

CASA

CYBER SECURITY IN THE AGE
OF LARGE-SCALE ADVERSARIES

Cybersicherheit, machbar

Sichere Routinen im digitalen Alltag

M. Angela Sasse | Chair for Human-Centred Security
Ruhr University Bochum | Cluster of Excellence - CASA

RUHR
UNIVERSITÄT
BOCHUM

RUB

Gefördert durch

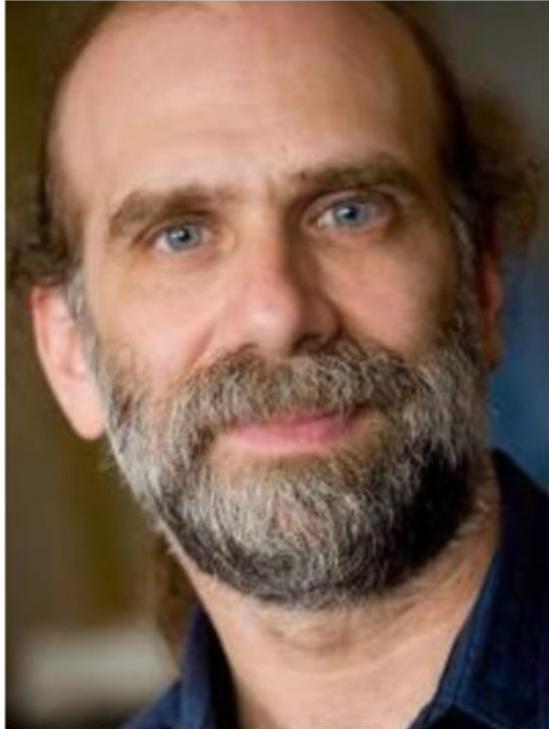
DFG

Deutsche
Forschungsgemeinschaft

HGI
HORST
GÖRTZ
INSTITUT

Lehrstuhl Human-Centred Security





People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems.

— *Bruce Schneier* —

AZ QUOTES

UNPREDICTABLE HUMANS: Still the weakest link in data security

Insider threat
emanates from unintentional or malicious behavior by employees, former employees, contractors or partners with knowledge of the network and security practices.

78%

of security professionals say the biggest threat to endpoint security is negligent or careless employees who do not follow security policies



The average organization experiences **9.3 insider threats** per month*

90%

of organizations experience at least one insider threat each month*



In 2003, U.S. companies suffered **\$40 billion** in losses from unauthorized use of computers by employees*

95%

of all successful cyber attacks is caused by human error

Source: IBM Cyber Security Intelligence Index



THE HUMAN FACTOR THE WEAKEST LINK IN DATA PROTECTION

A company's greatest asset — its employees — can also be its weakest link. Improperly trained and/or negligent employees can be the biggest hole in a company's security protection.

EMPLOYEE NEGLIGENCE PUTS AN ORGANIZATION AT RISK.

>78% of organizations have suffered from at least one data breach over the past two years.

8% of organizations alter internal controls as the main reason for a data breach despite the growing

J
♠

Are
YOU
the weakest



LINK?

The chain of security
is in your hands.



Humans are the weakest link



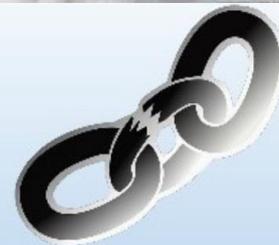
Page 4

Security Analyst Summit 2013, Puerto Rico

KASPERSKY

Weakest Link?

- No matter how strong your:
 - Firewalls
 - Intrusion Detection Systems
 - Cryptography
 - Anti-virus software
- **You** are the **weakest link** in computer security!
 - People are more vulnerable than computers
- "The weakest link in the security chain is the human element" -Kevin Mitnick



Falscher Ausgangspunkt:
Die Menschen sind
“defekt”, und müssen
durch Schulungen
“repariert” werden



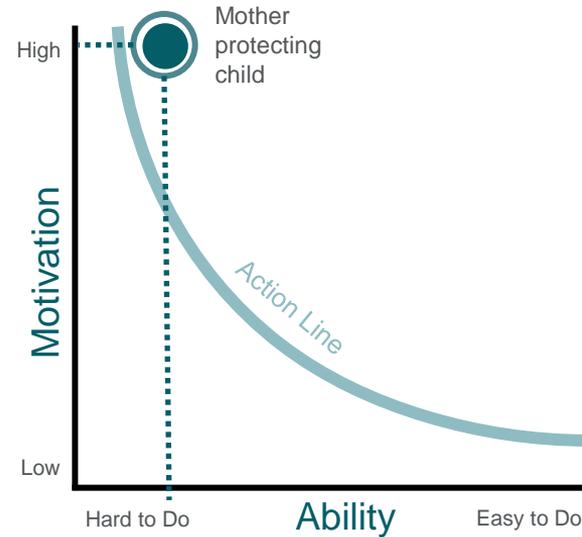
FOGG BEHAVIOR MODEL

Voraussetzung für
erfolgreiche
Verhaltensänderung:
Motivation +
Machbarkeit.
Dann können Auslöser
effektiv sein



MOTIVATION REICHT NICHT

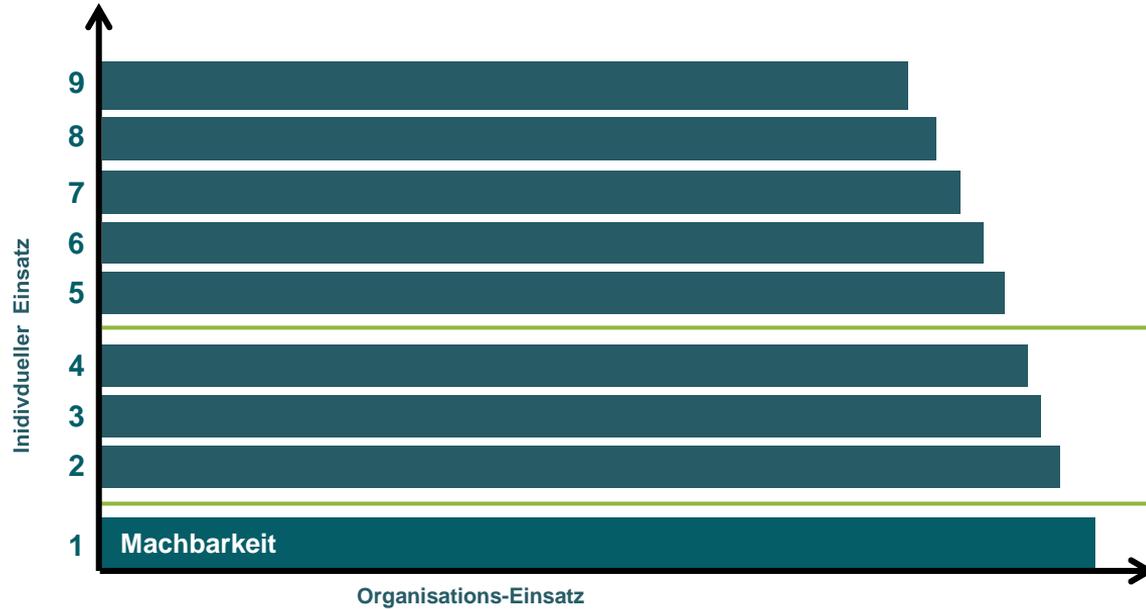
Viel Motivation kann kurzfristig Aktivität auslösen – aber ohne Machbarkeit keine nachhaltige Verhaltensänderung



Die Sicherheits-Lernkurve

Sichere Routinen im digitalen Alltag

DIE SICHERHEITS-LERNKURVE



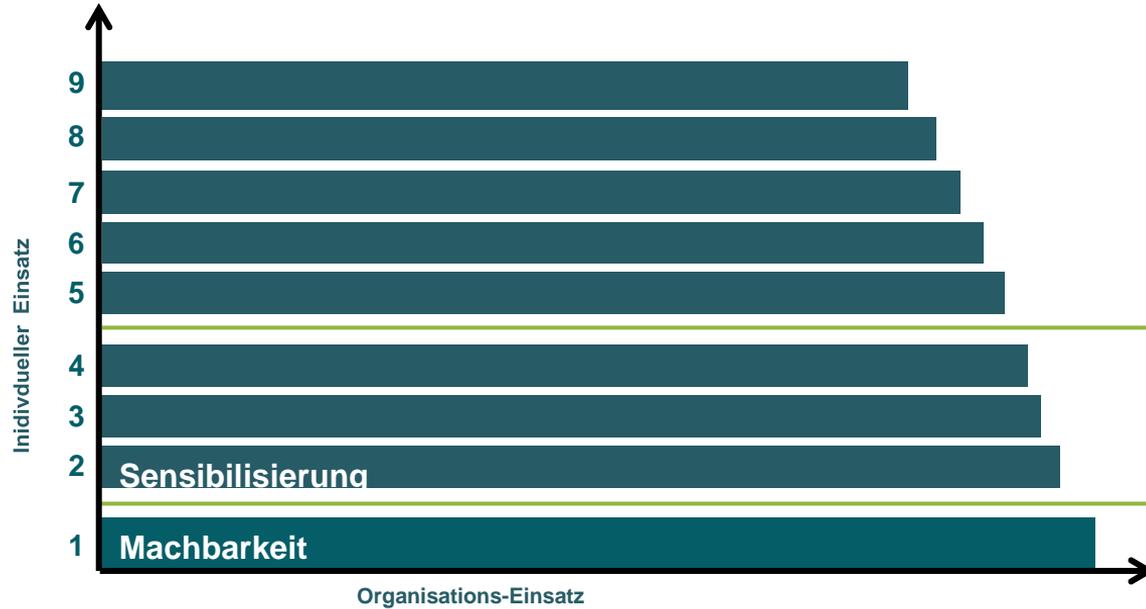
VORAUSSETZUNG: MACHBARKEIT

Ständiges
Wiederholen von
nicht-machbaren
Regeln ist
kontraproduktiv



“Never give an order that can’t be obeyed”
General Douglas MacArthur 1880-1964

DIE SICHERHEITS-LERNKURVE



THE SECURITY LEARNING CURVE

Steps to transforming security behavior (based on HPE Awareness Maturity Curve)



INFORMATION: WENIGER IST MEHR

Nicht sinnvoll: Nutzer zu “mini-me”
Sicherheitsexperten machen

Inhalt von Sicherheitskommunikation:
Relevanz, Konsistenz,
nutzergerechte Sprache

Relevante Kommunikations-Kanäle
nutzen



THE SECURITY LEARNING CURVE

Steps to transforming security behavior (based on HPE Awareness Maturity Curve)



THE SECURITY LEARNING CURVE

Steps to transforming security behavior (based on HPE Awareness Maturity Curve)



KONKORDANZ

Verhandeln

Verpflichten



REAKTANZ: ERKENNEN

- Instinktiver Widerstand, weil: Veränderung ist schwer
- Menschen reagieren so wenn
 - Sie nicht mit Zielen übereinstimmen
 - Die Regeln keinen Sinn machen
 - Passive Gefolgschaft erwartet wird
 - Führungskräften nicht vertraut wird



REAKTANZ: GEGENSTEUERN

1. **Zuhören!** (bloss nicht sofort Gegendruck machen)
 - Mit Verstand zuhören: was ist das Problem?
 - Mit Gefühl zuhören: was verärgert, ängstigt?
2. **Gemeinsame Ziele und Werte** finden, Sicherheitsverhalten herleiten
3. **Auslöser** für die negative Reaktion finden, entfernen

DIE SICHERHEITS-LERNKURVE



DIE SICHERHEITS-LERNKURVE

Steps to transforming security behavior (based on HPE Awareness Maturity Curve)



SEBLSTWIRKSAMKEIT: ICH SCHAFFE DAS!

1. Verhalten ausprobieren können, ohne Druck
2. Gemeinsam Lernen ist effektiver als allein!
3. Positive Erfahrungen und Beispiele schaffen

DIE SICHERHEITS-LERNKURVE



INTENTIONALES VERGESSEN

1. Bestehende Routinen "bewusst vergessen"
2. Auslöser für unsicheres Verhalten finden und entfernen:
Namen, Objekte, Bildschirme
3. Kollektives Vergessen ist noch schwieriger als
individuelles Vergessen – gegenseitig erinnern
4. Beispiel wie man es nicht macht: "Passwort-Manager"

DIE SICHERHEITS-LERNKURVE



EINBETTEN

1. Verhalten im Handlungs-Kontext ausführen
2. Wiederholen, wiederholen, wiederholen
3. Rückmeldung und Belohnung/Sanktionen

DIE SICHERHEITS-LERNKURVE



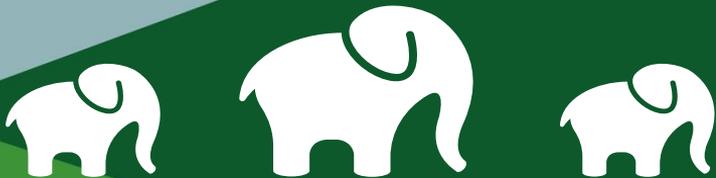
ZUSAMMENFASSUNG

1. Sicheres Verhalten muss machbar sein.
2. Lernende müssen Risiken und Konsequenzen verstehen
3. Zielsetzung und Gestaltung von Sicherheitsmassnahmen gemeinsam erarbeiten
4. Selbstwirksamkeit stärken: positive Erfahrungen schaffen, dass sicheres Verhalten möglich ist
5. Auslöser von unsicherem Verhalten identifizieren & entfernen
6. “Einbetten” durch Wiederholung, positives Feedback

CASA

CYBER SECURITY IN THE AGE
OF LARGE-SCALE ADVERSARIES

Fragen?



casa.rub.de