viadee
IT-Unternehmensberatung

kvw Kommunale Versorgungskassen Westfalen-Lippe

Sicherheitskultur stärken:

Von Richtlinien zu gelebter Informationssicherheit

Nicklas Baier, Kommunale Versorgungkassen Westfalen-Lippe

Don Diephaus, viadee Unternehmensberatung AG

// Wer sind wir?

IT-Sicherheitsbeauftragter

- IT-Sicherheitsbeauftragter für kvw & Mandanten
- UNIX/Linux, Netzwerk & regulatorische IT-Sicherheit (DORA, NIS2)
- Awareness- & Phishingkampagnen, Förderung der IT-Sicherheitskultur

Nicklas Baier | kvw

IT-Berater

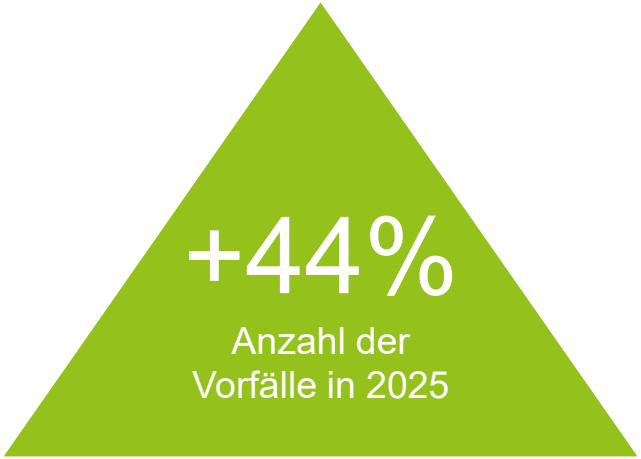
- IT-Security Management & Awareness
- Web-Security Testing
- Software Entwicklung

Don Diephaus | viadee

Kommunale
Versorgungskassen
Westfalen-Lippe

// Motivation

// Cyberangriffe nehmen rasant zu



https://www.orangecyberdefense.com/global/white-papers/security-navigator-2025
https://www.security-insider.de/alarmierender-anstieg-cyberkriminalitaet-europa-a-9c06fd96fb6c74ff31b921608618eee9/

// Öffentlicher Dienst zunehmend im Fokus

Angriffsmotive

- Finanzieller Anreiz
- Hochsensible Daten
- Politische Instabilität

Fallbeispiel:
Südwestfalen IT: Ransomware-Angriff

- 2,8 Mio EUR Schaden
- 22.000 Arbeitsplätze lahmgelegt
- 70+ Kommunen
- 1,6 Mio. Bürger:innen betroffen

https://www1.wdr.de/nachrichten/westfalen-lippe/ein-jahr-nach-cyberangriff-suedwestfalen-it-100.html
https://www.zeit.de/news/2025-11/11/oeffentliche-verwaltung-im-visier-von-cyberspionen
https://www.bmi.bund.de/DE/themen/sicherheit/spionageabwehr-wirtschafts-und-geheimschutz/cyberspionage/cyberspionage-artikel.html

// Faktor Mensch – das größte Einfallstor

Schwache Passwörter

Unachtsamkeit

Phishing

Fehlkonfigurationen

Social Engineering

74 %

Aller Sicherheitsvorfälle sind auf menschliches Fehlverhalten zurückzuführen

Vishing

...

Deepfakes

https://www.security-insider.de/resilienz-kultur-sicherheit-audit-a-995ae51bcb1e9c07b24eb000be8d72ef/

// Das Vorgehen im Überblick

// Grundlagen

// Drei Säulen der Informationssicherheit

// Was ist Sicherheitskultur?

> *„Geteilte Werte, Normen und Verhaltensweisen aller Mitarbeitenden zum Schutz von Informationen – **Sicherheit als gelebter Alltag nicht als Pflicht**.“*

Organisation

- ✓ Führung lebt Sicherheit vor
- ✓ Klare Verantwortlichkeiten
- ✓ Offene Fehlerkultur

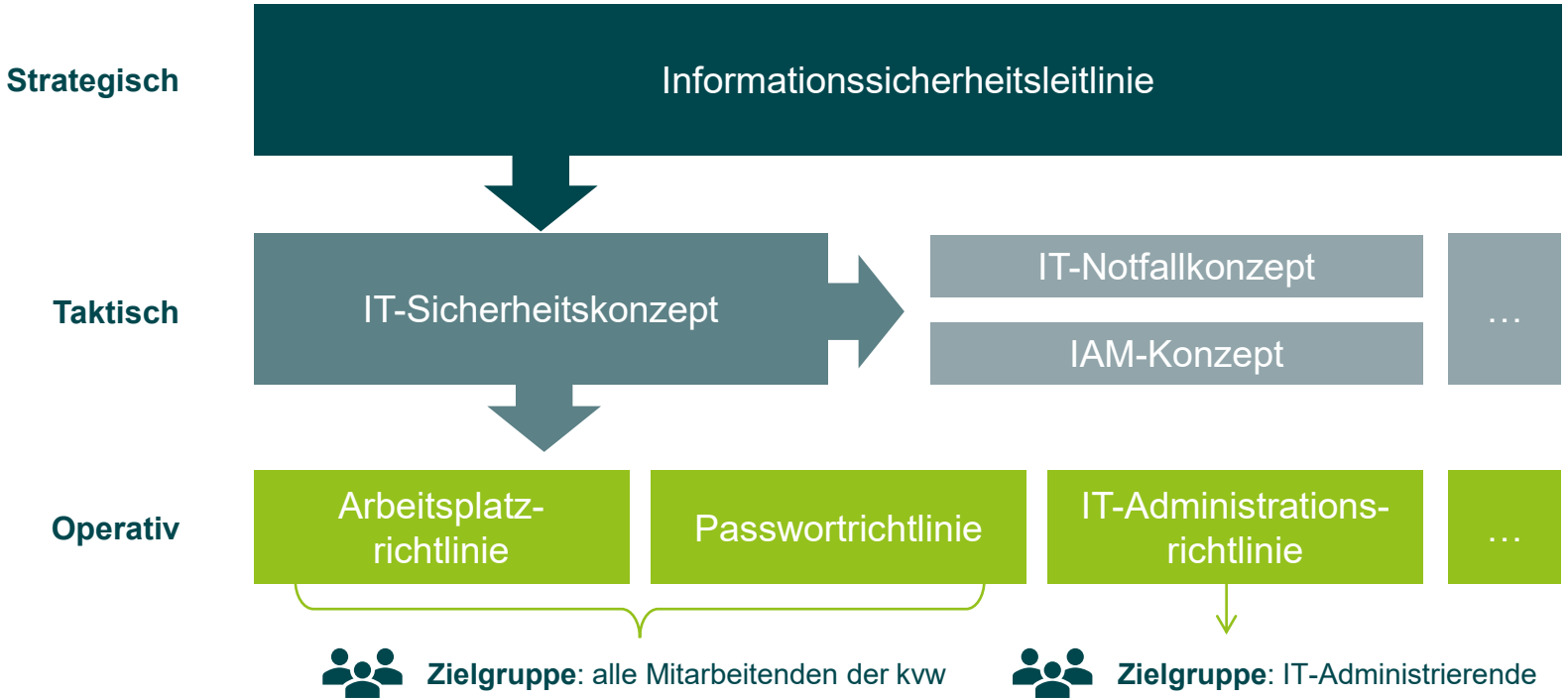
Mitarbeitende

- ✓ Fühlen sich mitverantwortlich
- ✓ Kennen aktuelle Bedrohungen
- ✓ Melden Vorfälle proaktiv

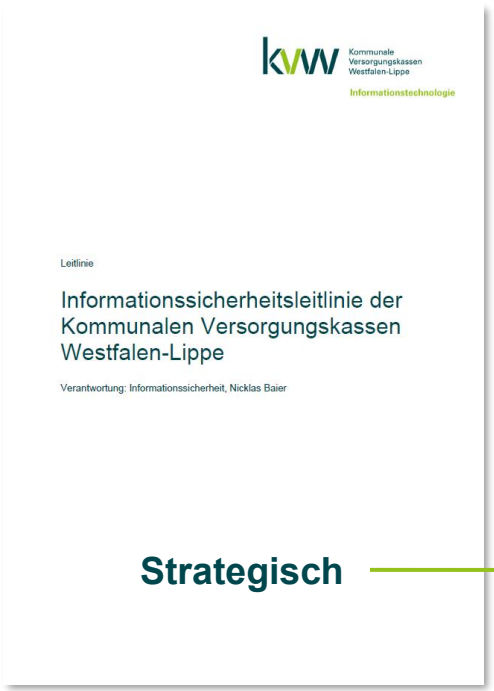
kvw Kommunale Versorgungskassen Westfalen-Lippe

// Sicherheitdokumentation @ kvw-IT

// Struktur der Sicherheitsdokumentation

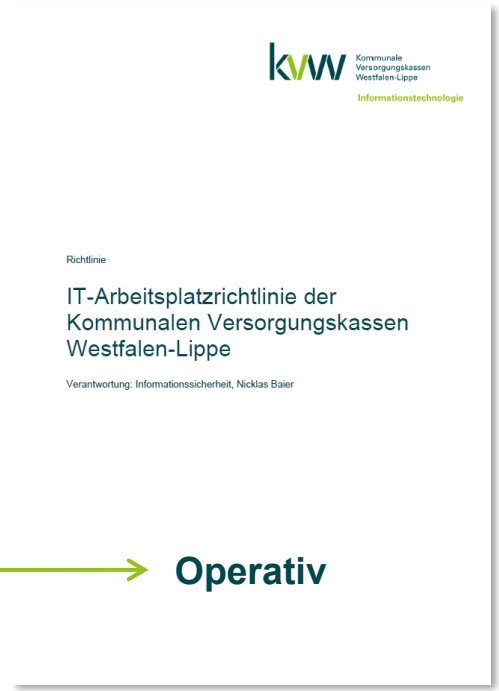


// Wie alles zusammenhängt



Strategisch

Taktisch



Operativ

// Einblick in die IT-Arbeitsplatzrichtlinie

Inhaltsverzeichnis

// Unsere Inspiration: IT-Grundschutz-Kompendium

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.2: Desktop-Systeme

SYS.2.1: Allgemeiner Client

SYS.2.1.A1 Sichere Benutzerauthentisierung (B)

Um den Client zu nutzen, MÜSSEN sich die Benutzer gegenüber dem IT-System authentisieren. Benutzer MÜSSEN eine Bildschirmsperre verwenden, wenn sie den Client unbeaufsichtigt betreiben. Die Bildschirmsperre SOLLTE automatisch aktiviert werden, wenn für eine festgelegte Zeitspanne keine Aktion durch den Benutzer durchgeführt wurde. Die Bildschirmsperre DARF NUR durch eine erfolgreiche Benutzerauthentisierung deaktiviert werden können. Die Benutzer SOLLTEN verpflichtet werden, sich nach Aufgabenerfüllung vom IT-System bzw. von der IT-Anwendung abzumelden.

Richtlinie

kvw Kommunale Versorgungskassen Westfalen-Lippe

Informationstechnologie

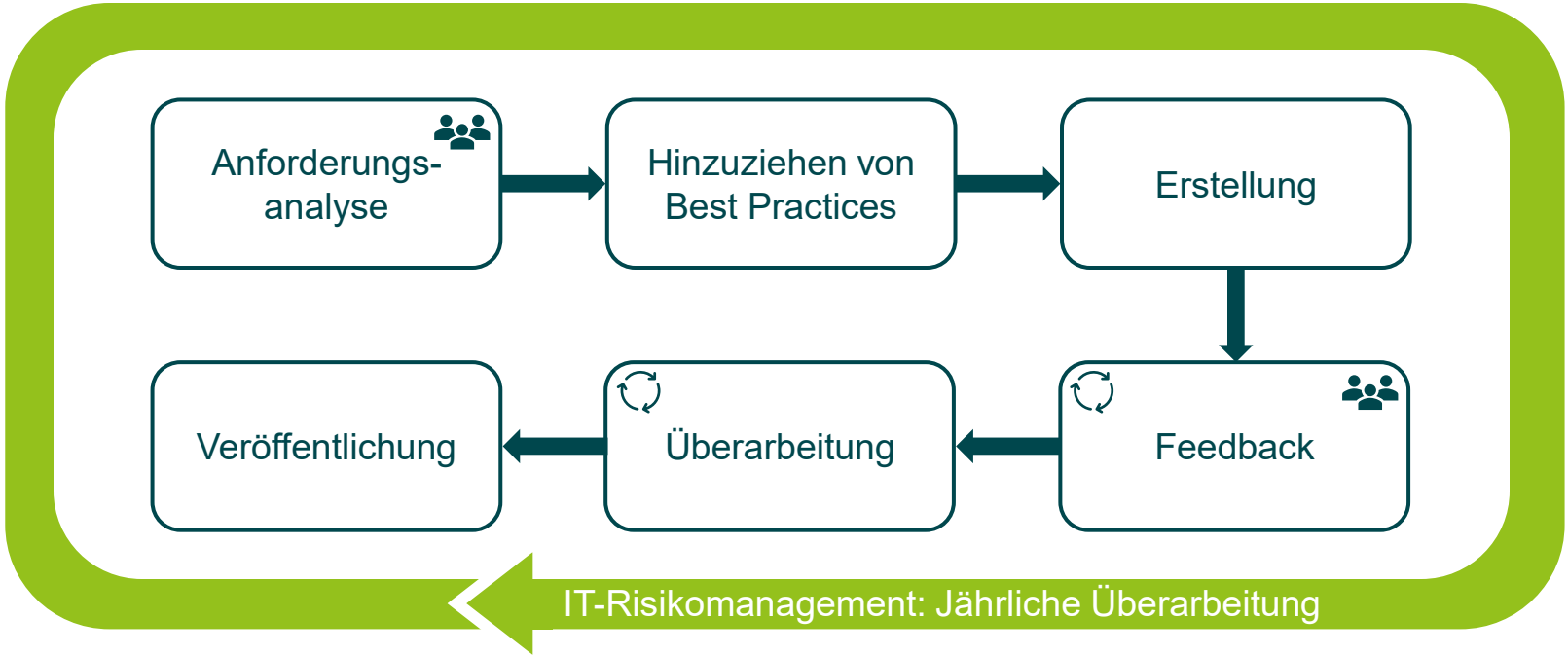
IT-Arbeitsplatzrichtlinie der Kommunalen Versorgungskassen Westfalen-Lippe

Verantwortung: Informationssicherheit, Nicklas Baier

3.2 Verlassen des Arbeitsplatzes

Die Benutzer:innen **MÜSSEN** dafür Sorge zu tragen, dass beim Verlassen des Arbeitsplatzes das Notebook manuell gesperrt wird (Windowstaste + L oder Strg + Alt + Entf und dann Sperren).

// Der Erstellungsprozess im Überblick




Und jetzt?

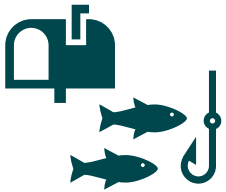
Kommunale Versorgungskassen Westfalen-Lippe

//  Von Richtlinien zu gelebter Praxis

// Unsere Werkzeuge

Richtlinien

Awareness Schulungen



Phishing-Kampagnen

Offene Kommunikation

Förderung der Sicherheitskultur

// Awareness Schulung

Kurs

+

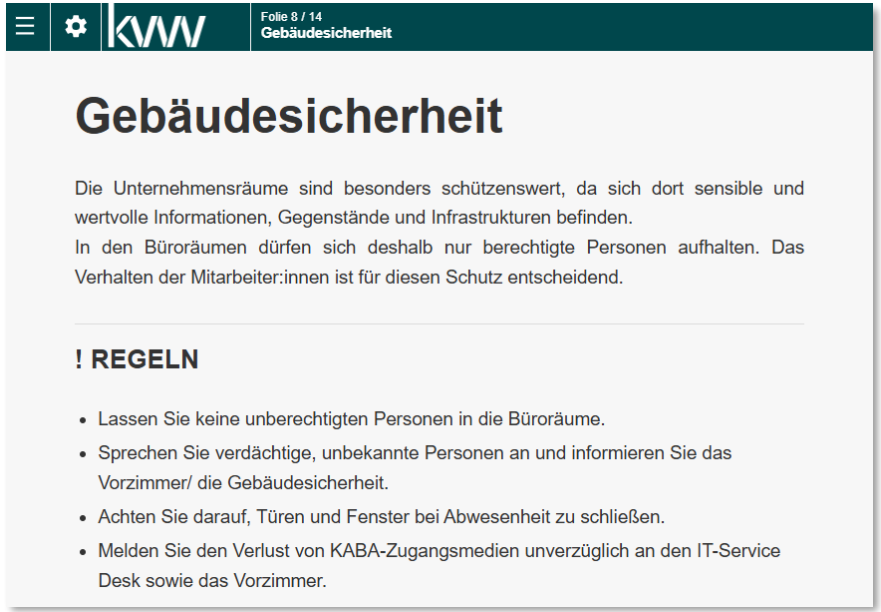
Prüfung

1x
jährlich

30
min

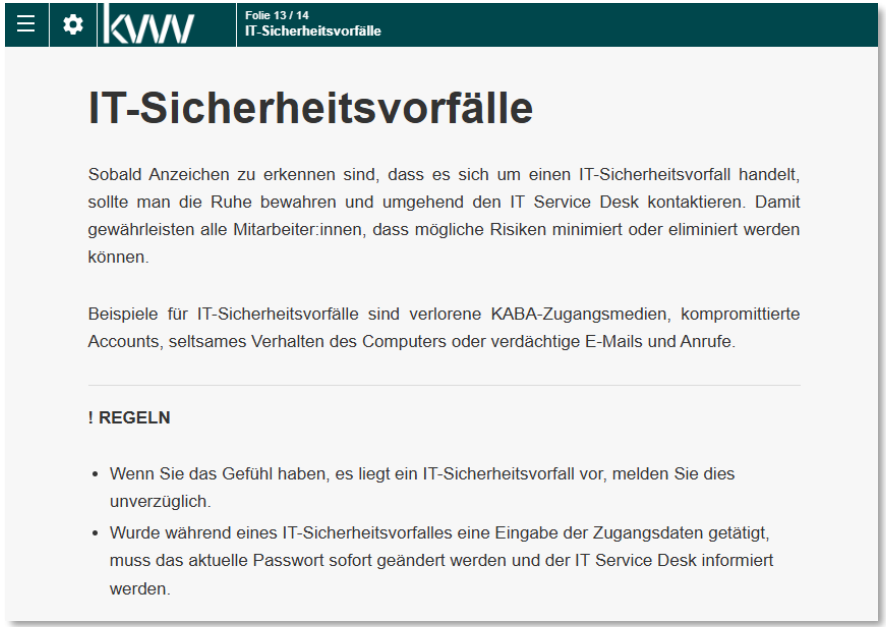
// Awareness Schulung: Kurse

- Klar und in aller Kürze: Anforderungen der Richtlinien



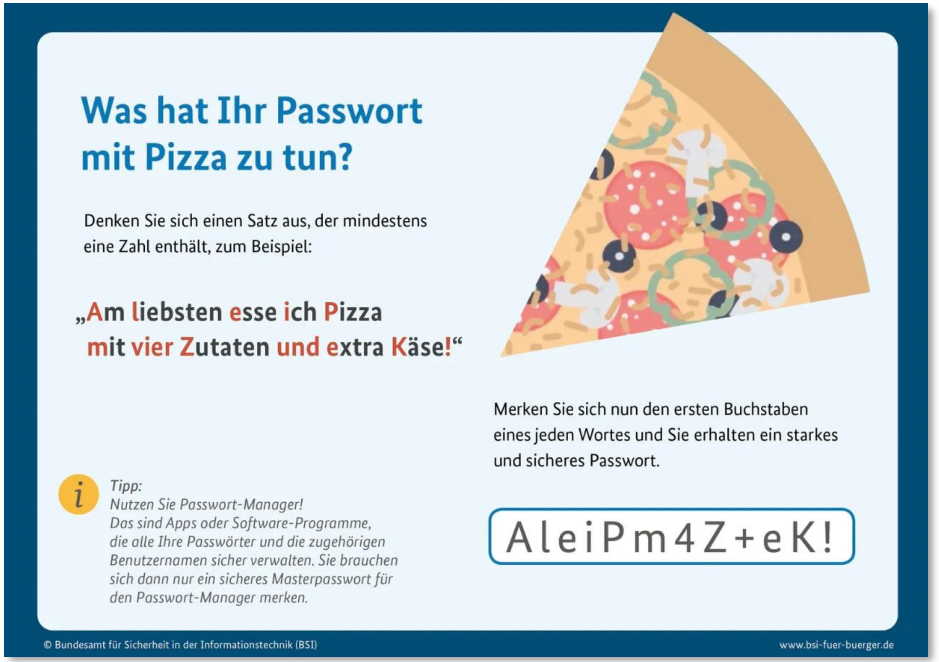
// Awareness Schulung: Kurse

- Für Gefahren sensibilisieren und auf den Ernstfall vorbereiten



// Awareness Schulung: Kurse

- Tipps und praktisches Wissen vermitteln



// Awareness Schulung: Prüfung

- Erlerntes festigen

Sie benötigen ein neues Passwort. Wie gehen Sie bei der Erstellung vor?

- Ich kombiniere Sonderzeichen, Groß- und Kleinbuchstaben zu einem möglichst komplexen Passwort (z.B.: „W@SSerIstNaSS!“).
- Ich bilde einen Merksatz, leite aus diesem Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen ab, um ein möglichst komplexes und langes Passwort zu erstellen.
- Ich verwende ein möglichst komplexes und langes Passwort, das ich mir merken kann, da ich es für etliche private und geschäftliche Dienste verwende.
- Als Standardbenutzer wähle ich ein komplexes Passwort mit einer Mindestlänge von 10 Zeichen.
- Ich entscheide mich für das Passwort "Schalke04!!!", da es alle Kriterien der Passwortrichtlinie erfüllt.

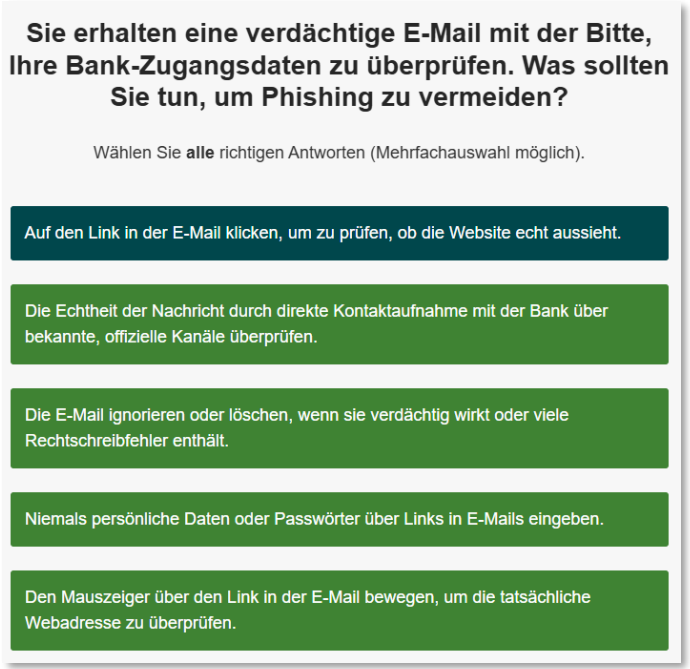
Die Passwortrichtlinie schreibt eine mind. 12 Zeichen lange Kombination aus Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen vor.

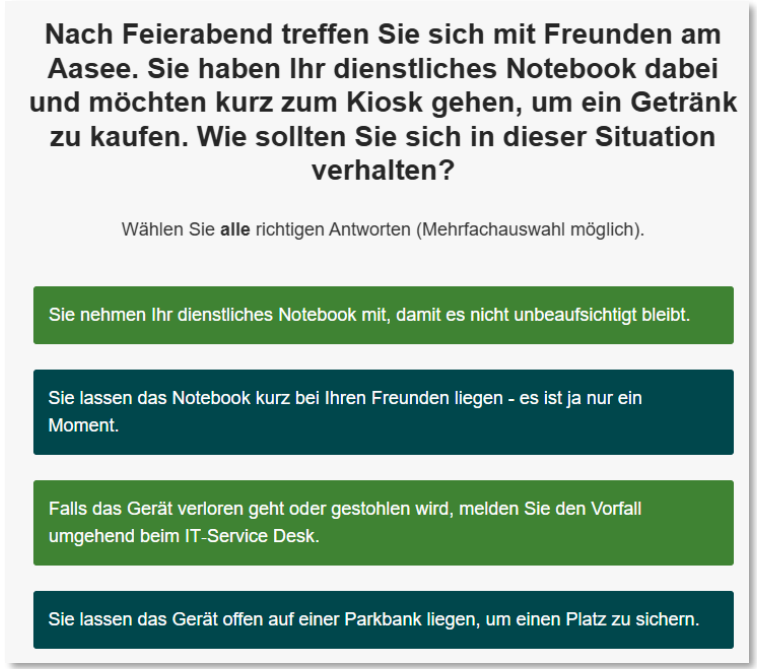
Es bietet sich an einen Merksatz zu bilden, aus dem Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen abgeleitet werden können.
Beispiel: „Am Aasee kann ich im Sommer fünf Stunden lang sitzen, während es im Winter eher 20 Minuten sind!“ --> „AAkiiS5Sls,weiWe20Ms!“.

Verwenden Sie Passwörter einmalig je Dienst und vermeiden Sie triviale Passwörter bzw. solche die in bekannten Datenlecks veröffentlicht wurden, etwa „Schalke04!!!“. Eine Prüfung, ob ein Passwort kompromittiert wurde, kann über folgende Plattform erfolgen: https://haveibeenpwned.com/Passwords

// Awareness Schulung: Prüfung

- Teilnehmende in alltagsnahe Szenarien versetzen





// Awareness Schulung: Prüfung

- Für Gefahren sensibilisieren

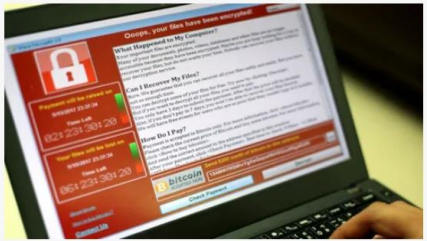
Welche der folgenden Informationen könnten Social Engineers versuchen von Ihnen zu erlangen?

Wählen Sie **alle** richtigen Antworten (Mehrfachauswahl möglich).

- Persönliche Informationen über Mitarbeitende, etwa Geburtstage oder Hobbys.
- Intern verwendete Begriffe, Abkürzungen oder Prozesse.
- Das Wetter am Unternehmensstandort.
- Öffentliche Pressemitteilungen der kvw.
- System- und Netzwerkkonfigurationen der kvw.
- Zugangsdaten wie Benutzername und Passwort.
- Informationen über aktuelle Sicherheitslücken der kvw.

Sie arbeiten an Ihrem Laptop, als plötzlich folgende unbekannte Meldung angezeigt wird. Was sollten Sie jetzt tun?

Wählen Sie **alle** richtigen Antworten (Mehrfachauswahl möglich).



- Erst mal einen Kaffee holen.

Welche IT-Sicherheitsverstöße können Sie im folgenden mobilen Arbeitsszenario identifizieren?

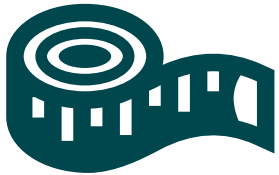
- Private Hardware ist am Dienstgerät angeschlossen.
- Mobiles Arbeiten in der Öffentlichkeit ist grundsätzlich nicht erlaubt.
- Unberechtigte Personen haben Einsicht auf potenziell geschäftliche Daten auf dem Bildschirm.
- Es sind keine IT-Sicherheitsverstöße zu erkennen.
- Getränke stehen offen direkt neben elektronischen Geräten.

// Frage an das Publikum!

- Welche IT-Sicherheitsverstöße identifizieren Sie?

// Phishing Kampagnen

+



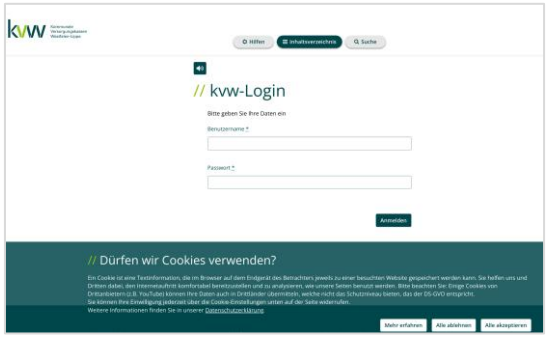
1-2x
jährlich

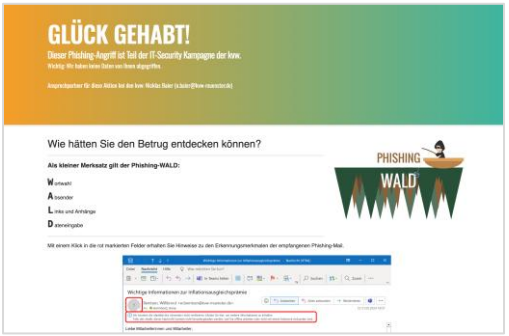
Sensibilisierung

Messinstrument

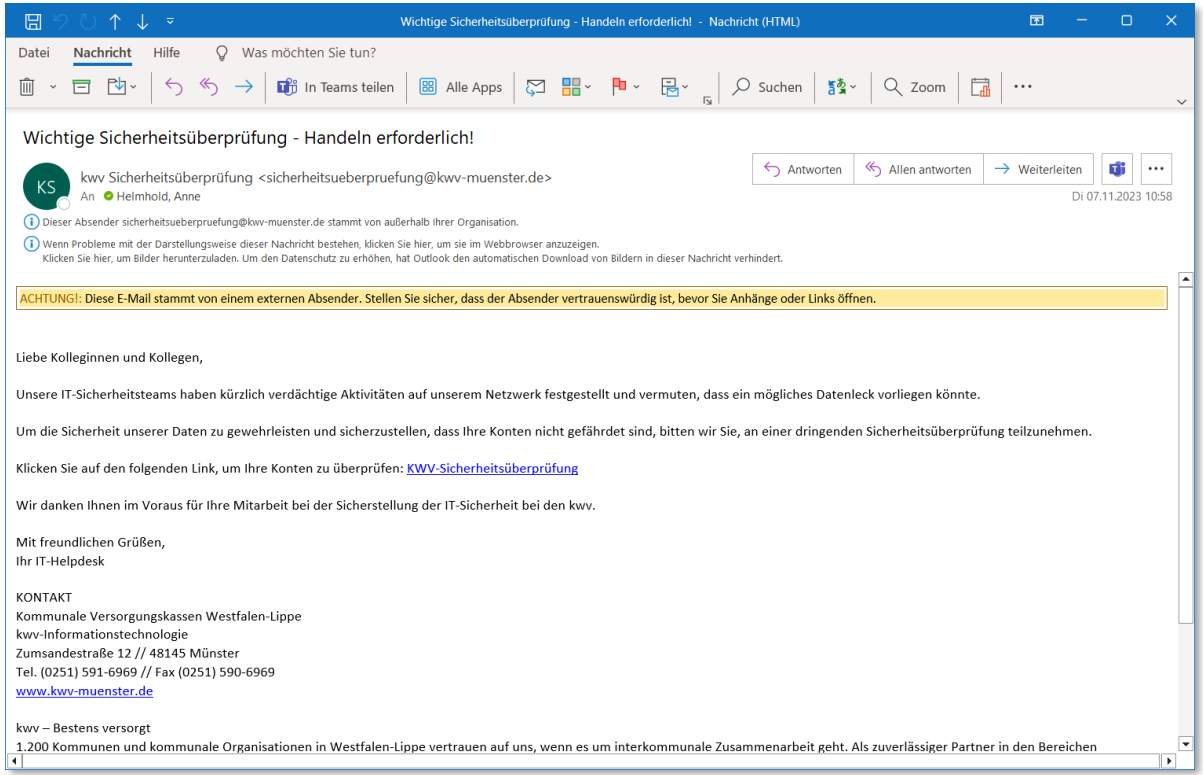
// Klassisches Format

Phishing-Mail → Landing-Page → Learning-Page





// Phishing-Mail



Wichtige Sicherheitsüberprüfung - Handeln erforderlich! - Nachricht (HTML)

Datei Nachricht Hilfe Was möchten Sie tun?

In Teams teilen | Alle Apps | Suchen | Zoom

Wichtige Sicherheitsüberprüfung - Handeln erforderlich!

KS kwv Sicherheitsüberprüfung <sicherheitsueberpruefung@kwv-muenster.de>
An Helmhold, Anne

Antworten | Allen antworten | Weiterleiten

Di 07.11.2023 10:58

Dieser Absender sicherheitsueberpruefung@kwv-muenster.de stammt von außerhalb Ihrer Organisation.

Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.
Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.

ACHTUNG!: Diese E-Mail stammt von einem externen Absender. Stellen Sie sicher, dass der Absender vertrauenswürdig ist, bevor Sie Anhänge oder Links öffnen.

Liebe Kolleginnen und Kollegen,

Unsere IT-Sicherheitsteams haben kürzlich verdächtige Aktivitäten auf unserem Netzwerk festgestellt und vermuten, dass ein mögliches Datenleck vorliegen könnte.

Um die Sicherheit unserer Daten zu gewehrleisten und sicherzustellen, dass Ihre Konten nicht gefährdet sind, bitten wir Sie, an einer dringenden Sicherheitsüberprüfung teilzunehmen.

Klicken Sie auf den folgenden Link, um Ihre Konten zu überprüfen: KWV-Sicherheitsüberprüfung

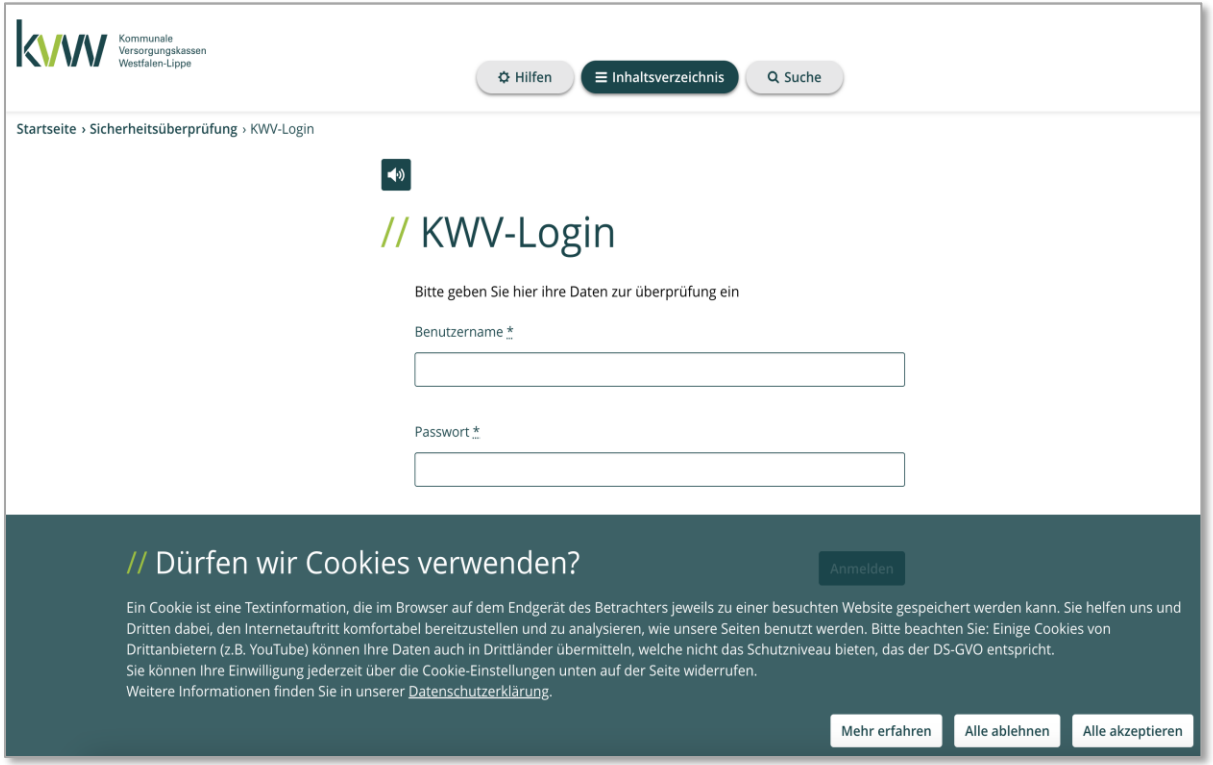
Wir danken Ihnen im Voraus für Ihre Mitarbeit bei der Sicherstellung der IT-Sicherheit bei den kwv.

Mit freundlichen Grüßen,
Ihr IT-Helpdesk

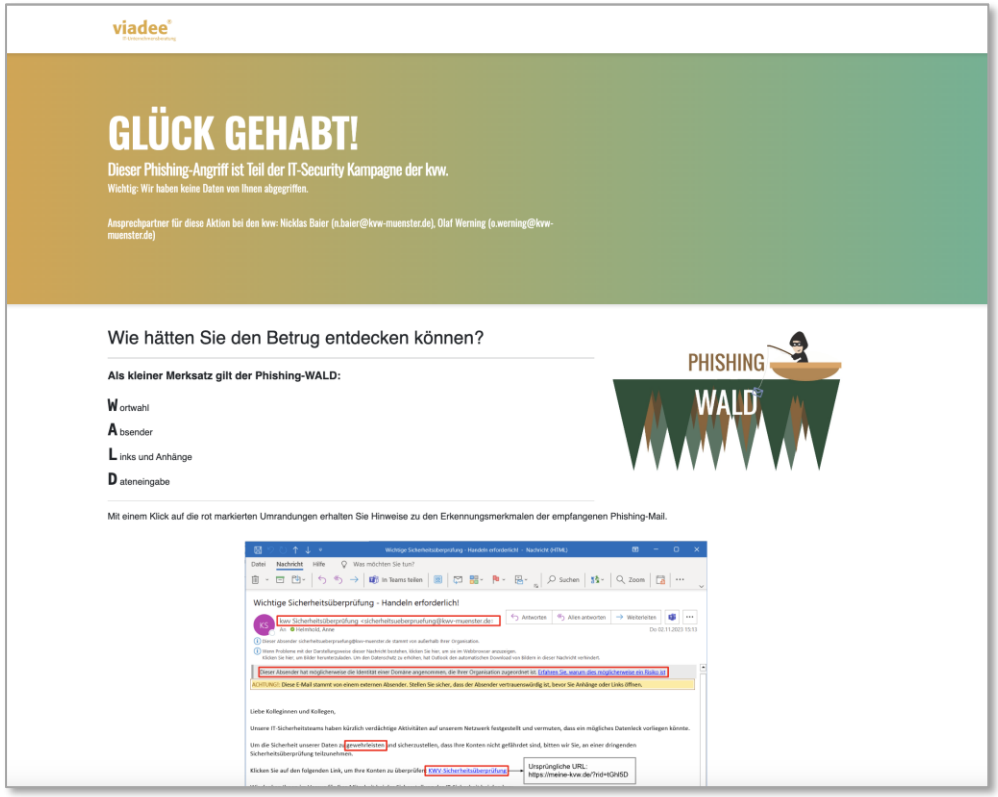
KONTAKT
Kommunale Versorgungskassen Westfalen-Lippe
kwv-Informationstechnologie
Zumsandestraße 12 // 48145 Münster
Tel. (0251) 591-6969 // Fax (0251) 590-6969
www.kwv-muenster.de

kwv – Bestens versorgt
1.200 Kommunen und kommunale Organisationen in Westfalen-Lippe vertrauen auf uns, wenn es um interkommunale Zusammenarbeit geht. Als zuverlässiger Partner in den Bereichen

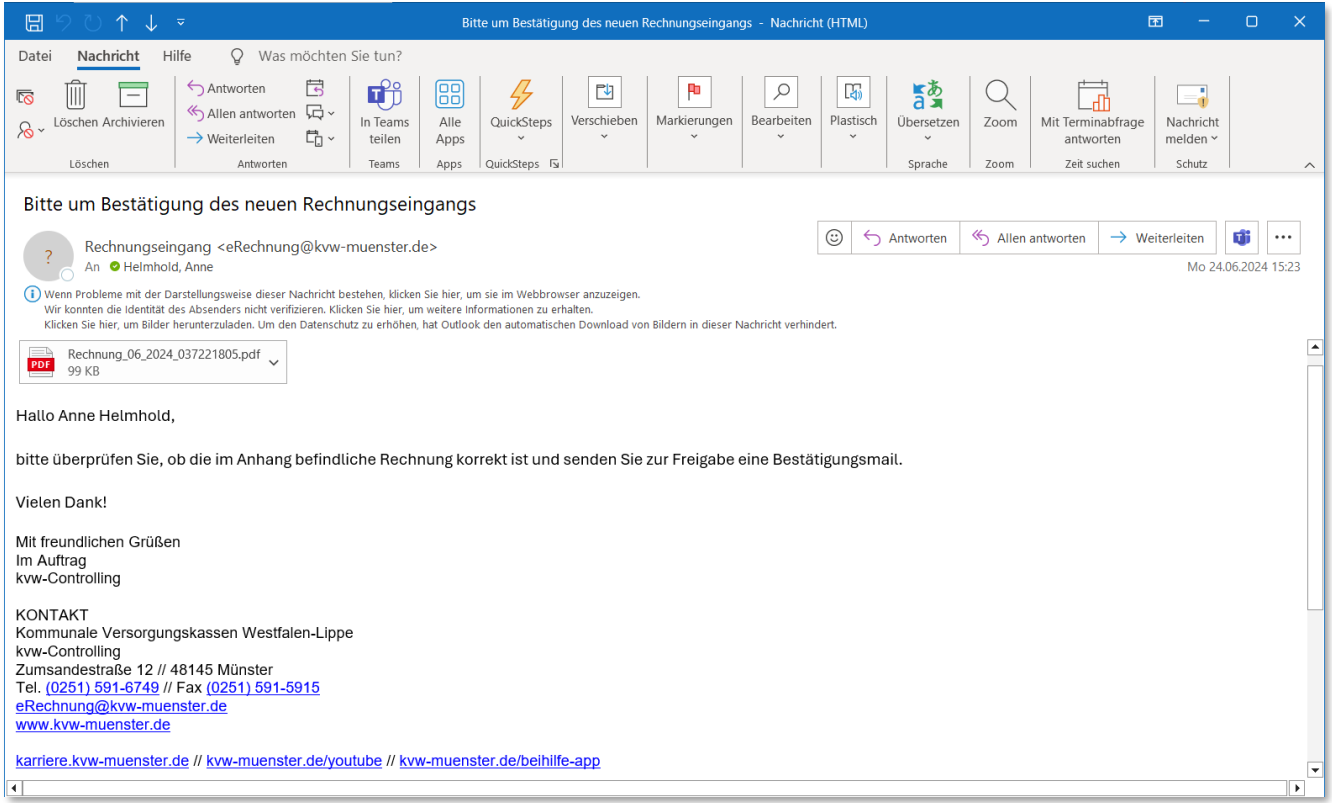
// Landing-Page



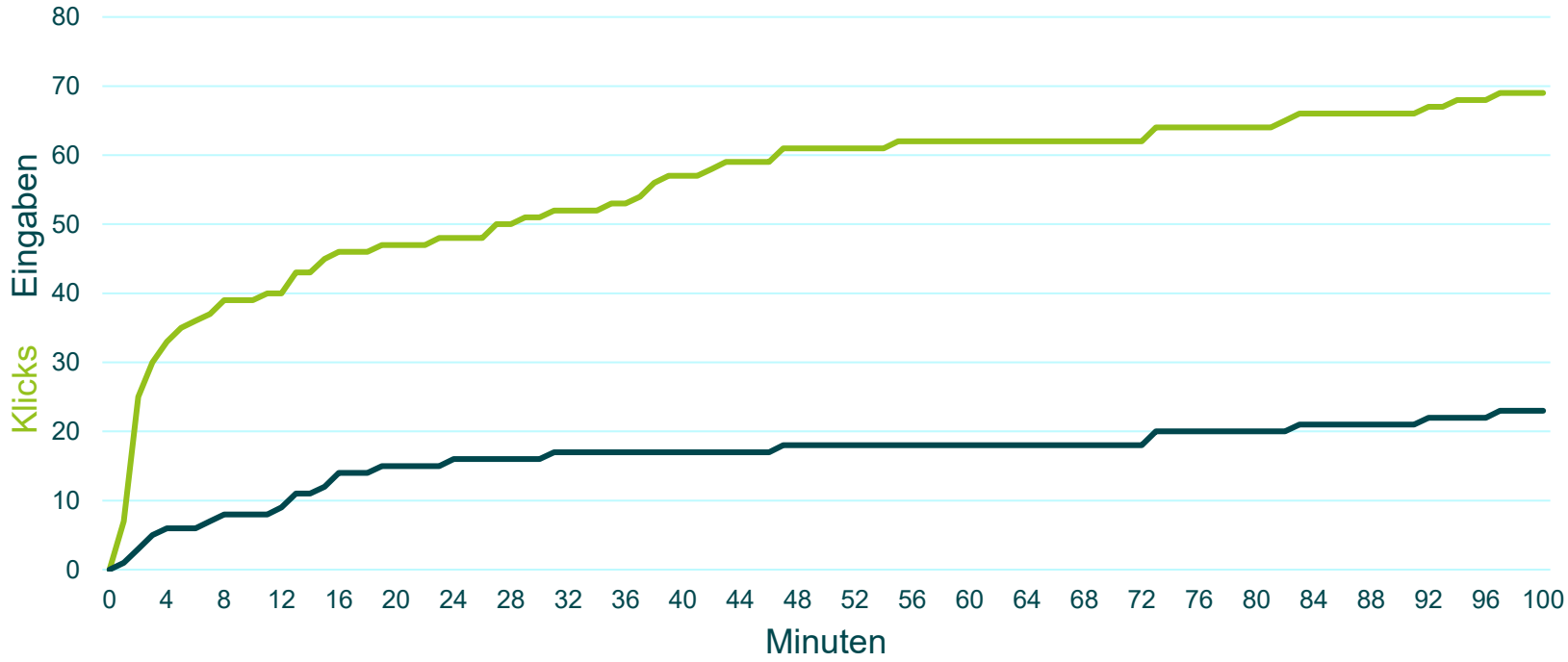
// Learning-Page



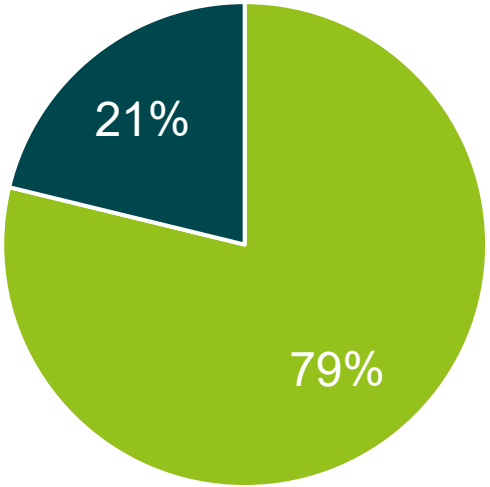
// Alternative Formate



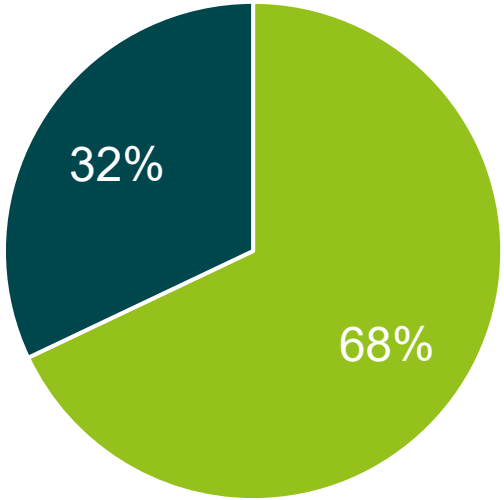
// Messinstrument: Klickzahlen



// Messinstrument: Datenangaben & Reports



■ Link nicht angeklickt ■ Link angeklickt



■ Zugangsdaten nicht eingegeben ■ Zugangsdaten eingegeben

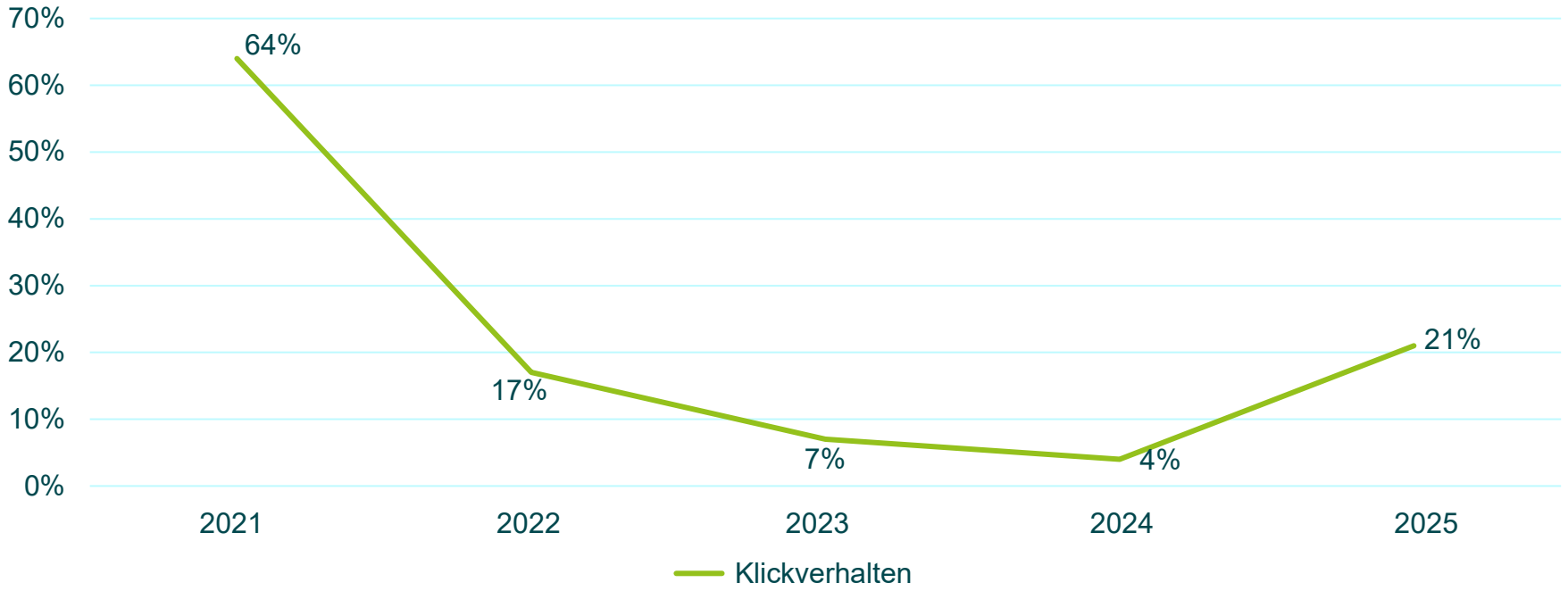
47

Reports in Outlook

Kommunale Versorgungskassen Westfalen-Lippe

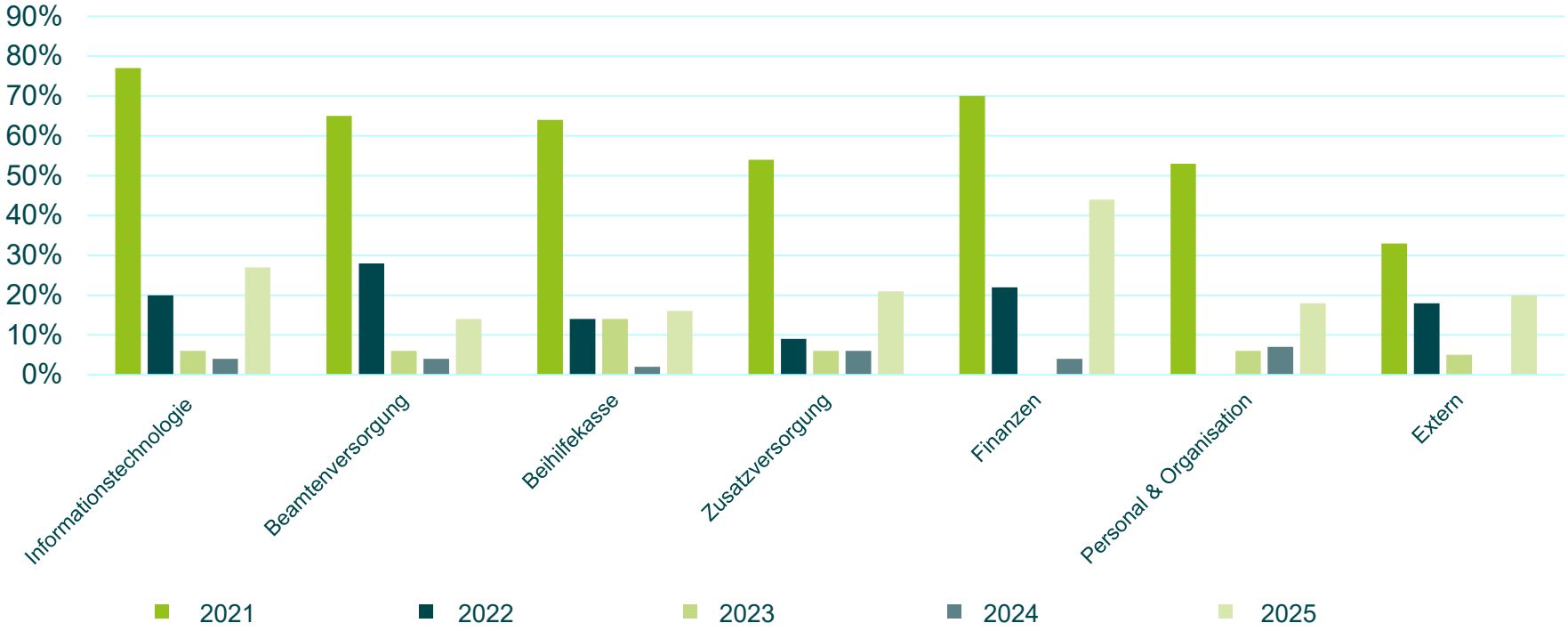
// Und was hat‘s gebracht?

// Klickraten im zeitlichen Verlauf



// Klickraten je Unternehmensbereich

ca. 450 Mitarbeitende



// Auf der Tonspur:

„Klar strukturierte und umsetzbare Richtlinien.“

„Hilft mir auch privat, mich und meine Familie besser zu schützen!“

„Überraschend praxisnahe Schulung – einiges konnte ich direkt im Job anwenden!“

„Ich schaue mir E-Mail deutlich kritischer an!“

“Ich weiß jetzt, wie ich mich im Ernstfall richtig verhalte!“

„Ich weiß an wen ich mich wenden kann, wenn etwas verdächtig ist.“

„Habe ein besseres Gefühl für aktuelle Bedrohungen“

„Wir sprechen im Team offener über Sicherheit.“

// Ein kleiner Ausblick

Trends und Regulatorik im Blick behalten

- Künstliche Intelligenz & neue Technologien
- Wandelnde regulatorische Anforderungen

Wir haben noch einige Ideen!

- USB-Drop-Kampagnen
- Physische Security Awareness
- Neue Phishing-Varianten
  Voice-Phishing / QR-Code-Phishing / Deepfakes
- Aufbau einer Community of Practice

Kein Projekt, sondern ein fortlaufender Prozess!

// Auflösung des Ratespiels

- ✓ Vertrauliche Dokumente offen sichtbar
- ✓ Zugangsdaten einsehbar
- ✓ Computer nicht gesperrt