



# Phishing-Analyse Report

Security Awareness Auswertung

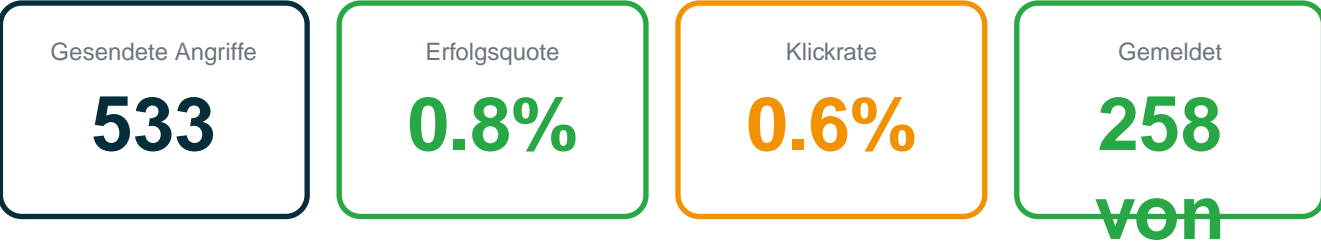
Kunde: Bilz Vibrationstechnologie AG

Erstellt am: 6. Januar 2026

Sicherheitsbewertung

**NIEDRIG**

# 1. Zusammenfassung



Bei 533 533 durchgeführten Phishing-Simulationen wurden 4 erfolgreiche Angriffe verzeichnet. Dies entspricht einer Erfolgsquote von 0.8%. 258 Angriffe wurden von Mitarbeitern gemeldet. Basierend auf dieser Auswertung wird die Sicherheitslage als **NIEDRIG** eingestuft.

## 2. Gefährlichste Phishing-Szenarien

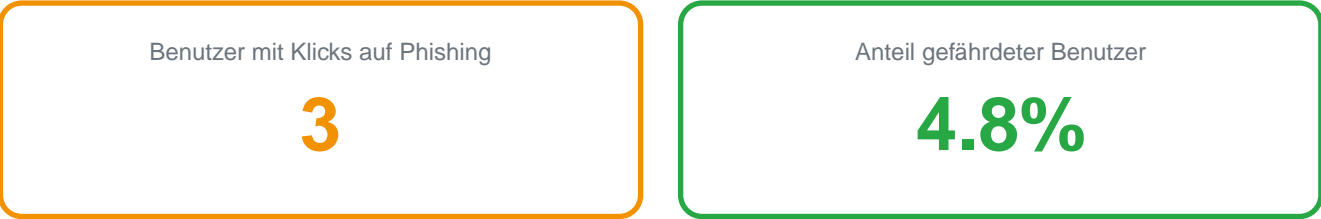
### Top 3 Szenarien mit höchster Erfolgsquote

Beschreibung	Angriffe	Erfolgsquote
Migration to Outlook 2019	2	0.5%
Interpol warning about ChatGPT phishing	3	0.3%
Inquiry about quotation (.xlsm)	12	0.1%

### Häufigste psychologische Trigger

- 1. ['curiosity'] (18 Szenarien)
- 2. 'fear'] (15 Szenarien)
- 3. ['fear'] (14 Szenarien)
- 4. ['curiosity'] (12 Szenarien)
- 5. 'time\_pressure'] (12 Szenarien)

### 3. Benutzerverhalten - Übersicht



Erfolgsquote nach Sicherheitslevel

Level	Gesendete Angriffe	Erfolgreiche Angriffe	Erfolgsquote
Level 1	144	2	1.4%
Level 2	22	0	0%
Level 3	1	0	0%
Level 4	366	2	0.5%
Level 5	0	0	0%

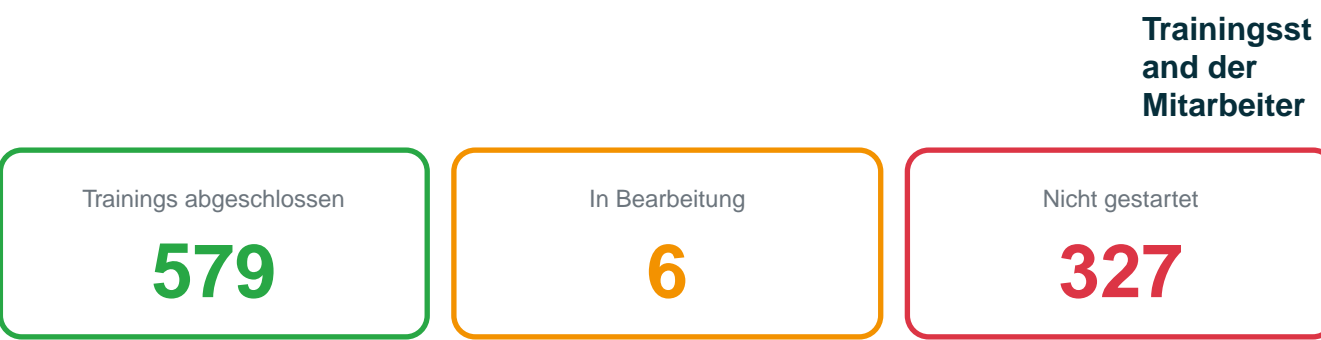
Was bedeuten die Sicherheitslevel?

- Level 1: Einstiegslevel - Neue Mitarbeiter ohne Security-Training
- Level 2: Grundkenntnisse - Basis-Schulung absolviert
- Level 3: Fortgeschritten - Regelmäßige Trainings und gutes Bewusstsein
- Level 4: Experte - Hohe Sensibilität und vorbildliches Verhalten
- Level 5: Security Champion - Multiplikator und Vorbild für andere

## 4. Anfälligste Benutzer - Detailanalyse

Die folgende Tabelle zeigt die Mitarbeiter mit der höchsten Anfälligkeit für Phishing-Angriffe. Rot markierte Benutzer sind besonders gefährdet und sollten prioritär geschult werden.

E-Mail	Level	Gesende	Erfolge	Klicks	Training	Anfälligkeit
intadmin@bilz.ag	4	9	2	2	10	22.2%
rueckert@bilz.ag	4	8	1	0	8	12.5%
petrovic@bilz.ag	4	9	1	1	16	11.1%
baeuerle@bilz.ag	5	9	0	0	16	0%
becker@bilz.ag	5	9	0	0	1	0%
beraldi@bilz.ag	4	9	0	0	13	0%
boettle@bilz.ag	4	9	0	0	0	0%
brenk@bilz.ag	5	9	0	0	15	0%
daxer@bilz.ag	4	9	0	0	16	0%
falkenstein@bilz.ag	4	9	0	0	0	0%



Durchschnittlich 9.3 Trainings pro Mitarbeiter

### Mitarbeiter-Verteilung nach Level

Level	Anzahl Mitarbeiter	Ø erfolgreiche Angriffe	Ø Trainings
1	3	0	0
2	2	0	0
3	1	0	9
4	32	0.1	8.3
5	24	0	12.7

## 5. Angriffstypen - Detailanalyse

### Erfolgsquote nach Angriffstyp

Angriffstyp	Szenarien	Ø Erfolgsrate	Angriffe	Erfolgreich
Link mit Login	5	0.1%	12	1
link-doc	79	0%	443	2
attachment-docm	15	0%	78	1

#### Szenario-Zusammenfassung

Insgesamt wurde n 99 v erschieden e Phi shing-Szen arien getest et. Die d urchs chnittl iche Erfolg squot e über alle S zenari en be trägt 0.8%. Die g efährli chste n Ang riffsty pen sind oben aufge führt.

## 6. Training-Effektivität

Vergleich der Erfolgsquote bei Phishing-Angriffen zwischen Mitarbeitern mit und ohne abgeschlossene Trainings.



Achtung: Mitarbeiter mit Trainings zeigen eine höhere Erfolgsquote. Dies sollte analysiert werden.

### Trainingsabschluss nach Level

Level	Anzahl Mitarbeiter	Ø erfolgreiche Angriffe	Ø Trainings
1	3	0	0
2	2	0	0
3	1	0	9
4	32	0.1	8.3
5	24	0	12.7

## 7. Fazit und Handlungsempfehlungen

---

Gesamtbewertung der Sicherheitslage

**NIEDRIG**

### Empfohlene Maßnahmen

1. Aufrechterhaltung des aktuellen Schulungsniveaus
2. Kontinuierliche Phishing-Simulationen zur Wachsamkeit (halbjährlich)
3. Positive Verstärkung des guten Meldeverhaltens
4. Meldesysteme weiter stärken und bekannt machen
5. Best-Practice-Sharing zwischen den Sicherheitslevels
6. Regelmäßige Auffrischkurse für alle Mitarbeiter

Dieser Report wurde automatisch generiert und enthält ausschließlich aggregierte, anonymisierte Daten.

© 2026 Intelego Awareness Tool - Powered by Hornetsecurity