

# Cyber Security

# Cyber Security im Unternehmens- umfeld

# Schulung und Sensibili- sierung



# Mitarbeiter als primäre Cyberangriffsfläche?

## Why Are People the Weakest Link in Cybersecurity?

Cybersecurity professionals focus on three primary categories to protect data: people, processes, and technology. Each of these provides insight into why it's easy to consider people the weakest link.

### Technology

Technology, in itself, never makes mistakes. People then technology does what people tell it to do. It can provide repeatable outputs, and even artificial intelligence of algorithms programmed by people.

While technology may be flawed, as evidenced in software, it is logical and obedient. We can catch security patch updates.

### Processes

Similar to technology, processes do not "act" of their own accord. They are a set of steps that people follow so they can repeat

## Cybersicherheit: Der Mensch, das vermeintlich schwächste Glied

20.22 April 2023 15:05:12



Eine der schlimmsten Phrasen in der Cybersicherheit? Unter anderem Sätze wie dieser: "Das schwächste Glied der Sicherheitskette". Das Einzige, was man mit negativen Affirmationen erreichen kann, ist, Mitarbeitende von den richtigen Verhaltensweisen abzuhalten.

Einbeziehen statt abgrenzen: Warum der Begriff „Benutzer“ nicht immer hilfreich ist  
Erstens: Wenn Sie Mitarbeitende, Partner, Kunden, Lieferanten, Freunde und Familie als "Benutzer" bezeichnen, zieht das eine psychologische Grenze zwischen Ihnen und den anderen. Der Begriff schafft so eine Distanz, obwohl wir in der Wirklichkeit alle durch gemeinsamen Technologien verbunden sind. Zudem ist der Begriff "User" in anderen Zusammenhängen

## The Human Element is the Weakest Link in Cybersecurity



Mousam Khatri

Counsellor at Confederation of Indian Industry  
Veröffentlicht: 2. Aug. 2023

In today's digital world, cybersecurity is more important than ever. Businesses of all sizes are constantly under threat from cyberattacks, and the human element is often the weakest link.

India Witnessed 13.9 Lakh Cybersecurity Incidents In 2022: Govt. The numbers still do not give an entire picture of cyberattacks on the country as these statistics only include information reported to and tracked by the Indian Computer Emergency Response Team (CERT-In).

Cybercriminals are well aware of this, and they often exploit human error to gain access to sensitive data or systems. They use phishing emails, social engineering

# Methoden zur Sensibilisierung von Mitarbeitern

## **Bewusstsein für Bedrohungen schaffen:**

- Schulungen helfen Mitarbeitern, aktuelle und potenzielle Netzwerksicherheitsbedrohungen wie Phishing, Malware, Ransomware und andere Cyberangriffe zu verstehen.

## **Richtlinien und Verfahren vermitteln:**

- Mitarbeiter werden mit den Sicherheitsrichtlinien, -verfahren und Best Practices der Organisation vertraut gemacht, was zu einer stärkeren Compliance führt.



# Methoden zur Sensibilisierung von Mitarbeitern

## **Förderung einer Sicherheitskultur:**

- Regelmäßige Schulungen tragen dazu bei, eine Kultur der Sicherheit innerhalb der Organisation zu etablieren, bei der Sicherheit als gemeinsame Verantwortung angesehen wird.

## **Reaktion auf Vorfälle:**

- Mitarbeiterschulungen umfassen oft Protokolle zur Reaktion auf Sicherheitsvorfälle, damit Mitarbeiter wissen, wie sie im Falle einer Sicherheitsverletzung reagieren sollen.



# Methoden zur Sensibilisierung von Mitarbeitern

## **Umgang mit sensiblen Daten:**

- Die Schulung betont die Bedeutung des Schutzes sensibler Daten und lehrt Methoden zur sicheren Handhabung und Speicherung von Informationen.

## **Physische Sicherheit:**

- Schulungen decken auch Aspekte der physischen Sicherheit ab, wie den sicheren Umgang mit Hardware und den Zugang zu gesicherten Bereichen.



# Methoden zur Sensibilisierung von Mitarbeitern

## **Aktualisierung des Wissens:**

- Regelmäßige Schulungsprogramme stellen sicher, dass das Personal über die neuesten Sicherheitsbedrohungen und -technologien auf dem Laufenden bleibt.

## **Simulation von Sicherheitsvorfällen:**

- Durch die Durchführung von simulierten Angriffen oder Sicherheitsübungen können Mitarbeiter praktische Erfahrungen im Umgang mit potenziellen Sicherheitsvorfällen sammeln.





# Methoden zur Sensibilisierung von Mitarbeitern

## **Stärkung des Passwort-Managements:**

- Schulungen betonen die Bedeutung starker Passwörter und lehren Best Practices für die Erstellung und Verwaltung von Passwörtern.



# Sensibilisierungsthemen: Erkennung von Phishing

## **Ungewöhnliche Absenderadresse:**

- Überprüfen, ob die E-Mail-Adresse des Absenders legitim ist. Oft sind Phishing-Mails von Adressen gesendet, die bekannten Unternehmen ähnlich sehen, aber geringfügige Abweichungen aufweisen, wie zusätzliche Buchstaben oder verdächtige Domains.

## **Dringlichkeit und Angstmacherei:**

- Phishing-Mails enthalten oft dringende oder bedrohliche Nachrichten, die den Empfänger dazu bringen sollen, schnell zu handeln, ohne die Legitimität der E-Mail zu hinterfragen. Beispielsweise Warnungen vor Kontosperrung oder dringende Anfragen um vertrauliche Informationen.



# Sensibilisierungsthemen: Erkennung von Phishing

## **Ungebetene Anhänge oder Links:**

- Vorsicht mit E-Mails, die ungebetene Anhänge oder Links enthalten. Öffnen Sie keine Anhänge oder klicken Sie nicht auf Links, wenn Sie sich nicht sicher sind, dass die E-Mail vertrauenswürdig ist.

## **Rechtschreib- und Grammatikfehler:**

- Phishing-E-Mails enthalten oft Rechtschreib- und Grammatikfehler. Professionelle Organisationen überprüfen ihre Kommunikation in der Regel sorgfältig, daher können solche Fehler ein Hinweis auf eine betrügerische E-Mail sein.



# Sensibilisierungsthemen: Erkennung von Phishing

## **Aufforderung zur Eingabe persönlicher Informationen:**

- Besondere Vorsicht ist geboten, wenn E-Mails dazu auffordern, persönliche oder finanzielle Informationen preiszugeben, wie Passwörter, Kontonummern oder Sozialversicherungsnummern. Legitime Unternehmen fordern solche Informationen normalerweise nicht per E-Mail an.



# Sensibilisierungsthemen: Physische Sicherheit

## **Zugangskontrolle:**

- Ausschließlich autorisiertes Personal sollte Zugang zu sensiblen oder gesicherten Bereichen erhalten. Die Nutzung von Sicherheitskarten, Codes oder biometrischen Systemen kann dabei helfen, den Zugang zu kontrollieren und zu überwachen.

## **Sicherer Umgang mit Besuchern:**

- Besucher sollten immer registriert und während ihres Aufenthalts im Unternehmen begleitet werden. Dies verhindert unautorisierten Zugriff auf sensible Bereiche und schützt vertrauliche Informationen.



# Sensibilisierungsthemen:

## Physische Sicherheit

### **Schutz sensibler Informationen:**

- Wichtige Dokumente und Datenträger sollten sicher aufbewahrt werden, vorzugsweise in abgeschlossenen Schränken oder Räumen. Es sollte stets darauf geachtet werden, dass sensible Informationen nicht offen auf Schreibtischen oder in für jeden zugänglichen Bereichen liegen.

### **Bewusstsein für verdächtige Aktivitäten:**

- Mitarbeiter sollten ermutigt werden, auf ungewöhnliche oder verdächtige Aktivitäten zu achten, wie unbekannte Personen in gesicherten Bereichen oder ungewöhnliche Anfragen nach Informationen oder Zugang.



# Sensibilisierungsthemen: Physische Sicherheit

## **Sicherheitsbewusstes Verhalten:**

- Die Wichtigkeit von sicherheitsbewusstem Verhalten, wie das Verriegeln von Türen, das sichere Verwahren von Schlüsseln oder Zugangskarten und das Ausschalten nicht genutzter Geräte, sollte betont werden. Dies trägt dazu bei, die physische Sicherheit im Unternehmen zu stärken.



# Simulation

## **Realistische Szenarien:**

- Entwickeln realistischer Szenarien, die auf tatsächlichen Sicherheitsrisiken basieren, denen die jeweilige Organisation ausgesetzt sein könnte. Dies kann von Phishing-Angriffen über Datenlecks bis hin zu physischen Sicherheitsverletzungen reichen.

## **Einbindung sämtlicher Ebenen:**

- Sicherheitssimulationen sollten Mitarbeiter aller Ebenen einbeziehen, von der Geschäftsführung bis hin zu den operativen Teams. Jeder sollte verstehen, wie er auf verschiedene Arten von Sicherheitsvorfällen reagieren muss.





# Simulation

## **Debriefing und Feedback:**

- Nach jeder Simulation ist ein Debriefing entscheidend. Hierbei handelt es sich um eine Besprechung der Simulation, um zukünftige Trainings und Sicherheitsprotokolle zu verbessern.

## **Klare Kommunikation:**

- Allgemein ist es stets wichtig, sicherzustellen, dass alle Beteiligten verstehen, dass es sich um eine Simulation handelt, um unnötigen Alarm oder Verwirrung zu vermeiden. Gleichzeitig sollte die Kommunikation während der Simulation realistisch gehalten werden, um eine echte Notfallsituation zu simulieren.



# Simulation

## **Regelmäßige Durchführung und Aktualisierung:**

- Sicherheitssimulationen sollten regelmäßig durchgeführt und ihre Szenarien aktualisiert werden, um mit den sich ändernden Sicherheitsbedrohungen Schritt zu halten. Dies stellt sicher, dass das Personal stets auf dem neuesten Stand ist und sich der besten Reaktionspraktiken bewusst ist.



# Tools: CanIPhish

**CanIPhish** ist ein Tool, welches vorgefertigte Vorlagen für Phishing-E-Mails bereitstellt, um das Sicherheitsbewusstsein der eigenen Belegschaft zu testen. Statt eines tatsächlichen Angriffs wird das Opfer zu einer Seite geleitet, die es auf seinen Fehler aufmerksam macht.



# Tools: CanIPhish

The screenshot displays the CanIPhish website interface. At the top, the navigation bar includes links for Platform, Inbox Simulator, Tools, Pricing, Partners, Resources, and About, along with 'Try it free' and 'Log in' buttons. The main heading is 'Phishing Email Templates'. Below this, a sub-header states: 'CanIPhish maintains an ever-evolving library of free phishing email templates that mimic the latest trends. Take a look at our library and see the email templates that are most effective today.' The section 'How phishing emails trick victims' explains that phishing emails typically have a 'common set of goals' such as credential harvesting, endpoint compromise, or business email compromise. It further details how attackers craft emails with malicious links or attachments to trick victims. A call to action encourages users to create a free account or try the email inbox simulator. Below this, there are three featured email templates: 'Fake Email Templates' (77), 'Wire Transfer Confirmation Email', and 'QR Code Enter to Win £1000'. A sidebar on the right shows a 'CanIPhish Training' video player with a 'Watch on YouTube' button. The bottom right corner features a 'Learn to spot the phish' section with a 'Begin the Guided Tour' button.

caniphish Platform Inbox Simulator Tools Pricing Partners Resources About Try it free Log in

## Phishing Email Templates

CanIPhish maintains an ever-evolving library of free phishing email templates that mimic the latest trends. Take a look at our library and see the email templates that are most effective today.

### How phishing emails trick victims

Phishing emails typically have a **common set of goals** that can be used to identify what type of attack is being attempted. These goals include credential harvesting, endpoint compromise, or business email compromise (i.e., reply-to attacks). Armed with this information, an attacker's goal is, you can identify the techniques an attacker will likely use to trick its victim into interacting with the email.

For credential harvesting, an attacker will craft a phishing email that contains links or buttons that lead to a malicious website. For endpoint compromise, an attacker will craft a phishing email that contains a malicious attachment, enticing the victim to download and open the file. For business email compromise, an attacker will craft a phishing email that attempts to trick the victim into sending a wire transfer or making a purchase. All phishing emails have a malicious goal and intention behind them.

Equipped with this information, take a look at our fake email templates and see if you can spot the goals of the email. **Create a free account or try our email inbox simulator to see the unique way CanIPhish can help you protect your organization.**

#### Fake Email Templates 77

- OneDrive Excel Share Email
- OneDrive Word Share Email

#### Wire Transfer Confirmation Email

Dear John,

We're excited to announce that our updated Remote Working Policy is now in effect. To ensure you receive the latest information, we've updated your email address. Please confirm your new email address by clicking the link below.

**Give your feedback and go into the draw to win an iPhone 15!**

All employees who participate in the review will be entered into a lucky draw to win an iPhone 15. The draw will close on 15th Dec 2023.

Best regards,  
John Doe

#### QR Code Enter to Win £1000

Dear John,

We're excited to announce that our updated Remote Working Policy is now in effect. To ensure you receive the latest information, we've updated your email address. Please confirm your new email address by clicking the link below.

**Give your feedback and go into the draw to win an iPhone 15!**

All employees who participate in the review will be entered into a lucky draw to win an iPhone 15. The draw will close on 15th Dec 2023.

Best regards,  
John Doe

#### Oops! That was a phishing email!

This was an authorised phishing simulation run as part of a security awareness training exercise.

#### What is phishing?

Phishing is a type of social engineering attack often used to steal user data (e.g. login credentials and credit card numbers) or compromise computer networks. It occurs when an attacker, masquerading as a trusted entity and entices their recipients into opening an email, instant message, or text message.

Phishing attacks remain among the most common methods used by malicious cyber actors to target organisations. While phishing messages are commonly sent out to large groups of people, targeted phishing campaigns are typically aimed at a particular group of recipients.

Read more on the types of phishing attacks to better understand the signs of phishing and learn some simple tricks.

#### Learn to spot the phish

Curious how you can spot the phish in the future? Take a look at our guided tour which highlights how attackers use a combination of urgency, fraudulent sender addresses, engaging content and malicious websites or attachments to compromise their victims.

[Begin the Guided Tour](#)

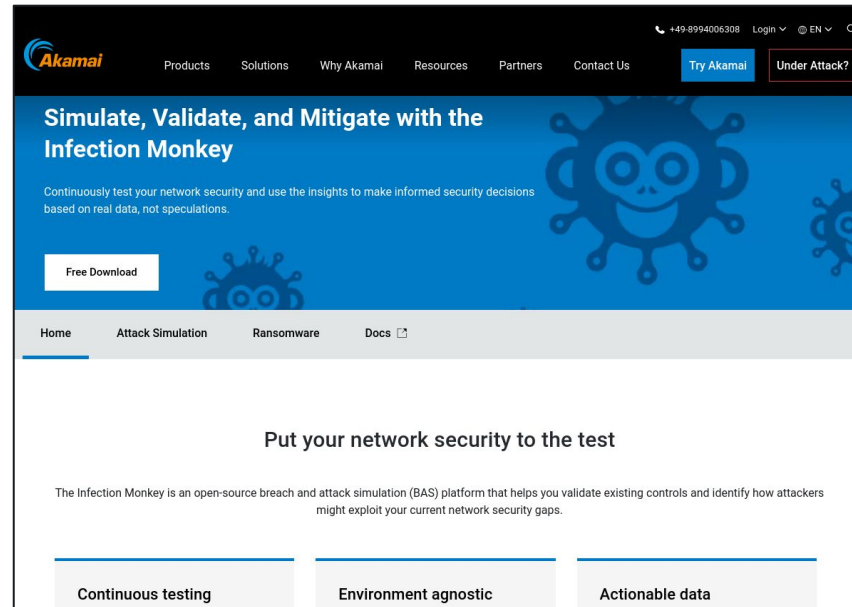


# Tools: Infection Monkey

**Infection Monkey** ist eine Open-Source Simulationsplattform für verschiedene Angriffe auf Netzwerke mit anschließender Auswertung und Verbesserungsvorschlägen.

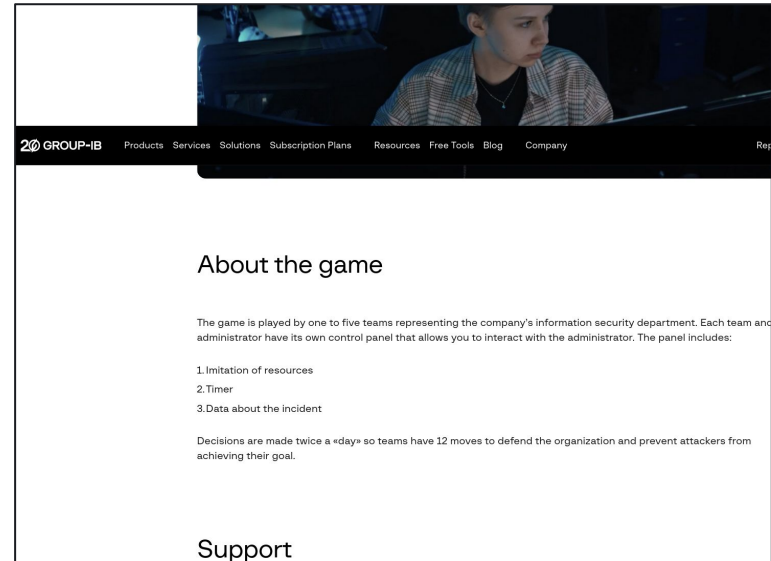


# Tools: Infection Monkey



# Tools: Spielerische Simulationsprogramme

Verschiedene Firmen wie etwa Group-IB bieten spielerische Simulationstrainings, welches Mitarbeiter auf unterhaltsame Weise die Wichtigkeit von IT-Sicherheitsbewusstsein vor Augen führen.





# CloudCommand