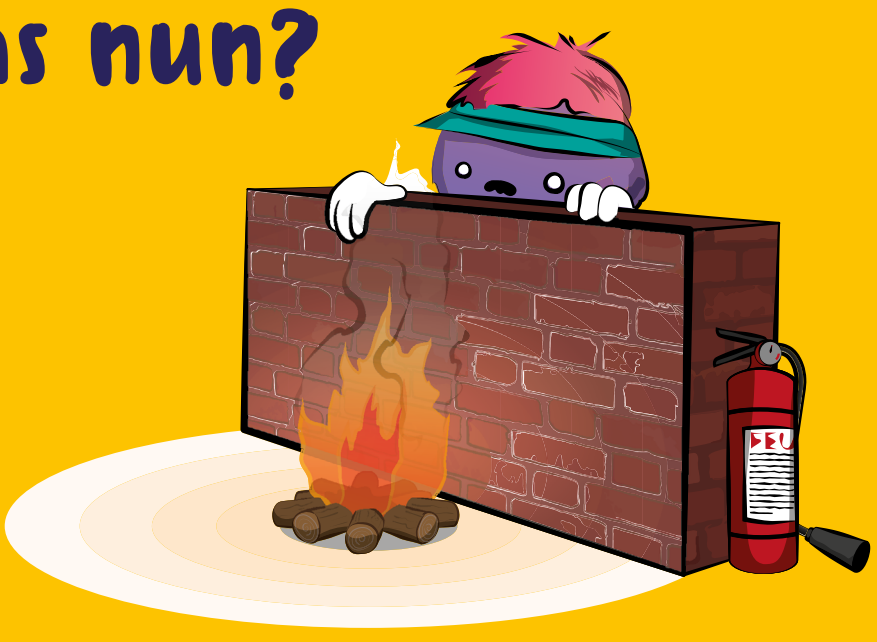
Wumbel®

Cyberangriffe was nun?

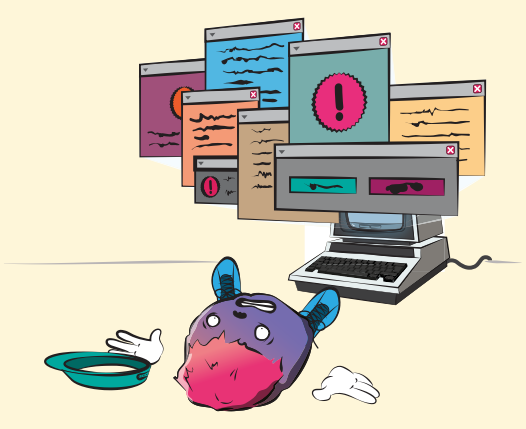


DR. BITTNER GROUP

Stellen Sie sich vor, der IT-Support erhält einen Anruf: **„Mein Passwort funktioniert nicht mehr - bitte setzen Sie es zurück.“** Hinter der Stimme verbirgt sich jedoch ein Angreifer, der zuvor durch SIM-Swapping Zugriff auf eine Telefonnummer erlangt hat. Genau so wurden Mitarbeiter britischer Firmen getäuscht.

Oder ein anderes Szenario: Sie sind in einer Videokonferenz, eine vermeintliche Führungskraft erteilt die klare Anweisung Zehntausende zu überweisen. Alles wirkt real. Doch die Teilnehmer sind KI-generierte Deepfakes. **Nur Sie sind echt.**

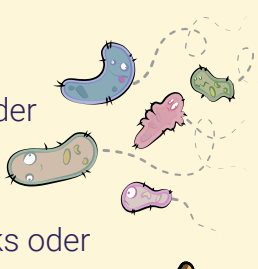
Diese Beispiele zeigen: Cyberangriffe spielen längst auf der menschlichen Ebene. Sie setzen nicht mehr allein auf technische Schwachstellen, sondern auf **Täuschung, Vertrauen und Zeitdruck.**



Was fällt unter Cyberangriffe?

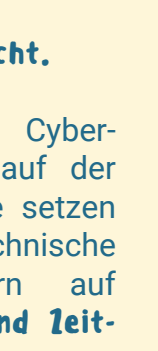
Cyberangriffe sind vielfältig. Neben klassischem Hacking über Schadsoftware oder das Ausnutzen von Sicherheitslücken gibt es zunehmend Angriffe, die direkt den Menschen ins Visier nehmen.
Typische Methoden sind:

Phishing und Spear-Phishing:
Täuschend echte E-Mails oder Nachrichten, die sensible Daten abfragen oder schädliche Links enthalten.



Vishing (Voice-Phishing):
Betrugsanrufe, bei denen Angreifer vorgeben, Support oder Bankangestellte zu sein.

Smishing:
Manipulative SMS oder Messenger-Nachrichten mit Links oder Aufforderungen zu Datenweitergaben.



SIM-Swapping:
Angreifer übernehmen Ihre Mobilfunknummer, indem sie eine Ersatz-SIM auf ihren Namen aktivieren lassen.

Business E-Mail Compromise (BEC):
Gefälschte E-Mails im Namen von Führungskräften mit dem Ziel, Überweisungen oder sensible Informationen zu erschleichen.

Deepfakes:
KI-generierte Stimmen und Videos, die täuschend echt erscheinen und in Meetings oder Anrufen eingesetzt werden.

Was macht Cyberangriffe so gefährlich?

1. Soziale Manipulation statt klassischem Hacking:
Firewalls und Antivirenprogramme können ausgetrickst werden, wenn Menschen manipuliert werden.

2. Datenschutz im Fokus: Bereits scheinbar harmlose Daten wie Telefonnummern, E-Mail-Adressen oder Mitgliedsnummern gelten nach der DSGVO als personenbezogen und sind schützenswert.

3. Unmittelbare Auswirkungen: Gestohlene Daten, gestörte Lieferketten oder Millionenverluste sind keine Seltenheit.

Typische Angriffsmethoden im Überblick

Helpdesk-Manipulation: Angreifer überzeugen den IT-Support, Passwörter zurückzusetzen, unterstützt durch SIM-Swapping.

Gefälschte Support-Anrufe: Angreifer geben sich als IT-Mitarbeitende aus, um zum Herunterladen von Schadsoftware zu verleiten.

Deepfake-Betrug: KI-generierte Videokonferenzen, in denen Führungskräfte imitiert wurden, um Überweisungen zu erschleichen.

Wie können Sie sich schützen?

1. Eindeutige Verifikationsprozesse: Passwort-Resets nur nach strenger Prüfung, z. B. durch Rückruf über bekannte Nummern oder Multi-Faktor-Authentifizierung über unabhängige Kanäle.

2. Regelmäßige Sensibilisierung: Schulungen zu Social Engineering, Deepfakes und gefälschten Support-Anfragen - praxisnah und wiederholt.

3. Klare interne Kommunikation: Fest verankern und bekannt machen: „Wir fragen niemals per Telefon, Teams oder SMS nach Passwörtern. Offizielle Anfragen laufen ausschließlich über definierte Support-Kanäle.“

4. Schnelles Handeln im Ernstfall: Verdächtige Anrufe, Nachrichten oder Videokonferenzen sofort der IT-Sicherheit melden und alle Details dokumentieren.

Fazit: Die letzte Verteidigungslinie sind Sie!

Cyberangriffe sind längst Teil des Alltags – und sie zielen auf das schwächste Glied: den Menschen. Sie setzen auf Vertrauen, Täuschung und Zeitdruck. **Wer klare Prozesse etabliert, seine Mitarbeitenden kontinuierlich sensibilisiert und offizielle Kommunikationswege absichert, macht die Organisation widerstandsfähig.**

So wird aus einem scheinbar harmlosen Anruf oder einer täuschend echten Videokonferenz kein millionenschwerer Sicherheitsvorfall.

Dr. Bittner Consulting
GmbH & Co. KG

Podbielskistraße 386
30659 Hannover

Servicenummer: 0800 88446688
E-Mail: office@drbg.de

DR. BITTNER GROUP