

Quishing, Smishing & Co.

Die unterschätzten Einfallstore in die
medizinische Infrastruktur

Torsten Herbert, sepp.med gmbh

Wir machen Digitalisierung – aber sicher!

- Software-Entwicklung
- QS & Test
- Security
- Beratung
- Akademie



sepp.med ist mehr als nur ein Dienstleister: Wir sind strategischer Partner

Unsere Kernkompetenzen:

- Softwareentwicklung im regulierten Umfeld
- Qualitätssicherung und Softwaretest
- IT-Sicherheit und Software Security
- Regulatorische Beratung
- Schulungen und Trainings

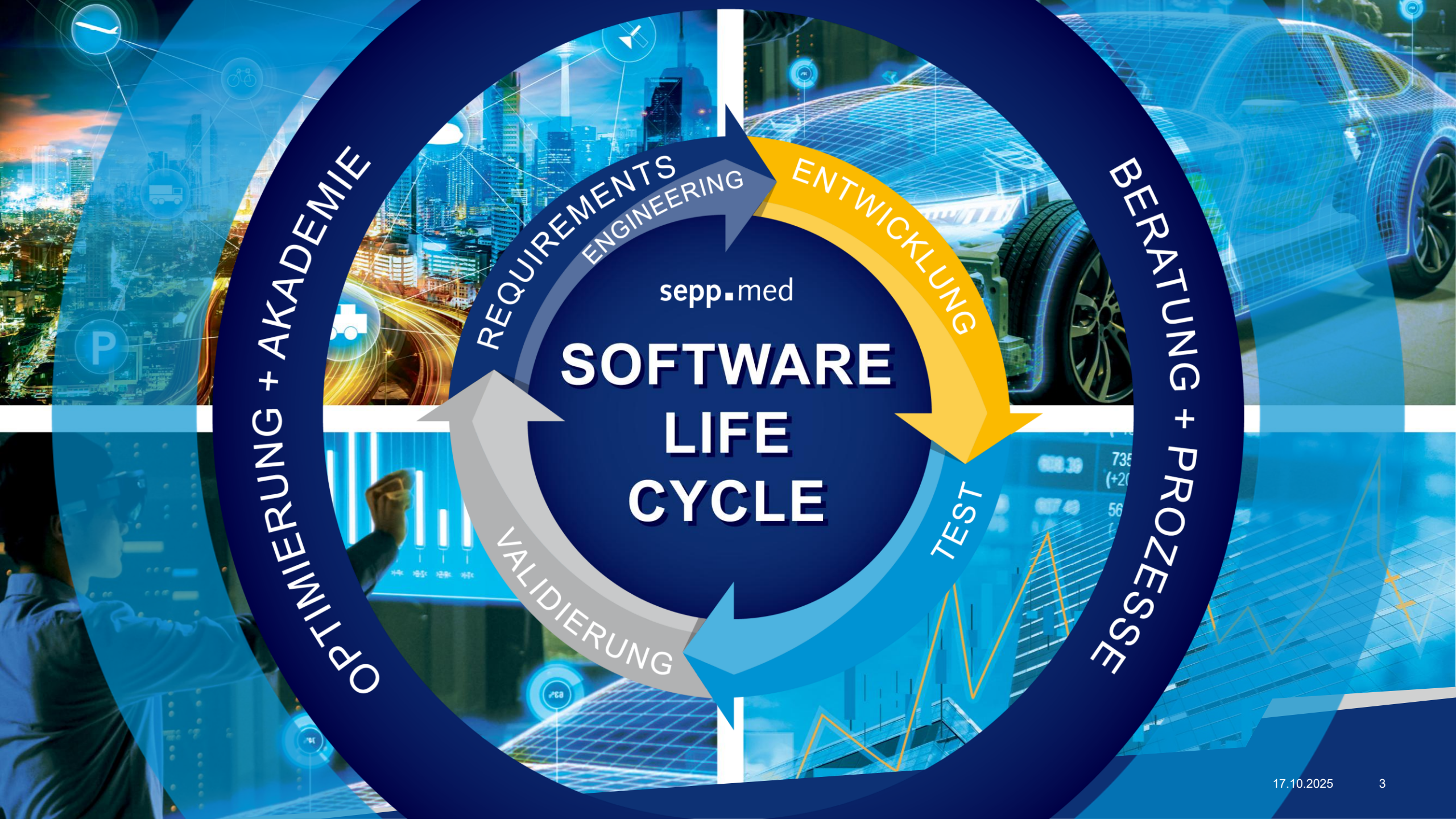
Beratungshaus

Toolhersteller

IT-Dienstleister



**Familienunternehmen
Inhabergeführt
Mittelständler**



sepp.med

**SOFTWARE
LIFE
CYCLE**

REQUIREMENTS
ENGINEERING

ENTWICKLUNG

TEST

VALIDIERUNG

OPTIMIERUNG + AKADEMIE

BERATUNG + PROZESSE

Wir stehen für ausgezeichnete Expertise

■ im industriellen Umfeld:

- Medizintechnik, Sport & Lifesciences
- Automotive, Avionik, Automation & Train
- Anlagenbau und IoT

■ im administrativen Umfeld:

- Öffentlicher Sektor
- Finanzindustrie und Versicherungen

■ für unsere Kunden:

- DAX- & MDAX-Unternehmen
- Global Player
- Mittelstand der DACH-Region
- Öffentliche Verwaltung



Mit über 150 Mitarbeiter vor Ort, remote, verlässlich

- **Ihr Ansprechpartner:**
 - ein Single Point of Contact
- **Teams und Personen:**
 - Projektleiter & POs
 - Agile Coaches & Scrum Master
 - Architekten & Business Analysten
- **Branchenübergreifende Experten:**
 - Software-Experten
 - QS-Experten
 - DevOps-Experten
 - Consultants & Trainer für Normen & Security



Wir sind mehr als
ein Lieferant –
**wir sind
strategischer
Partner!**

Quishing, Smishing & Co.

Die unterschätzten Einfallstore in die
medizinische Infrastruktur

Torsten Herbert, sepp.med gmbh

Wir machen Digitalisierung – aber sicher!

- Software-Entwicklung
- QS & Test
- Security
- Beratung
- Akademie



**Alles, was getan wird, ist es Wert,
gut getan zu werden.**

Aristoteles, 384-322 v. Chr.

Agenda

Einführung: Warum Social Engineering unterschätzt wird

Moderne Angriffstechniken: Phishing, Quishing, Smishing, Vishing

Praxisbeispiele: Aktuelle Angriffe in der Medizinbranche

Live Demonstration: Wie Quishing-Angriffe funktionieren

Präventionsstrategien: Technisch, organisatorisch, menschlich

Zusammenfassung: Was nehme ich aus dem Vortrag mit?



Einführung



Einführung

Fokus auf technische Sicherheit

Unternehmen setzen zum Schutz ihrer digitalen Ressourcen auf Firewalls, Zero Trust, Netzwerksegmentierung und MFA.

Der Mensch als Angriffsvektor

Angreifer nutzen menschliches Verhalten aus, um technische Sicherheitsvorkehrungen zu umgehen, was ein erhebliches Risiko darstellt.



Einführung

Moderne Social-Engineering-Techniken

Techniken wie Phishing, Quishing, Smishing und Vishing ermöglichen es Angreifern, ihre Opfer direkt und effektiv zu manipulieren.

Bewusstseinsbildung

Das Verständnis dieser Social-Engineering-Methoden hilft, Angriffe ohne Malware oder Exploits zu verhindern.



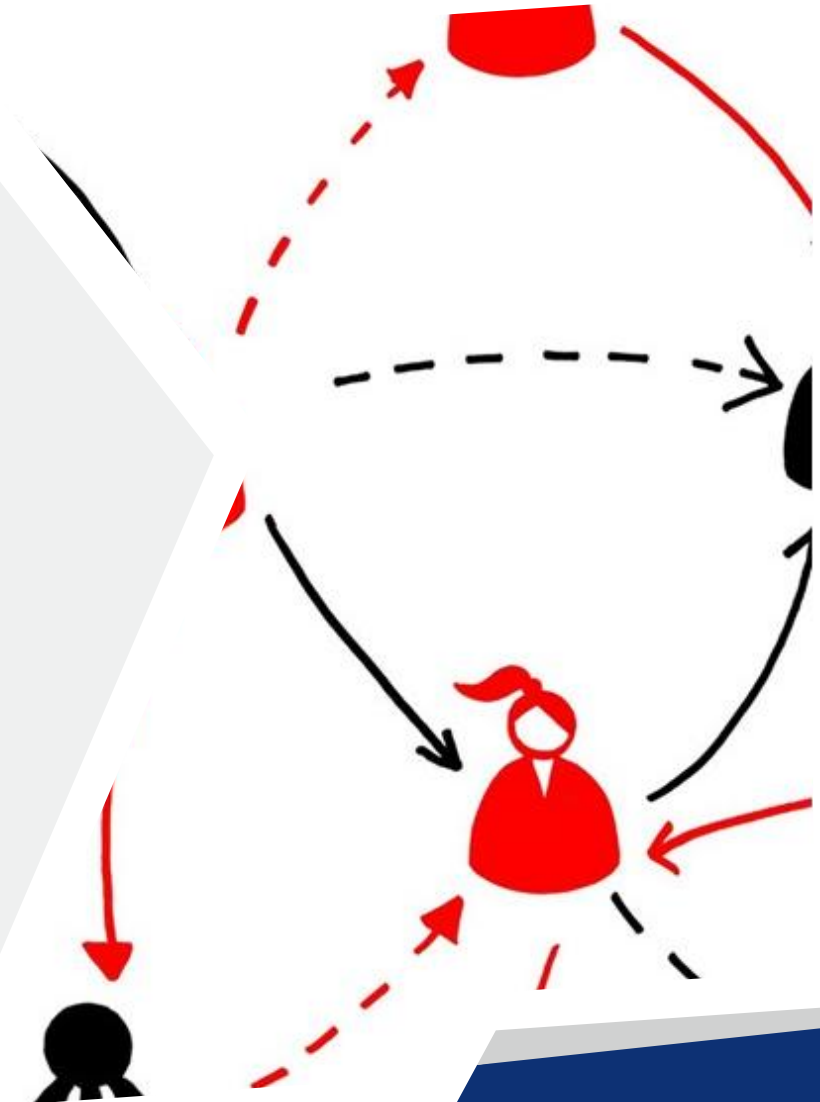
Social Engineering: Der Mensch als Ziel

Ausnutzung menschlichen Verhaltens

Social Engineering nutzt menschliches Verhalten durch Vertrauensbildung, Neugierde und Routinehandlungen aus, um sich vertraulichen Zugang zu verschaffen.

Ausgefeilte Angriffstechniken

Angreifer verwenden realistische E-Mails, QR-Codes, SMS und Anrufe, um Mitarbeiter dazu zu verleiten, sensible Daten preiszugeben oder auf bösartige Links zu klicken.



Psychologische Tricks im Social Engineering

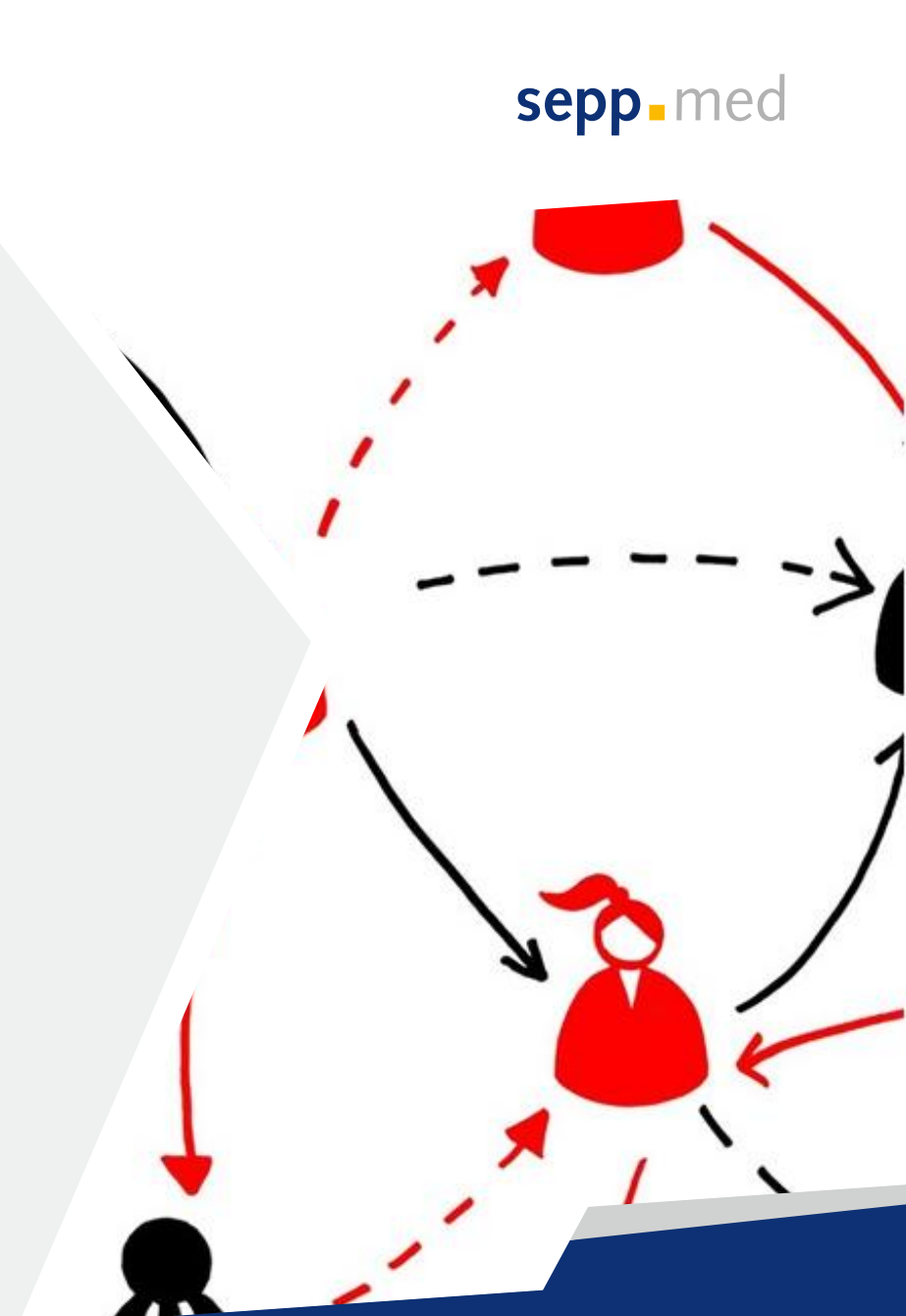
Autorität: Angreifer geben sich als Vorgesetzte, IT-Admins oder Behörden aus.

Dringlichkeit: Zeitdruck erzeugt Stress und senkt die Hemmschwelle.

Knappheit: „Nur heute verfügbar“ – Nutzer handeln unüberlegt.

Reziprozität: Kleine Gefälligkeiten erzeugen unbewusste Verpflichtung.

Soziale Bewährtheit: „Alle anderen haben es auch gemacht.“



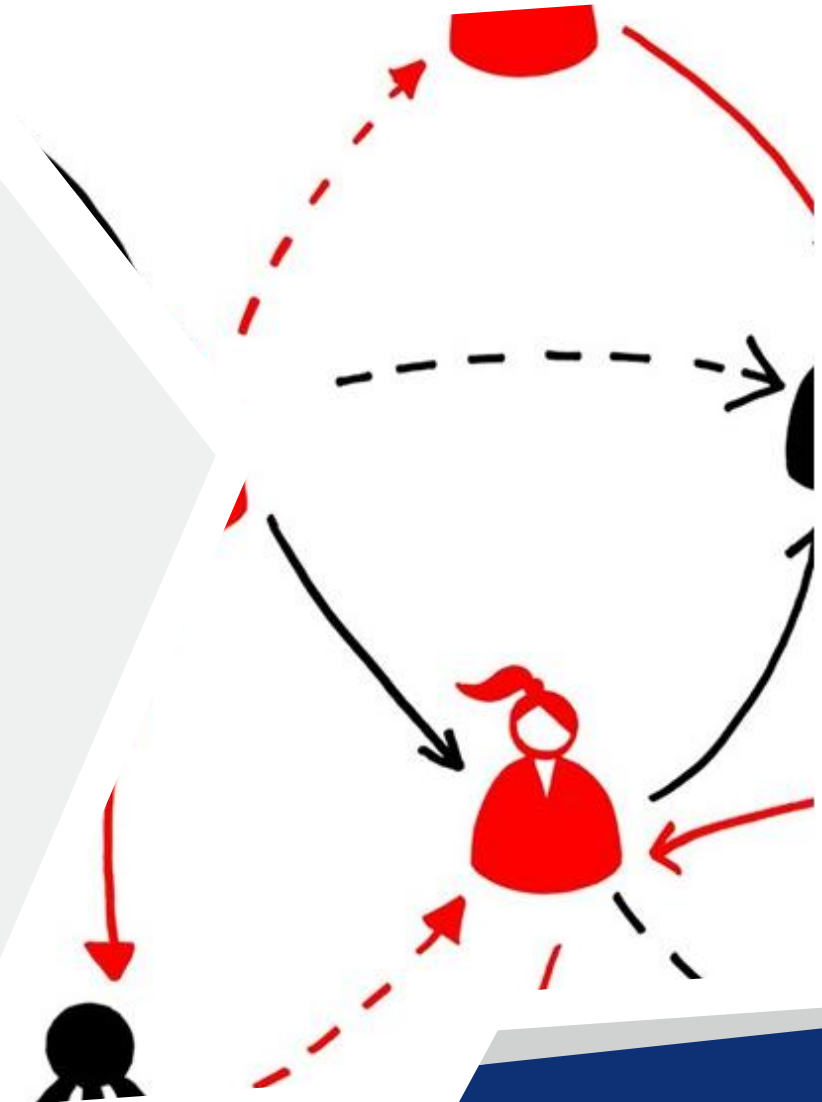
Social Engineering: Der Mensch als Ziel

Risiken in medizinischen Einrichtungen

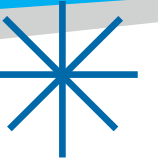
Social-Engineering-Angriffe in medizinischen Einrichtungen gefährden sensible Patientendaten und erfordern integrierte Sicherheitsansätze.

Bedeutung des menschlichen Faktors

Sicherheitsstrategien müssen sowohl technische und organisatorische als auch menschliche Schwachstellen berücksichtigen, um Social-Engineering-Angriffe wirksam zu verhindern.



Moderne Angriffstechniken



Phishing – Die klassische Methode

Definition Phishing

Neologismus und Kompositum von „*fishing*“, engl. für „Angeln“ und „phreaking“ für „Hacken“.

Umsetzung und Vorgehen

Betrugsversuche per E-Mail, die Nutzer dazu bringen sollen, auf schädliche Links zu klicken oder vertrauliche Daten preiszugeben.



Quishing: Phishing via QR-Code



Quishing-Angriffsmethode

Quishing nutzt manipulierte QR-Codes als Phishing-Vektoren, um Nutzer auf gefälschte Websites umzuleiten.

Schwierigkeit der Erkennung

QR-Codes sind visuell schwer zu überprüfen, was Manipulationen erleichtert und den Erfolg von Angriffen erhöht.

Smishing & Vishing: SMS and Telefon Attacken

Smishing per SMS

Beim Smishing werden gefälschte SMS-Nachrichten verwendet, um Nutzer dazu zu verleiten, persönliche Daten preiszugeben oder auf bösartige Links zu klicken.

Vishing per Telefon

Beim Vishing wird in einem Telefonanruf durch einen Angreifer eine falsche Rolle eingenommen. Im Gespräch wird versucht das Vertrauen zu gewinnen, als auch zeitlichen Druck aufzubauen.



Ziele und Risiken von Social-Engineering-Angriffen

Angreiferziele	Risiken für Einrichtungen
Diebstahl von Zugangsdaten	Unbefugter Zugriff auf Patientendaten
Identitätsmissbrauch	Betriebsunterbrechung
Zugang zu internen Systemen	Vertrauensverlust bei Patienten

„Laut BSI-Bericht 2024 sind 30 % der Vorfälle im Gesundheitswesen auf Social Engineering zurückzuführen.“



Auswirkungen erfolgreicher Angriffe

Patientensicherheit gefährdet: Manipulierte Daten können zu Fehlbehandlungen führen.

Reputationsverlust: Vertrauensverlust bei Patienten und Partnern.

Rechtliche Konsequenzen: DSGVO-Verstöße, Bußgelder, Haftungsfragen.

Betriebsunterbrechungen: IT-Ausfälle durch Ransomware oder Datenverlust.

Kosten: Wiederherstellung, Forensik, rechtliche Beratung, Imagekampagnen.



Deepfakes & KI im Social Engineering

Deepfake-Anrufe

Stimmen von Vorgesetzten oder Ärzten werden imitiert.

KI-generierte E-Mails

Täuschend echte Texte, angepasst an Zielperson.

Gefahr: Hohe Glaubwürdigkeit, schwer zu erkennen.



Praxisbeispiele



Praxisbeispiele

Manipulation von QR-Codes

Angreifer veränderten den QR-Code eines Krankenhausplakats, um Mitarbeiter auf eine gefälschte Anmeldeseite umzuleiten und so Anmeldedaten zu stehlen.

Phishing per SMS

Benutzer erhielten betrügerische SMS mit gefälschten Paketlinks, die zu Phishing-Websites weiterleiteten.

Betrug durch Identitätsdiebstahl am Telefon

Ein Angreifer gab sich als IT-Support aus, um einen Mitarbeiter dazu zu bringen, sein Passwort zu ändern und preiszugeben.

Oder die Betrüger gaben sich als Beamte aus und versuchen, sensible Informationen zu erlangen oder Geldzahlungen zu veranlassen.



Praxisbeispiele

Beispiel 1:

Ein Angreifer ruft als „IT-Support“ an, verweist auf ein angebliches Sicherheitsproblem und fordert zur sofortigen Passwortänderung auf – inklusive Weitergabe des neuen Passworts.

Beispiel 2:

Ein Krankenhaus in Deutschland musste nach einem Ransomware-Angriff ausgelöst durch Weitergabe eines Benutzeraccounts inklusive Passwort mehrere Tage den Betrieb einschränken – geplante Operationen wurden verschoben.

Beispiel 3: CEO-Fraud mit KI-generierter Stimme – Mitarbeiter überweist 200.000 €.



Praxisbeispiele

https://www.mathias-jaekel.de/it/beispiele-fuer-phishing-mails-galerie/#Gut_gemachte_Phishing_Mails_-_Galerie

The collage displays four phishing emails with red arrows highlighting key elements:

- Vodafone Email:**
 - Allgemeiner Betreff:** Bestätigungshinweis 03-06-2020
 - Absender:** Vodafone-team <emurueta@dientes.euskaltel.es>
 - Inhalt:** Ihr Vodafone-Team, Sie bekommen mit dieser E-Mail wichtige Informationen zu Ihrem...
 - fehlendes Impressum:** This email was automatically sent to you. Please do not click on "Antworten" or "Reply" in your E-Mail program!
- DHL Email:**
 - Header:** Ihr Paket wurde zurückgeschickt
 - Content:** Diese Sendung wird abgewickelt von: DHL Express letzte Mahnung. Lieber Kunde, Ihr Paket konnte am 03.03.2023 nicht geliefert werden, da kein Zoll bezahlt wurde (9.89 EUR)...
 - Action:** Jetzt Bestätigen
- DKB Email:**
 - Header:** DKB - Bitte aktivieren Sie das neue Sicherheitssystem
 - Content:** Sehr geehrter Kunde, Ab dem 15. Juni 2022 können Sie Ihre Karte nicht mehr verwenden, wenn Sie das neue Web-Sicherheitssystem nicht aktiviert haben...
 - Action:** Klicken Sie hier
- PayPal Email:**
 - Header:** Von: "Sicherheitsteam" <sicherheitsbenachrichtigung@gmx.de>
 - Content:** Sehr geehrte Kundin, sehr geehrter Kunde, aufgrund geänderter Nutzungsbedingungen steht eine Aktualisierung Ihrer Daten an...
 - Action:** Weiter zu PayPal

Praxisbeispiele

Telefon (Vishing) - Rollenspiel

Guten Tag, hier ist Anna Müller (IT).

Wir haben Sicherheitswarnungen bei Ihrem Account.

Ich benötige Ihre Benutzer-ID und einen SMS-Code zur Verifizierung.

Nennen Sie bitte kurz Ihren Benutzernamen.



Live- Demonstration



Live-Demonstration

Aufruf der demo_quishing_beispiel.html Seite über einen QR Code:

**Klinikum Musterstadt – Patientenportal**
Sicherer Zugang zu Befunden & Terminen

Kontakt IT: +49 123 456 789
Hotline: it-support@klinikum-muster.de

Anmeldung – Patientenbereich

Bitte melden Sie sich mit Ihrem Benutzernamen und Passwort an, um Untersuchungsergebnisse und Termine zu sehen.

Benutzername

Passwort

Anmelden

Schnellzugriff

Befunde prüfen
Zugang über Ihr Patientenportal

Kontakt & Sicherheit
Bei Unsicherheit: IT-Hotline anrufen oder Formular bei Empfang abgeben.

© Klinikum Musterstadt / sepp.med – Demo



Ersatz-Demonstration

Welcher QR-Code ist Quishing, welcher ist echt?

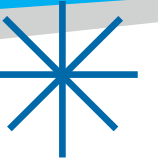
1)



2)



Präventions- und Abwehrstrategien



Prävention- und Abwehrstrategien

Technische und psychologische Bedrohung

Die Kombination aus einfachen Techniken und psychologischen Tricks macht diese Angriffe zu äußerst wirksamen Bedrohungen.

Notwendigkeit von Schutzmechanismen

Diese Fälle unterstreichen die Notwendigkeit, sowohl technische als auch menschliche Abwehrmaßnahmen gegen Social-Engineering-Angriffe zu etablieren.

Umfassender Sicherheitsansatz

Ganzheitlicher Ansatz mit Integration von Technologie, der Organisation und menschlichen Faktoren gewährleistet einen robusten Schutz der Infrastrukturen, Unternehmen und der Menschen.



Strategien zur Abwehr

Technische Abwehrmaßnahmen

E-Mail-Filter, Anruferkennung und SMS-Check erkennen und verhindern Social-Engineering-Angriffe frühzeitig.

Sicheres Scannen von QR-Codes

Die Verwendung von QR-Code-Scannern mit integrierten Sicherheitsprüfungen verhindert das unbemerkte Scannen manipulierten Codes.

Authentifizierung für die Kommunikation

Die Implementierung einer Authentifizierung für Emails, SMS und Anrufe überprüft die Identität des Absenders und Gesprächspartners, um Betrug noch rechtzeitig zu verhindern.



Strategien zur Abwehr

Organisatorische Prozesse

Klare Prozesse und Richtlinien zur Reaktion auf Vorfälle (Incidents), für Notfallpläne und zu Eskalationswege stärken die Abwehr von Angriffen.

Aufklärungskampagnen

Regelmäßig aktualisierte Kampagnen sensibilisieren für Social Engineering und passen sich aktuellen Bedrohungen effektiv an.



Erste-Hilfe-Workflow

1 Ruhe bewahren

Gibt die Person vor, von einem Unternehmen zu sein?

Lassen Sie sich im Zweifelsfall von dem Unternehmen bestätigen, dass es sich um einen echten Kontakt handelt.



2 Zeit nehmen

Setzt man Sie unter Druck? **Übermäßige Dringlichkeit** ist ein **Warnsignal**, nehmen Sie sich die Zeit, um alles zu überdenken.



3 Unabhängig prüfen

Fordert die Person sensible Daten?

Lassen Sie sich nicht zu einer Herausgabe drängen und rufen Sie stattdessen die Website direkt auf.



4 Nicht anklicken

Öffnet ein Link eine Nachricht? Nehmen Sie **Kontakt zum IT-Support auf**, bevor Sie auf den Link tippen.



Prävention und Sensibilisierung

Effektive Maßnahmen

Eine effektive Prävention und Sensibilisierung erfordert eine Kombination aus strategischen Ansätzen und praxisnahen Methoden.

Mitarbeiter-Awarenesstraining

Regelmäßige Schulungen mit realistischen Szenarien und Mustern helfen den Mitarbeitern, Social-Engineering-Angriffe zu **erkennen** und angemessen darauf zu **reagieren**.



Prävention und Sensibilisierung

Phishing-Tests und Berichterstattung

Regelmäßige Phishing-Tests und klare Berichterstattungskanäle verbessern das Sicherheitsbewusstsein und die Sicherheitskultur.

Fehlerkultur vs. Sicherheitskultur

Eine offene Fehlerkultur, in der Fehlverhalten nicht sanktioniert, sondern als Lernchance genutzt wird, trägt ebenfalls zur Stärkung der Sicherheitskultur bei.



Prävention und Sensibilisierung

Gamification & Nudging in der Awareness

- **Gamification:** Interaktive Lernformate, z. B. Phishing-Quiz, Escape Rooms.
- **Nudging:** Sanfte Verhaltenslenkung durch visuelle Hinweise oder Default-Einstellungen.
- **Vorteile:** Höhere Motivation, bessere Erinnerung, nachhaltiger Lerneffekt, stärkere Akzeptanz.

Beispiel:

Ein Krankenhaus führt monatliche Mini-Challenges durch („Phishing-Mail erkennen“) mit kleinen Belohnungen – die Melderate verdächtiger Mails stieg um 60 %.



Zusammen- fassung



Nur ein Pflaster drauf reicht nicht!



Handlungsempfehlungen

Risikobewertung durchführen: Wo sind menschliche Schwachstellen?

Awareness-Programme etablieren: Regelmäßige Schulungen & Tests.

Technische Schutzmaßnahmen ergänzen: QR-Code-Scanner, E-Mail-Filter, MFA.

Notfallpläne definieren: Was tun im Ernstfall? Probelauf !

Kultur fördern: Offenheit, Transparenz keine Schuldzuweisungen bei Falschmeldungen.



Was nehme ich aus dem Vortrag mit?

01

**Technische Maßnahmen
sind wichtig.**

02

**Ergänzt um Organisatorische
Maßnahmen.**

03

**Menschliche Aufmerksamkeit
ist entscheidend.**

04

**Regelmäßig Awareness-
Maßnahmen durchführen.**

05

**Notwendiges Wissen und
Qualifikation aufbauen.**

Was soll gemacht werden,
Wie soll es gemacht werden,
Zukunftsfrage,
Testbarkeit

**Anforde-
rungen**

**Software-
entwicklung**

Architektur
und Design,
Wartbarkeit,
Testbarkeit,
Performance
und Skalierbarkeit

**Qualitäts-
sicherung
und Test**

Überprüfung
und Sicherstellen,
Verifikation,
Validierung,
Automatisierung,
Security-Testing,
App-Testing

Ausbildung

Technische Ausbildung,
Domainspezifische Ausbildung,
Social Skills,
Lebenslanges Lernen

**Regula-
torische
Beratung**

SPICE,
MDR,
Gamp5,
Security,
Safety

Portfolio sepp.med GmbH



Vielen Dank!

**Torsten Herbert,
Teamlead Medical Engineering, Integrations-/Systemtest**

Tel.: +49 (0) 171-2756131

E-Mail: torsten.herbert@seppmed.de

LinkedIn: [linkedin.com/in/torsten-herbert-13969714b](https://www.linkedin.com/in/torsten-herbert-13969714b)

www.seppmed.de

