KnowBe4

PHISHING-BENCHMARKING 2023

Report für Deutschland, Österreich und die Schweiz

*Von **Dr. Martin J. Kraemer**, Security Awareness Advocate, KnowBe4*

Die häufigste Ursache für Datenschutzverletzungen ist der Faktor Mensch. Sicherheitsverantwortliche, die nach wie vor nur in neue Sicherheitstechnologien investieren, übersehen möglicherweise eine bewährte Best Practice zur Gefahrenabwehr: Security Awareness Training in Verbindung mit regelmäßigen Social-Engineering-Simulationen. Dieser Ansatz schärft das Bewusstsein der Belegschaft für die Bedrohung durch Cyberkriminalität und schafft zugleich das Fundament für eine robuste Sicherheitskultur.

Die derzeitigen geopolitischen Verwerfungen verändern auch die Dynamik im Bereich der Cyberkriminalität. Vor diesem Hintergrund müssen Unternehmen, Institutionen und Organisationen beim größten Risiko für die Cybersicherheit ansetzen: dem Faktor Mensch. Mangelt es bei Ihren Mitarbeitenden an Wissen, Aufmerksamkeit und Engagement, können Cyberkriminelle sie zu sicherheitsrelevanten Fehlentscheidungen verleiten. Schon eine kleine Unachtsamkeit kann Cyberkriminellen ein Einfallstor bieten.

Sicherheitsverantwortliche müssen Gewissheit darüber haben, wie ihre Mitarbeitenden auf Phishing-E-Mails reagieren: Klicken sie auf den Link? Tappen sie in die Falle und geben sie Anmeldedaten heraus? Laden sie einen Anhang mit Malware herunter? Ignorieren oder löschen sie verdächtige E-Mails, ohne das Sicherheitsteam wie vorgesehen zu informieren? Oder melden sie mögliche Phishing-Versuche und nehmen eine aktive Rolle bei der Gefahrenabwehr ein?

Die Wahrscheinlichkeit, mit der Mitarbeitende auf einen Phishing-Versuch hereinfallen, wird als Phish-prone™ Percentage (PPP) bezeichnet. Mit diesem aussagekräftigen Wert können Unternehmen, Institutionen und Organisationen die Wahrscheinlichkeit, dass ein Angriff erfolgreich ist, besser einschätzen und gezielt Trainings anbieten.

KnowBe4 führt jährlich eine Erhebung durch, bei der die Phishing-Anfälligkeit aufgeschlüsselt nach Region und Umfang der Unternehmen, Institutionen und Organisationen (klein, mittel, groß) ermittelt wird, damit diese ihren jeweiligen PPP im relevanten Kontext betrachten können. Das vorliegende Dokument gibt einen Überblick über die wichtigsten Ergebnisse für Deutschland, Österreich und die Schweiz (DACH) im Vergleich zum Rest der Welt.

Globale Studie zum Phishing-Risiko im Branchenvergleich 2023

Selbstverständlich möchten alle Unternehmen, Institutionen und Organisationen wissen, wie sie in der jeweiligen Branche und/oder im weltweiten Vergleich abschneiden. Voraussetzung dafür, dass ein solcher Vergleich aussagekräftige Ergebnisse liefert, sind jedoch belastbare Daten sowie eine bewährte wissenschaftliche Methodik. Die Frage nach dem Abschneiden im Branchenvergleich ist also keineswegs einfach zu beantworten. Im Rahmen der Studie zum Phishing-Risiko im Branchenvergleich 2023 wurden Daten von mehr als 12,5 Millionen Nutzer:innen in 35.681 Unternehmen, Institutionen und Organisationen aus weltweit 19 Branchen analysiert. Über 32,1 Millionen simulierte Phishing Security Tests wurden durchgeführt.

In unserem Report 2023 gehen wir ausführlich auf die folgenden drei Phasen ein:

PHASE 1

Sie haben Ihre Nutzer:innen noch nicht geschult und führen einen simulierten Phishing-Angriff durch. Wie hoch liegt der anfängliche PPP?

Hierfür erfassen wir die Anfälligkeit der Mitarbeitenden bei einem ersten simulierten Phishing Security Test. In die Berechnung fließen alle Vorfälle mit ungeschulten Nutzer:innen ein, die auf einen simulierten Phishing Security Test hereinfallen.

PHASE 2

Wie hoch liegt der PPP Ihrer Nutzer:innen, wenn innerhalb von 90 Tagen nach dem ersten Training ein Phishing Security Test durchgeführt wird?

In diese Berechnung fließen alle Nutzer:innen ein, die ihr erstes Training absolviert haben, sowie alle simulierten Phishing-Versuche innerhalb von 90 Tagen nach Abschluss des Trainings.

PHASE 3

Wie hoch liegt der endgültige PPP Ihrer Nutzer:innen, wenn diese an fortlaufenden Trainings teilnehmen und jeden Monat Tests mit simulierten Phishing-Versuchen durchgeführt werden?

Die Berechnung erfolgt, wenn mindestens zwölf Monate lang fortlaufende Trainings und Phishing Security Tests stattgefunden haben. In die Berechnung fließen die Ergebnisse des letzten Phishing-Tests der Nutzer:innen ein, die ihr erstes Training mindestens ein Jahr zuvor abgeschlossen haben.

Ergebnisse des internationalen Branchenvergleichs zum Phishing-Risiko nach Region

Phase 1
Baseline Phishing-Testergebnisse

Phase 2
Phishing-Testergebnisse innerhalb von 90 Tagen nach dem ersten Training

Phase 3
Phishing-Testergebnisse nach mindestens einem Jahr mit fortlaufenden Trainings

	BASELINE			90 TAGE			1 JAHR		
Größe der Unternehmen, Institutionen bzw. Organisationen	**1–249**	**250–999**	**1.000 und mehr**	**1–249**	**250–999**	**1.000 und mehr**	**1–249**	**250–999**	**1.000 und mehr**
Nordamerika	28 %	30,1 %	37,1 %	18,5 %	19 %	18,4 %	4,2 %	5,1 %	5,7 %
	INSGESAMT: 33,1 %			**INSGESAMT: 18,6 %**			**INSGESAMT: 5,1 %**		
Afrika	30 %	29,4 %	33,3 %	25,2 %	22,7 %	19,3 %	9 %	10,5 %	5,7 %
	INSGESAMT: 32,8 %			**INSGESAMT: 20,5 %**			**INSGESAMT: 6,6 %**		
Asien	32,6 %	33,2 %	28,8 %	20,9 %	19,6 %	13 %	7,3 %	7,4 %	6 %
	INSGESAMT: 30 %			**INSGESAMT: 14,9 %**			**INSGESAMT: 6,5 %**		
Australien und Neuseeland	27,1 %	30,9 %	41,1 %	21,1 %	19,9 %	15,3 %	6,3 %	7,7 %	5,4 %
	INSGESAMT: 34,8 %			**INSGESAMT: 17,8 %**			**INSGESAMT: 6,4 %**		
Europa	26,5 %	28 %	36,2 %	19,1 %	19,7 %	19,4 %	6,7 %	7,6 %	6,1 %
	INSGESAMT: 32,9 %			**INSGESAMT: 19,4 %**			**INSGESAMT: 6,5 %**		
Südamerika	34 %	27,7 %	49,5 %	23 %	25,8 %	18,7 %	6,4 %	10,2 %	5,1 %
	INSGESAMT: 41,1 %			**INSGESAMT: 21,3 %**			**INSGESAMT: 6,9 %**		
Vereinigtes Königreich und Irland	26,3 %	28 %	39,6 %	18,5 %	18,1 %	17,6 %	6,1 %	8,1 %	4,9 %
	INSGESAMT: 35,2 %			**INSGESAMT: 17,8 %**			**INSGESAMT: 5,8 %**		

Die drängendsten Anliegen in Europa

Der Konflikt zwischen Russland und der Ukraine wirkt sich auf zahlreiche europäische Länder aus. Der ENISA Threat Landscape Report 2022 spricht von einer Zunahme der Hackeraktivitäten während des Kriegsverlaufs sowie deren Nutzung und Förderung durch staatliche Stellen. Vor dem Hintergrund des russisch-ukrainischen Konflikts ist Desinformation zur wichtigsten Waffe im Cyberkrieg geworden. Auf dem Gebiet der künstlichen Intelligenz (KI) wurden große technologische Fortschritte erzielt, insbesondere in den Bereichen generative KI und maschinelles Lernen. Selbstverständlich ergeben sich hierdurch auch neue Möglichkeiten für den Missbrauch dieser Technologien durch Cyberkriminelle. KI-gestützte Social-Engineering-Angriffe, Desinformation und Deep Fakes sind zu realen Bedrohungen geworden, vor denen sich Unternehmen, Institutionen und Organisationen nun schützen müssen.

Die verbreitetsten Cyberbedrohungen in der Region sind nach wie vor Ransomware, Malware und Social Engineering. Laut dem jüngsten „What CEOs talked about"-Report von IOT Analytics ist die unsichere Wirtschaftslage (Inflation, Rezession und Zinssätze) nach wie vor das, was Führungskräfte am meisten beschäftigt. Selbstverständlich sind dies äußerst wichtige Themen. Dennoch verdient die anhaltende Bedrohung durch Cyberkriminalität mehr Aufmerksamkeit von Seiten der Unternehmensleitung. Wird dieser Bereich vernachlässigt, können Bedrohungsakteure in unvorbereiteten Unternehmen, Institutionen und Organisationen ungehindert ans Werk gehen.

Wirtschaftlicher Schaden

Die wirtschaftlichen Folgen der Cyberkriminalität in Europa lassen sich nur schwer genau beziffern, ihr finanzielles Schadenspotenzial steht jedoch außer Zweifel.

Gemäß der Datenschutzgrundverordnung (DSGVO) sind Unternehmen, Institutionen und Organisationen im Fall von Datenschutzverletzungen verpflichtet, den betroffenen Kund:innen Schadensersatz zu leisten. Prozesskosten, Bußgelder für Verstöße und die Kosten für die Untersuchung von Vorfällen können in die Millionen gehen. Hinzu kommen die Folgen einer möglichen Beeinträchtigung (oder Einstellung) der Produktion, Verzögerungen bei der Auftragserfüllung und die Schädigung des Rufs bei Lieferant:innen und Kund:innen.

Die wirtschaftlichen Auswirkungen der Cyberkriminalität betreffen alle Unternehmen, Institutionen und Organisationen, nicht nur diejenigen, die Opfer von Cyberangriffen geworden sind. Der zunehmende Mangel an Fachkräften im Bereich der Cybersicherheit und die damit einhergehende wachsende Qualifikationslücke zwingen Unternehmen zu zusätzlichen Ausgaben im Bereich Sicherheit. Höhere Arbeitsbelastung, unbesetzte Stellen und Burnout führen dazu, dass Sicherheitsabteilungen personell unterbesetzt sind. Nach Angaben des Weltwirtschaftsforums muss das für die Cybersicherheit zuständige Personal in Unternehmen, Institutionen und Organisationen um 65 % aufgestockt werden, um kritische Assets zu schützen. Dadurch werden die ohnehin bereits kaum ausreichenden Budgets für IT-Sicherheit weiter strapaziert.

DACH	BASELINE	90 TAGE	1 JAHR
1–249	26,3 %	17,4 %	7,7 %
250–999	26 %	19,1 %	7,8 %
1.000 und mehr	34,1 %	21 %	4,5 %
Durchschnittlicher PPP unabhängig von der Mitarbeiteranzahl	30,9 %	20 %	5,6 %
Durchschnittlicher PPP unabhängig von der Mitarbeiteranzahl (Europa)	32,9 %	19,4 %	6,8 %

Typisches Unternehmensprofil

Im Allgemeinen schneidet die DACH-Region gleich gut oder etwas besser ab als das übrige Europa. Der durchschnittliche PPP aller Unternehmen, Institutionen und Organisationen in der DACH-Region für Phase 1 und Phase 3 liegt leicht über dem entsprechenden Wert für Gesamteuropa (siehe Tabelle oben).

In der DACH-Region schneiden mittlere Unternehmen, Institutionen und Organisationen (250–999 Mitarbeitende) vor dem ersten Training am besten ab. Der branchenübergreifende PPP liegt hier bei 26 %. Hierauf folgen kleine Unternehmen, Institutionen und Organisationen (1–249 Mitarbeitende) mit einem durchschnittlichen PPP von 26,32 % und große Unternehmen, Institutionen und Organisationen (über 1.000 Mitarbeitende) mit einem durchschnittlichen PPP von 34 %.

99 % aller Unternehmen in der EU sind kleine und mittlere Unternehmen. Laut Statista waren 2020 ca. 93,3 % der europäischen Unternehmen außerhalb des Finanzsektors Kleinstunternehmen mit maximal neun Mitarbeitenden. Im gleichen Jahr wurden ca. 5,7 % als Kleinunternehmen (10–49 Mitarbeitende), 0,9 % als mittlere Unternehmen (50–249 Mitarbeitende) und 0,2 % als Großunternehmen mit mehr als 250 Mitarbeitenden erfasst.

Wichtige Erkenntnisse

Drei wichtige Erkenntnisse sind:

- ✓ Die Anstrengungen zur Erhöhung der Resilienz von Unternehmen, Institutionen und Organisationen in Europa müssen verstärkt werden. Geopolitische und wirtschaftliche Verwerfungen haben das Thema Cybersicherheit aus dem Fokus gerückt. Der Anstieg der Hackeraktivitäten in der Region ist relativ gering und die Aufmerksamkeit der Entscheidungsträger:innen richtet sich auf die Veränderungen in der geopolitischen Lage.
- ✓ Eine Sensibilisierung im Hinblick auf die Bedrohung durch KI-gestützte Cyberangriffe und deren Folgen ist unerlässlich. Mit den Entwicklungen im Bereich des maschinellen Lernens (z. B. bei Deep Fakes und Stimmbiometrie) verfügen Bedrohungsakteure nun über leistungsstarke Werkzeuge zur Erstellung irreführender Inhalte, mit denen die Raffinesse dieser ohnehin schon gefährlichen Angriffe noch weiter gesteigert werden kann. Desinformation stellt daher eine wachsende Bedrohung dar. Da die neuen Werkzeuge bereits genutzte Angriffsformen realistischer machen, ist es unerlässlich, Mitarbeitende für diese Entwicklungen zu sensibilisieren.
- ✓ Die Anstrengungen zum Aufbau einer robusten Sicherheitskultur müssen verstärkt werden. Der ganzheitliche Ansatz, der Security Awareness und die Ausbildung sicherheitsbewusster Verhaltensformen vereint, ist eine bewährte Methode, mit der sich Risiken mindern und zugleich geschäftliche Vorteile erzielen lassen. Security-Awareness-Expert:innen müssen weiterhin Kampagnen zur Stärkung sicherheitsbewusster Verhaltensweisen durchführen. Unternehmen, Institutionen und Organisationen müssen ihre Resilienz im Bereich Cybersicherheit erhöhen.

Phishing-Risiko nach Branchen: Benchmarking-Report 2023 herunterladen

HERUNTERLADEN