IT-SEAL

SOCIAL ENGINEERING ANALYSIS LABS

Awareness messen - Do’s and Dont’s

David Kelm, Geschäftsführer

David Kelm
Gründer & Geschäftsführer IT-Seal

- M.Sc. Informatik, M.Sc. IT-Security
- Best Student Award des BSI
- Europäischer Social Engineering Award
- Zertifizierter IT-Risk Manager (ISO 31000 / BSI Grundschutz)

David Kelm

Produktmanagement

Was ist Human Hacking?

POLITICS

Russia's Hackers Took Only a Week to Pry Into Clinton Camp

By THE ASSOCIATED PRESS NOV. 4, 2017, 3:36 P.M. E.D.T.

Angriff per Mail 21.09.2016 19:13 Uhr

Cyberattacke auf deutsche Politiker alarmiert Sicherheitsbehörden

Ransomware-Virus legt Krankenhaus lahm

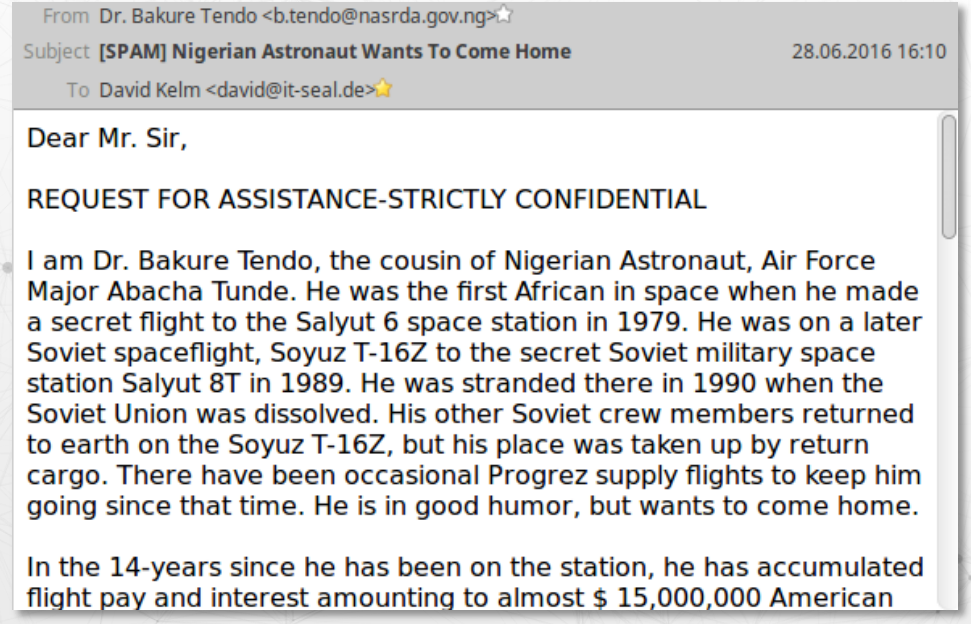
12.02.2016 12:48 Uhr – Detlef Borchers

CEO-FRAUD

Autozulieferer Leoni um 40 Millionen Euro betrogen

Phishing – die größte Bedrohung

- Mass Phishing


From Dr. Bakure Tendo <b.tendo@nasrda.gov.ng>
Subject **[SPAM] Nigerian Astronaut Wants To Come Home** 28.06.2016 16:10
To David Kelm <david@it-seal.de>

Dear Mr. Sir,

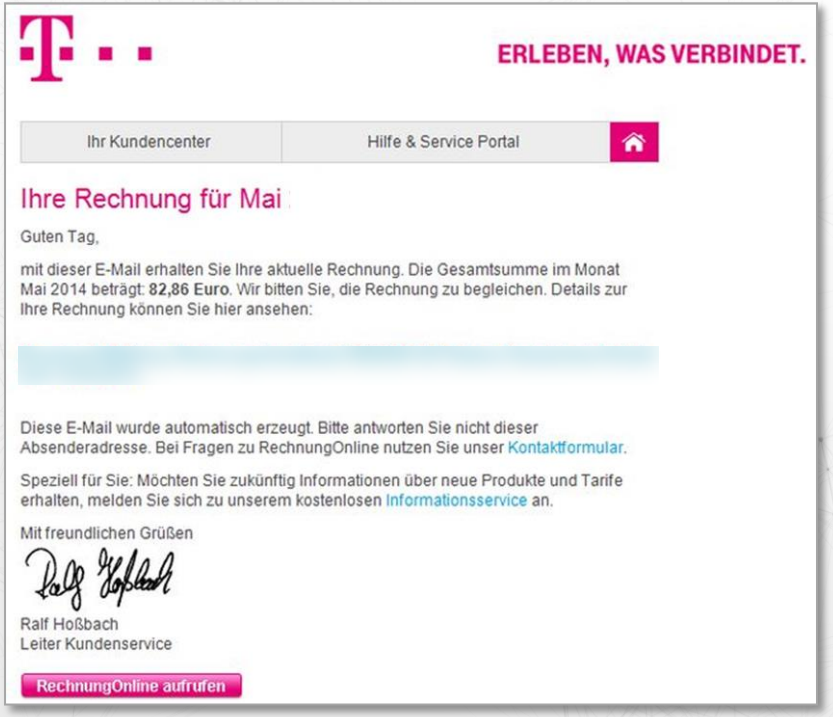
REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL

I am Dr. Bakure Tendo, the cousin of Nigerian Astronaut, Air Force Major Abacha Tunde. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989. He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progrez supply flights to keep him going since that time. He is in good humor, but wants to come home.

In the 14-years since he has been on the station, he has accumulated flight pay and interest amounting to almost $ 15,000,000 American

Phishing – die größte Bedrohung

- Mass Phishing
- Clone Phishing



ERLEBEN, WAS VERBINDET.

Ihr Kundencenter | Hilfe & Service Portal

Ihre Rechnung für Mai

Guten Tag,

mit dieser E-Mail erhalten Sie Ihre aktuelle Rechnung. Die Gesamtsumme im Monat Mai 2014 beträgt: **82,86 Euro**. Wir bitten Sie, die Rechnung zu begleichen. Details zur Ihre Rechnung können Sie hier ansehen:

Diese E-Mail wurde automatisch erzeugt. Bitte antworten Sie nicht dieser Absenderadresse. Bei Fragen zu RechnungOnline nutzen Sie unser Kontaktformular.

Speziell für Sie: Möchten Sie zukünftig Informationen über neue Produkte und Tarife erhalten, melden Sie sich zu unserem kostenlosen Informationsservice an.

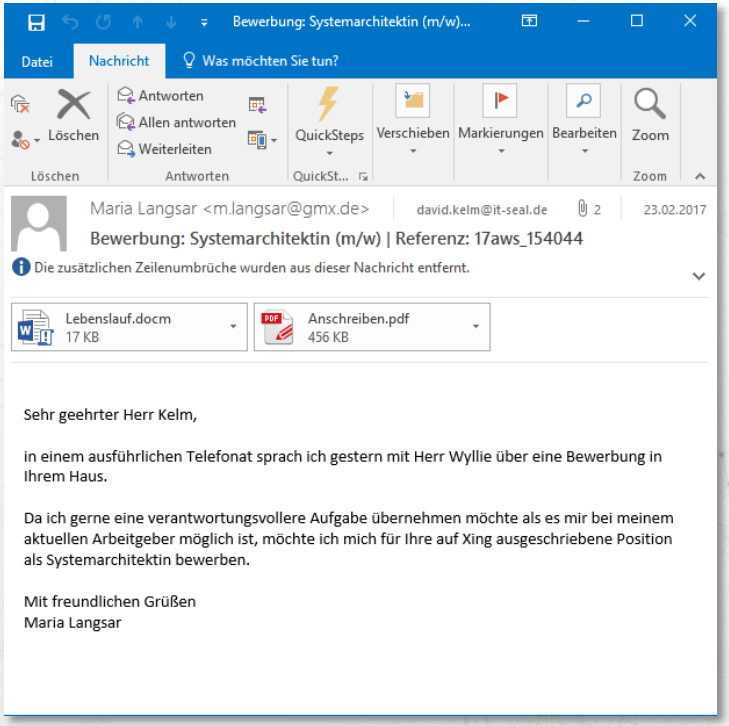
Mit freundlichen Grüßen

Ralf Hoßbach
Leiter Kundenservice

RechnungOnline aufrufen

Phishing – die größte Bedrohung

- Mass Phishing
- Clone Phishing
- Spear Phishing



Soziale Medien:
Öffentliche Informationen über…

Hobbies

Geburtstag

Veranstaltungen

Arbeitgeber

Freunde

Ausbildung

Fotos

Aufenthaltsorte

Mitgliedschaften

Urlaub

Kontakte

Sprachen

Interessen

Wie wird vorgegangen?

Psychologische Faktoren

- Hilfsbereitschaft
- nett sein
- Vorurteile/Erwartungen
- **Autoritäten**
- Automatismen
- Verlangen
- **Neugier**
- **Angst**

Manipulationstechniken

- Verbindung aufbauen
- Informationen herauslocken
- Gegenseitigkeit
- Schuldgefühle
- Konsistenz
- Verpflichtung
- sozialer Beweis
- **Zeitdruck**

Was ist Awareness?

Security Awareness ist das **Wissen und Verhalten** von Mitarbeitern bezüglich des **Schutzes von Informationen** innerhalb der Organisation.

Wie bringt man das Kollegen bei?

Wie bringt man das Kollegen bei?

	Ziel	Direkte Einbindung	Zeiteffizient	Skalierbar	Wirksamkeit messbar	Weitergehende Informationen
Präsenzschulung	Wissensvermittlung	✓ (bei kleinen Gruppen)	✗	✗	✗	✓
E-Learning/Webinar	Wissensvermittlung	✗	✗	✓	✗	✓
Phishing Akademie	Verhaltensänderung Wissensvermittlung Effekte messen	✓	✓	✓	✓	✗

Wie maximiere ich den Nutzen einer solchen Maßnahme?

Worauf ist zu achten?

1. Realitätsnahe Simulation

Realitätsnahe Simulation

Amazon

Meine Bestellungen | Mein Konto | Amazon.de

Amazon Sicherheitswarnung

Ihr Account wurde eingeschränkt

Guten Tag Frau Ney,

Ihr Amazon-Nutzerkonto wurde auf Grund von verdächtigen Aktivitäten eingeschränkt. Aus Sicherheitsgründen ist die Eingabe Ihrer hinterlegten Daten notwendig.

Kommen Sie dieser E-Mail innerhalb 7 Tagen nicht nach, wird Ihr Nutzerkonto aus Datenschutzgründen gesperrt. Auf Grund einer manuellen Überprüfung dieses Sachverhaltes, müssen wir eine Bearbeitungsgebühr in Höhe von 39,95 EUR erheben.

Um Ihr Konto bei uns wie gewohnt im vollen Umfang nutzen zu können, klicken Sie bitte auf diesen Link.

Vielen Dank!

Ihr Amazon-Supportteam

Realitätsnahe Simulation

From: Alex Wyllie < alex@it-sea1.de>
To: David Kelm
Cc:
Subject: Notfall

Hallo David,

ich schreibe nur kurz, weil wir gerade ein dringendes Problem haben. Könnten Sie mal nachschauen?
Hier der Link mit den Infos:
http://intern.it-sea1.de/login/task?id=?wDE-l0zM

Danke!

IT-Seal - Social Engineering Analysis Labs

Telefon: +49 6151 493 89 89
Email: alex.wyllie@it-seal.de

Fallen Sie oder Ihre Kollegen auf gefälschte E-Mails rein? Finden Sie es praxisnah heraus!
Innerhalb von zwei Minuten zum kostenlosen Phishing Training anmelden: https://demo.it-seal.de/signup
---
IT-Seal GmbH
Hilpertstr. 31, 64295 Darmstadt

Realitätsnahe Simulation

Aufenthaltsorte
Interessen
Kollegen
Kontakte
Sprachen
Arbeitgeber

Soziale Medien

Urlaub
Hobbies

Individuelles Szenario, individueller Zeitpunkt


From: Alex Wyllie < alex@it-sea1.de>
To: David Kelm
Cc:
Subject: Notfall

Hallo David,

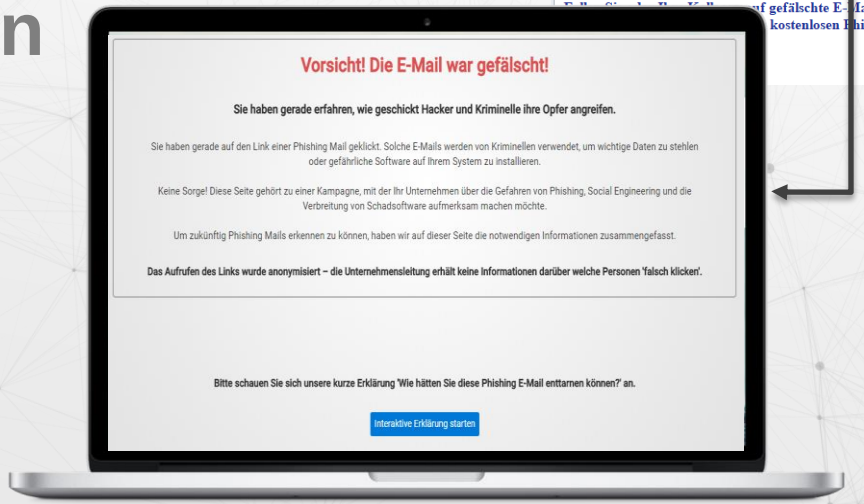
ich schreibe nur kurz, weil wir gerade ein dringendes Problem haben. Könnten Sie mal nachschauen?
Hier der Link mit den Infos:
http://intern.it-sea1.de/login/task?id=?wDE-l0zM

Danke!

IT-Seal - Social Engineering Analysis Labs

Telefon: +49 6151 493 89 89
Email: alex.wyllie@it-seal.de

gefälschte E-Mails rein? Finden Sie es praxisnah heraus!
kostenlosen Phishing Training anmelden: https://demo.it-seal.de/signup



★★★★★	61%
★★★★	21%
★★★	3%
★★	10%
★	9%

Angriffspotentialcheck

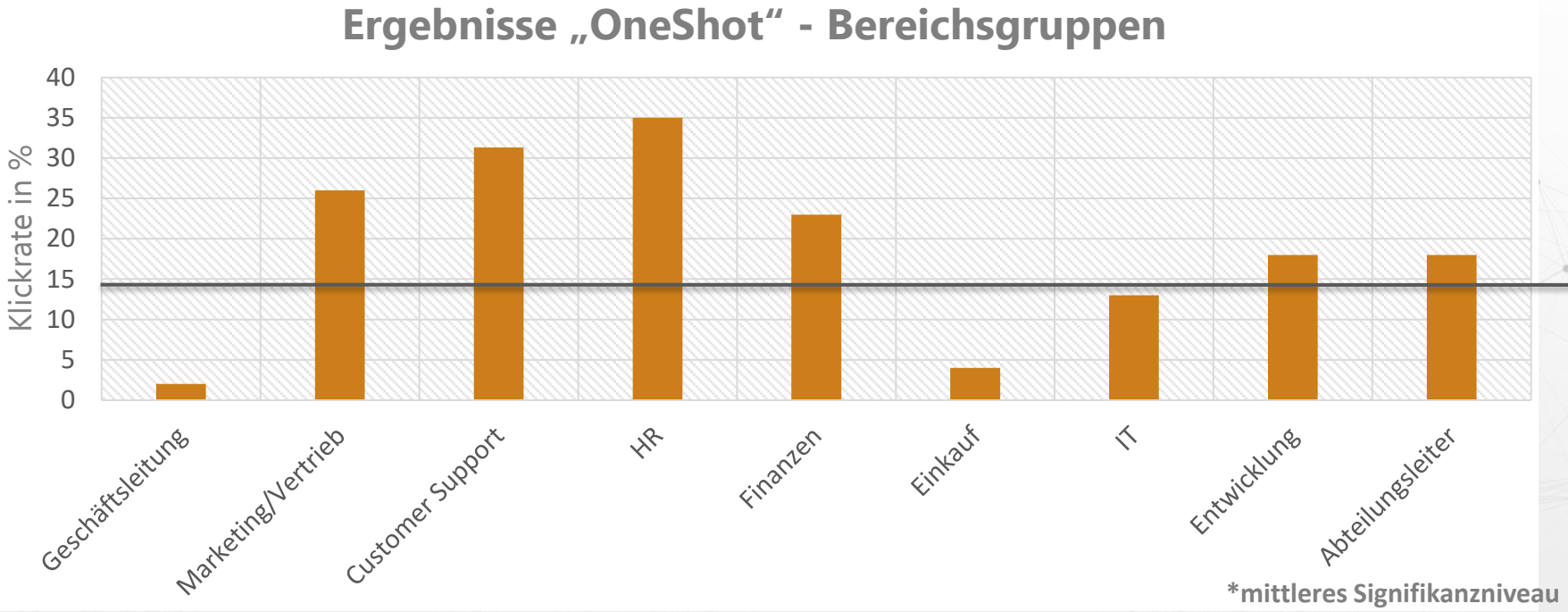
Level	Zeitaufwand eines Angreifers
1	ca. 1h
2	ca. 4h
3	ca. 10h

Teachable Moment testen: http://phishing-academy.it-seal.de

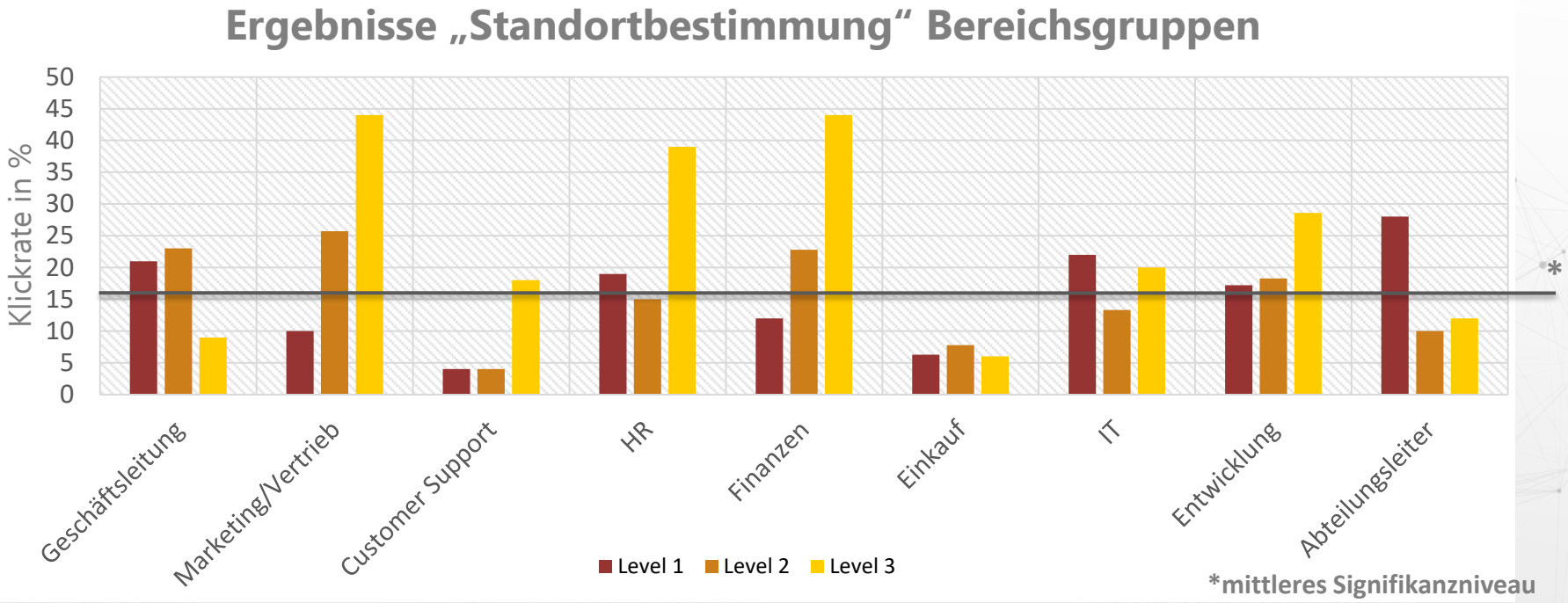
Worauf ist zu achten?

1. Realitätsnahe Simulation
2. Aussagekraft Ergebnisse

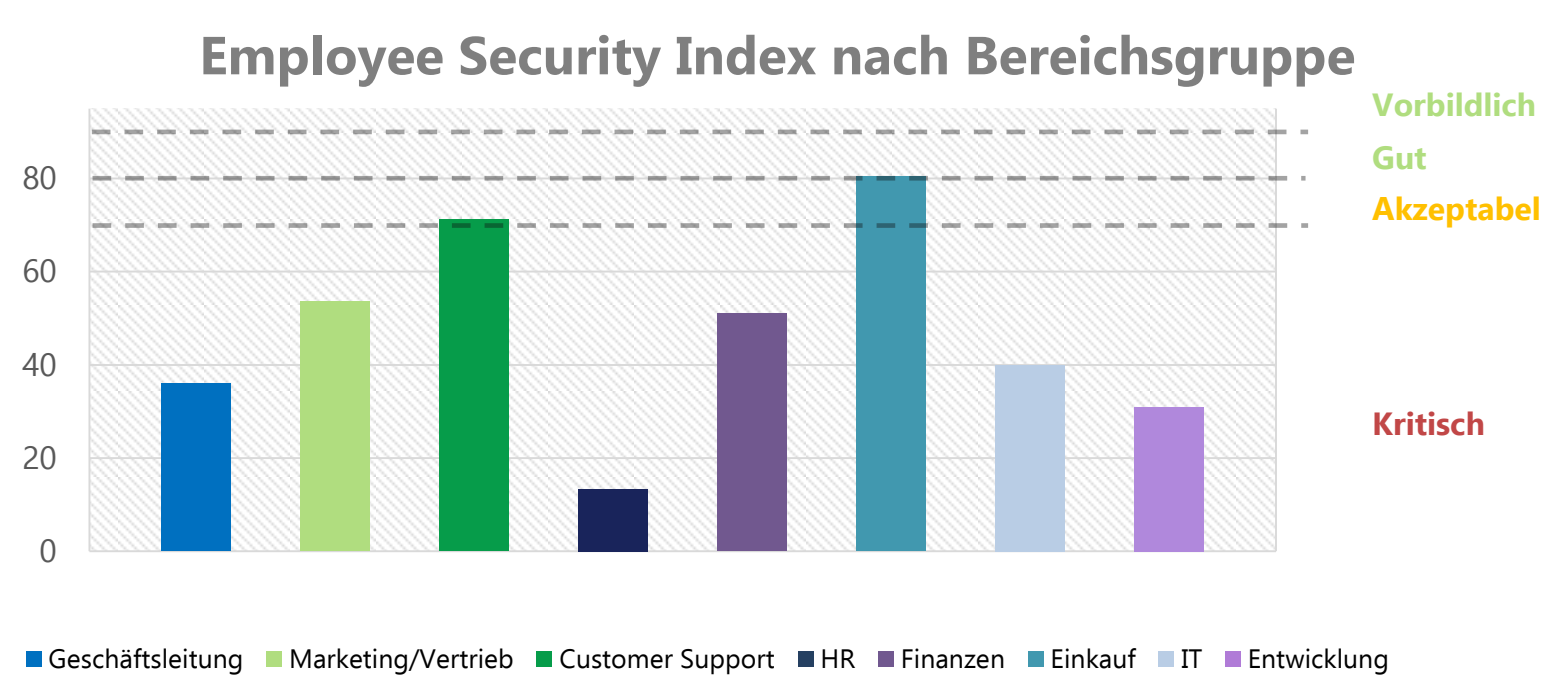
Aussagekraft der Ergebnisse



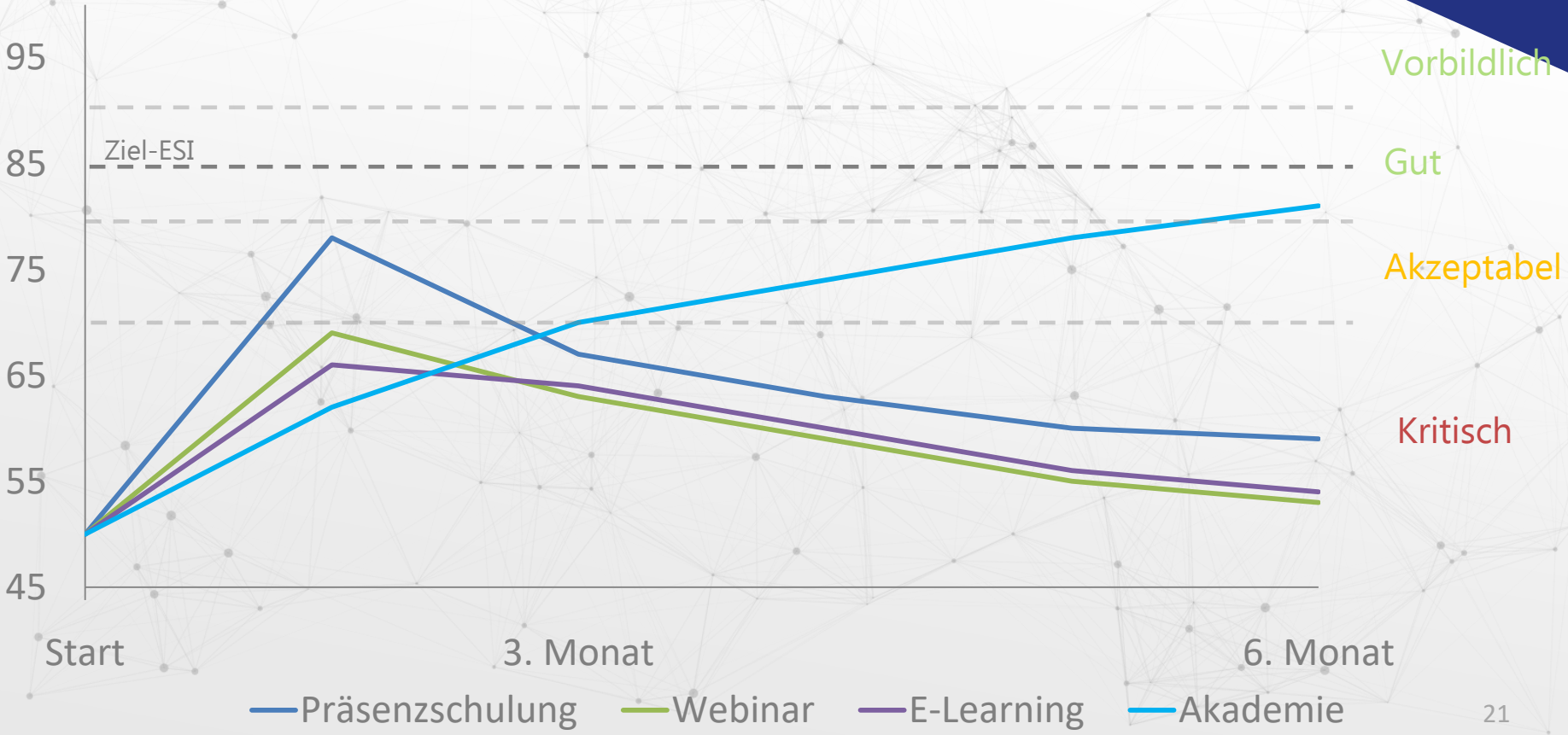
Aussagekraft der Ergebnisse



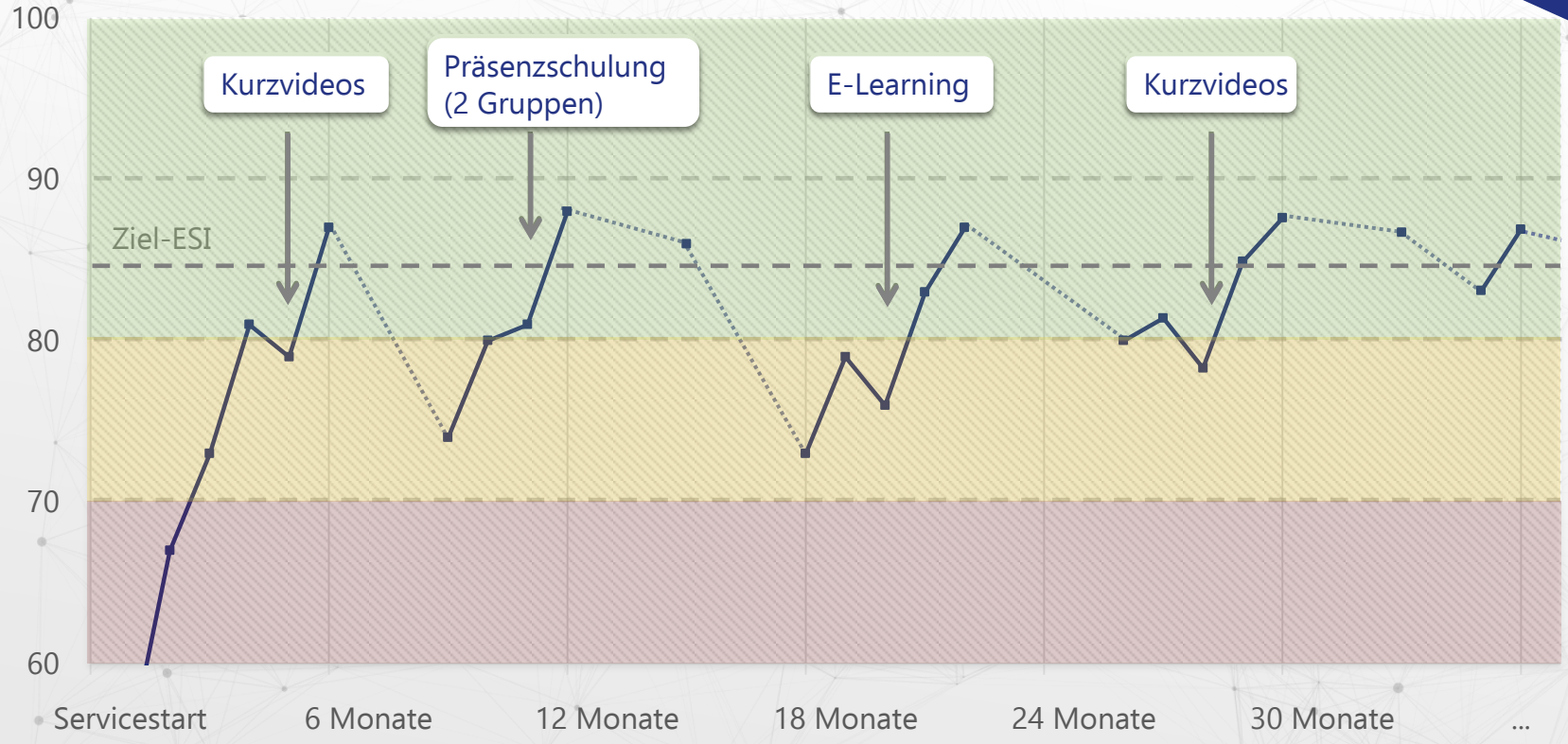
Aussagekraft der Ergebnisse



Anhaltender Lerneffekt



Nachhaltiges Awarenessprogramm



Worauf ist zu achten?

1. Realitätsnahe Simulation
2. Aussagekraft Ergebnisse
3. Unternehmenskultur

Projektablauf

persönliches Kennenlernen

Dashboard-Zugang, Starterpaket:

- Template MA-Liste
- Whitelisting
- Entwurf Ankündigung
- IT Support-FAQ

Auswahl der teilnehmenden Mitarbeiter

Gruppeneinteilung

interne Ankündigung

Test-E-Mail

heute

~ 4 Wochen vor Projektstart

~ 2 Wochen vor Projektstart

Worauf ist zu achten?

1. Realitätsnahe Simulation
2. Aussagekraft Ergebnisse
3. Unternehmenskultur
4. Betriebsrat-Einbindung

Betriebsrat-Einbindung

- Ergebnisse anonymisieren
- Frühzeitig und Transparent kommunizieren
- Training in Fokus rücken
- Fragen klären
- Ergebnisse kommunizieren

Kontaktdaten

- Individualisiertes Phishing Awareness-Training im Full Service
- Erstklassiger Mitarbeiter- und Datenschutz
- ESI® - konkrete Kennzahl durch wissenschaftlichen Ansatz

David Kelm

david.kelm@it-seal.de

www.it-seal.de
06151 / 493 89 89

In den folgenden Branchen machen wir unsere Kunden bereits zu Vorreitern in Sachen Social Engineering-Awareness ...

Automotive | Finanzen | Gesundheit | Energie | Logistik | Universität | Kanzlei | Industrie