Warum wir auf Phishing hereinfallen

Und was man dagegen
tun kann.

Werner Degenhardt, Code and Concept

Abstract & Agenda

Abstract

Phishing ist das wichtigste Einfallstor für Schadsoftware und überhaupt Schaden aller Art. Bei mehr als 90% aller erfolgreichen Cyber-Angriffe war eine Phishing-Email das wichtigste Werkzeug des Angreifers.

Tatsächlich fallen Nutzer selbst auf die einfachsten Phishing-Emails herein. Viele Techniker und Sicherheitsexperten sind deswegen verwirrt, wissen nicht, wie sie reagieren sollen und kommen zur Meinung, dass Benutzer nicht in der Lage sind die nötigen Sicherheitsaufgaben zu erledigen und die richtigen Entscheidungen zu treffen.

Sie neigen dazu, den Benutzer als "Weakest Link" als dauerhaft inkompetent anzusehen und beschäftigen sich lieber mit technischen Lösungen als mit der Härtung der "Human Firewall".

Agenda

- Anatomie eines erfolgreichen Ransomware-Angriffs
- Wie konnte das passieren?
- Wie der Mensch wirklich funktioniert
- Kognitive und soziale Heuristiken
- Warum gute Menschen schlechte Entscheidungen treffen
- Härten der „Human Firewall“: Awarenesskampagnen, Training, Ausbildung
- Sicherheitskultur fehlertoleranter Organisationen

codeandconcept

Agenda

- Anatomie eines erfolgreichen Ransomware-Angriffs
- Wie konnte das passieren?
- Wie der Mensch wirklich funktioniert
- Kognitive und soziale Heuristiken
- Warum gute Menschen schlechte Entscheidungen treffen
- Härten der „Human Firewall“: Awarenesskampagnen, Training, Ausbildung
- Sicherheitskultur fehlertoleranter Organisationen


Haupteingang
Besucher
Lukaskranken haus
Picasa
Bedingungen
Datenschutz

codeandconcept

Agenda

- Anatomie eines erfolgreichen Ransomware-Angriffs
- Wie konnte das passieren?
- Wie der Mensch wirklich funktioniert
- Kognitive und soziale Heuristiken
- Warum gute Menschen schlechte Entscheidungen treffen
- Härten der „Human Firewall“: Awarenesskampagnen, Training, Ausbildung
- Sicherheitskultur fehlertoleranter Organisationen

Die Leute sind die letzte Verteidigungslinie …

- 91% aller erfolgreichen Sicherheitsvorfälle begannen mit einer Phishing E-Mail (Trend Micro)
- Es ist faszinierend — und entmutigend — dass über 95% aller untersuchten Vorfälle einen “human error” als kausalen Faktor nennen (IBM).
- Der Schaden durch CEO Fraud wird mit 5.3 Milliarden Dollar jährlich beziffert
- Ransomware setzte 2017 1 Milliarde Dollar um und wächst weiterhin exponentiell

… aber sie tun nicht so, wie sie tun sollen

Alle Sicherheitssysteme hängen von Menschen ab, und Menschen sind fehleranfällig, leichtgläubig, bestechlich, emotional, und gierig.

(Fred Sampson, A penny for your thoughts, a latte for your password)

Gleichgültigkeit, Ignoranz, Nachlässigkeit, mangelhaftes Sicherheitsbewusstsein, Boshaftigkeit and Widerstand gegen Sicherheitsrichtlinien sind in vielen Fällen der eigentliche Grund für Sicherheitsvorfälle.

(Safa, Nader et al., Human aspects of information security in organisations)

3 Wahrheiten über die menschliche Natur: Wir sind faul, wir sind sozial, und wir sind Gewohnheitstiere. Produkte und Verfahren müssen für diese Realität entwickelt werden.

http://bit.ly/bjfoggcamp

Infosec‘s dirty little secret …

"Eine Armee talentierter Mathematiker, Computer-wissenschaftler und Ingenieure haben über Jahrzehnte hinweg eine elegante Lösung nach der anderen zur Lösung der Probleme der IT-Sicherheit vorgeschlagen.

Die Benutzer haben bisher alle Bemühungen boykottiert."

Greenwald, Infosec's dirty little secret, NSPW 2004

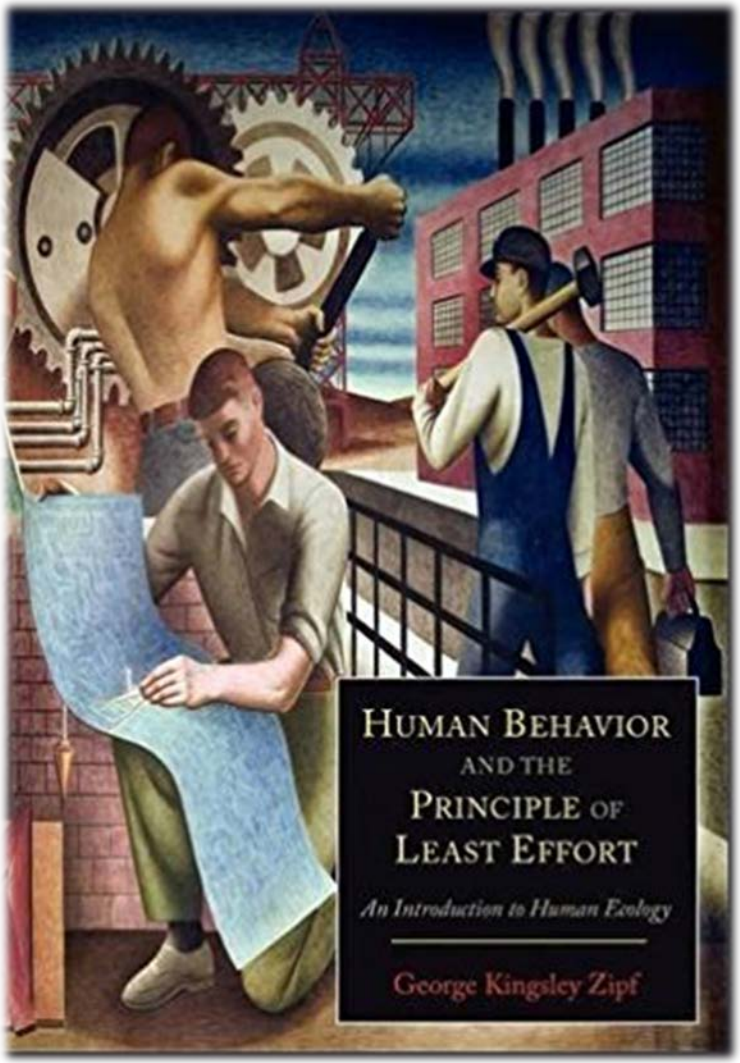
-

codeandconcept

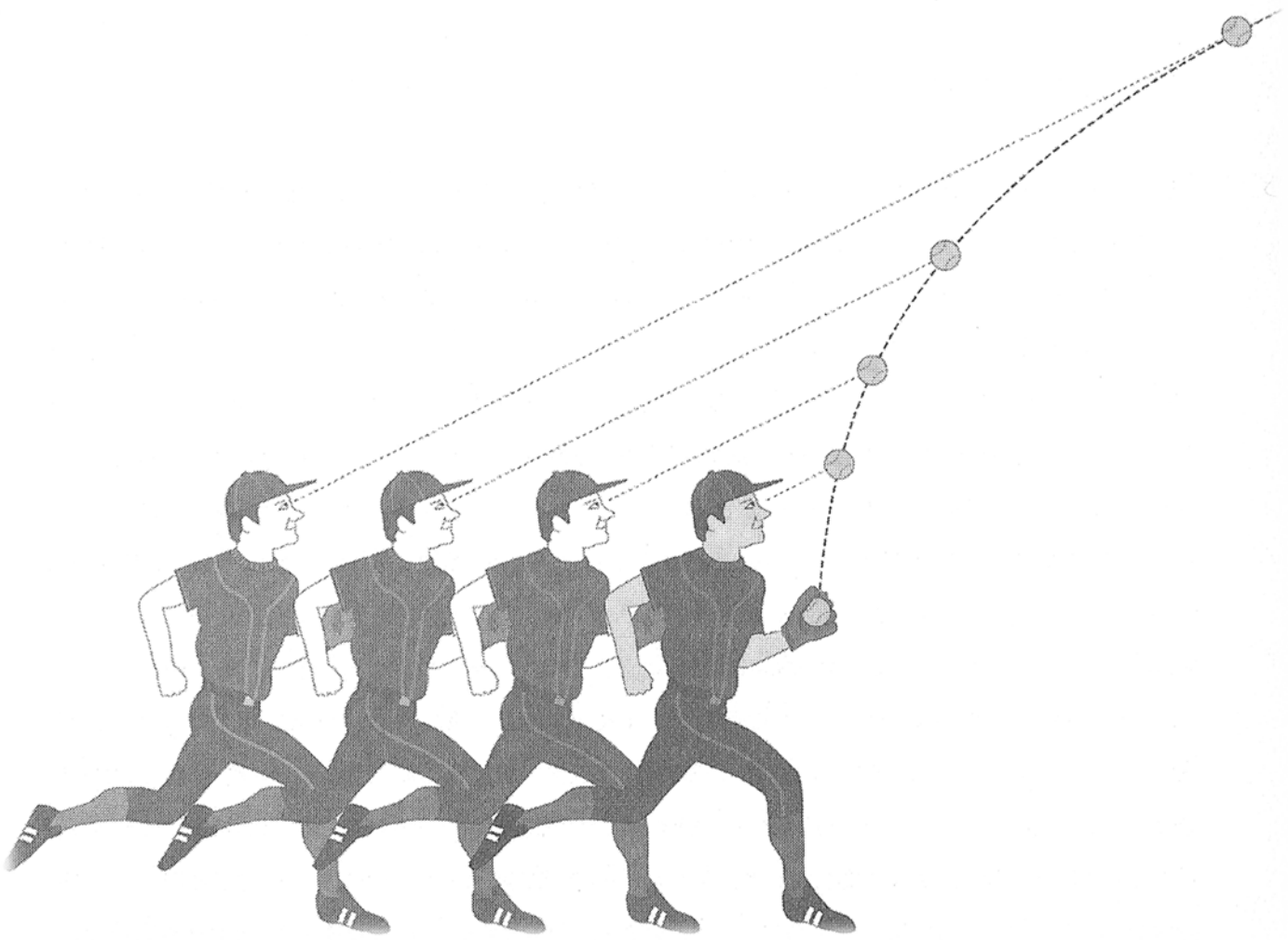
Agenda

- Anatomie eines erfolgreichen Ransomware-Angriffs
- Wie konnte das passieren?
- Wie der Mensch wirklich funktioniert
- Kognitive und soziale Heuristiken
- Warum gute Menschen schlechte Entscheidungen treffen
- Härten der „Human Firewall“: Awarenesskampagnen, Training, Ausbildung
- Sicherheitskultur fehlertoleranter Organisationen

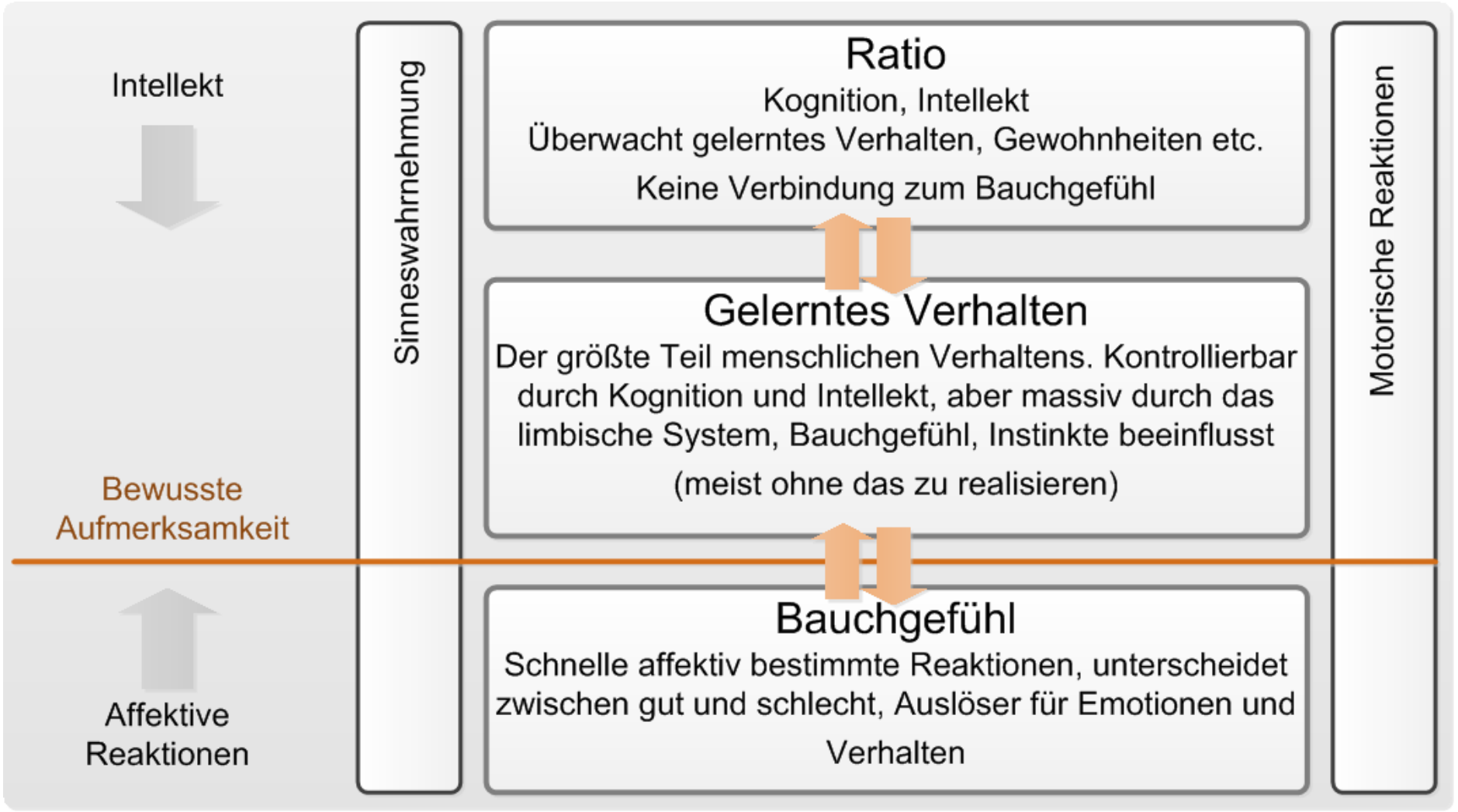
Menschen sind intelligent und effizient …



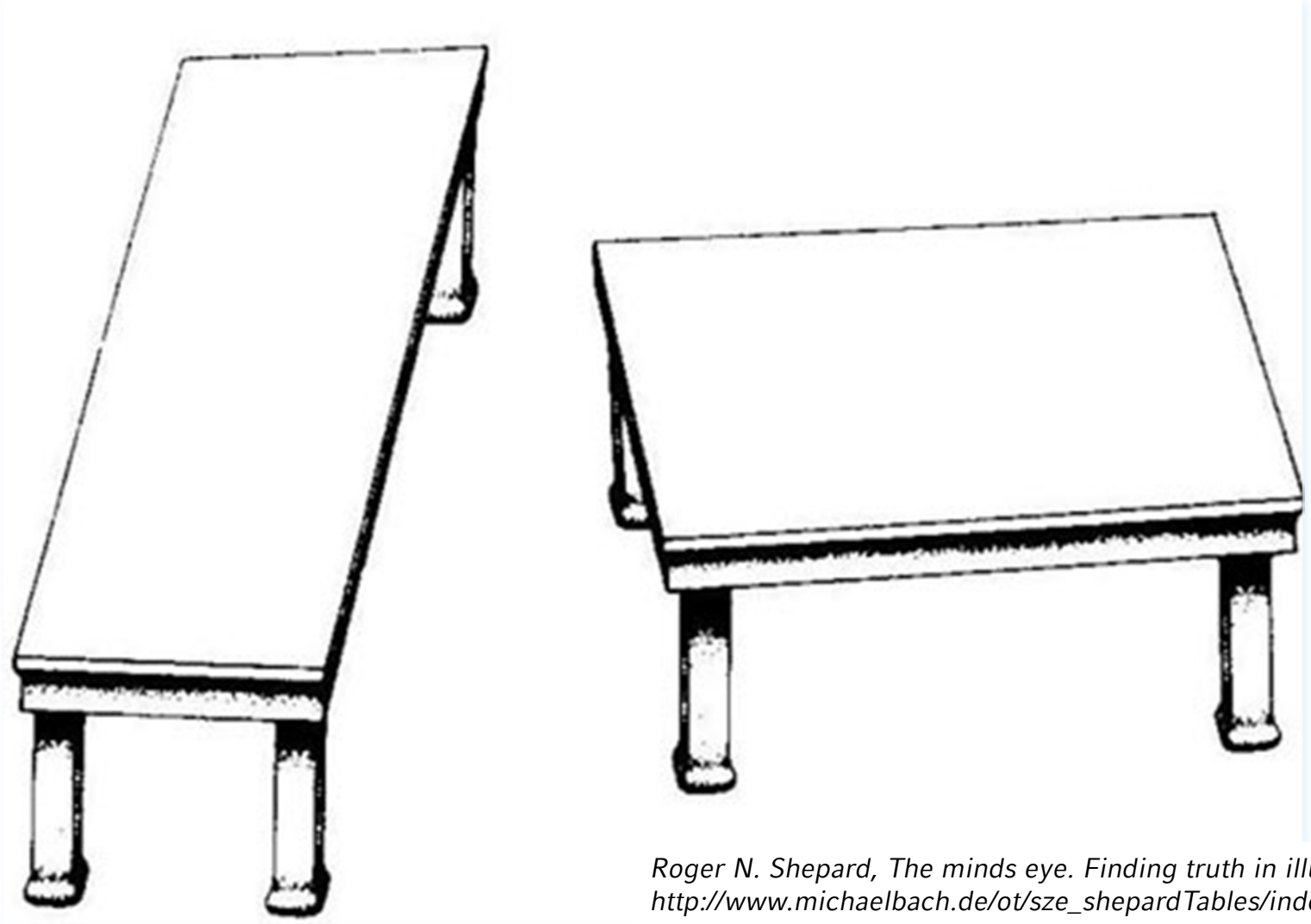
… vor allem, weil sie Heuristiken folgen



Menschliches Verhalten



Ist menschliches Verhalten fest verdrahtet?



Roger N. Shepard, The minds eye. Finding truth in illusion
http://www.michaelbach.de/ot/sze_shepardTables/index.html

Bauchgefühl: Partnerwahl 1

- Der Astronom Johannes Kepler begann nach einer arrangierten und unglücklichen ersten Ehe mit einer systematischen Suche nach seiner zweiten Frau.
- Er prüfte elf mögliche Kandidatinnen in zwei Jahren. Freunde drängten ihn, Kandidatin Nummer vier zu heiraten, eine Dame von Stand mit einer verlockenden Mitgift, doch er war fest entschlossen, seine Nachforschungen fortzusetzen.
- Schließlich wies ihn diese perfekt passenden Bewerberin beleidigt zurück, weil er zu lang mit ihr gespielt habe. Ihr Entschluss war unwiderruflich.

Bauchgefühl: Partnerwahl 2

Ein Mann kann klein und dick und kahlköpfig sein – wenn er feurig ist, mögen ihn die Frauen.

Mae West

-

One Reason Decision Making

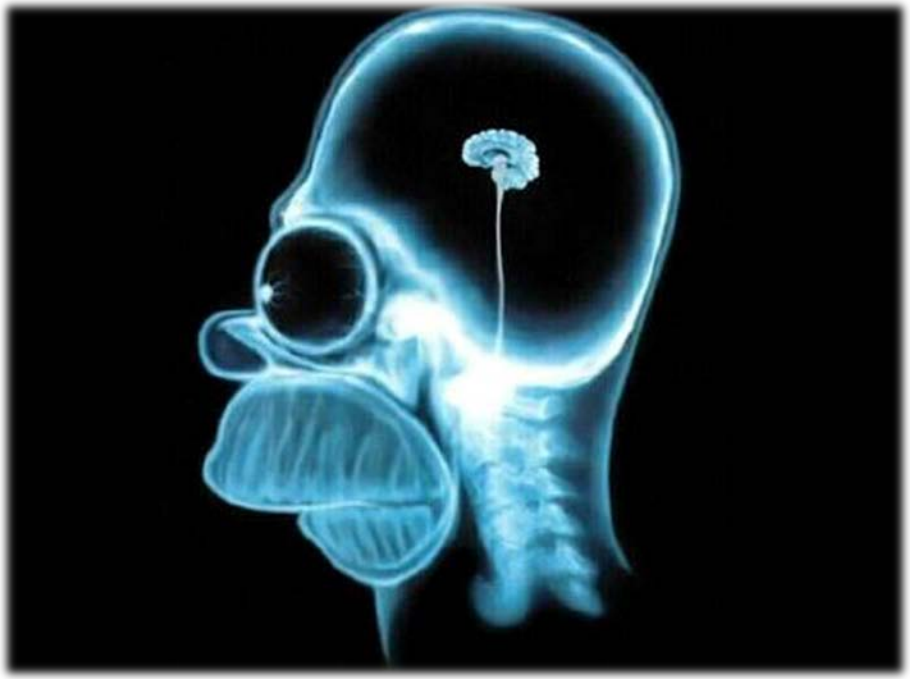
- Menschen haben nur begrenzte Kapazität für die Verarbeitung von Informationen. Wir verwenden Multitasking und sind nur begrenzt aufmerksam.
- Menschen bevorzugen schnelle Entscheidungen auf der Basis von gelernten Regeln und einfachen Heuristiken.
- "One reason decision making" ist hocheffizient und – in der analogen Welt – gut genug.

Gelerntes Verhalten

Irrationaler Problemlöser

Die Mechanik des menschlichen Denkens ist in der Evolution erfunden worden, um Probleme „ad hoc“ zu bewältigen.

Er spielt die Rolle eines Problemlösers, der dann ausnahmsweise eingesetzt wird, um Situationen zu bewältigen, die mit Instinkt, Gewohnheit, Sitte und Tradition nicht zu bewältigen sind.



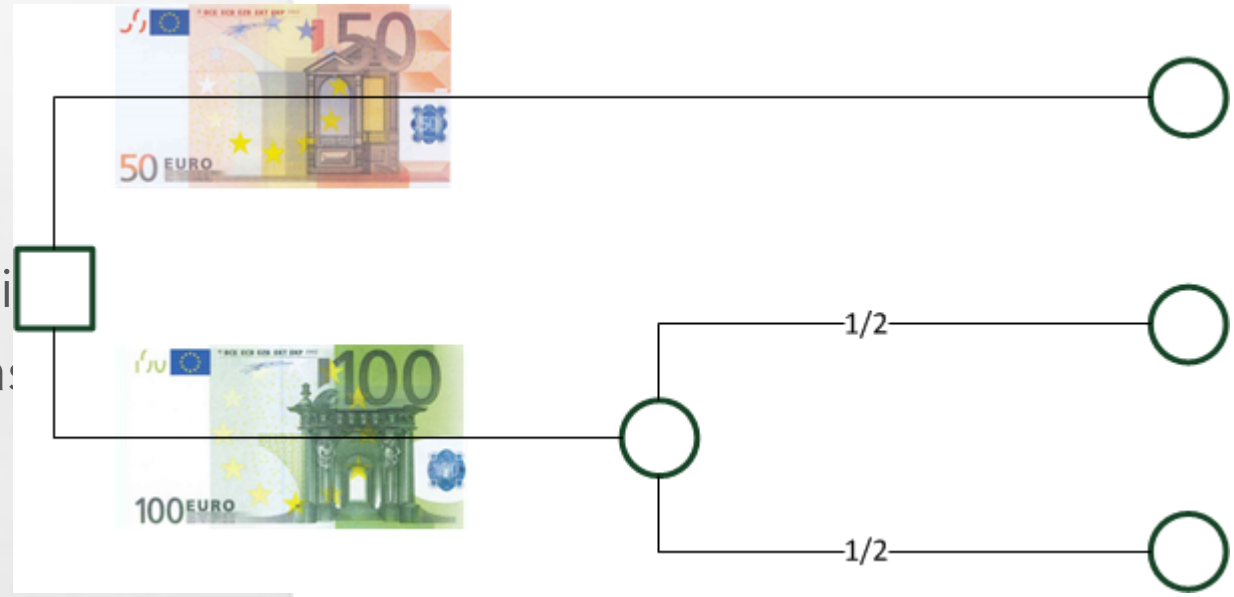
codeandconcept

Agenda

- Anatomie eines erfolgreichen Ransomware-Angriffs
- Wie konnte das passieren?
- Wie der Mensch wirklich funktioniert
- Kognitive und soziale Heuristiken
- Warum gute Menschen schlechte Entscheidungen treffen
- Härten der „Human Firewall“: Awarenesskampagnen, Training, Ausbildung
- Sicherheitskultur fehlertoleranter Organisationen

Kognitive Heuristiken

1. Sure Gain Heuristic
2. Optimism Bias
3. Control Bias
4. Affect Heuristic
5. Availability Heuri
6. Confirmation Bia
7. u.v.a.m



Soziale Heuristiken

1. Reziprozität
2. Commitment & Konsistenz
3. Soziale Bewährtheit
4. Autorität
5. Sympathie
6. Knappheit

1. Vertrauen
2. Moral (ethischer Kompass)

U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: .....MITNICK, KEVIN DAVID
AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office. (Telephone: 213-894-2485).
If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102; (24 hour telephone contact) NLETS access code is VAUSMOOOO.

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

Form USM-13
(Rev. 3/2/82)

November 1992

codeandconcept

Agenda

- Anatomie eines erfolgreichen Ransomware-Angriffs
- Wie konnte das passieren?
- Wie der Mensch wirklich funktioniert
- Kognitive und soziale Heuristiken
- Warum gute Menschen schlechte Entscheidungen treffen
- Härten der „Human Firewall“: Awarenesskampagnen, Training, Ausbildung
- Sicherheitskultur fehlertoleranter Organisationen

Cyberbiologie des Phishing: Arten

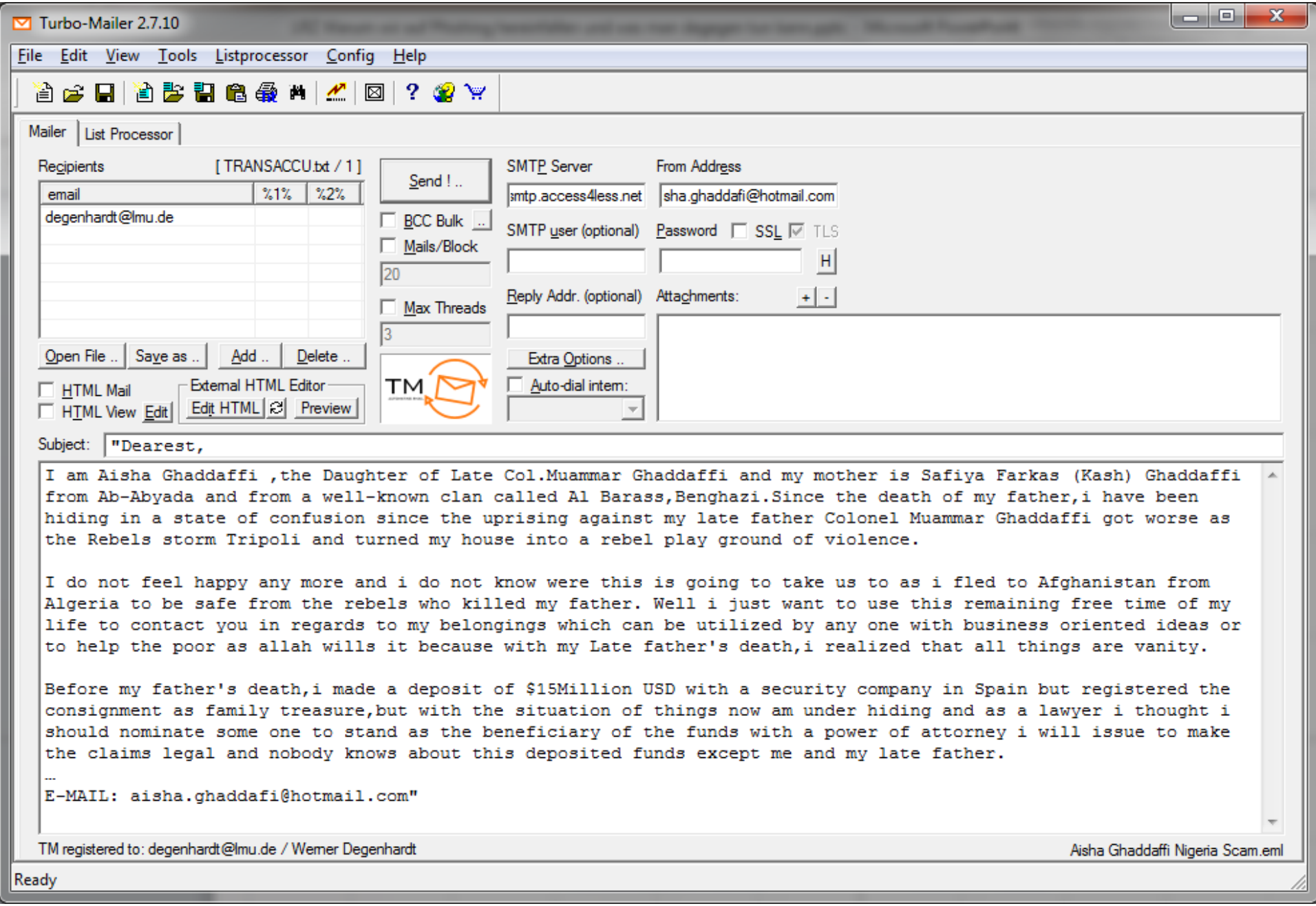
Aufforderung

- Nigeria Scam
- Datei Download

Link

Anhang

Formular


Turbo-Mailer 2.7.10
File Edit View Tools Listprocessor Config Help
Mailer
List Processor
Recipients
[TRANSACCU.txt / 1]
email
%1%
%2%
degenhardt@lmu.de
Open File ..
Save as ..
Add ..
Delete ..
HTML Mail
HTML View
Edit
External HTML Editor
Edit HTML
Preview
Send ! ..
BCC Bulk
Mails/Block
20
Max Threads
3
TM
SMTP Server
smtp.access4less.net
From Address
sha.ghaddafi@hotmail.com
SMTP user (optional)
Password
SSL
TLS
H
Reply Addr. (optional)
Attachments:
+
-
Extra Options ..
Auto-dial intern:
Subject: "Dearest,
I am Aisha Ghaddaffi ,the Daughter of Late Col.Muammar Ghaddaffi and my mother is Safiya Farkas (Kash) Ghaddaffi from Ab-Abyada and from a well-known clan called Al Barass,Benghazi.Since the death of my father,i have been hiding in a state of confusion since the uprising against my late father Colonel Muammar Ghaddaffi got worse as the Rebels storm Tripoli and turned my house into a rebel play ground of violence.
I do not feel happy any more and i do not know were this is going to take us to as i fled to Afghanistan from Algeria to be safe from the rebels who killed my father. Well i just want to use this remaining free time of my life to contact you in regards to my belongings which can be utilized by any one with business oriented ideas or to help the poor as allah wills it because with my Late father's death,i realized that all things are vanity.
Before my father's death,i made a deposit of $15Million USD with a security company in Spain but registered the consignment as family treasure,but with the situation of things now am under hiding and as a lawyer i thought i should nominate some one to stand as the beneficiary of the funds with a power of attorney i will issue to make the claims legal and nobody knows about this deposited funds except me and my late father.
...
E-MAIL: aisha.ghaddafi@hotmail.com"
TM registered to: degenhardt@lmu.de / Werner Degenhardt
Aisha Ghaddaffi Nigeria Scam.eml
Ready

Cyberbiologi

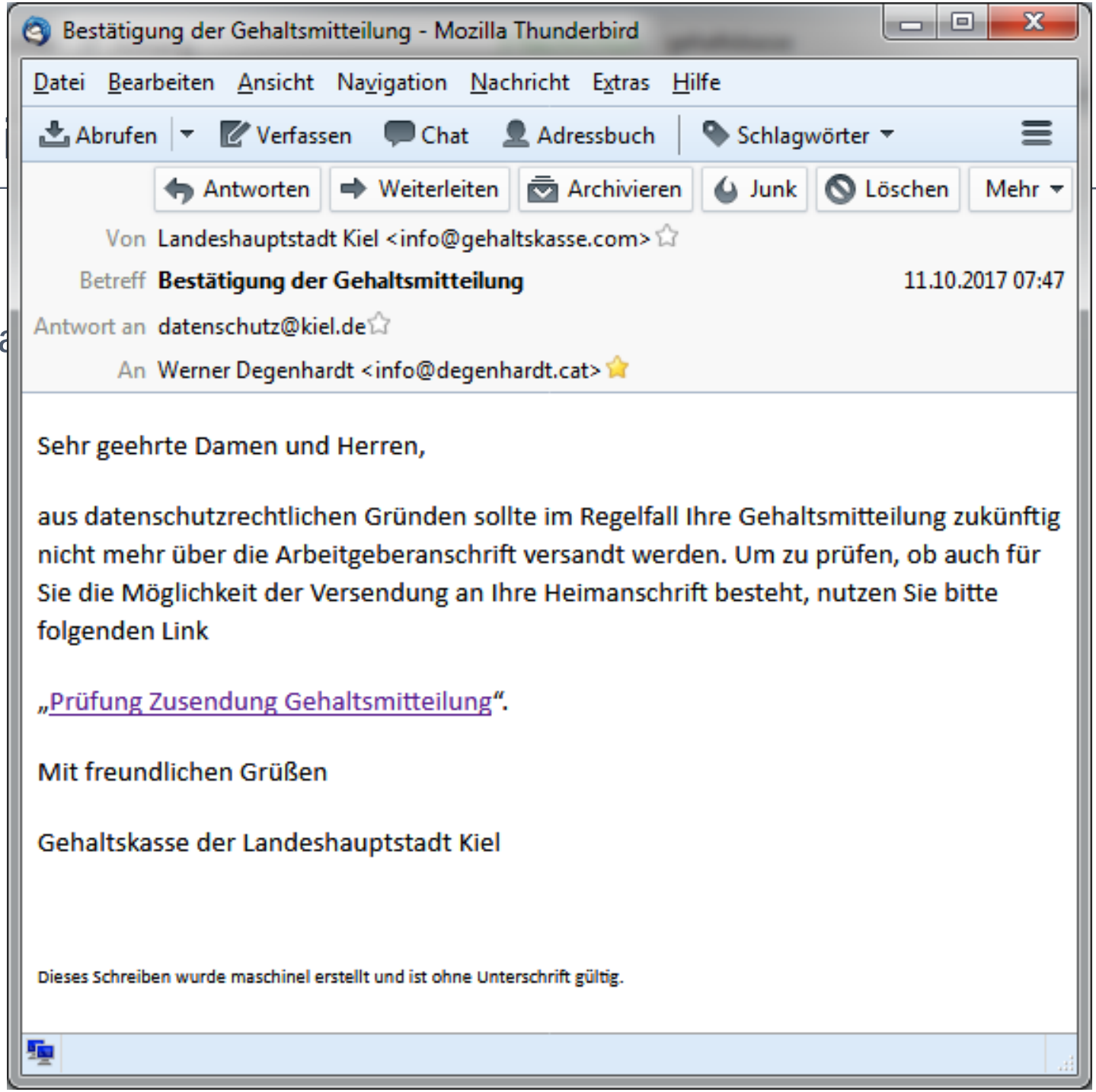
Aufforderung

- Nigeria Scam
- Datei Downloa

Link

Anhang

Formular



Cyberb

Aufforderu

- Nigeria
- Datei D

Link

Anhang

Formular

Cyberbiol

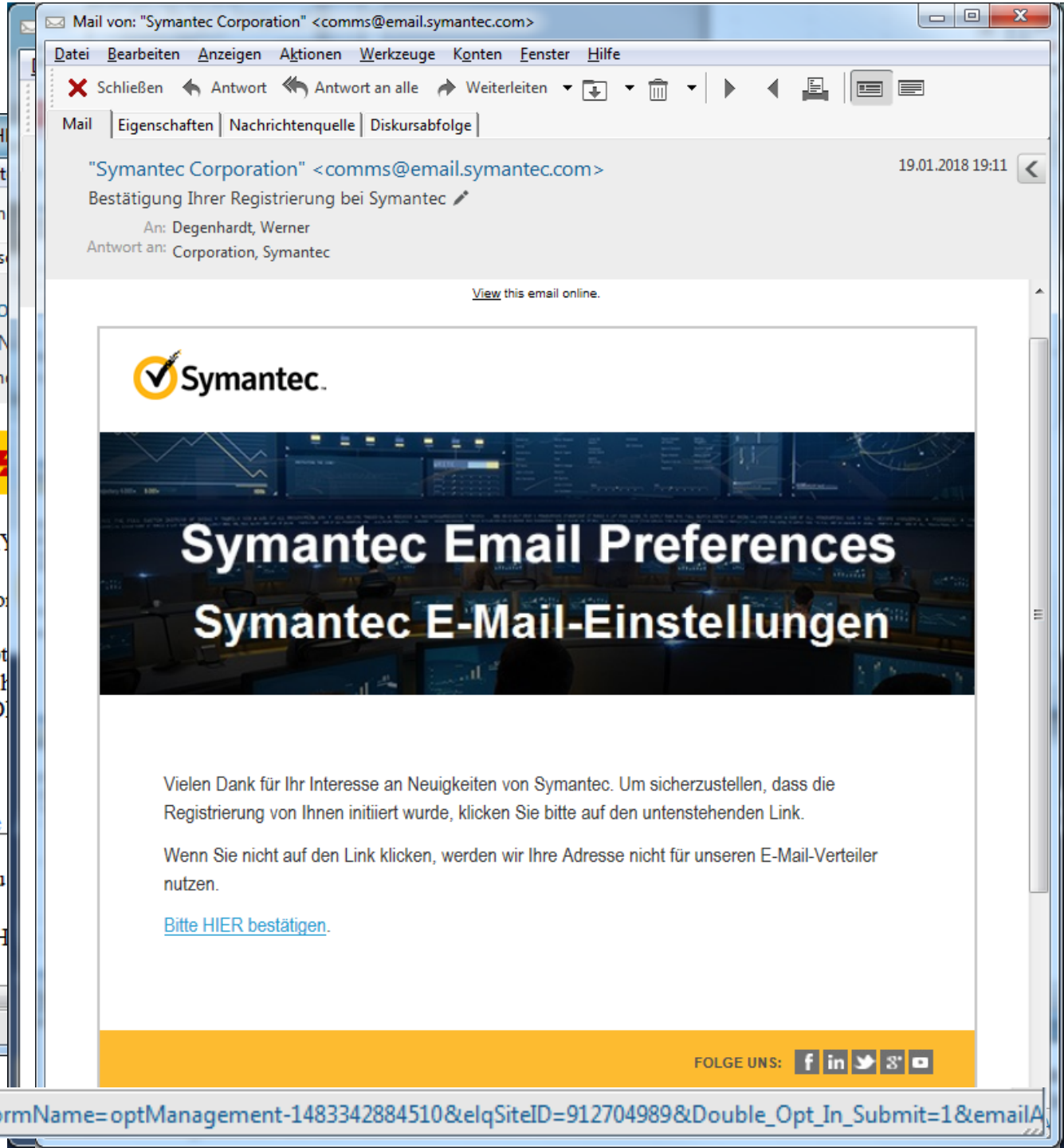
Aufforderung

- Nigeria Sc
- Datei Dow

Link

Anhang

Formular



codeandconcept

Agenda

- Anatomie eines erfolgreichen Ransomware-Angriffs
- Wie konnte das passieren?
- Wie der Mensch wirklich funktioniert
- Kognitive und soziale Heuristiken
- Warum gute Menschen schlechte Entscheidungen treffen
- Härten der „Human Firewall“: Awarenesskampagnen, Training, Ausbildung
- Sicherheitskultur fehlertoleranter Organisationen

Mail von: Luis Helfer <jigvaleq@outlook.com>

Datei Bearbeiten Anzeigen Aktionen Werkzeuge Konten Fenster Hilfe

Schließen Antwort Dem Originalsender antworten Weiterleiten

Mail | Eigenschaften | Nachrichtenquelle | Diskursabfolge

Luis Helfer <jigvaleq@outlook.com>
15.07.2018 20:50
degenhardt - covadis
An: Degenhardt, Werner

Let's get straight to the point. I know that covadis is your password. Moreover, I know about your secret and I've proof of this. You don't know me personally and nobody hired me to check out you.

It's just your misfortune that I came across your bad deeds. Let me tell you, I setup a malware on the adult vids (sexually graphic) and you visited this site to have fun (you know what I mean). While you were busy watching video clips, your internet browser started operating as a Rdp (Remote desktop) that has a keylogger which gave me access to your display screen and also web camera. Right after that, my software program collected all of your contacts from social networks, and e-mail.

Next, I gave in more time than I should have looking into your life and generated a double-screen video. First part shows the video you had been watching and second part shows the capture from your web cam (its you doing nasty things).

Honestly, I am ready to forget all information about you and allow you to continue with your life. And I am about to give you two options that may accomplish that. Those two options are either to ignore this letter, or simply pay me $2900. Let's examine those two options in more details.

Option 1 is to ignore this e-mail. Let me tell you what will happen if you opt this path. I will, no doubt send out your video recording to all your contacts including friends and family, colleagues, etc. It does not protect you from the humiliation your household will ought to face when family and friends learn your sordid videos from me.

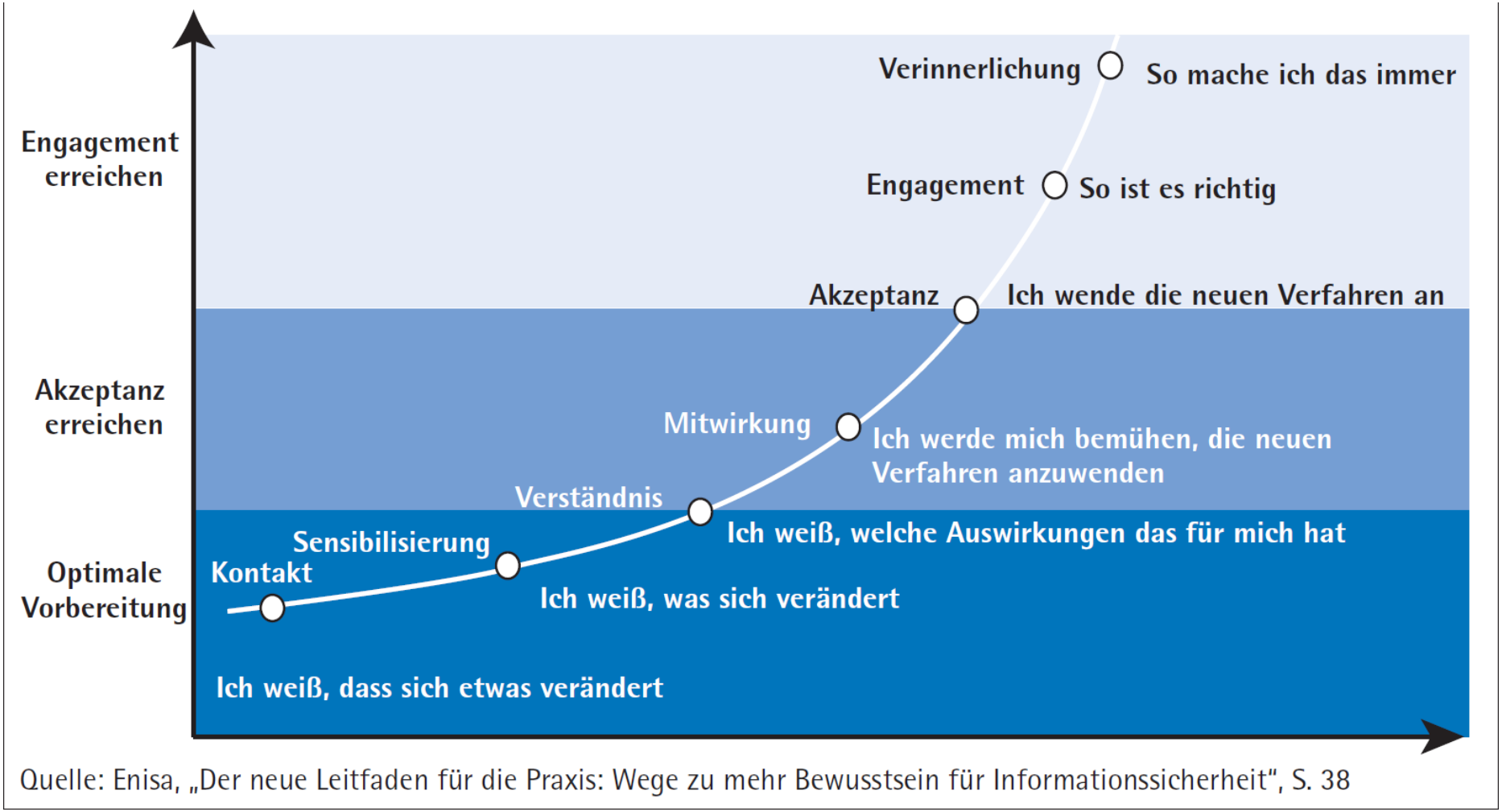
Other Option is to send me $2900. We'll call this my "privacy tip". Now let me tell you what happens if you choose this path. Your secret remains your secret. I will erase the video immediately. You continue on with your daily life as though nothing like this ever happened.

Es muss etwas geschehen …

EU-DSGVO und die „Human Firewall“

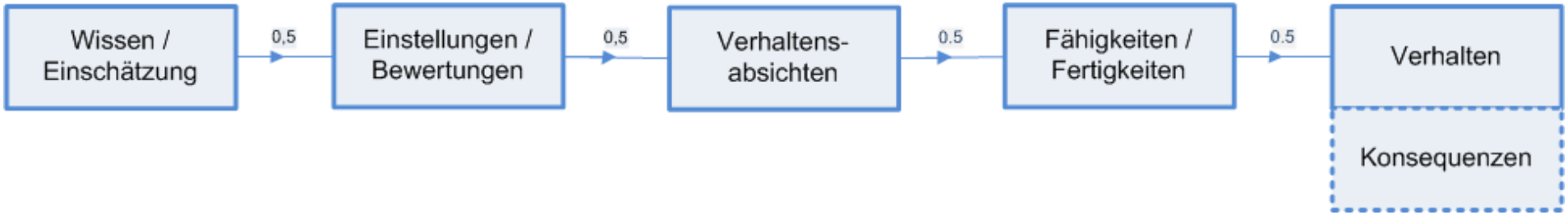
- Art. 32 (Sicherheit der Verarbeitung)
  1.d „ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“
- Art. 39 (Aufgaben des Datenschutzbeauftragten)
  1.b „Überwachung … der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen“
- Art. 47 (Verbindliche interne Datenschutzvorschriften)
  2.n „geeignete Datenschutzschulungen für Personal mit ständigem oder regelmäßigem Zugang zu personenbezogenen Daten“

… und es kann etwas geschehen

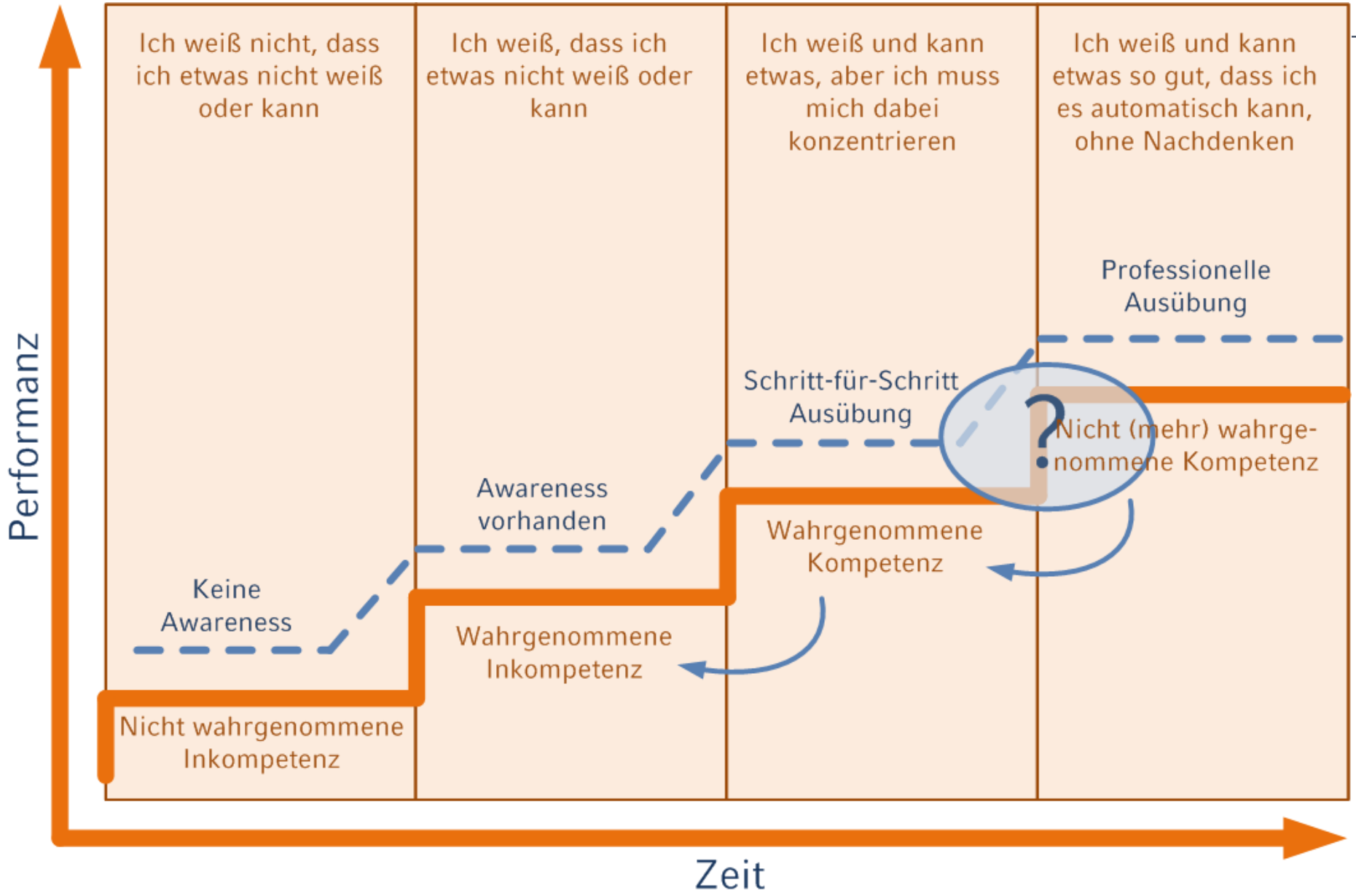


Quelle: Enisa, „Der neue Leitfaden für die Praxis: Wege zu mehr Bewusstsein für Informationssicherheit", S. 38

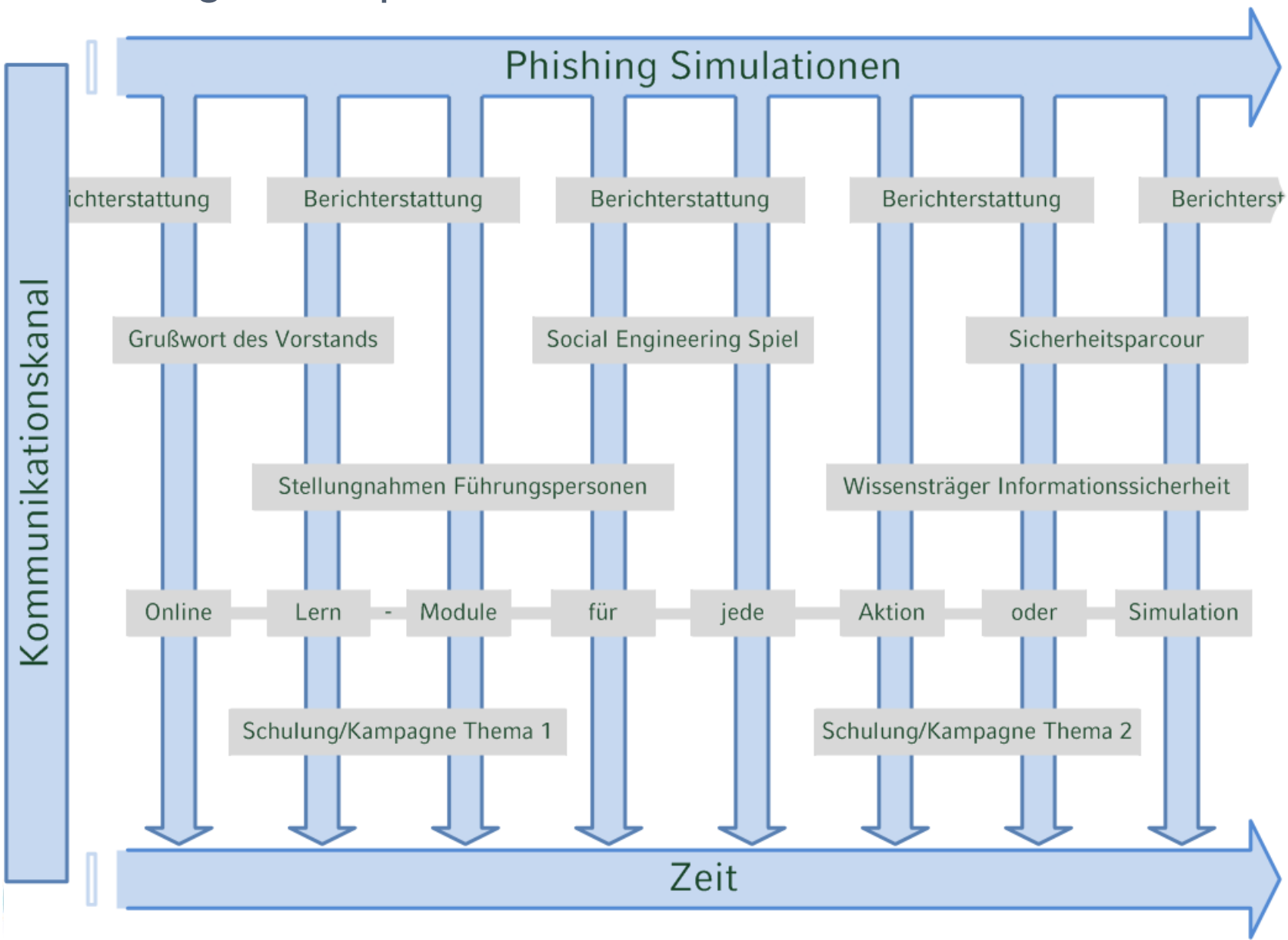
Leider ist der Weg weit vom Wissen zum richtigen Verhalten



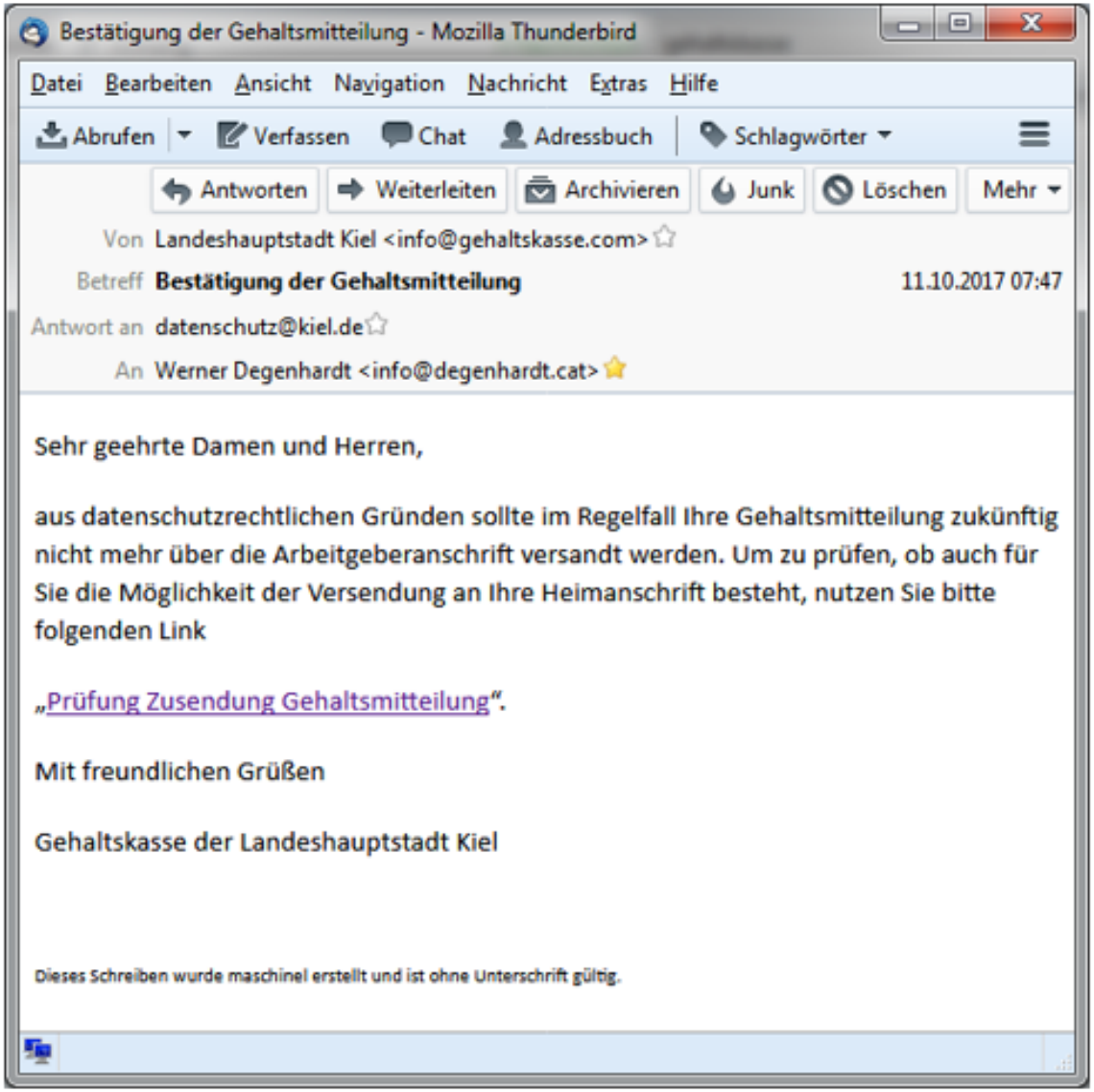
Die 4 Stufen der Kompetenz



Schulungskonzept

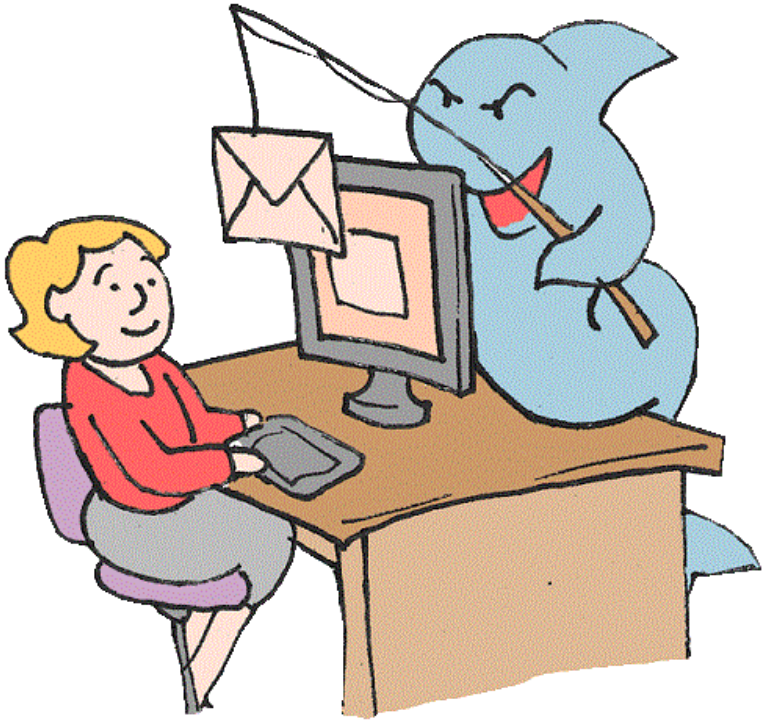


Live Phishing Training LH Kiel



codeandconcept

Sie wurden gefischt!



Die E-Mail, die Sie erhalten haben und die Sie auf diese Seite gebracht hat, imitiert eine Phishing-E-Mail. Es ist eine Phishing-Simulation.

Phishing-E-Mails verschleiern ihre Herkunft und sollen Sie dazu bringen, auf bösartige Links zu klicken.
Sie haben diese Phishing-Simulation bekommen, um zu zeigen, wie ein Phishing-Betrug tatsächlich durchgeführt wird und wie einfach es ist, von diesen cleveren Betrügereien getäuscht zu werden.

Aber keine Sorge! Dies ist keine Prüfung oder dergleichen. Auch Ihre Daten werden nicht gespeichert.

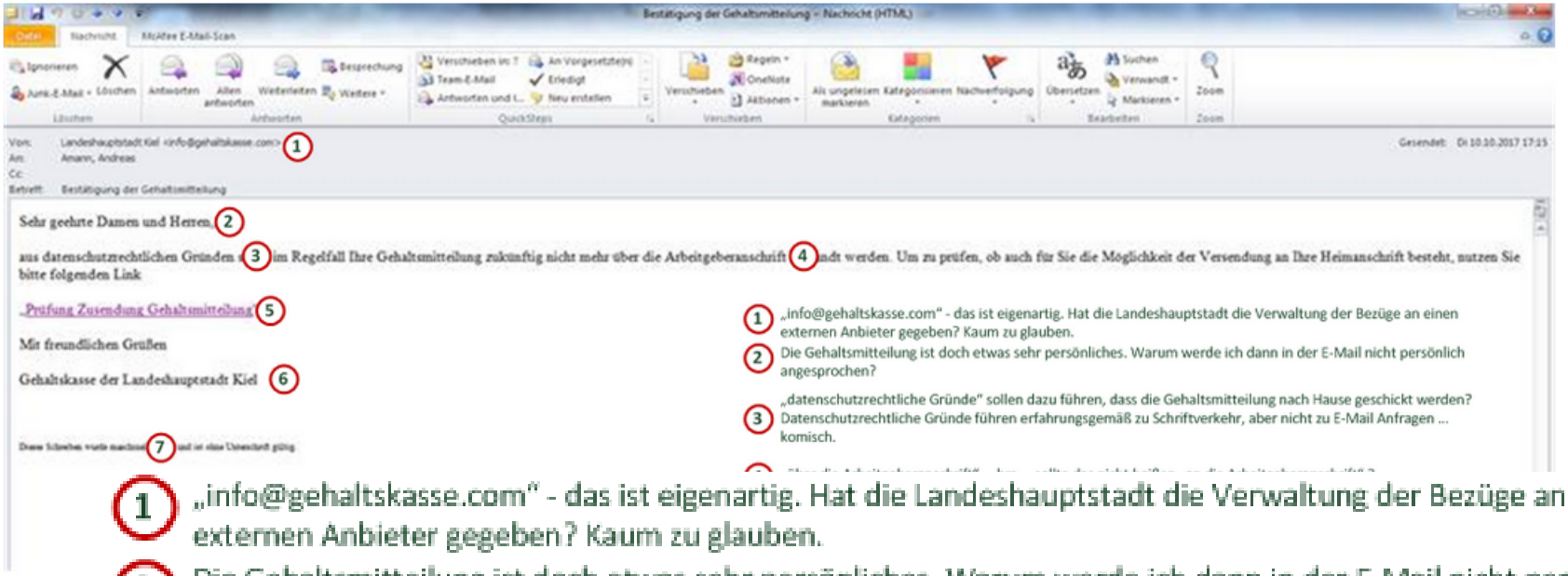
Was wäre passiert, wenn dies ein echte Phishing-Mail gewesen wäre, wenn es sich um einen echten Phishing-Betrug gehandelt hätte? Dann hätten Betrüger Ihren Computer mit einem Trojaner infizieren können, indem Sie einfach auf den Link in der E-Mail klicken. Oder, wenn Sie Ihren Benutzernamen und Kennwort oder andere sensible Informationen zur Verfügung gestellt hätten, könnte sogar Schlimmeres passieren. Stellen Sie sich vor, was diese Person mit den von Ihnen gestohlenen Informationen alles anfangen könnte? Im Prinzip reicht ein infizierter Rechner, um das gesamte Netzwerk der Landeshauptstadt Kiel in Schwierigkeiten zu bringen oder ganz lahm zu legen.

Aber, wie gesagt, das war keine echte Phishing-Mail, sondern ganz im Gegenteil: wir möchten Ihnen helfen, nicht noch einmal auf diesen Trick hereinzufallen.

Sie sehen unten ein Bildschirmfoto dieser E-Mail mit Hinweisen auf Merkmale, die Misstrauen erregen könnten und sollten.

Außerdem finden Sie am Ende dieser Seite einen Link zum Behörden-IT-Sicherheitstraining der Landeshauptstadt Kiel, das Ihnen helfen soll, diese bösartigen Mails zu erkennen und Ihre Daten zu schützen. Die Teilnahme ist freiwillig und zu jeder Zeit möglich. Informationen über Teilnahme oder gar Erfolg des Trainings werden nicht erfasst, personenbezogene Auswertungen finden nicht statt.

Wie erkenne ich eine Phishing-Mail?



1 „info@gehaltskasse.com" - das ist eigenartig. Hat die Landeshauptstadt die Verwaltung der Bezüge an einen externen Anbieter gegeben? Kaum zu glauben.

2 Die Gehaltsmitteilung ist doch etwas sehr persönliches. Warum werde ich dann in der E-Mail nicht persönlich angesprochen?

Aber Achtu 3 „datenschutzrechtliche Gründe" sollen dazu führen, dass die Gehaltsmitteilung nach Hause geschickt werden? Datenschutzrechtliche Gründe führen erfahrungsgemäß zu Schriftverkehr, aber nicht zu E-Mail Anfragen ... komisch.

4 „über die Arbeitgeberanschrift" ... hm ... sollte das nicht heißen „an die Arbeitgeberanschrift" ?

Wenn Si 5 Neinnein, die Landeshauptstadt Kiel schickt an ihre Mitarbeiterinnen und Mitarbeiter keine E-Mails in denen über einen Link etwas bestätigt wird. Sicher nicht datenschutzrechtlich Relevantes und sicher nichts, was das Gehalt betrifft.

Für den F

6 Das sieht nicht nach einer seriösen Signatur einer seriösen Behörde aus. Zumindest ein i.A. (Name des Sachbearbeiters) kann man doch erwarten

Kopieren S

7 „maschinel" ... da ist ein Schreibfehler übersehen worden – typisch für Phishing-Mails

Awareness – Training – Bildung

Awarenessmaßnahmen

sind Maßnahmen zur Steigerung der Aufmerksamkeit für das Thema Informationssicherheit. Informationssicherheit soll den Benutzerinnen und Benutzern als wichtiges Thema bekannt sein und als bedeutsames Thema für den eigenen Arbeits- und Wirkungsbereich anerkannt werden.

Beispiele sind Präsentationen zum Datenschutzrecht, Veranstaltungen wie „Die Hacker kommen“, Verteilen von Anleitungen, Rundschreiben des Vorstands, Hinweise auf Berichterstattung in der Presse.

Awareness – Training – Bildung

Training

will relevante Fähigkeiten und Fertigkeiten vermitteln, richtiges Verhalten stärken, falsche Verhaltensweisen löschen. Training ist für Trainer und Trainierte aufwendiger (aber nicht teuerer) als Awarenessmaßnahmen und hat starke Übungsanteile.

Awareness – Training – Bildung

Bildung

bezieht sich auf die Ausbildung von Personen, die sich der Informationssicherheit als Profession verschrieben haben. Bildung bezeichnet Spezialisten mit großer Erfahrung und tiefem Verständnis, mit Weitblick und der Fähigkeit schon Anzeichen von Schadsituationen zu erkennen und proaktiv zu reagieren.

Schulung – Methoden und Medien

- Präsenzseminare
- Online-Lernen
- Microteaching
- Simulationen

Phishing Simulation, Du tust so gut …

Im Ergebnis bin ich vom Erfolg der Kampagne vollkommen überzeugt.
Ein schönes Beispiel ist diese E-Mail:

Hallo Herr [Datenschutzbeauftragter],

ich habe eine email von "Splendid research“ erhalten. (Führungskräftefeedback der LHK Kiel)

Den Absender kenne ich nicht.
Darf ich die öffnen? Oder ist dies eine Phishingmail?

Eine solche Frage habe ich in meiner 4-jährigen Datenschützer-Tätigkeit vor unserer Maßnahme kein einziges Mal(!) bekommen. Jetzt ist es ein Beispiel von vielen (geschätzt um die 40) gleichartigen Anfragen seit Oktober ... (nicht gerechnet diejenigen, die bei unserem helpdesk auflaufen).

Herzliche Grüße, [Datenschutzbeauftragter]

codeandconcept

Agenda

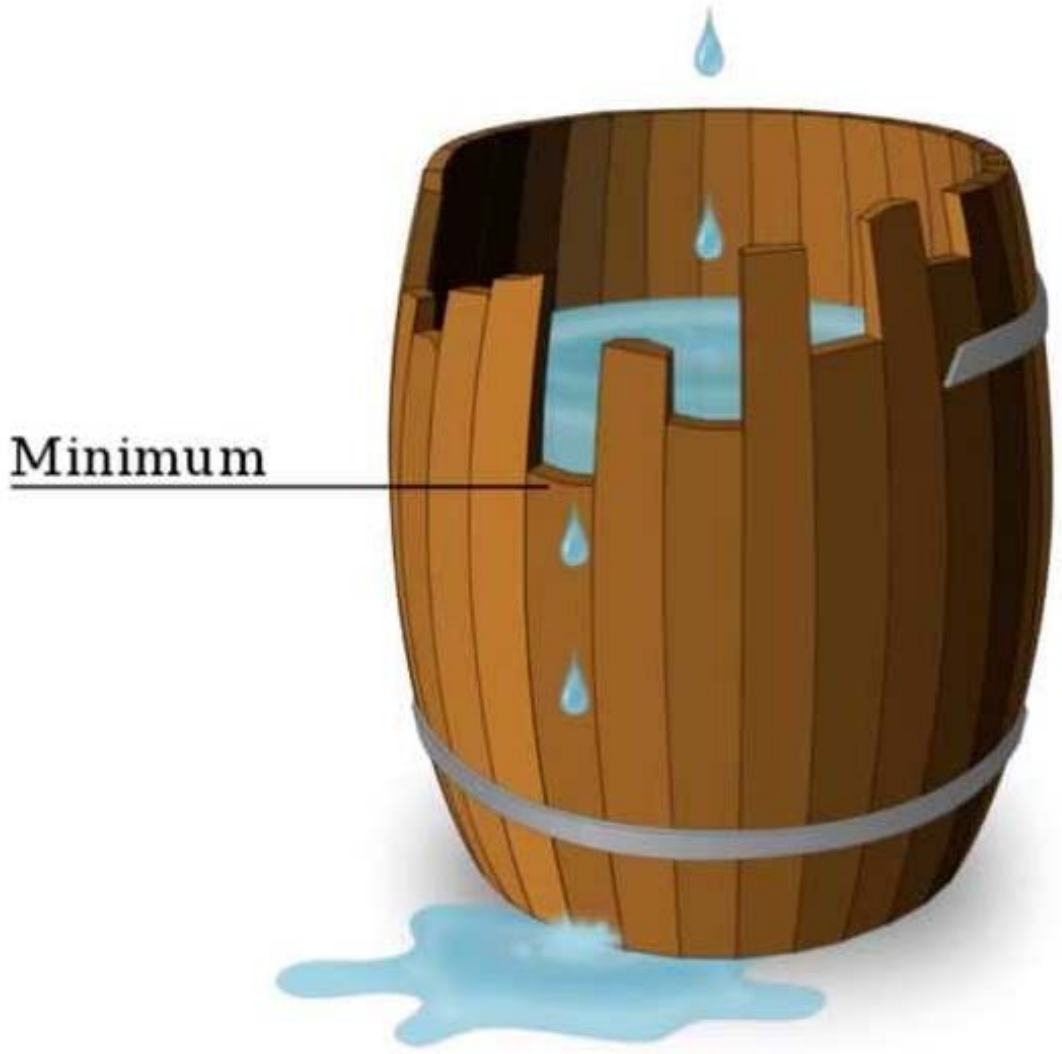
- Anatomie eines erfolgreichen Ransomware-Angriffs
- Wie konnte das passieren?
- Wie der Mensch wirklich funktioniert
- Kognitive und soziale Heuristiken
- Warum gute Menschen schlechte Entscheidungen treffen
- Härten der „Human Firewall“: Awarenesskampagnen, Training, Ausbildung
- Sicherheitskultur fehlertoleranter Organisationen

Sicherheitskultur

Element	Eigenschaften
Offenheit	Mitarbeiter können ohne Angst Sicherheitsvorfälle und Sicherheitsfragen Kollegen und Vorgesetzten diskutieren
Gerechtigkeit	Mitarbeiter, Sicherheitspersonal und Betroffene werden fair, mit Einfühlungsvermögen und unter Berücksichtigung der Umstände behandelt, wenn sie in einen Sicherheitsvorfall verwickelt sind oder auf mögliche Gefährdungen der Sicherheit hinweisen
Berichterstattung	Mitarbeiter haben Vertrauen zum Berichtssystem und nutzen es um die zuständigen Manager (z.B. Fachvorgesetzte, Datenschutzbeauftragte, Sicherheitsbeauftragte, etc.) über Sicherheitsvorfälle oder Sicherheitsgefährdungen zu informieren Technische, soziale und prozedurale Barrieren der Berichterstattung wurden erkannt und sind beseitigt.
Lernen	Die Organisation hat sich dazu verpflichtet aus Sicherheitsvorfällen zu lernen, kommuniziert das Gerlernte an die Mitarbeiter und hat Vorkehrungen getroffen, das Gelernte nicht zu vergessen.
Informiertheit	Die Organisation hat die Fähigkeit entwickelt aus der Vergangenheit zu lernen und benutzt dieses Wissen, um mögliche zukünftige Vorfälle zu identifizieren und zu entschärfen

Latente Bedingungen, aktive Fehler

Die menschliche Natur können wir nicht ändern. Aber die Bedingungen unter den Menschen arbeiten.



Wir fassen zusammen …

1. Lerninhalte und Training müssen für die Benutzer relevant sein
2. Es muss Spaß machen
3. Live Phishing muss häufig wiederholt werden, um sichere Reflexe auszubilden
4. Messen Sie den Erfolg und berichten Sie davon
5. Passen Sie das Schulungskonzept an die spezielle Organisationskultur Ihrer Einrichtung an
6. Denken Sie wie ein Human Factors Spezialist, handeln Sie wie ein Angreifer

Code and Concept

Erik Ebell und Christian Giese GbR

Breisacherstraße 4 Rgb

81667 München

Sie erreichen uns per E-Mail, Telefon und Fax:

E-Mail: info@codeandconcept.de

Telefon: +49 (0)89 642 90 320

Fax: +49 (0)89 642 90 322