# Cyber Training **Guide**

## Was bedroht Ihr Unternehmen?

brother at your side | in[ctrl]

in Kooperation mit KnowBe4 Human error. Conquered.

**Durch eine Datenschutzverletzung entstanden 2023 weltweit Kosten von durchschnittlich € 4,05 Millionen[1] – das entspricht einem Anstieg von 15 % innerhalb von 3 Jahren.**

**Wenn Fernarbeit an einer Datenschutzverletzung beteiligt ist, liegen die durchschnittlichen Kosten noch um €157.506[2] höher.**

**54% der Unternehmen sind der Meinung, dass ihre IT-Abteilungen nicht das nötige Know-how dafür haben, taktisch gut geplante Cyberangriffe abzuwehren.[3]**

Wenn Hacker heute versuchen würden, Ihre Cyberabwehr außer Kraft zu setzen, würde ihnen das gelingen? Wenn Sie nicht ohne zu zögern mit Nein antworten können, weil Sie fest von der Stärke der Cybersicherheit Ihres Unternehmens überzeugt sind, haben Sie ein großes Problem. Und damit sind Sie nicht allein. Einen starken Schutz aller IT-Systeme dauerhaft zu gewährleisten, ist und bleibt eine der größten Herausforderungen für IT-Entscheidungsträger (IT Decision Makers, kurz ITDMs). Da die Cyberkriminellen immer raffinierter werden und Unternehmen immer stärker von ihren digitalen Systemen abhängig sind, ist die Gefahr eines erfolgreichen Angriffs heute größer als je zuvor.

Laut unseren Studien fühlen sich viele IT-Abteilungen nicht gut genug darauf vorbereitet, diese Herausforderung zu bewältigen. Der Mangel an finanziellen Mitteln und benötigten Ressourcen sowie den richtigen Tools ist nur einer der Gründe dafür, weshalb sich viele ITDMs vor Cyberangriffen fürchten und sich fragen, ob sie ausreichend für deren Abwehr gerüstet sind.

**54 % der ITDMs sagen, dass sie zunehmend mehr Geld für den Schutz ihrer IT-Systeme ausgeben.**

**Dennoch betrachten 44 % Prozent den dauerhaften Schutz ihrer IT-Systeme weiterhin als ihre größte Herausforderung und sind der Meinung, dass die Mittel, die ihrem Unternehmen zur Verfügung stehen, wahrscheinlich nicht besonders zielführend verwendet werden.**

Wir haben Daten von Brother zusammengestellt und uns mit KnowBe4 zusammengesetzt, um Ihnen im Anschluss einige der Gefahren vorstellen zu können, die Unternehmen heute drohen. Außerdem werden Sie erfahren, wie der Aufbau einer Kultur der ständigen Weiterbildung und Wissensanhäufung in Sachen IT-Schutz und -Sicherheit Unternehmen helfen kann, sich langfristig zu schützen und auf mögliche Angriffe vorzubereiten.

Menschen sind immer die „letzte Verteidigungslinie“, wenn es um die Cybersicherheit eines Unternehmens geht. Und obwohl die IT-Abteilung natürlich die Hauptverantwortung für alle Aspekte der Cybersicherheit trägt, ist jeder Mitarbeiter zu einem gewissen Grad mitverantwortlich dafür, Datenschutzverletzungen zu verhindern. Deshalb sollte jede Cybersicherheitsstrategie eines Unternehmens gewährleisten, dass alle Beschäftigten ihre Mitverantwortung erkennen und die Schulungen und Weiterbildungen bekommen, die sie brauchen, um Cybersicherheitsbedrohungen frühzeitig zu entdecken und abzuwehren.

Menschengemachte Fehler sind an 95 % der durch Cyberangriffe verursachten Datenschutzverletzungen erheblich beteiligt.[4]

**Basil Fuchs**
Chief Information Officer
Brother International Europe

**„Die Cybersicherheit von Unternehmen wird immer stärker bedroht – nicht zuletzt, weil die Cyberkriminellen immer besser im Social Engineering werden, also darin, Menschen zu ihren Zwecken zu beeinflussen. So teilen sie einem Mitarbeiter zum Beispiel mit, dass sie ihm „aus gutem Grund“ in Kürze eine E-Mail schicken werden, damit er sie dann ohne zu zögern öffnet. Dabei machen sie sich oft die Tatsache zunutze, dass viele Mitarbeiter unter großem Druck stehen und nicht die Zeit haben, eine E-Mail auf Betrugshinweise zu untersuchen.“**

[1]IBM [2]IBM [3]Sophos [4]IIBM Cyber Security Intelligence Index Report

brother at your side | KnowBe4 Human error. Conquered.

# Die größten Bedrohungen für Unternehmen

Brother hat in seinen Studien viele ITDMs in ganz Europa befragt und von ihnen zum Beispiel wissen wollen, welchen Cybersicherheitsbedrohungen sie sich nicht ausreichend gewachsen fühlen. Bei allen Bedrohungen, die sie uns genannt haben, spielen menschengemachte Fehler eine große Rolle.

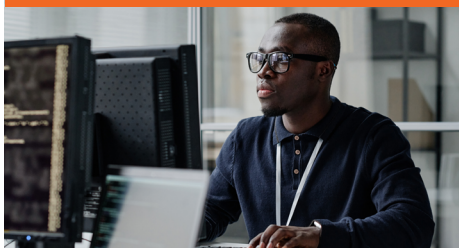
In diesem Handbuch werden wir uns mit den drei Arten von Cybersicherheitsbedrohungen beschäftigen, denen sich die befragten ITDMs am wenigsten gewachsen fühlen und Ihnen die Tools und Techniken vorstellen, die Ihr Unternehmen verwenden kann, um seine Verteidigungslinien zu stärken und die Gefahr einer Datenschutzverletzung zu minimieren.

## Zu diesen Bedrohungen gehören:

**Phishing-Angriffe**

**Malware**

**Mangelnde Netzwerksicherheit**



Eine der größten Schwierigkeiten von ITDMs besteht darin, sich und andere durch Schulungen auf die Abwehr von Cyberangriffen vorzubereiten, weil oft die Zeit oder das Geld dafür fehlt. Da Menschen bei jeder dieser Cyberbedrohungen „die letzte Verteidigungslinie“ sind, müssen sie erfahren, wie man die Angriffe frühzeitig erkennen und abwehren kann. Und da viele Unternehmen, darunter auch Brother, nicht selbst über die personellen und anderen Ressourcen verfügen, die sie für diese wichtige Wissensvermittlung brauchen, beauftragen sie andere Anbieter damit.

**Russell Johnson**
Business Partner and Global Cyber Security Lead
Brother International Europe

**„Einige Unternehmen meinen, das nötige Know-how dafür zu haben, solche Sicherheitsschulungen selbst durchzuführen und befürchten vielleicht sogar, ihre Cybersicherheit zu gefährden, wenn sie einen externen Anbieter in ihre Sicherheitspraktiken einweihen. Deshalb führen sie solche Schulungen und Weiterbildungen lieber selbst durch. Allerdings können Mitarbeiter Cyberangriffe nur dann wirklich effektiv abwehren, wenn sie wirklich die neusten Tricks der Cyberkriminellen vermittelt bekommen. Wenn nicht, bleibt ihr Unternehmen angreifbar.“**

4 IBM Cyber Security Intelligence Index Report

# Menschen spielen die größte Rolle beim nachhaltigen Schutz Ihres Unternehmens

In unseren Studien haben wir die ITDMs auch gefragt, ob die IT-Herausforderungen ihrer Meinung nach eher größer oder kleiner werden. Genau die Hälfte der Befragten war der Ansicht, dass es schwieriger wird, die IT-Systeme zu schützen. Hacker entwickeln ständig neue Tools und Techniken, um die Cyberabwehrsysteme zu durchbrechen. Das macht es Unternehmen enorm schwer, die neusten Angriffsmethoden zu erkennen und sich dagegen zu wappnen. Doch auch das zunehmende Wachstum des Internet of Things (IoT) verschafft Hackern neue Angriffsziele.

Da ein Unternehmen so viele verschiedene Angriffspunkte hat und so viele Menschen mit den unterschiedlichsten Geräten an verschiedenen Orten online arbeiten, sind die Mitarbeiter eines Unternehmens oft das schwächste Glied in der Cybersicherheitsstrategie. Denn sie sind nicht nur das größte Gut eines Unternehmens, sondern können auch zu seiner größten Schwachstelle werden – wenn sie nicht ausreichend geschult wurden, auf die Tricks von Cyberkriminellen hereinfallen oder die bewährten Praktiken der Cybersicherheit vergessen oder einfach nicht anwenden.

Für nur 29 % der ITDMs hat die Sicherheitsschulung der Benutzer höchste Priorität.

**Nur jedes neunte britische Unternehmen hat im Jahr 2022 eine Cybersicherheitsschulung für seine Nicht-IT-Mitarbeiter durchgeführt.**

**Javvad Malik**
Lead Security Awareness Advocate
KnowBe4

**„Die richtigen Technologien und Schulungen tragen gemeinsam dazu bei, das Sicherheitsbewusstsein zu erhöhen, da digitale Tools effektiv dafür verwendet werden können, Mitarbeiter umfassend weiterzubilden. Hochmoderne Technologie erleichtert den Einsatz von interaktiven Modulen, Phishing-Simulationen und Online-Ressourcen und hilft so zu gewährleisten, dass die Mitarbeiter die Grundsätze der Cybersicherheit richtig verstehen. Schulungen ergänzen diesen Ansatz, indem sie die Mitarbeiter zum kritischen Denken anregen und zum Einsatz bewährter Praktiken motivieren und ihnen so helfen, auf Angriffe richtig zu reagieren. Gemeinsam schaffen sie ein dynamisches Lernumfeld, in dem die Mitarbeiter nicht nur die Cybersicherheitsrisiken kennenlernen, sondern auch lernen, sie zu mindern. Regelmäßige Updates, Auffrischungsübungen und Feedback-Prozesse sorgen dafür, dass alle über die neusten Bedrohungen informiert sind und fördern somit eine Kultur der Wachsamkeit und Widerstandsfähigkeit im gesamten Unternehmen.“**

Hacker machen vor keinem Unternehmen halt. Allerdings sind die kleinen und mittelgroßen Unternehmen oft besonders leichte Beute für sie, weil sie nicht viel in eine defensive Cybersicherheit investieren können. Und wenn die Fernarbeit auch in diesen Unternehmen Einzug gehalten hat, können sie oft nur schwer gewährleisten, dass die Mitarbeiter auch in puncto Cybersicherheit bewährte Praktiken anwenden.

# Warum Sie eine Kultur der Cybersicherheit in Ihrem Unternehmen etablieren sollten

Regelmäßiges Cybersicherheitstraining sollte ein fester Bestandteil der beruflichen Weiterentwicklung jedes Beschäftigten sein. Doch leider hat sich das noch nicht bei allen Unternehmen herumgesprochen. Denn zum effektiven Cybersicherheitstraining gehört mehr, als nur manchmal bewusstseinsbildende Programme für Mitarbeiter durchzuführen. Die Unternehmen, die wirklich gut auf Angriffe vorbereitet sind und sie am besten abwehren können, haben die Cybersicherheit fest in ihre Kultur integriert und erreicht, dass ihre Mitarbeiter die Cyberabwehr Tag für Tag stärken.

**Russell Johnson**
Business Partner and Global Cyber Security Lead
Brother International Europe

**„Brother hat sich entschlossen, im eigenen Unternehmen eine Kultur der Cybersicherheit zu etablieren, die sich über alle Bereiche erstreckt. Diese Entscheidung beruht auf der Überzeugung, dass Cybersicherheit nichts ist, was man einfach so abhaken kann – sondern eine kollektive Aufgabe, die Bestand haben muss. Unsere Cybersicherheit ist nur so stark, wie unsere Mitarbeiter es sind und deshalb können wir uns am besten schützen, indem wir in unsere Leute investieren und ihnen die Kenntnisse und Fähigkeiten mit auf den Weg geben, die sie brauchen, um Cyberbedrohungen frühzeitig zu erkennen und abzuwehren – wann und wo immer sie auftreten.“**


# Wie Sie Ihre Mitarbeiter erfolgreich in Ihr Cybersicherheitskonzept einbinden können

Studien belegen, dass in den meisten Unternehmen die IT-Abteilung für den Aufbau einer Cybersicherheitskultur verantwortlich ist. Das kann es Menschen, die nur über ein begrenztes Wissen und begrenzte Ressourcen auf diesem Gebiet verfügen, schwer machen, sich diese Kultur zu eigen zu machen. Dabei müssen auch und gerade sie von ihrem Unternehmen geschützt werden.

**60%** der ITDMs von kleinen und mittelgroßen Unternehmen sagen, dass ihre IT-Abteilung für das **firmenweite Cybersicherheitstraining** verantwortlich ist.

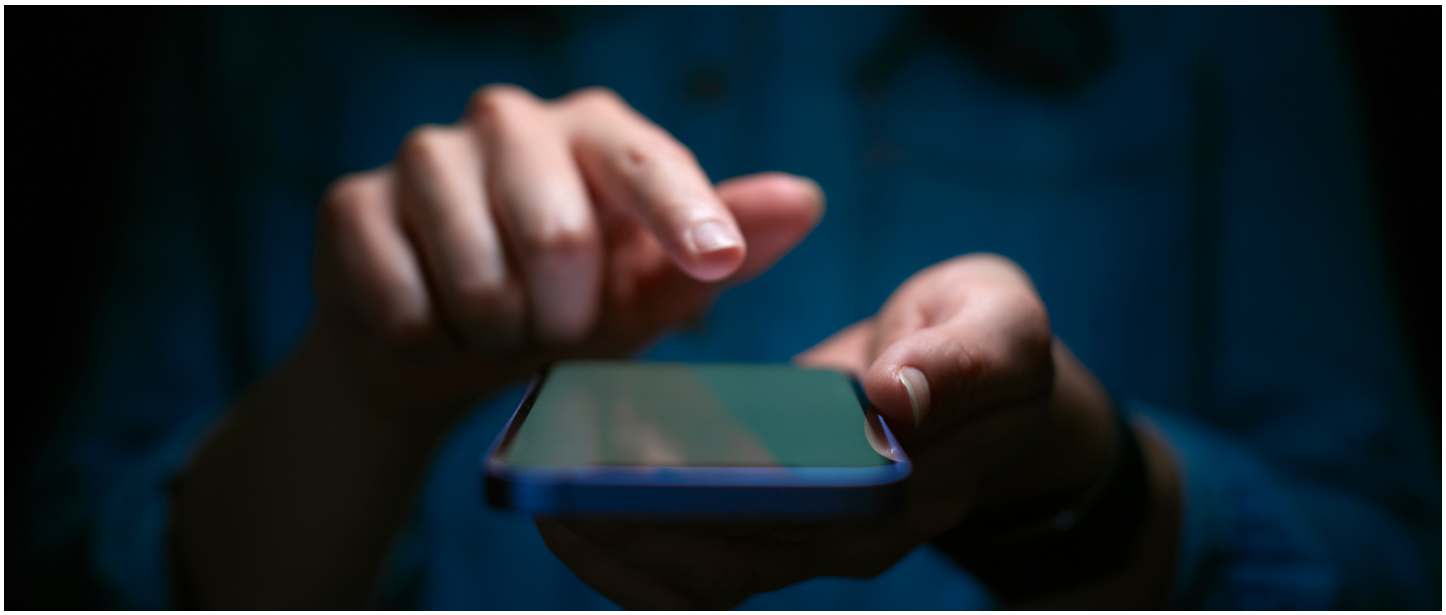
**Russell Johnson**
Business Partner and Global Cyber Security Lead
Brother International Europe

**„In den letzten Jahren haben wir das Cybersicherheitsbewusstsein bei Brother enorm erhöht, indem wir die Kenntnisse, die Fähigkeiten und die Wachsamkeit auf diesem Gebiet regelmäßig überprüft und Schulungen zur Beseitigung der erkannten Schwachstellen durchgeführt haben, die in hohem Maße auf die Bedürfnisse der Benutzer zugeschnitten waren. Außerdem veröffentlichen wir mindestens alle zwei Wochen Artikel über die neusten Entwicklungen und Trends in Sachen Cybersicherheit und veranstalten vierteljährlich sogenannte Techbars mit interaktiven Elementen und Gastreferenten, um unsere Teams auf den neusten Stand zu bringen.“**

## Für eine gute Einbindung muss ein Unternehmen:

- Inhalte und Schulungsunterlagen erstellen, die bei allen Mitarbeitern im Unternehmen gut ankommen und von ihnen verstanden werden
- sicherstellen, dass die Schulungsmaterialien und -inhalte unmissverständlich, zweckdienlich und durch gute Beispiele aus der Praxis untermauert sind
- den Lehrstoff so aufbereiten, dass alle Rezipienten etwas mit ihm anfangen können und dass er für lange Zeit im Gedächtnis haften bleibt
- verschiedene Techniken anwenden, um die Cybersicherheitsbildung fest in der Firmenkultur zu verankern – z. B. mit Newslettern, Videos, Postern und Veranstaltungen
- die Inhalte der Lehrmaterialien, wenn das Unternehmen in mehreren Ländern tätig ist, nicht nur richtig zu übersetzen, sondern auch regionenspezifisch anzupassen, damit sie die größtmögliche Wirkung haben
- gute Beziehungen zwischen IT- und Nicht-IT-Mitarbeitern im Unternehmen aufbauen und allen, die verdächtige Verhaltensweisen oder E-Mails melden, positives Feedback geben und sie als Rollenvorbilder für alle darstellen, damit sie wissen, dass ihre Beiträge gewürdigt werden
- Führungskräfte dazu zu bewegen, andere an ihren Erfahrungen teilhaben zu lassen und mit gutem Beispiel voranzugehen

brother at your side | KnowBe4 Human error. Conquered.



# Phishing Angriffe

Beim Phishing geben sich Cyberkriminelle als vertrauenswürdige Personen oder Unternehmen aus, wenn sie – in der Regel per E-Mail, per Telefon oder in den sozialen Netzwerken – versuchen, sensible Informationen wie Passwörter oder Kreditkartendaten zu erlangen. So verbreiten sie auch Malware (Schadsoftware). Phishing gehört zu den von Cyberkriminellen am häufigsten verwendeten Formen des Social Engineerings.

**74 % aller Datenschutzverletzungen führen auf menschliches Verhalten zurück.[5]**

Da Unternehmen in der Regel stark von ihren digitalen Kommunikationskanälen abhängig sind, sind diese der perfekte Angriffspunkt für Cyberkriminelle. Und die Fähigkeit, einen Phishing-Angriff erfolgreich abzuwehren, steht und fällt mit der Fähigkeit der Mitarbeiter, ihn rechtzeitig zu erkennen und abzuwehren.

Leider bedienen sich Online-Betrüger oft sehr bekannter Marken wie Microsoft, Amazon, DocuSign und Google, um die Anwender aufs Glatteis zu führen. So wurden zum Beispiel allein 2022 mehr als 30 Millionen Phishing-Nachrichten versandt, die scheinbar von Microsoft kamen oder auf Microsoft-Produkte Bezug nahmen.[6]

28 % der ITDMs kleiner und mittelgroßer Unternehmen sagen, dass Phishing-Angriffe die Art von Cybersicherheitsbedrohungen sind, der sie sich am wenigsten gewachsen fühlen.

**96 % aller Unternehmen in Großbritannien – der höchste Wert in Europa – sind von Phishing-Angriffen betroffen, gefolgt von 94 % der Unternehmen in Spanien, 85 % in Frankreich und 79 % in Italien.[7]**

[5]Verizon's 2023 Data Breach Investigation Report [6]Forbes, 2023 [7]IT Governance

brother at your side | KnowBe4 Human error. Conquered.

# Wie können sich ITDMs vor Phishing-Angriffen schützen?

Da die Cyberkriminellen bei Phishing-Angriffen menschliche Schwächen zu ihrem Vorteil nutzen, kann sich ein Unternehmen nur dadurch vor ihnen schützen, dass es seinen Mitarbeitern durch Schulungen vermittelt, woran man solche Angriffe erkennt und wie man sie abwehrt. Da sich auch die Cyberkriminellen weiterentwickeln und ihre Phishing-Methoden ständig verfeinern, sollten Schulungen und Weiterbildungen zu den neusten Phishing-Techniken nicht als einmalige Angelegenheit, sondern als regelmäßig zu nutzende Gelegenheit betrachtet werden, alle Mitarbeiter mit den Gefahren vertraut zu machen – egal, welche Rolle sie im Unternehmen spielen.

Zur zusätzlichen Sicherheit sollten ITDMs auch spezielle Softwareprogramme zum Schutz vor Phishing implementieren. Sie analysieren verschiedene Elemente einer Nachricht und kennzeichnen die Nachricht gegebenenfalls als verdächtig oder blockieren sie, bevor sie das Postfach oder den Browser des Benutzers erreicht.

# Warnsignale für Phishing

Ziel des Phishings ist es, Menschen dazu zu bewegen, auf etwas zu klicken und/oder etwas zu teilen, das sie lieber nicht hätten anklicken oder teilen sollten. Und die einzige Möglichkeit, solche Fehler zu verhindern, besteht darin, sie regelmäßig zu schulen und an die Warnsignale zu erinnern, die darauf hindeuten, dass eine Nachricht zu Phishing-Zwecken versendet wurde.

### Warnsignale, auf die man achten sollte:

- Die Nachricht stammt von einer Domain, die nicht die des Unternehmens ist, von der sie vorgibt zu kommen
- Schwer nachvollziehbare und kryptische URLs
- Rechtschreib- und Grammatikfehler
- Gebrauch unüblicher Schriftarten, vor allem dann, wenn sich die Schriftart mitten im Wort zu ändern scheint
- Es wird der Anschein von Dringlichkeit erweckt, z. B. durch Formulierungen wie „Dieser Link ist nur 48 Stunden lang gültig“ oder „Bestätigen Sie unverzüglich Ihre Identität“
- Verwendung einer ungewöhnlichen Anrede wie etwa „Hallo, meine Liebe“

Wie gut sind Ihre Teams darin, eine Phishing-E-Mail oder -Nachricht als solche zu erkennen? Früher konnte man solche E-Mails ziemlich leicht daran erkennen, dass sie voll von Rechtschreib- und Grammatikfehlern waren. Leider haben die Kriminellen diese Hürde durch den Einsatz generativer KI inzwischen weitestgehend genommen, was es zunehmend schwerer macht, Phishing zu entdecken. Eine Möglichkeit herauszufinden, wie gut Teams auf solche Angriffe vorbereitet sind, besteht darin, die Phish-prone™ Percentage des Unternehmens durch Phishing-Tests zu ermitteln.

Deshalb sollten solche regelmäßigen Tests fest im Cybersicherheitsplan jedes Unternehmens verankert sein.

**Russell Johnson**
Business Partner and Global Cyber Security Lead
Brother International Europe

**„Wir haben eine ganze Reihe von Maßnahmen ergriffen, um die Gefahr eines erfolgreichen Phishing-Angriffs zu minimieren. Diese Phishing-Simulationen haben wir im Rahmen unserer Cyberstrategie unter anderem verwendet:**

- **Nachrichten, die von der Personalabteilung zu kommen scheinen, zu Themen wie Krankschreibung, Jahresurlaub und der Unterzeichnung neuer Richtlinien**
- **Nachrichten, die von Vorgesetzten zu kommen scheinen, in denen die Mitarbeiter z. B. aufgefordert werden, Dokumente unverzüglich zu öffnen/lesen/unterschreiben**
- **Nachrichten, die vom System zu kommen scheinen, z. B. mit Links zur Unterzeichnung eines Google Docs oder zum Zugang zu einem SharePoint.“**

# Phish-prone™ Percentage:
# Was ist das und warum ist das wichtig?

Die „Phish-prone™ Percentage“ Ihres Unternehmens besagt, wie viele Ihrer Mitarbeiter dafür anfällig sind, auf Phishing-Links zu klicken oder auf eine Phishing-Nachricht falsch zur reagieren. Eine solche Reaktion könnte beispielsweise darin bestehen, Daten in ein Online-Formular auf einer Fake-Webseite einzugeben, einen E-Mail-Anhang zu öffnen oder auf eine Nachricht zu antworten.

Die Phish-prone™ Percentage wird dadurch berechnet, dass die Anzahl der Mitarbeiter, die einen Phishing-Test nicht bestanden haben, durch die Anzahl aller geprüften Mitarbeiter geteilt wird. Das Ergebnis wird mit 100 multipliziert, um den Prozentsatz zu erhalten. So liegt die Phish-prone™ Percentage zum Beispiel bei 20 %, wenn 20 der 100 geprüften Mitarbeiter eines Unternehmens bei einem Phishing-Test auf eine Phishing-Mail zum Thema Druckersicherheit geklickt haben.


**„Machen Sie sich keine allzu großen Sorgen, wenn Ihre Phish-prone™-Quote anfangs höher ist als gedacht. Das ist ganz normal, wenn Sie noch nie einen Phishing-Test durchgeführt haben. Wir von Brother konnten unsere Phish-prone™-Quote innerhalb ziemlich kurzer Zeit erheblich senken – mithilfe einer ganzen Reihe von Schulungs-Tools und simulierten Phishing-Tests. Inzwischen haben wir sogar unsere Branchen-Benchmark von 6 % geknackt, was einmal mehr belegt, wie wirkungsvoll ständiges Testen und Schulungen sein können.“**

# Phishing-Tests und Schulungen in der Praxis

Phishing-Tests gehören zu den effektivsten Möglichkeiten, herauszufinden, wie gut Ihre Teams auf einen Phishing-Angriff vorbereitet sind und die Phish-prone™-Quote Ihres Unternehmens zu verringern.[8] Außerdem sind sie ziemlich leicht durchzuführen. Sie müssen Ihren Mitarbeitern nur eine simulierte Phishing-Nachricht schicken (oder von einem darauf spezialisierten Anbieter schicken lassen), die sie dazu zu verleiten versucht, sensible Informationen preiszugeben. Am Ende des Tests können Sie Ihre Phish-prone™ Percentage berechnen und (anhand eines Benchmark-Werts) mit dem Wert anderer Unternehmen in Ihrer Branche vergleichen.

**Javvad Malik**
Lead Security Awareness Advocate
KnowBe4

**„Laut KnowBe4s Phishing by Industry Benchmarking Report von 2023 fallen 33,2 % aller ungeschulten Benutzer bei einem Phishing-Test durch. Durch konsequente Sicherheitsschulungen und Etablierung einer Kultur der Cybersicherheit können Unternehmen ihre Quote jedoch auf einen Wert senken, der unter der Branchen-Benchmark von 5,9 % liegt.“**

**Russell Johnson**
Business Partner and Global Cyber Security Lead
Brother International Europe

**„Wir von Brother haben unsere Phish-prone™-Quote in den letzten Jahren erheblich senken können. Wie haben wir das geschafft? Im März 2022 haben wir einen Baseline-Phishing-Test durchgeführt, der eine Phish-prone™ Percentage (PPP) von 11,5 % ergab. Danach haben wir umfangreiche Tests und Übungen zum Thema Cybersicherheit durchgeführt, um die größten Schwachstellen in unserem Unternehmen zu erkennen. Anhand der dabei gewonnenen Erkenntnisse konnten wir Schulungen entwickeln, die uns halfen, diese Schwachstellen weitestgehend zu beseitigen. Dabei haben wir mehr als 30.000 Phishing-Mails versandt, allein 17.000 in den letzten 12 Monaten. Inzwischen beträgt unsere PPP nur noch 5,2 % und wir haben uns vorgenommen, auf unter 2 % zu kommen.“**

## Die Branchen-Benchmark für Phishing wird in drei Phasen ermittelt:

**1. Phase:** Eine simulierte Phishing-Mail wird an alle Benutzer geschickt, die noch nicht zu diesem Thema geschult wurden. Der prozentuale Anteil der Benutzer, die auf diese Phishing-E-Mail hereinfallen, ist der Grundlinien-Anteil. Im weltweiten Durchschnitt fallen 33,2 % der Mitarbeiter auf eine solche Phishing-E-Mail herein.

**2. Phase:** Die Benutzer absolvieren eine entsprechende Schulung und werden 90 Tage nach dem ersten Phishing-Test einem zweiten Test unterzogen.

**3. Phase:** Der Test wird nach 12 Monaten wiederholt.

Bei einem Test mit 32,1 Millionen Phishing-Mails, die an 12,5 Millionen Benutzer geschickt wurden, war der Anteil der Benutzer, die auf Phishing-Mails hereingefallen sind, nach 90 Tagen Schulung weltweit von 33,2 % auf 18,5 % gesunken. Nach 12 Monaten waren es sogar nur noch 5,4 %.

Diese Prozentwerte variieren jedoch je nach Branche, Standort und Größe des Unternehmens.

## 91 % der erfolgreichen Cyberangriffe mit anschließenden Datenschutzverletzungen begannen mit einem Spear-Phishing-Angriff.[9]

### Was ist Spear-Phishing?

Spear-Phishing ist eine Art des Phishings, bei dem Cyberkriminelle versuchen, bestimmte Personen oder Unternehmen (meist) mit betrügerischen E-Mails zu „ködern“. Dadurch versuchen sie an sensible Informationen wie Zugangsdaten zu gelangen oder das Gerät ihres Opfers mit Schadsoftware zu infizieren.

[8]KnowBe4 [9]KnowBe4


# Malware

Eine der größten Ängste der von uns befragten ITDMs besteht darin, dass „Malware“, also Schadsoftware, in ihr IT-System eindringt.

**34 % der ITDMs kleiner und mittelgroßer Unternehmen sagen, dass Malware / Ransomware die Arten von Cybersicherheits-bedrohungen sind, denen sie sich am wenigsten gewachsen fühlen.[10]**

### Was ist Malware?

Malware ist Software, die eigens dafür konzipiert wurde, ein Computersystem zu stören, zu beschädigen oder sich unbefugt Zugang zu ihm zu verschaffen. Wie wir alle wissen, werden Phishing-Nachrichten oft dazu verwendet, Malware auf Systeme zu übertragen – indem Benutzer dazu verleitet werden, auf einen Link in einer solchen Nachricht zu klicken oder einen Anhang herunterzuladen.

### Es gibt aber noch andere Möglichkeiten, sich Malware „einzufangen“:

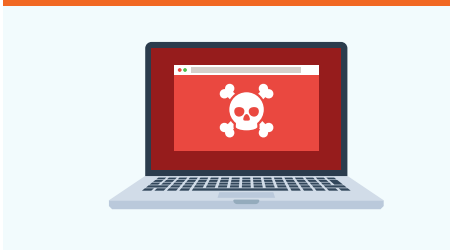
- Automatische Downloads von kompromittierten Websites
- Installation von infizierter Software auf einem Gerät
- Übertragung durch Medienträger wie USB-Laufwerke und externe Festplatten
- Verwendung veralteter Software, die Sicherheitslücken hat

Allein im **Dezember 2023** wurden nachweislich mehr als **100.884.532** Daten-sätze[11] in Europa geknackt.

[10]2023 Brother X Savanta ITDM priority survey [11]IT Governance

# Die gefährlichsten Arten von Malware im Überblick

## Trojaner



Ein Trojaner ist ein Virus, der so einiges kann: Ihre Dateien schädigen, Ihre Daten verändern, Ihre Aktivitäten überwachen, sensible Informationen von Ihrem Gerät stehlen, Datenströme im Internet umlenken oder sogar Zugangspunkte zu Ihrem System schaffen – ohne dass Sie es überhaupt merken.

## Ransomware


Ransomware ist eine Art Schadsoftware, die dazu verwendet wird, Ihnen den Zugriff auf Ihr Gerät und die darauf befindlichen Daten solange zu verwehren, bis Sie dem Angreifer ein „Lösegeld“ („ransom“) bezahlen. Dabei werden Ihre Dateien meist so verschlüsselt, dass Sie sie nicht mehr sehen oder verwenden können.

## Würmer

Würmer sind zwar auch eine Form des Trojaners, aber ihre Hauptaufgabe besteht darin, sich zu „vermehren“ und andere Geräte zu infizieren. Dabei bleiben sie auch in den Systemen aktiv, die ursprünglich infiziert wurden.

# Wie können sich ITDMs vor Ransomware-Angriffen schützen?

## Im Januar 2023 fiel der nationale Postdienst Großbritanniens, Royal Mail, einem der gefährlichsten Ransomwares der Welt zum Opfer: LockBit. Die Erpresser verlangten ein Lösegeld von 80 Millionen US-Dollar.[12]

Viele Ransomware-Angriffe werden erst durch erfolgreiches Phishing ermöglicht, bei dem Menschen dazu verleitet werden, auf Links zu Seiten zu klicken, über die Cyberkriminelle schädliche Software auf das Gerät des Betroffenen übertragen. Deshalb können Sie Ihr Unternehmen am besten davor schützen, indem Sie Ihren Mitarbeitern beibringen, wie man Phishing-Angriffe erkennt und erfolgreich abwehrt. Ein vertrauenswürdiger Partner, der sich mit solchen Dingen auskennt, wird Ihnen genau sagen können, wie gut Ihre Teams schon darin sind, solche Angriffe zu erkennen.

**Diese weiteren Maßnahmen können Sie zum Schutz Ihres Unternehmens vor Ransomware-Angriffen ergreifen:**

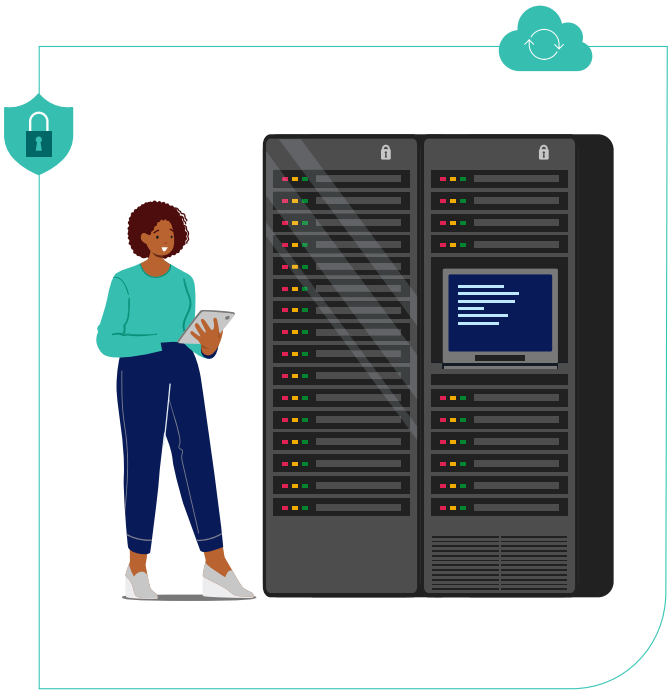
- Ihre Software auf dem neusten Stand halten
- Zwei-Faktoren-Authentifizierung verwenden, vor allem für Fernarbeiter
- Von den Benutzern verlangen, ihre Passwörter regelmäßig zu wechseln
- Sicherheits-Hardware und -Software wie Firewalls, Antivirenprogramme und Spam-und-Phishing-Filter für E-Mails verwenden
- Regelmäßig Datensicherungen (Backups) vornehmen und alles in einer separaten Netzwerkumgebung speichern.

Eine weitere Möglichkeit besteht in der Implementierung von SOAR (Security Orchestration Automation and Response). Es wurde für die Verhinderung und Abwehr von Phishing-Angriffen konzipiert und kann Ihre durchschnittliche Reaktionszeit (Mean Time To Respond, kurz MTTR) auf solche Angriffe verringern und Phishing-Nachrichten abfangen, bevor sie ins Postfach Ihrer Mitarbeiter gelangen.[13] Dieser proaktive Umgang mit Phishing wird durch weitere nützliche Funktionen unterstützt, wie etwa:

- Automatisierte E-Mail-Antworten, die es der IT-Abteilung ermöglichen, im Ernstfall schnell mit den Mitarbeitern zu kommunizieren, wodurch sich die Ausfallzeit verkürzt
- Mustererkennung, die Ihre Incident Response Teams in die Lage versetzt, weitreichende Angriffe schnell zu entdecken
- Entwicklung von Übungen und Modellen durch Simulation von tatsächlich erfolgten Angriffen, um die Fähigkeiten und Erfahrungen Ihrer Mitarbeiter zu erweitern.

**Javvad Malik**
Lead Security Awareness Advocate
KnowBe4

**„Um sich auf Ransomware-Angriffe vorzubereiten, können Unternehmen Tools wie RanSim verwenden, die ihnen ein genaues Bild davon vermitteln, wie gut (oder schlecht) sie schon (oder noch) auf einen Angriff vorbereitet sind. RanSim simuliert 24 verschiedene Szenarien einer Ransomware-Infektion und ein Szenario einer Cryptomining-Infektion, um herauszufinden, ob eine Workstation angreifbar ist.“**



[12]bbc.co.uk [13]KnowBe4

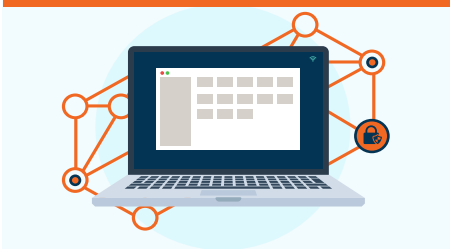
# Netzwersicherheit

Etwas, das viele Unternehmen leider immer noch nicht ernst genug nehmen, ist die Netzwerksicherheit. Dabei kann mangelnde Netzwerksicherheit verheerende Folgen haben. Dennoch wird sie oft vernachlässigt. Die Netzwerksicherheit bezieht sich auf die Prozesse und Softwareprodukte, die Sie verwenden, um Ihre Computer, Drucker, Daten und Ihr ganzes Netzwerk zu schützen. Sie wird in der Regel in drei Bereiche unterteilt:

**Physisch**

Sicherheitsvorkehrungen, die dazu dienen, den unbefugten Zugriff auf physische Netzwerke wie Drucker, Router und Festplatten (Endpunkte) zu verhindern.

**Technisch**



Sicherheitsvorkehrungen, durch die die Daten geschützt werden, die ins Netzwerk hineingehen, aus ihm herausgehen und in ihm gespeichert werden.

**Administrativ**


Sicherheitsvorkehrungen zur Beeinflussung des Benutzerverhaltens, zum Beispiel durch das Erteilen von Zugriffsrechten und dem Festlegen von Authentifizierungsschritten.

Der am wenigsten sichere Teil jedes Netzwerks ist der Endpunkt. Und an dieser Stelle kommen wieder die Benutzer ins Spiel. Das hybride Arbeiten stellt Unternehmen vor neue Herausforderungen, auch und vor allem im Hinblick auf ihre Netzwerksicherheit. Denn oft können Mitarbeiter, die von unterwegs aus arbeiten, über öffentliche Netzwerke auf Firmenserver zugreifen. Diese Netzwerke bieten aber einen viel geringeren Schutz als das Netzwerk des Unternehmens. Sie haben eine größere Angriffsfläche mit vielen Zugangspunkten, die Cyberkriminelle für ihre Zwecke nutzen können. Außerdem erschweren sie es den IT-Teams, Angriffe zu erkennen und auf sie zu reagieren.

**Basil Fuchs**
Chief Information Officer
Brother International Europe

**„In der digitalen und flexiblen Arbeitswelt von heute ist der Schutz von Netzwerken für den Schutz sensibler Daten unerlässlich. Die Anwendung des Zero-Trust-Modells, das davon ausgeht, dass man niemandem auf den ersten Blick vertrauen kann, gewährleistet, dass alle Benutzer und Geräte verifiziert werden, bevor sie Zugang zu einem Netzwerk bekommen. Indem es die Zugangs- und Zugriffsmöglichkeiten auf das Nötigste beschränkt, verringert es die Gefahr der unbefugten lateralen Bewegung.“**

Der Netzwerkzugang nach dem Zero-Trust-Prinzip ist ein sehr effektives Sicherheitsmodell, das gewährleistet, dass die Benutzer nur die Zugangsrechte und Genehmigungen bekommen, die sie wirklich brauchen, um ihre Aufgaben zu erfüllen. Dieser Ansatz unterscheidet sich grundlegend von dem der Standard-VPNs, die allen Benutzern Zugang zum ganzen Netzwerk gewähren. Der Vorteil eines Zero-Trust-Ansatzes besteht darin, dass Hacker, wenn nur ein Benutzer kompromittiert ist, nur auf die Daten zugreifen können, auf die auch er Zugriff hat und nicht auf das ganze Netzwerk.

**So können Sie Ihre Netzwerksicherheit schnell erhöhen:**

1. SSL-Zertifikate verwenden
2. Von Ihren Mitarbeitern, die remote arbeiten, verlangen, dass sie ihr Heim-WLAN mit WPA2 verschlüsseln
3. Den Namen und das Passwort Ihres Routers ändern, um Ihre Identität zu verschleiern
4. WPS auf Routern deaktivieren
5. Alle Benutzer durch Nachrichten daran erinnern, regelmäßig Datensicherungen (Backups) von ihren Geräten wie z. B. Druckern und Scannern vorzunehmen und verfügbare Updates immer gleich zu installieren.

# Tipps für eine hohe Netzwerksicherheit

Die Netzwerksicherheit umfasst viele verschiedene Aspekte, die alle gleich wichtig sind. Das gilt vor allem im Zeitalter des hybriden Arbeitens und Fernarbeitens, da die ITDMs die Benutzer nicht einfach an ihrem Arbeitsplatz besuchen können, um ihre technischen Gegebenheiten zu überprüfen. Vor diesem Hintergrund haben wir für Sie unsere besten Tipps zusammengestellt, wie Sie trotzdem alles im Griff behalten können.

## SSL-Zertifikate verwenden

Ein SSL-(Secure-Sockets-Layer)-Zertifikat und HTTP zu verwenden, ist unerlässlich, wenn Sie Verkaufstätigkeiten über Ihr Netzwerk laufen lassen. Ein SSL-Zertifikat gewährleistet, dass keine Daten, die zwischen Ihren Servern und Clients ausgetauscht werden, von einem Dritten gestohlen werden können. Dabei bestätigt das Zertifikat die Identität des Servers und richtet einen verschlüsselten Kommunikationskanal ein, um abgesicherte Einkäufe zu ermöglichen.

## Router-Firmware auf dem neusten Stand halten

Das ist für Mitarbeiter, die remote arbeiten, besonders wichtig, da die Router-Firmware auf ihren Geräten vorinstalliert ist. Router-Firmware sollte mindestens einmal im Jahr aktualisiert werden, um die beste Verteidigung gegen Cyberbedrohungen leisten zu können.

## WPA2 verwenden

Wi-Fi Protected Access2, kurz WPA2, ist einer der stärksten und komplexesten Sicherheitsalgorithmen, die es derzeit zum Schutz Ihres Wi-Fi-Netzes gibt.

## Ein VPN implementieren

Virtual Private Networks, kurz VPNs, sind für Fernarbeiter unerlässlich, weil sie das Risiko verringern, dass Daten auf ihrem Weg zwischen Netzwerken abgefangen werden. VPNs helfen zu verhindern, dass Menschen bei der Fernarbeit aus Versehen angreifbare öffentliche Netzwerke verwenden.

## Firewalls verstärken

Auch wenn es selbstverständlich erscheint, wollen wir es an dieser Stelle noch einmal betonen: Starke Firewalls sind nach wie vor eine der effektivsten Cybersicherheitswaffen in Ihrem Arsenal. Deshalb sollten Sie sich sowohl eine interne als auch eine externe Firewall zulegen, nach Möglichkeit hardware- und softwarebasierte Firewalls aufeinanderschichten und sicherstellen, dass sie regelmäßig aktualisiert werden, um den größtmöglichen Schutz zu gewähren.

## Filesharing deaktivieren

Auch wenn die Möglichkeit, gemeinsam an Dokumenten zu arbeiten, für Fernarbeiter enorm wichtig ist, bietet das Filesharing Hackern oft die perfekte Gelegenheit, sensible Informationen abzurufen oder Systeme zu schädigen. Diese Gefahr können Sie minimieren, indem Sie cloudbasierte oder passwortgeschützte Systeme implementieren, die die Zusammenarbeit ermöglichen, Ihr Netzwerk angreifbar zu machen.

## Endpunkte schützen

Drucker und andere mobile Geräte wie Scanner und portable Festplatten werden oft übersehen, wenn es um die Netzwerksicherheit geht. Stellen Sie sicher, dass die Software dieser Maschinen und Geräte stets auf dem neusten Stand ist, und beschäftigen Sie sich auch einmal mit Secure Print – einer Funktion, die es dem Drucker erlaubt, den Ausdruck solange aufzuschieben, bis er vom Nutzer am Drucker freigegeben wurde.

# Druckersicherheit

Ein Aspekt des endpunktbezogenen Risikos, der leider auch oft übersehen wird, ist die Druckersicherheit. Auch wenn Drucker auf den ersten Blick relativ sicher zu sein scheinen, können sie doch von Hackern als willkommene Hintertür zu Ihrem Netzwerk verwendet werden. Und diese Tür wird öfter genutzt, als Sie vielleicht denken.

## An mehr als einem Zehntel aller Sicherheitsverletzungen in Unternehmen ist ein Drucker beteiligt.[14]

Das liegt daran, dass die meisten modernen Drucker ans Internet angeschlossen sind und diese Netzwerkverbindung nun einmal nach beiden Seiten besteht: von Ihrem Gerät zu Ihrem Drucker, aber eben auch von Ihrem Drucker zu Ihrem Gerät. Und während Benutzer sensible Daten bedenkenlos ausdrucken, nutzen clevere Hacker diese bilaterale Verbindung, um sie abzufangen, wenn Ihr Drucker nicht ebenso gut geschützt ist wie Ihr Computer.

Laut Studien von Brother beschäftigen sich 95 % aller Unternehmen damit, die Netzwerksicherheit für ihre hybrid arbeitenden Mitarbeiter zu gewährleisten.

**Security by Brother** ist unsere lösungsbasierte Herangehensweise an die Endpunkt-Sicherheit, die den Druck in Unternehmen wirklich sicher macht. Wir implementieren einen Schutz auf drei Ebenen – Netzwerk-, Geräte- und Dokumentenebene –, um sicherzustellen, dass wirklich nur die Menschen Informationen zu sehen bekommen, für die sie bestimmt sind.

[14]Quocirca.

# Und zu guter Letzt ...

... wollen wir Ihnen noch verraten, dass die Risikominderung nach dem Prinzip des „Must-have“ und „Nice-to-have“ unserer Ansicht nach die beste Möglichkeit ist, zu gewährleisten, dass die ITDMs zur Verfügung stehenden Mittel effektiv eingesetzt werden. Dabei gibt es:

**Unerlässliche Aspekte:** Vorkehrungen, die Sie für Ihren nachhaltigen Erfolg unbedingt brauchen, wie etwa eine konfigurierte Firewall, Antivirenprogramme, VPNs, grundlegende Cybersicherheitsschulungen und nicht zuletzt Passwort-Manager.

**Wünschenswerte Aspekte:** Vorkehrungen, die man zwar haben sollte, weil es vorteilhaft wäre, aber nicht unbedingt haben muss, um eine grundlegende Cybersicherheit zu gewährleisten, wie etwa multifaktorielle Authentifizierung und regelmäßig stattfindende Schulungen.

Mit dieser Methode können Sie, nachdem Sie die größten Risiken für Ihr Unternehmen erkannt haben, feststellen, welche Sicherheitsvorkehrungen Sie unbedingt treffen müssen, um Ihr Unternehmen nachhaltig ,zu schützen und welche Sie treffen sollten, wenn Sie das Geld dafür hätten. Übrigens liefert diese Methode ITDMs auch die perfekten Argumente bei der Beantragung weiterer Mittel für die Gefahrenabwehr.

Last but not least sollte die Cybersicherheit nichts sein, was Sie bei routinemäßigen Schulungen Ihrer Mitarbeiter einfach so abhaken. Sie sollte zum festen Bestandteil Ihrer Firmenkultur und Ihrer täglichen Arbeitsabläufe werden, damit Cyberbedrohungen am Ende genauso schnell erkannt werden wie etwa Gefahrenlagen im Straßenverkehr – denn nur so können Sie Ihre Systeme und Daten wirklich umfassend schützen.

brother at your side | KnowBe4 Human error. Conquered.

# Was bedroht Ihr Unternehmen?

**Kontaktieren Sie noch heute Ihren Sicherheitsexperten von Brother.**

brother at your side | in[ctrl]

In Kooperation mit KnowBe4 Human error. Conquered.