



# CYBER SECURITY AWARENESS TRENDS

Aktuelle Bedrohungen und Gesetze  
inkl. 5 Maßnahmen-Plan für Ihr Unternehmen

**skillsforwork**

Liebe Leserin, lieber Leser,

in meiner täglichen Arbeit dreht sich alles um Informationssicherheit und Datenschutz. Sie prägen nicht nur meine berufliche Laufbahn, sondern stellen auch eine persönliche Leidenschaft dar.

In diesem E-Book erhalten Sie Kennzahlen und Erkenntnisse aus dem letzten Jahr:

- Warum waren Cyberkriminelle so erfolgreich?
- Welche neuen Risiken erwarten uns?
- Welche Gesetze kommen auf Sie zu?
- Wie bereiten Sie sich vor – ohne hohe Investitionen und Ausbau Ihrer IT-Abteilung?

Die Landschaft der Informationssicherheit ist nicht statisch, sondern ändert sich kontinuierlich durch neue Techniken, Gesetze und Trends. Diese Entwicklungen rechtzeitig zu erkennen und entsprechend zu handeln, ist wichtig, um Ihr Unternehmen vor steigenden Angriffen zu schützen und den aktuellen Informationssicherheits-Standards zu entsprechen.

In diesem E-Book habe ich mein Wissen und meine Erfahrungen gebündelt, um Ihnen einen umfassenden Überblick über die wichtigsten Trends zu geben.

Beste Grüße,  
Thomas Floß

## Inhalt

---

Diese Angriffsform ist die größte Bedrohung .....	4
Völlig unerwartet: diese Zielgruppen stehen besonders im Visier der Hacker.....	4
Phishing-E-Mails als Hauptgefahr für Ransomware-Angriffe .....	5
Künstliche Intelligenz: Die wachsende Gefahr in der Cyberwelt .....	6
Angriffsziele: Diese „Schwachstellen“ sind für Hacker besonders attraktiv .....	7
Zwang zur Datensicherheit: Diese Gesetzesprojekte kommen auf Sie zu .....	9
Welche 5 Maßnahmen wirklich was bringen.....	11
So bauen Sie eine wirksame Awareness-Kampagne auf.....	13

## Diese Angriffsform ist die größte Bedrohung

---

Ransomware ist eine Art von Schadsoftware, die den Zugriff auf Daten oder Systeme zu sperren oder zu verschlüsseln. Nachdem die Daten oder Systeme erfolgreich verschlüsselt wurden, fordern die Kriminellen ein Lösegeld (engl. "ransom") von den Opfern, um den Zugriff auf ihre Daten wiederherzustellen.

Ransomware verbreitet sich oft durch Phishing-E-Mails, infizierte Software-Downloads oder die Ausnutzung von Sicherheitslücken in Netzwerken und Systemen. Einmal aktiviert, kann sie nicht nur einzelne Computer, sondern auch ganze Netzwerke infizieren, was zu erheblichen Störungen und Datenverlusten führen kann.

Ransomware war in den letzten Jahren die größte Bedrohung für Unternehmen. Laut Statista-Umfrage entstanden im Jahr 2023 16,1 Milliarden Euro Kosten durch gestohlene oder verschlüsselte Daten.<sup>1</sup> Experten gehen davon aus, dass diese Kosten stark ansteigen.

Ransomware ist damit auch aktuell die Angriffs-Technik, die den höchsten Schaden verursacht.

## Völlig unerwartet: diese Zielgruppen stehen besonders im Visier der Hacker

---

Lange glaubte man, dass nur große Unternehmen aufgrund ihres Umsatzes ins Visier der Angreifer geraten. Doch das ist schon lange nicht mehr der Fall. Insbesondere kleine Unternehmen sind interessant für die Angreifer, da diese oft über mangelnde Informationssicherheitsrichtlinien- und Maßnahmen verfügen und damit ein leichtes Ziel sind.

Ein Beispiel: Ein Angreifer tarnt sich als Handwerker, um unbefugten Zugang zu Firmenräumlichkeiten zu erhalten. Der freundliche Mitarbeiter, der die Tür öffnet, ahnt nicht, dass er gerade eine erhebliche Sicherheitslücke schafft. Diese Methode nutzt menschliche Hilfsbereitschaft aus, um physische

---

<sup>1</sup> Statista, Schäden durch Datendiebstahl, Industriespionage oder Sabotage in Deutschland im Jahr 2023, <https://de.statista.com/statistik/daten/studie/444719/umfrage/schaeden-durch-computerkriminalitaet-in-deutschen-unternehmen/>

Sicherheitsmaßnahmen zu umgehen. Einmal im Gebäude, könnte der vermeintliche Handwerker versuchen, Schadsoftware zu installieren, sensible Informationen zu stehlen oder Zugang zu kritischen Systemen zu erlangen. Die Risiken sind vielfältig: von Datenverlust über finanzielle Schäden bis hin zu Betriebsunterbrechungen.

Auch die kommunale Verwaltung ist ein primäres Angriffsziel. Im letzten Jahr wurden viele Kommunen in Nordrhein-Westfalen angegriffen. Die Services waren wochenlang nicht verfügbar. Der Schaden war immens. Anträge oder andere Dienstleitungen der Kommunen konnten wochenlang nicht bedient werden. Der Grund: Ein Ransomware-Angriff.

## Phishing-E-Mails als Hauptgefahr für Ransomware-Angriffe

66% der Spammails waren Cyberangriffe, davon 34% Erpressungsmails und 32% Betrugsmails.<sup>2</sup>

Insbesondere im Alltagsstress klicken Mitarbeiterinnen und Mitarbeiter auf eine gefälschte E-Mail, geben vertrauliche Daten ein oder laden eine Schadsoftware runter. Durchschnittlich wurden rund 775 Mails mit Schadprogramm und jeden Tag in deutschen Regierungsnetzen abgefangen. 370 Webseiten wurden im Durchschnitt an jedem Tag des Berichtszeitraum für den Zugriff auf Regierungsnetzen gesperrt.<sup>3</sup>

**Es ist also nicht mehr die Frage, ob es Sie treffen wird, sondern nur noch, wann es Sie treffen wird.**

Die Experten sind sich sicher: Die größte Bedrohung bleibt das Thema Ransomware, Datendiebstahl und Erpressung.

In meiner täglichen Arbeit überprüfen wir Sicherheitsmaßnahmen von Kunden und identifizieren, wie viele Informationen im Ernstfall gesammelt werden können. Bei einem dieser Tests haben wir versucht, das Zeiterfassungs-System

---

<sup>2</sup> Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2023.

<sup>3</sup> BSI, Die Lage der IT-Sicherheit in Deutschland 2023,

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?\\_\\_blob=publicationFile&v=7](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=7)

eines Kunden für einen Angriff zu nutzen. Dieser Test zeigt, wie einfach Kriminelle auf Strukturen zugreifen und diese für Ihre Angriffe missbrauchen können.

Wir wussten, dass bei diesem Kunden ein Zeiterfassung-System implementiert ist und das dieses System regelmäßig Mails an Beschäftigte verschickt. Diese Information konnte man im Internet nachlesen. Diese Informationsmail des Systems haben wir nachgebaut und gezielt genutzt, um Zugangsdaten zu erbeuten. Die Erfolgsquote lag bei 85%.

**Trainieren Sie nicht nur allgemeine Phishing-Situationen, sondern auch Ihre internen Systeme**, zum Beispiel E-Mails von Ihrem Zeiterfassungssystem oder anderen Tools, die Sie im Unternehmen nutzen. Angreifer werden immer besser und sammeln Informationen über Ihr Unternehmen – entweder über das Internet, Social Media oder vor Ort.

## **Künstliche Intelligenz: Die wachsende Gefahr in der Cyberwelt**

Eine der bedeutendsten Entwicklungen ist der Einsatz von Künstlicher Intelligenz (KI) in der Cyberkriminalität. KI bringt viele Vorteile mit sich und beschleunigt im Berufsalltag viele Prozesse. Doch sie hat auch eine dunkle Seite: KI kann eine mächtige Waffe in den Händen von Cyberkriminellen sein, mit der noch gezieltere Angriffe möglich sind.

### **Verstärkung von Phishing-Angriffen mit persönlichen E-Mails**

KI-Systeme können personalisierte Phishing-E-Mails in einem Maße erstellen, das bisher unvorstellbar war. Durch das Sammeln von Informationen aus sozialen Netzwerken und anderen öffentlichen Quellen können Angreifer überzeugende Nachrichten generieren, die speziell auf ihre Opfer zugeschnitten sind. Diese Techniken erhöhen die Erfolgsquote von Phishing-Kampagnen dramatisch.

### **Schnelle Entwicklung von Malware**

KI kann auch dazu verwendet werden, Malware zu entwickeln, die sich dynamisch an die Sicherheitsmaßnahmen eines Zielsystems anpasst. Solche KI-

basierten Malware-Programme können Erkennungswerkzeuge umgehen, indem sie ihr Verhalten ändern, um nicht entdeckt zu werden. Dies erschwert es Sicherheitsteams, Angriffe zu identifizieren und zu verhindern, bevor Schaden entsteht.

### **Automatisierung von Cyberangriffen mit Hilfe von Tools**

Durch den Einsatz von KI können Cyberkriminelle Angriffe auf eine Weise automatisieren, die menschliche Hacker in Bezug auf Geschwindigkeit und Effizienz bei weitem übertrifft. KI-Systeme können Schwachstellen in Netzwerken schneller identifizieren und ausnutzen, was zu einer Zunahme von Sicherheitsverletzungen führt. Diese Automatisierung ermöglicht es auch kleineren kriminellen Gruppen, Angriffe mit der Raffinesse und dem Umfang durchzuführen, die früher nur gut finanzierten Organisationen möglich waren.

### **Täuschend echte Fälschung von digitalen Identitäten**

Sogenannte Deepfakes – überzeugenden audiovisuellen Fälschungen, die mit KI erstellt wurden – sind eine weitere Bedrohung die durch den Einsatz von künstlicher Intelligenz ermöglicht wurde. Cyberkriminelle können diese Technologie nutzen, um Personen in Schlüsselpositionen zu imitieren und betrügerische Handlungen wie das Anfordern von Geldüberweisungen oder das Preisgeben vertraulicher Informationen zu initiieren.

## **Angriffsziele: Diese „Schwachstellen“ sind für Hacker besonders attraktiv**

### **Cloud-Dienste**

Cloud-Dienste ziehen Cyberkriminelle an, da sie eine zentrale Anlaufstelle für eine Vielzahl von Daten verschiedener Organisationen darstellen und bei einem Angriff Zugriff auf umfangreiche Informationen ermöglichen.

Noch ein Beispiel aus meinem Berufsalltag: Ein großer Cloud-Anbieter aus dem öffentlichen Bereich wurde durch eine sehr geschickte Ausnutzung von Sicherheitslücken angegriffen. Die Meldung zum Angriff erreichte mich an einem Freitag. Nach unseren Recherchen war am Donnerstagabend die Systemlücke veröffentlicht worden: Das BSI hat die Meldung rausgegeben und keine 24 Stunden später war das System angegriffen. Mein Kunde hat keine Chance zu

reagieren. Zum Glück wurde nur die erste Firewall angegriffen, die dahinterliegenden Systeme jedoch nicht. Das Schutzkonzept des Kunden hat gut funktioniert. Trotzdem ist ein Schaden entstanden, da der Kunde 7-8 Tage offline war für die Analyse des Angriffs. Dadurch kam ein großer Umsatzverlust zustande.

**Mein Tipp: Investieren Sie in Systeme, die Datenströme analysieren und Anomalien erkennen.** So können Sie eine Früherkennung sicherstellen. Darüber hinaus ist es sinnvoll, die Channels des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu überprüfen und sich auf dem Laufenden zu halten. Wenn dort kritische Meldungen eintreffen, müssen Sie sofort reagieren.

### **Lieferketten**

Lieferketten sind für Cyberkriminelle attraktiv, weil sie viele Beteiligte umfassen, wodurch sich die Angriffsfläche vergrößert und die Wahrscheinlichkeit von Schwachstellen erhöht wird. Da die Sicherheitsmaßnahmen zwischen den beteiligten Unternehmen unterschiedliche sein können, bieten weniger gut geschützte Unternehmen potenzielle Eintrittspunkte für Angriffe. Ein erfolgreich angegriffenes Unternehmen innerhalb einer Lieferkette kann also schnell zu einem Sicherheitsrisiko für andere Unternehmen werden. Außerdem werden bei einem Angriff oft nicht nur die Daten des angegriffenen Unternehmens, sondern auch die Daten aller Unternehmen aus der Lieferkette erbeutet.

Ziel der Angreifer ist es, die Lieferketten zu zerstören, sodass die gesamte Infrastruktur eines oder mehrerer Unternehmen flach liegt. Häufig passiert das nicht nur an einem Standort, sondern möglichst weltweit.

Ein Beispiel eines solchen Angriffs wäre ein Angriff auf eine Software, die viele Unternehmen nutzen. Der Schadcode wird sorgfältig in einer scheinbar harmlosen Aktualisierung versteckt, die eine neue "Sicherheitsverbesserung" verspricht. Sobald die Aktualisierung in den offiziellen Code eingefügt wird, verbreitet sie sich automatisch auf die Systeme aller Nutzer, die die neueste Version herunterladen.

## **Die Realität der digitalen Welt: Cyberangriffe auf smarte Geräte**

Wir stehen vor der Herausforderung von Cyberangriffen auf smarte Geräte, einschließlich smarter Autos. Hacker haben bereits gezeigt, dass sie Zugriff auf diese Fahrzeuge erlangen können. Die Trennung zwischen digitaler Welt und Informationssicherheit verschwindet.

Die gute Nachricht ist, dass viele Autohersteller regelmäßige Updates anbieten, um Sicherheitslücken zu schließen. Es ist von entscheidender Bedeutung, diese Updates zeitnah einzuspielen, da sie nicht nur Funktionen und Verbesserungen, sondern auch Sicherheitspatches enthalten. Dies ist heute mehr denn je Standardpraxis.

In der Vergangenheit konnten Hacker sogar Autoradios manipulieren, was die Dringlichkeit von regelmäßigen Updates unterstreicht. Nach dem Start eines Fahrzeugs kann das Betriebssystem offen sein, was potenziell gefährlich ist. Hacker können sich leicht koppeln und sogar interaktiv mit dem Fahrer interagieren.

## **Zwang zur Datensicherheit: Diese Gesetzesprojekte kommen auf Sie zu**

### **Die neue NIS-2-Richtlinie – mehr Sicherheit UND mehr Bürokratie!**

Die NIS-2-Richtlinie ist eine EU-weite Regelung zur Netzwerk- und Informationssicherheit mit dem Ziel, ein hohes gemeinsames Sicherheitsniveau für Netzwerk- und Informationssysteme zu gewährleisten. Sie ist am 16. Januar 2023 in Kraft getreten und muss bis zum 17. Oktober 2024 in nationales Recht umgesetzt werden.

Die Richtlinie gilt für Unternehmen ab 50 Beschäftigten und 10 Mio. Euro Umsatz in 18 Sektoren, u.a. Energie, Ernährung, Trinkwasser, Gesundheit, Ethik, Transport und Verkehr. Laut Aussage des BSI fallen deutschlandweit 29.000 Unternehmen unter diese Richtlinie.

Unternehmen, die unter die NIS-2-Richtlinie fallen, ...

- müssen umfassende technische und organisatorische Maßnahmen implementieren.
- Sie sind verpflichtet, erhebliche Sicherheitsvorfälle an zuständige nationale Behörden zu melden.
- Sie müssen regelmäßige Sicherheitsüberprüfungen, -audits und -tests durchführen, um die Effektivität ihrer Sicherheitsmaßnahmen zu gewährleisten.
- Darüber hinaus müssen sie die Sicherheit ihrer Lieferketten sicherstellen
- und sowohl Mitarbeiter als auch Lieferanten in Bezug auf Cybersicherheitspraktiken schulen und sensibilisieren.

### **Gesetzgebung zur KI**

Die rasante Entwicklung von Künstlicher Intelligenz (KI) birgt das Risiko von unbeabsichtigten Konsequenzen, wie der Verletzung von Copyright und der Schaffung von Sicherheitslücken.

Das KI-Gesetz der europäischen Union zielt darauf ab, ethische Standards und Verantwortlichkeiten zu definieren, um Missbrauch zu verhindern und die Entwicklung und Anwendung von KI im Einklang mit Menschenrechten und demokratischen Werten zu gewährleisten.

Gerade im Bereich Datenschutz ist Vorsicht geboten: Wenn Sie sich in einem Unternehmen zum Beispiel den Bewerbungsprozess vereinfachen möchten und eingehende Bewerbungen mit Hilfe von KI einschätzen wollen und dazu ein Bewerbungsschreiben hochladen mit allen Informationen eines Bewerbers, dann wird die KI daraus lernen. Sie geben damit personenbezogene Daten preis, die Sie so nicht hätten preisgeben dürfen. Und genau das ist einer der Aspekte, die das KI-Gesetz regeln wird.

Der europäische Gesetzgeber, das Europäische Parlament und der Rat der EU haben sich im Dezember 2023 auf das Gesetz über die Künstliche Intelligenz politisch geeinigt.

### **Data Act**

Primäres Ziel des Data Acts ist es, den Datenzugang und die Datennutzung für Verbraucher und Unternehmen zu erleichtern. Der Data Act betrifft Produkte, die Daten über Nutzung erzeugen und sammeln und übermitteln, zum Beispiel

Haushaltsgeräte. Das Gesetz betrifft Hersteller, Dateninhaber und Nutzer von vernetzten Geräten.

### **Cyber Resilience Act**

Der Cyber Resilience Act soll Verbraucher und Unternehmen schützen, die digitale Produkte oder Software nutzen. Er soll ein hohes Cybersicherheitsniveau für Produkte mit digitalen Elementen gewährleisten, um die Cyberangriffen zu verringern und das Vertrauen in den digitalen Markt zu fördern. Von dieser Verordnung betroffen sind Hersteller, Importeure und Händler von digitalen Produkten und verbundenen Dienstleistungen, da sie strenge Sicherheitsanforderungen einhalten und kontinuierliche Updates zur Behebung von Sicherheitslücken bereitstellen müssen. Der Act soll sicherstellen, dass digitale Produkte und Dienstleistungen, die auf dem EU-Markt angeboten werden, von der Entwurfsphase an sicher sind und Verbraucher sowie Unternehmen vor Cyberbedrohungen schützen.

## **Welche 5 Maßnahmen wirklich was bringen**

Unabhängig davon, ob Sie direkt von einem Gesetz betroffen sind oder nicht – diese Maßnahmen sollten Sie dennoch umsetzen, um Ihr Unternehmen wirksam vor Angriffen zu schützen:

### **1. Überprüfen Sie Ihre Systeme auf Aktualität**

Das regelmäßige Aktualisieren Ihrer Software und Betriebssysteme ist entscheidend, um bekannte Sicherheitslücken zu schließen und den Schutz gegen die neuesten Cyberbedrohungen zu verstärken. Veraltete Systeme bieten Angreifern leichtere Angriffspunkte und erhöhen das Risiko von Datenverlusten und Sicherheitsverletzungen.

### **2. Nutzen Sie Trojaner- und Virenschutz**

Ein zuverlässiger Virenschutz hilft, schädliche Software wie Trojaner, Viren und andere Malware zu identifizieren und zu blockieren, bevor sie Schaden anrichten kann. Es ist wichtig, dass die Schutzsoftware stets auf

dem neuesten Stand gehalten wird, um gegen aktuelle Bedrohungen gewappnet zu sein.

### **3. Machen Sie regelmäßige Backups**

Regelmäßige Sicherungskopien Ihrer Daten sind essentiell, um im Falle eines Cyberangriffs, wie beispielsweise einer Ransomware-Attacke, den Verlust wichtiger Informationen zu vermeiden. Diese Backups sollten idealerweise an einem sicheren Ort aufbewahrt werden, der physisch vom Hauptnetzwerk getrennt ist, um sie vor Angriffen zu schützen.

### **4. Überprüfen Sie Ihre Berechtigungen**

Stellen Sie sicher, dass nur autorisierte Personen Zugriff auf sensible Informationen und Systeme haben, indem Sie die Zugriffsrechte sorgfältig verwalten und regelmäßig überprüfen. Eine strikte Berechtigungsvergabe minimiert das Risiko von Datenmissbrauch und -lecks innerhalb Ihrer Organisation.

### **5. Schulen Sie Ihre Mitarbeiter**

Die Sensibilisierung und Schulung Ihrer Mitarbeiter ist unverzichtbar. Die meisten Sicherheitsverletzungen sind auf menschliche Fehler zurückzuführen. Ihre Mitarbeiter sind Ihr stärkster Schutzschild gegen Cyberangriffe. Wichtig für eine wirksame Sensibilisierung ist ein durchdachtes Schulungs-Konzept, das Ihre Mitarbeiter dauerhaft sensibilisiert und durch Simulationen auf reale Situationen vorbereitet. So erkennen Ihre Mitarbeiter auch in stressigen Alltagssituationen Angriffe direkt und handeln angemessen.

# So bauen Sie eine wirksame Awareness-Kampagne auf

Jeder einzelne Schritt Ihrer Awareness-Kampagne muss durchgeführt werden, um den gewünschten Effekt zu erzielen. Planen Sie deshalb diese Bestandteile Ihrer Kampagne ein:

## **Schritt 1: Mit guter Vorbereitung legen Sie den Grundstein für Ihren Erfolg**

Definieren Sie als erstes Ihr Ziel für die Awareness-Kampagne und messen Sie Ihren Status-Quo. Hierfür eignet sich der Versand einer Phishing-Simulation. Anhand der jeweiligen Klickraten auf das Mailing sehen Sie, wie gefährdet Ihr Unternehmen ist und können daraufhin weitere Maßnahmen ergreifen.

**Achtung: Diese Kollegen müssen VORHER informiert werden!** Bevor Sie Ihren simulierten „Angriff“ per E-Mail starten, müssen Sie sicherstellen, dass Datenschutzbeauftragte, der IT- sowie der Informations-Sicherheitsbeauftragte an einem Strang ziehen und den Betriebsrat informiert ist. Die Kollegen aus der IT müssen darauf vorbereitet sein, dass Mitarbeiter beim Support nachfragen, was denn das für eine E-Mail sei usw.

## **Schritt 2: Versenden Sie eine Phishing-Simulation und messen Sie Ihr Awareness-Level**

Hierzu müssen Sie sich zunächst ein Szenario ausdenken, mit dem Sie die Mitarbeiter ködern können. Versuchen Sie, ein realistisches Szenario zu finden, das zu Ihrem Unternehmen passt.

Bereiten Sie z. B. eine E-Mail vor, in der Sie nachfolgendes Szenario beschreiben: Im Unternehmen sollen iPhones eingeführt werden. Die IT-Abteilung sucht nun Mitarbeiter, die bereit sind, die neuen Geräte auf Herz und Nieren zu testen. Die Testpersonen können die iPhones als Dankeschön am Ende des Tests behalten. Da nur eine begrenzte Anzahl von Testgeräten bereitsteht, werden die Teilnehmer ausgelost. Die Interessenten müssen sich auf der Internetseite des Unternehmens mit ihrem Benutzeraccount und Passwort registrieren.

## **Alternativ: Benutzen Sie einfach diese fix und fertige Phishing-Simulation**

Wenn Sie den Aufwand der Erstellung von E-Mail und dazugehöriger Internetseite nicht leisten wollen oder können, bietet sich skillsforwork als perfekte Lösung an:

[skillsforwork](#) bietet für Ihre Phishing-Simulation bereits fertige Lösungen, die individuell auf Ihr Unternehmen abgestimmt werden. So sparen Sie sich viel Aufwand! Wir kümmern uns um die Erstellung der Mails, Versand und Auswertung Ihrer Kampagne. [Hier mehr Informationen erhalten.](#)

## **Schritt 3: Starten Sie Ihre Sensibilisierungs-Kampagne**

Nachdem Sie Ihre erste Phishing-Simulation versendet haben, schauen Sie sich die Ergebnisse an und besprechen diese mit der Geschäftsleitung. Präsentieren Sie die Ergebnisse danach allen Mitarbeitern. Präsentationen zu Awareness-Kampagnen müssen zentrale Botschaften und kein Fachwissen vermitteln. Sie müssen die Mitarbeiter begeistern und nicht langweilen. Bewährt haben sich auch kleine Live Hacking-Beiträge, bei denen z.B. gezeigt wird, wie schnell Passwörter gehackt werden oder wie leicht man mit einem USB-Stick Daten ausspionieren kann.

### **Kontinuität bringt den Erfolg**

Ganz wichtig: Eine einmalige Kampagne wird Ihre Mitarbeiter nicht dauerhaft schulen, denn Sie ist schnell vergessen. Für einen wirksamen Effekt müssen Sie Ihre Mitarbeiter dauerhaft sensibilisieren. Im Idealfall nutzen Sie kurze Lerneinheiten und unterschiedliche Simulationen, damit die Mitarbeiter jedes Mal aufs Neue überrascht werden.

Auch das macht eine Kampagne mit skillsforwork für Sie besonders attraktiv: skillsforwork wertet alle Phishing-Kampagnen auf Abteilungsebene für Sie aus und erstellt passende Grafiken, mit denen Sie Ihre Mitarbeiter überzeugen können. Monatliche, spannende E-Learnings inkl. Videos und Interaktionen unterstützen Sie bei der Präsentation in Ihrem Unternehmen. [Jetzt gratis 7 Tage skillsforwork testen – keine Abmeldung notwendig!](#)

#### **Schritt 4: Messen Sie den Erfolg Ihrer Awareness-Kampagne**

Erfolgsmessungen machen transparent, ob Sie mit Ihren Sensibilisierungsmaßnahmen gegen Dynamik, Beharrlichkeit und Trotz der Mitarbeiter erfolgreich waren und ob in den Trainings nachhaltig Fachwissen vermittelt wurde. Aus den Ergebnissen können Sie direkt erkennen, an welchen Themen Sie weiterarbeiten müssen.

Mit genauen Kennzahlen können Sie Ihrer Geschäftsleitung nachweisen, dass sich die Security Awareness-Kampagne bezahlt gemacht hat, und die Mitarbeiter können Sie für ihre Sensibilität und ihr Fachwissen loben.

Verschlechtern sich die Ergebnisse, müssen Sie themengerecht Trainings oder Sensibilisierungsmaßnahmen durchführen. So können Sie sehr genau steuern, in welchen Themenbereichen Sie aktiv Maßnahmen ergreifen müssen.

#### **skillsforwork macht Ihnen das Messen Ihrer Awareness-Kampagne besonders leicht:**

Denn es bietet Ihnen automatische Auswertungen Ihrer Phishing-E-Mails auf Abteilungsebene. So sehen Sie direkt, welche Abteilung Schulungsbedarf hat und wo Sicherheitslücken entstanden sind. Passend dazu können Sie direkt unsere E-Learning Einheiten nutzen und die Abteilungen zu den digitalen Trainings einladen. Im Anschluss erhalten Sie einen Nachweis über die Sensibilisierungsmaßnahme für Ihre Unterlagen. [Jetzt skillsforwork 7 Tage gratis testen!](#)

## Impressum

---

skillsforwork- ein Unternehmensbereich der VNR Verlag für die Deutsche  
Wirtschaft AG  
Theodor-Heuss-Str. 2-4  
53095 Bonn

Telefon: 0228 9550-160  
Fax: 0228 3696480  
E-Mail: [vertrieb@skillsforwork.de](mailto:vertrieb@skillsforwork.de)  
Internet: [www.skillsforwork.de](http://www.skillsforwork.de)

Vorstand: Richard Rentrop, Bonn

Herausgeber und redaktioneller Verantwortlicher i.S.d.P.: Michael Jodda, Bonn

Bildnachweise Titelseite: Adobe Stock - insta\_photos

Alle Angaben wurden mit äußerster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden. Vervielfältigungen jeder Art sind nur mit Genehmigung des Verlags gestattet.

Diese Publikation richtet sich gleichermaßen an weibliche und männliche Leser. Aus Gründen der Lesbarkeit wird die männliche Schreibweise (z. B. Unternehmer, Mitarbeiter) gewählt. Diese schließt stets alle Geschlechterformen mit ein.

© 2024 by skillsforwork – ein Unternehmensbereich der Verlag für die Deutsche  
Wirtschaft AG

Bonn • Berlin • Bukarest • Jacksonville • Manchester • Warschau • Passau