KnowBe4

PHISHING-BENCHMARKING 2024 – REPORT FÜR EUROPA

EINFÜHRUNG

Die Internetkriminalität nimmt Jahr für Jahr zu und es sind immer mehr Opfer betroffen – sowohl im beruflichen als auch im privaten Kontext. Cyberkriminelle sind nicht wählerisch. Alle sich bietenden Ziele werden ins Visier genommen – jederzeit und überall. Doch auch die technischen Maßnahmen zur Cyberabwehr entwickeln sich weiter. Aus diesem Grund verlagern Cyberkriminelle ihren Schwerpunkt auf das verletzlichste der Ziele: den Menschen. Menschliche Schwächen sind nach wie vor ein wichtiger Ansatzpunkt für Kriminelle. Sie haben es auf Mitarbeitende in allen Branchen und sämtlichen Funktionen innerhalb von Unternehmen, Institutionen und Organisationen abgesehen. Viele davon investieren unverhältnismäßig viel in technische Sicherheitsmaßnahmen und vernachlässigen dagegen häufig die entscheidende Bedeutung des Risikomanagements in Bezug auf den Faktor Mensch.

Künstliche Intelligenz (KI) wird mittlerweile umfassend eingesetzt und hat ungeahnte technologische Möglichkeiten hervorgebracht. Vor diesem Hintergrund ist der Fokus auf Cybersicherheit wichtiger denn je. KI-Systeme können umfangreiche Datensätze schnell analysieren und dabei Muster wesentlich besser erkennen als Menschen. Hierbei handelt es sich um ein zweischneidiges Schwert: Einerseits kann diese Fähigkeit zu einer wesentlichen Verbesserung von Cybersicherheitsmaßnahmen beitragen, andererseits liefert sie Cyberkriminellen ausgefeilte Werkzeuge für die Ausnutzung von Schwachstellen.

Cyberkriminelle dringen mithilfe einer Kombination aus bewährten Taktiken und neuartigen Techniken in digitale Bereiche ein und umgehen damit Sicherheitsmaßnahmen, die vom Faktor Mensch abhängen. Voraussetzung für wirksame Schutzmaßnahmen ist ein entsprechendes Problembewusstsein bei Mitarbeitenden, die durch ihr Verhalten zu einer soliden Sicherheitskultur beitragen. Alle Mitarbeitenden von Unternehmen, Institutionen und Organisationen müssen sich als integralen Bestandteil der Verteidigung gegen Cyberangriffe wahrnehmen und wissen, wie sich ihr Handeln auf die allgemeine Sicherheit auswirkt.

Menschliche Schwächen sind für Cyberkriminelle wahres Gold. Sie nutzen Wissenslücken aus, machen sich Emotionen zunutze und profitieren von Ablenkungen und Bequemlichkeit. Diese auf den Faktor Mensch abzielenden Taktiken haben sich als äußerst effektiv erwiesen, da bereits ein Fehler oder mangelndes Sicherheitsbewusstsein eines einzelnen Mitarbeitenden ausreicht, um selbst die robustesten technischen Sicherheitsmaßnahmen wirkungslos zu machen.

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? Mitarbeitende müssen kein Risikofaktor sein. Im Gegenteil. Indem Unternehmen, Institutionen und Organisationen die notwendigen Kenntnisse und Kompetenzen vermitteln sowie die passenden Tools bereitstellen, machen sie sich ihre Mitarbeitenden zu wertvollen Verbündeten bei der Abwehr von Cyberbedrohungen.

RISIKO NACH BRANCHE

Die Anfälligkeit von Unternehmen, Institutionen und Organisationen gegenüber Phishing-Versuchen wird mit der als Phish-prone™ Percentage (PPP) bezeichneten Kennzahl angegeben. Dank dieser Quantifizierung können Führungskräfte das potenzielle Risiko von Datenschutzverletzungen einschätzen und die Anfälligkeit ihrer Mitarbeitenden gegenüber Cyberbedrohungen durch gezieltes Training verringern.

Die Phishing-Anfälligkeit gibt Auskunft darüber, wie viel Prozent der Mitarbeitenden zu einem gegebenen Zeitpunkt wahrscheinlich auf einen Social-Engineering- oder Phishing-Versuch hereinfallen. Damit ist dieser Wert ein guter Indikator für das Risiko und die Widerstandsfähigkeit von Unternehmen, Institutionen und Organisationen im Fall eines Angriffs.

Je höher die Phishing-Anfälligkeit, desto höher das Risiko, da voraussichtlich mehr Mitarbeitende Betrugsversuchen zum Opfer fallen. Umgekehrt bedeutet eine niedrige Phishing-Anfälligkeit, dass die Belegschaft eher zur Stärkung der Sicherheit beiträgt, als diese zu schwächen. Optimal ist eine niedrige Phishing-Anfälligkeit. Diese deutet darauf hin, dass Mitarbeitende sicherheitsbewusst sind und wissen, wie sie Betrugsversuche erkennen und abwehren.

Damit Unternehmen, Institutionen und Organisationen ihre Phishing-Anfälligkeit und ihr Ranking besser einschätzen können, erstellt KnowBe4 in einer jährlich durchgeführten Studie einen Vergleich nach Branche, Anzahl der Mitarbeitenden und Region. Der vorliegende Report bietet einen Überblick über die wichtigsten Ergebnisse für Europa.

GLOBALE STUDIE ZUM PHISHING-RISIKO IM BRANCHENVERGLEICH 2024

Selbstverständlich möchten Unternehmen, Institutionen und Organisationen wissen, wie sie im Vergleich zu anderen in der Branche dastehen. Voraussetzung für einen aussagekräftigen Vergleich sind hierbei umfassende Daten und ein wissenschaftlich fundiertes Konzept, das belastbare Ergebnisse liefert. Unternehmen, Institutionen und Organisationen können die Frage zu ihrem Abschneiden im Vergleich mit anderen daher nur schwer beantworten.

Hier kommt unsere jährliche Studie zum Phishing-Risiko im Branchenvergleich ins Spiel. Im Rahmen der Studie für 2024 wurden Daten von mehr als 54 Millionen Phishing-Simulationen von 11,9 Millionen Nutzern und Nutzerinnen in 55.675 Unternehmen, Institutionen und Organisationen aus 19 Branchen analysiert.

Methodik der diesjährigen Studie

Der Datenbestand wurde nach Branche und Größe kategorisiert. Die Phishing-Anfälligkeit der einzelnen Unternehmen, Institutionen und Organisationen berechnet sich aus dem Anteil der Mitarbeitenden, die während einer KnowBe4-Testkampagne auf einen simulierten Phishing-Link geklickt oder einen simulierten Malware-Anhang geöffnet haben.

Auch im Bericht für 2024 werden die Ergebnisse nach folgenden Benchmark-Phasen aufgeschlüsselt:

- **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

INTERNATIONALE PHISHING-VERGLEICHSZAHLEN 2024

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/Mitarbeiteranzahl	1–249	250–999	1.000 und mehr	1–249	250–999	1.000 und mehr	1–249	250–999	1.000 und mehr
REGION	Nordamerika	29 %	32,6 %	39,1 %	19,8 %	19,9 %	17,9 %	4,3 %	4,6 %	4,6 %
		INSGESAMT: 35,1 %			INSGESAMT: 18,9 %			INSGESAMT: 4,5 %		
	Afrika	29,7 %	32,8 %	38 %	23,7 %	28,7 %	20,2 %	3,6 %	5,4 %	6,2 %
		INSGESAMT: 36,7 %			INSGESAMT: 22 %			INSGESAMT: 5,9 %		
	Asien	31,5 %	31,6 %	27,4 %	20,3 %	17,6 %	16,6 %	5,4 %	4,5 %	5,9 %
		INSGESAMT: 28,4 %			INSGESAMT: 17 %			INSGESAMT: 5,5 %		
	Australien und Neuseeland	27,8 %	32,5 %	40,3 %	21,4 %	20,3 %	16,5 %	4,9 %	5,3 %	4,7 %
		INSGESAMT: 34,4 %			INSGESAMT: 19,1 %			INSGESAMT: 5 %		
	Europa	26,5 %	26,9 %	35,6 %	19,3 %	20,2 %	20,6 %	4,1 %	4,9 %	5,9 %
		INSGESAMT: 32,6 %			INSGESAMT: 20,3 %			INSGESAMT: 5,5 %		
	Südamerika	32,7 %	29,4 %	44,9 %	24,4 %	22,5 %	16,8 %	5,2 %	5,2 %	3 %
		INSGESAMT: 39,2 %			INSGESAMT: 18,7 %			INSGESAMT: 3,9 %		
	Vereinigtes Königreich und Irland	26,5 %	30,2 %	35,2 %	20 %	21 %	16,5 %	4,1 %	4,3 %	4,8 %
		INSGESAMT: 32,3 %			INSGESAMT: 18,4 %			INSGESAMT: 4,5 %		

EUROPA

Von Martin Krämer

Benchmark-Daten

Gegenüber den Zahlen im Report für 2023 zeigt sich bei den für das Jahr 2024 ausgewerteten Unternehmen, Institutionen und Organisationen insgesamt eine Verschlechterung. Betrachtet man Unternehmen, Institutionen und Organisationen aller Größen gemeinsam, sank der Baseline-Wert um 3,2 %. Der 90-Tage-Wert stieg zwar um 0,6 %, jedoch ging der 1-Jahres-Wert um 1,5 % zurück. Europäische Unternehmen, Institutionen und Organisationen der drei unterschiedlichen Größenkategorien (1–249, 250–999 und ab 1.000 Mitarbeitende) schnitten besser ab als der weltweite Durchschnitt. Vor dem Training schnitten kleine Unternehmen, Institutionen und Organisationen (26,5 %) am besten ab, gefolgt von mittleren (26,8 %) und großen (35,6 %). Diese Zahlen sind gegenüber dem letzten Jahr praktisch unverändert und entsprechen mehr oder weniger den Ergebnissen früherer Jahre. Diese stagnierenden Ergebnisse deuten darauf hin, dass viele Unternehmen, Institutionen und Organisationen ihr Engagement in Bezug auf Security Awareness noch weiter verstärken müssen. Es geht darum, zu erkennen, dass dem Verhalten der Belegschaft eine entscheidende Rolle bei der Cyberabwehr zukommen muss und dass Phishing den wichtigsten Angriffsvektor für Social Engineering bildet. Vielversprechend ist diesbezüglich, dass europäische Unternehmen, Institutionen und Organisationen vor dem Training im Allgemeinen bessere Ergebnisse erzielten als der Rest der Welt.

Typisches Unternehmensprofil

In Europa wächst die Zahl kleiner und mittlerer Unternehmen. Die überwiegende Mehrheit der Unternehmen hat 10 bis 49 Mitarbeitende. Nur bei weniger als einem Prozent übersteigt die Anzahl der Mitarbeitenden 250. Mehr als 70 % der kleinen Unternehmen stehen laut **Eurostat** bei der digitalen Transformation noch am Anfang. Mittlere und große Unternehmen sind in diesem Bereich bereits weiter. (Nur etwa 40 % bzw. 20 % kommen auf niedrige oder sehr niedrige Werte.) Der Indikator basiert auf einer Reihe von Kennzahlen, wie der Nutzung von Remote-Working-Tools und Online-Konferenz-Software, dem Vorhandensein von Sicherheitsmaßnahmen und dem Einsatz von Robotern in der Fertigung.

Kleine und mittlere Unternehmen sind mittlerweile ein gängiges Ziel für Cyberangriffe, unabhängig davon, ob es sich um lokale Behörden, Handwerksbetriebe oder Zulieferer handelt. Sie müssen sich entsprechend vorbereiten. Immer häufiger kommen bei Angriffen kompromittierte Lieferanten-E-Mails zum Einsatz, da Lieferanten die Einfallstore zu ihren Geschäftspartnern bilden. Großunternehmen, bei denen das funktioniert, sind die lukrativeren Ziele für Cyberkriminelle.

Die drängendsten Anliegen

Laut dem **ENISA Threat Landscape Report 2023** sind Unternehmen, Institutionen und Organisationen in der Region häufig Ziel von DDoS- und Ransomware-Angriffen. Phishing ist nach wie vor der wichtigste Angriffsvektor. Jedoch ist eine Zunahme von Social-Engineering-Angriffen zu verzeichnen, bei denen KI und andere neue Verfahren zum Einsatz kommen. Auch vom weltweiten Trend zu neuen Erpressungstaktiken auf Basis immer professionellerer As-a-Service-Programme ist die Region nicht verschont geblieben. Noch vor Privatpersonen und Einrichtungen des Gesundheitswesens standen insbesondere Behörden im Zentrum solcher Angriffe. Die Agentur der Europäischen Union für Cybersicherheit (ENISA) berichtet außerdem von einer Zunahme manipulierter Informationen, beispielsweise im Zusammenhang mit dem Krieg Russlands in der Ukraine, sowie von einer allgemeinen Zunahme geopolitisch motivierter Cyberkriminalität.

Insgesamt entspricht die Situation im Wesentlichen der in den Vorjahren. Ransomware bleibt eine der größten Cyberbedrohungen, wobei auch hier Phishing den gängigsten Angriffsvektor darstellt. Besondere Aufmerksamkeit muss auch den immer häufiger werdenden Supply-Chain-Angriffen zukommen.

Wirtschaftliche Auswirkungen

Der durch Cyberkriminalität insgesamt verursachte wirtschaftliche Schaden lässt sich nur schwer beziffern. An einzelnen Fällen zeigt sich jedoch, wie gravierend die Folgen von Datenschutzverletzungen sein können. Upguard schätzte bereits 2018 den Gesamtschaden in Europa auf etwa 0,84 % des BIP. Die Zahl der Ransomware-Angriffe ist seitdem Jahr für Jahr mit hohen zweistelligen Wachstumsraten gestiegen. Es ist unwahrscheinlich, dass sich dies in absehbarer Zeit ändern wird. Im Gegenteil, Cyberkriminalität gilt mittlerweile als **drittgrößter Wirtschaftszweig der Welt**.

Der in Europa entstandene Schaden lässt sich auch an der Schwere aktueller Datenschutzverletzungen ablesen – von dem Angriff auf französische Krankenversicherungen, bei dem Daten von 33 Millionen Versicherten entwendet wurden, bis hin zu den Folgen der MOVEit-Sicherheitslücke, von der mehr als 100 Unternehmen, Institutionen und Organisationen in ganz Europa betroffen waren. Hierzu gehörten auch zahlreiche deutsche Behörden. Kreditscoring-Agenturen im Vereinigten Königreich rieten Kunden, ihre Scores einzufrieren. Ransomware-Banden treiben nach wie vor ihr Unwesen in Europa und setzen dabei auch neue Erpressungsmethoden ein. Durch die von Europol koordinierten Maßnahmen zur Zerschlagung der LockBit-Bande wurden weitere Datenschutzverletzungen bekannt. Die Bande hat vorerst den Zugang zu ihrer Infrastruktur verloren. Das ist ein harter Schlag. Die langfristigen Auswirkungen sind jedoch ungewiss. Voraussichtlich werden sich die beteiligten Cyberkriminellen neu formieren.

Zu all dem kommt hinzu, dass in Europa unter der Federführung der Europäischen Union besonders strenge gesetzliche Regelungen erlassen wurden. Hierzu gehören die Datenschutz-Grundverordnung (DSGVO), die EU-Cybersicherheitsrichtline (NIS2) und der Digital Operational Resilience Act (DORA). Bei Verstößen drohen empfindliche Geldbußen mit teils drastischen Auswirkungen auf die Bilanz.

Anpassung der Unternehmenskultur und allgemeine Einstellungen

Die Einstellungen zur Cybersicherheit gehen in ganz Europa weit auseinander. Hierzu gehören die Bedeutung, die Menschen der Cybersicherheit beimessen, wie sie ihre diesbezügliche Verantwortung im beruflichen Kontext wahrnehmen und inwieweit sie sich in der Lage sehen, sich selbst zu schützen. Im Allgemeinen haben die Einwohnenden Mitteleuropas einschließlich des Vereinigten Königreichs und Irlands ein höheres Bewusstsein in Bezug auf Cybersicherheit und die Unternehmen in der Region sind in diesem Bereich weiter fortgeschritten. Dies deckt sich mit den Ergebnissen des **Reports zur Sicherheitskultur** von KnowBe4. Dieser zeigt, dass Unternehmen in West-, Ost- und Südeuropa im Vergleich zu anderen Regionen weniger vertraut mit dem Thema Cybersicherheit sind und diesem geringere Bedeutung beimessen.

Im Hinblick auf Security Awareness setzt sich die Erkenntnis durch, dass die gesamte Belegschaft einen Beitrag zur Cyberabwehr leisten muss. Unternehmen, Institutionen und Organisationen aller Größen und Branchen erkennen an, wie wichtig es ist, Mitarbeitenden die Möglichkeit an die Hand zu geben, eine aktive Rolle beim Schutz vor Bedrohungen einzunehmen. Inwiefern diese Erkenntnis einen Wandel hin zu einer Strategie hervorbringt, die der Cybersicherheit Priorität einräumt, variiert jedoch deutlich. Während die Cybersicherheit mittlerweile weniger als lästige Pflicht, sondern viel eher als strategische Initiative wahrgenommen wird, kommt die Umsetzung notwendiger Veränderungen nur langsam voran.

Laut dem **ISACA State of Cybersecurity Report 2023** erfolgt in nur 32 bis 35 % der europäischen Unternehmen, Institutionen und Organisationen mehr als einmal im Jahr eine Bewertung der Cyberrisiken. Diese Zahl ist in den letzten drei Jahren konstant geblieben und unterstreicht, wie schwierig es für Unternehmen, Institutionen und Organisationen ist, die erforderlichen Ressourcen bereitzustellen. Ursächlich hierfür sind anhaltende Budgetbeschränkungen und der Mangel an Cybersicherheitsfachkräften, der nach wie vor eine der größten Herausforderungen darstellt. Für große Fortschritte fehlt es schlicht an Personal.

Der Einfluss von KI

Die ENISA sieht in Fehlinformationen und Desinformation eine Bedrohung für die Cybersicherheit von Unternehmen, Institutionen und Organisationen. Das herausragendste Beispiel hierfür sind Angriffe auf Unternehmen, Institutionen und Organisationen, die die Verteidigung der Ukraine gegen Russlands Angriffskrieg unterstützen. Im Anschluss an Desinformationskampagnen nehmen Cyberkriminelle diese Unternehmen, Institutionen und Organisationen ins Visier. Mithilfe von KI können Bedrohungsakteure Falschmeldungen und Desinformation heute schneller verbreiten als je zuvor.

Unternehmen, Institutionen und Organisationen in Europa sind, ebenso wie in anderen Ländern, besonders daran interessiert, von der frühzeitigen Einführung von Abwehrmaßnahmen durch Tools zu profitieren, die ebenfalls KI-gestützt sind. Typischerweise agieren Großunternehmen risikobewusster. Vor dem Hintergrund der zahlreichen Risiken in Bezug auf den Datenschutz, die Sicherheit und weitere ethische Fragen sind diese daher eher zurückhaltend, was den Einsatz von KI angeht. In dieses Bild passt auch das vorübergehende Verbot von ChatGPT durch die italienische Datenschutzbehörde. Mittlerweile ist das Tool im Land wieder verfügbar. Unternehmen, Institutionen und Organisationen arbeiten weiterhin an der Einführung erforderlicher Schutzmaßnahmen im Zusammenhang mit KI-Tools und müssen ihre Mitarbeitenden entsprechend schulen.

Auch Europa ist von der weltweit wachsenden Flut an Phishing-E-Mails betroffen, die zumindest teilweise mithilfe von KI generiert werden. Die gilt vor allem für Spear-Phishing- und Pretexting-Angriffe. Daneben gibt es selbstverständlich weiterhin klassische Phishing-E-Mails, die den bekannten Mustern folgen. Die Entwicklung von KI-gestütztem Phishing steht noch am Anfang. Unternehmen, Institutionen und Organisationen müssen jedoch mit einer weiteren Professionalisierung und Automatisierung beim sogenannten Phishing-as-a-Service rechnen. Phishing wird auch in Zukunft der Hauptangriffsvektor bleiben.

Wichtige Erkenntnisse

- ✓ Europäische Unternehmen schneiden im Durchschnitt besser ab als der Rest der Welt. Hieran zeigt sich, dass Cybersicherheit zunehmende Bedeutung beigemessen wird und das allgemeine Bewusstsein für Onlinebetrug wächst. Dies lässt sich vermutlich zumindest teilweise auf die viel diskutierte strenge Regulierung und Gesetzgebung zurückführen.
- ✓ Die Ergebnisse der Unternehmen, Institutionen und Organisationen in Bezug auf nachhaltiges, langfristiges Engagement lassen noch zu wünschen übrig. Die Phishing-Anfälligkeit mittlerer und großer Unternehmen bleibt hier hinter dem weltweiten Durchschnitt zurück.
- ✓ Damit die Region ihre Position halten kann, sind vor dem Hintergrund des zunehmenden Einsatzes von KI-Tools in Unternehmen, Institutionen und Organisationen weitere regulatorische Maßnahmen in den Bereichen Datenschutz und KI erforderlich.

EUROPA	BASELINE	90 TAGE	1 JAHR
1–249	26,5 %	19,3 %	4,1 %
250–999	26,9 %	20,2 %	4,9 %
1.000 und mehr	35,6 %	20,6 %	5,9 %
Durchschnittliche PA (%) unabhängig von der Mitarbeiteranzahl	32,6 %	20,3 %	5,5 %

Kompletten Report lesen →

© 2024 KnowBe4, Inc. Alle Rechte vorbehalten. Andere genannte Produkt- und Firmennamen sind eventuell Marken und/oder eingetragene Marken ihrer jeweiligen Unternehmen.