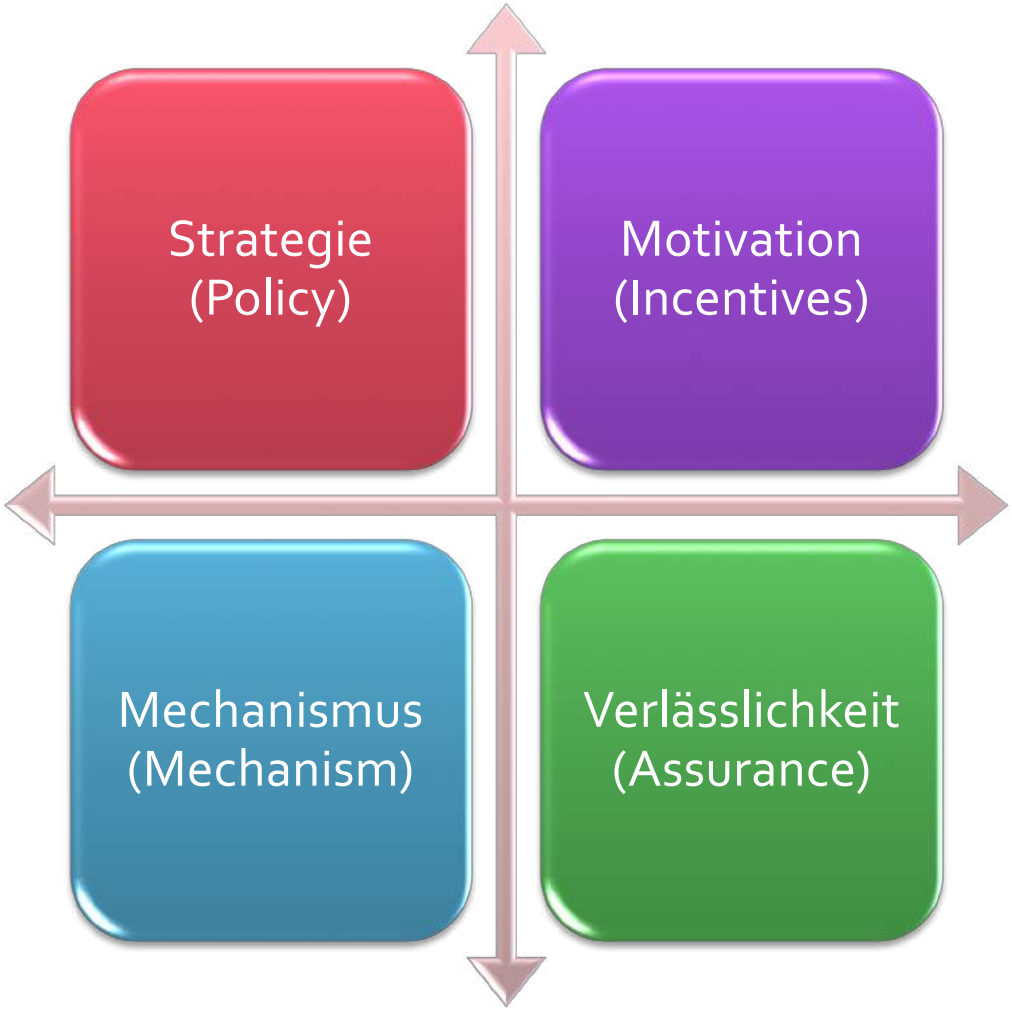
Elemente


LÖSCHKONZEPT
Verfahrensverzeichnis
Datenschutz-beauftragter
Informationssicherheit
Wissens-Management
Informations-Management
IT-Security
Datenschutz
Datensicherheit
IT-Sicherheit
IT-Mangement
Client
Server

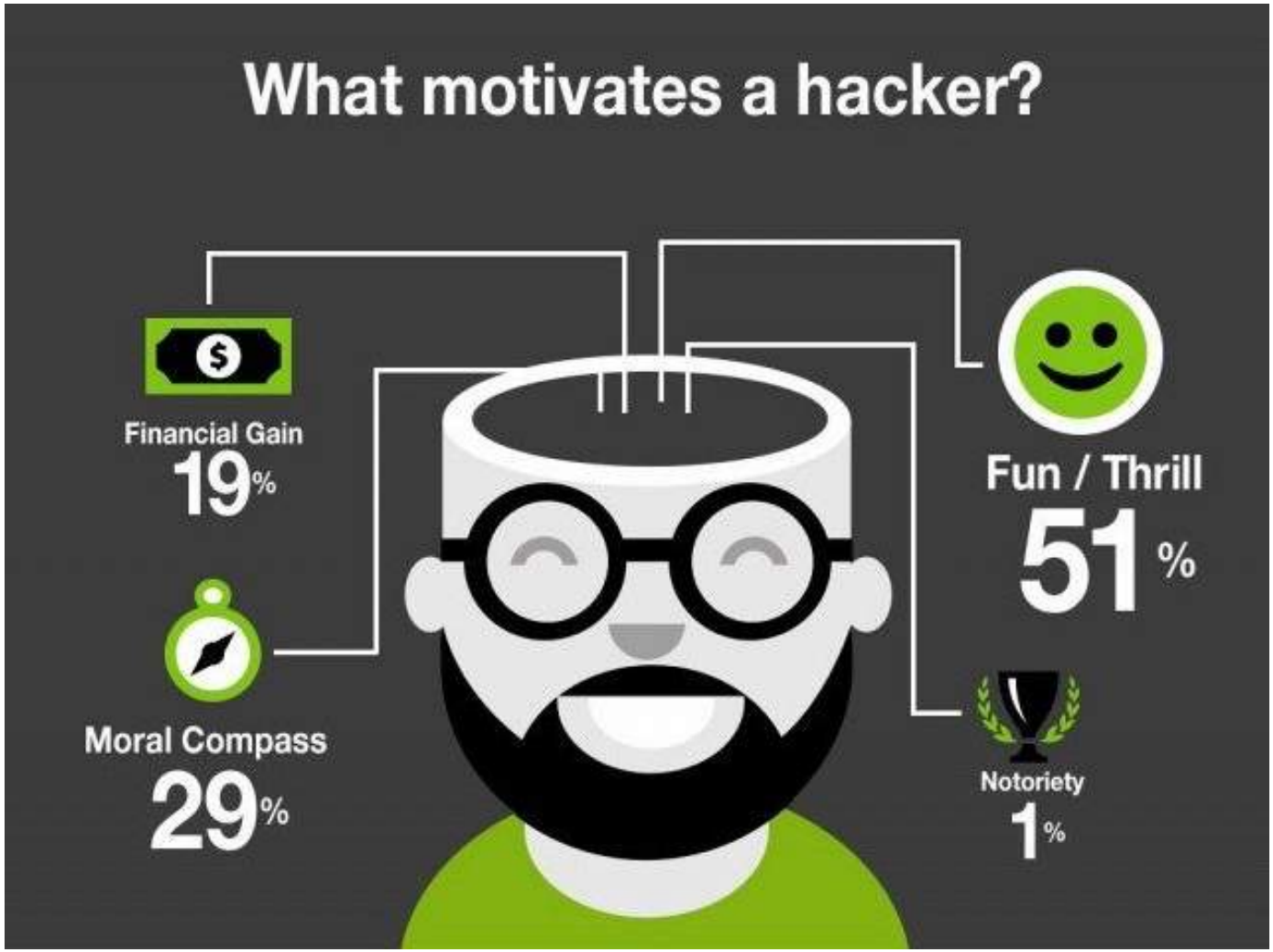
Abwehr Org.Prozess



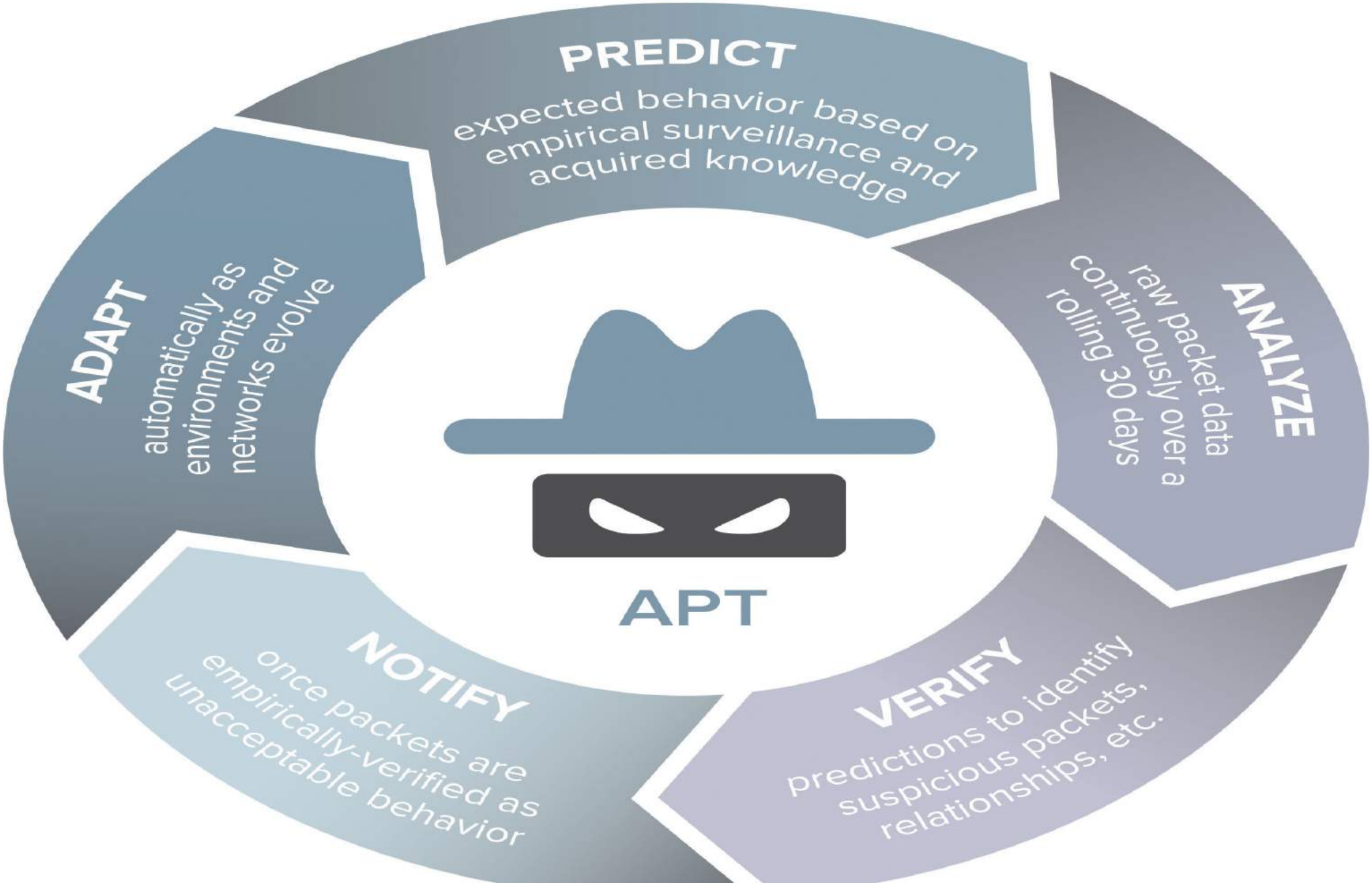
Security Framework



basierend auf Security Engineering, Anderson, 2008


What motivates a hacker?
Financial Gain
19%
Moral Compass
29%
Fun / Thrill
51%
Notoriety
1%

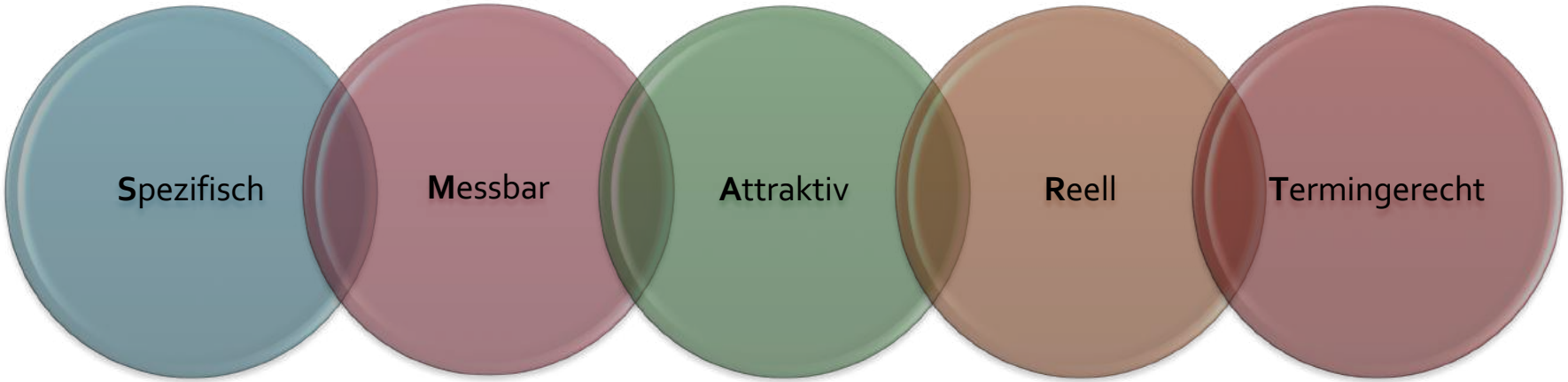
Advanced Persistent Threat Management



Schulung nach Grabl/Kortschak

- Sensibilisierung der Gefahr
- Auflistung der Angriffstechniken
- Lernen diese zu identifizieren
- Handlungsverfahren schulen
- Unternehmenskultur gegen SE aufbauen

SMARTE Ziele



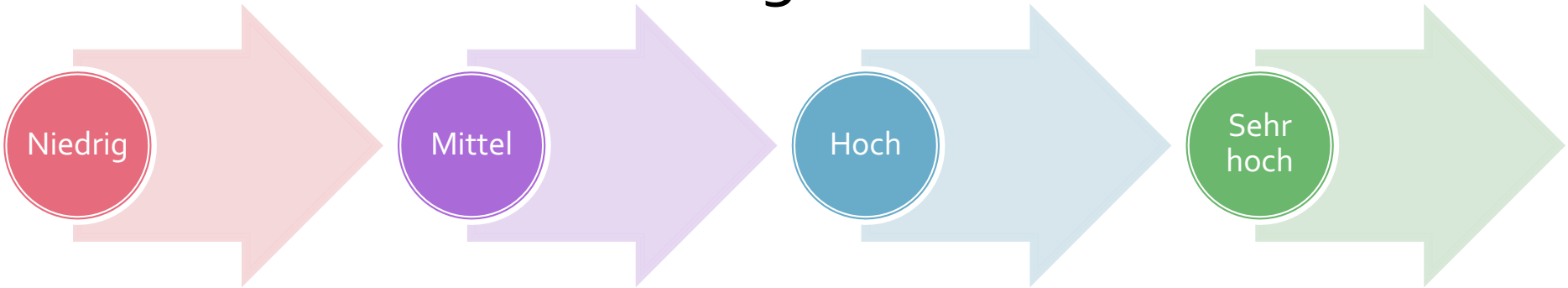
Risikoabschätzung - Beispiel

$$R = E \times A == (B \times V) \times A$$

$$E = B \times V$$

Risiko = Eintrittswahrscheinlichkeit x Auswirkung

EW = Bedrohung x Verwundbarkeit



Behandlung von Risiko / Restrisiko?

Eliminieren
- Systemwechsel
- Prozessänderung

Reduzieren
- Abwehrmaßnahmen
- Gegenmaßnahmen (Firewall, IPS, IDS, ...)

Akzeptieren
- "is so"
- Entscheidung der GF

Transferieren
- Risiko abwälzen (Versicherung)
- Risiko auslagern (Rechenzentrum)

Wir weisen ausdrücklich darauf hin, dass es sich bei den vorliegenden Unterlagen um ein Service der Autoren handelt und die Informationen keine Unternehmensberatung darstellen. Jegliche Haftung für die Aktualität, Richtigkeit und Vollständigkeit der dargestellten Informationen wird ausgeschlossen.

Alle Rechte, insbesondere das Recht der Vervielfältigung und Verbreitung sowie der Übersetzung, vorbehalten. Kein Teil dieser PowerPoint-Präsentation darf in irgendeiner Form ausserhalb des UBIT-Bildungsportales (durch Fotokopie, Mikrofilm oder ein anderes Verfahren) ohne schriftliche Genehmigung der Autoren reproduziert oder unter Verwendung elektronischer Systeme gespeichert, verarbeitet, vervielfältigt oder verbreitet werden.

Die für Schulen und Hochschulen vorgesehene freie Werknutzung „Vervielfältigung zum eigenen Schulgebrauch" gilt für dieses Werk nicht, weil es seiner Beschaffenheit und Bezeichnung nach nicht zum Unterrichtsgebrauch bestimmt ist.