CGM CompuGroup Medical

Wissenswertes zur IT-Sicherheit

in Arztpraxen

Phishing

Definition

Phishing ist eine betrügerische Methode, bei der Angreifer versuchen, persönliche Informationen wie Passwörter, Kreditkartennummern oder andere vertrauliche Daten zu erlangen. Dies geschieht häufig über geschickt gefälschte E-Mails, Websites oder Nachrichten.

Cyberkriminelle nutzen menschliche Verhaltensweisen und Emotionen, um ihre Opfer zur Herausgabe von sensiblen Informationen zu manipulieren, z. B. indem sie ein Gefühl der Dringlichkeit vermitteln, sich als vertrauenswürdige Institutionen ausgeben, Neugierde wecken („Sie haben gewonnen!“) oder mit negativen Konsequenzen (z. B. Kontosperrung) drohen.

Diese psychologische Manipulation macht Phishing so erfolgreich.

Arten
von Phishing

Spear Phising

Gezielte Angriffe auf bestimmte Personen oder Unternehmen. Die Angreifer personalisieren ihre Nachrichten, um glaubwürdiger zu wirken.

Whaling

Eine Form des Spear Phishing, die sich speziell an hochrangige Führungskräfte oder Entscheidungsträger richtet.

Vishing (Voice Phishing)

Telefonanrufe, bei denen Betrüger versuchen, Informationen von Opfern zu erhalten, indem sie sich als vertrauenswürdige Institution ausgeben.

Smishing (SMS Phishing)

Betrügerische SMS-Nachrichten, die darauf abzielen, Benutzer zur Weitergabe persönlicher Daten zu verleiten oder sie auf schädliche Links zu klicken.

QR Code Phishing

Gefälschte QR-Codes führen zu bösartigen Websites, über die Angreifer persönliche Informationen stehlen können.

Ziele
von Phishing

Datenklau

Diebstahl sensibler Informationen wie Passwörter, Kreditkartennummern oder persönliche Identifikationsdaten.

Finanzieller Betrug

Durchführung unbefugter Transaktionen durch Zugriff auf Bankkonten oder Zahlungsinformationen.

Malware-Verbreitung

Verbreitung von Schadsoftware, die Systeme infiziert und Daten kompromittiert.

Identitäts-Diebstahl

Mit gestohlenen Informationen können Angreifer Identitäten übernehmen und in deren Namen Betrug begehen.

Zugriff auf Konten

Angreifer zielen darauf ab, auf soziale Medien, E-Mail-Konten oder andere Online-Dienste zuzugreifen.

Prävention
Vor Angriffen schützen

E-Mail-Überprüfung

Überprüfen Sie Absenderadressen oder Telefonnummern – oft sind diese leicht verändert! Achten Sie auf Rechtschreibfehler in E-Mails und misstrauen Sie stets unerwarteten Anfragen nach persönlichen Informationen.

Think before you click

Warnungen, die sofortiges Handeln erfordern, sind verdächtig! Vertrauenswürdige Unternehmen fordern niemals sensible Informationen per E-Mail oder SMS an.

Links vorsichtig behandeln

Bewegen Sie den Mauszeiger zunächst über Links, um die Ziel-URL anzuzeigen, bevor Sie klicken. Gehen Sie direkt zur Website, anstatt Links in E-Mails zu folgen.

Dateianhänge

Dateianhänge in Phishing-E-Mails sind häufige Mittel zur Verbreitung von Malware: Bleiben Sie misstrauisch, vor allem bei unerwarteten Dateien von bekannten Kontakten.

Prävention
Vor Angriffen schützen

Zwei-Faktor-Authentifizierung

Aktivieren Sie die Zwei-Faktor-Authentifizierung um eine zusätzliche Sicherheitsebene hinzuzufügen.

Aktualisierung von Software

Achten Sie darauf, dass Betriebssysteme, Browser und Anwendungen stets auf dem neuesten Stand sind, um Sicherheitslücken zu schließen.

Misstrauen gegenüber Dringlichkeit

Seien Sie vorsichtig bei E-Mails, die zur sofortigen Handlung drängen oder drohen, sonstige Maßnahmen zu ergreifen.

Prüfe QR-Codes kritisch

Überprüfen Sie die URL nach dem Scannen, bevor Sie klicken oder Informationen eingeben. Achten Sie darauf, dass die URL vertrauenswürdig aussieht und mit HTTPS beginnt, um zusätzliche Sicherheit zu gewährleisten.

Passwörter
und Passphrases

Starke Passwörter schützen

Cyberkriminelle haben es besonders auf Passwörter abgesehen, denn mit diesen erhalten sie Zugriff auf Benutzerkonten, Systeme und vertrauliche Informationen.

Bei einem sogenannten Brute-Force-Angriff versuchen Angreifer, Passwörter systematisch zu erraten, indem sie mögliche Kombinationen testen. Starke Passwörter, die lang und komplex sind und darüber hinaus zufällige Zeichenkombinationen enthalten, machen diese Angriffe weniger effektiv und unwirtschaftlich.

Die Verwendung starker, einzigartiger Passwörter für verschiedene Konten hilft, die Auswirkungen eines einzelnen kompromittierten Passworts zu minimieren. Wenn ein Passwort bei einem Dienst gehackt wird, können Angreifer nicht einfach dieselben Zugangsdaten bei anderen Diensten verwenden.

Passwörter
oder Passphrase?

Der Hauptunterschied liegt in der Länge und der Zusammensetzung!

Passwort

- typischerweise kürzere Zeichenfolge, aus Buchstaben, Zahlen und Sonderzeichen bestehend.
- oft zwischen 8 und 12 Zeichen lang.
- basierend auf einem einzigen oder wenigen Wörtern.

Beispiele:

P@ssw0rd, R@nd0m123, Schalke04

Passphrase

- längere Zeichenkette, die aus mehreren Wörtern besteht.
- Wörter können zusammenhängend sein und einen ganzen Satz bilden.
- leichter zu merken als komplexe Passwörter!

Beispiele:

Th3QuickBrowNf0xJump$, S3cur3PhrasesAreSup3rior

Do’s & Dont’s
in Bezug auf Passwörter

- Passwörter sollten min. 12 Zeichen lang und komplex sein.
- ab 25 Zeichen reicht es, zwei Zeichenarten zu verwenden.
- Verwenden Sie möglichst alle verfügbaren Zeichen, inkl. Groß- und Kleinschreibung, Sonderzeichen & Ziffern!
- Zwei-Faktor-Authentifizierung, wo es möglich ist!

- Verwenden Sie keine bekannten oder persönlichen Informationen (Geburtsdatum, Name).
- Auf gängige Wiederholungs- und Tastaturmuster wie 1234 oder 666 verzichten.
- Ergänzen Sie das Passwort nicht nur mit einem Sonderzeichen am Anfang oder Ende.
- Das vollständige Passwort sollte nicht in einem Wörterbuch vorkommen.

Best Practices
Passwor-Management

Passphrasen statt Passwörter

Passphrasen sind besser, weil sie länger und damit schwieriger zu knacken sind. Sie bestehen aus einer Reihe von leicht zu merkenden Wörtern, was sie sicherer und einfacher zu merken macht.

Aktiver 2FA

Zusätzliche Sicherheitsebene: Neben einem Passwort sollte man einen zweiten Bestätigungsfaktor (Zwei-Faktor-Authentifizierung) eingeben. Dies macht es schwieriger für jemanden, unerlaubten Zugriff auf deine Konten zu erhalten.

Passwort-Manager

Passwort-Manager generieren komplexe Passwörter und speichern diese verschlüsselt, sodass man sich diese nicht merken musst.

Tipp: KeePass ist ein kostenloser Passwort-Manager für alle, die Passwörter lokal und ohne Cloud speichern möchten.

Social Engineering

Definition

Social Engineering bezeichnet gezielte Manipulationsversuche, bei denen Angreifer psychologische Tricks einsetzen, um Menschen zu bestimmten Handlungen zu bewegen – etwa dazu, vertrauliche Informationen preiszugeben oder Sicherheitsvorgaben zu umgehen.

Dabei nutzen sie häufig Vertrauen, Hilfsbereitschaft oder soziale Beziehungen aus. Im Gegensatz zu technischen Angriffen zielt Social Engineering nicht auf IT-Systeme ab, sondern direkt auf das Verhalten der Nutzer.

Social Engineering
typische Methoden & Kanäle

Phishing

gefälschte E-Mails oder Nachrichten mit dem Ziel, persönliche Daten zu stehlen. **Via E-Mail, SMS (Smishing), Instant Messaging, soziale Netzwerke.**

Vishing

Gefälschte Telefonanrufe, teilweise mittels KI-gestützter Sprachsynthese. **Via Telefon.**

Baiting

Lockangebote (z. B. geschenkte USB-Sticks mit Malware) werden verwendet, um Nutzer zu verleiten. **Via physischer Medien (z.B. USB-Sticks, Online-Werbung).**

Pretexting

Angreifer geben sich als vertrauenswürdige Person aus und erstellen einen Vorwand, um Informationen zu erhalten. **Via Telefon, E-Mail.**

Tailgaiting

Physisches Nachfolgen einer autorisierten Person in gesicherte Bereiche, um unbefugten Zugriff zu erlangen. **Via physischer Umgebung (z.B. Büro-Gebäude).**

Die Psychologie
hinter Social Engineering

Cyberkriminelle nutzen gezielt menschliche Emotionen und Verhaltensmuster, um ihre Opfer zu manipulieren:

- Häufig geben sich Angreifer als vertrauenswürdige Personen aus, um das Vertrauen ihrer Opfer zu gewinnen.

- Sie bringen ihre Opfer dazu, impulsiv zu handeln, indem menschliche Emotionen erzeugt werden: etwa Angst, Stress, Neugierde oder soziale Beeinflussung.

Insgesamt kombinieren Social Engineering-Techniken verschiedene Emotionen, um Menschen zu beeinträchtigen und sie dazu zu bringen, gegen ihre eigenen Interessen zu handeln.

Erkenne
Social Engineering Angriffe.

Ungewöhnliche Anfragen

E-Mails oder Anrufe, die ungewöhnliche Anfragen enthalten, wie dringende Geldüberweisungen oder die Freigabe sensibler Informationen.

Dringlichkeit und Druck

Angreifer nutzen oft Zeitdruck und Dringlichkeit, um das Opfer zu überstürzten Maßnahmen zu bewegen.

Auffällige Kommunikation

Etwa übertrieben freundlich oder auch übermäßig einschüchernd. Auch Sprach- oder Grammatikfehler sind möglich und sollten stutzig machen.

Falsche Identität

Anfragen von Personen, die sich als Mitarbeiter, Kunden oder Dienstleister ausgeben, ohne ausreichenden Kontext oder Glaubwürdigkeit.

Multi-Channel
Angriffe

Die Entwicklung geht hin zu sogenannten **Multi-Channel-Angriffen.**

Multi-Channel-Angriffe sind Attacken, bei denen Cyberkriminelle mehrere Kommunikationskanäle gleichzeitig nutzen, um die Wahrscheinlichkeit eines erfolgreichen Angriffs zu erhöhen!

Diese Kanäle können E-Mail, Telefon, Teams-Chat, soziale Medien und andere digitale Kommunikationsmittel umfassen.

Um sich vor Multi-Channel-Angriffen zu schützen, sollte man immer mehrschichtige Sicherheitsmaßnahmen implementieren.

Social Engineering
Prävention.

Sensibilisierung und Schulung

Regelmäßige Trainings können helfen, potenzielle Angriffe und Manipulationsversuche zu erkennen.

Verifikation

Verifiziere Identitiäten und Anfragen. Implementiere Zwei-Faktor-Authentifizierung, wo immer möglich, um zusätzliche Sicherheitsebenen zu schaffen.

Einschränkung des Zugriffs

Minimieren Sie den Zugang zu sensiblen Informationen und Systemen auf diejenigen, die diese unbedingt benötigen.

Im „BSI für Bürger“ und auf der IT-Sicherheitsseite der KBV finden Sie aktuelle Warnungen und Praxistipps – bleiben Sie informiert:

- www.bsi-fuer-buerger.de
- www.kbv.de/praxis/digitalisierung/it-sicherheit

Physische Sicherheit

Definition

Physische Sicherheit im Kontext der IT-Sicherheit bezieht sich auf die Schutzmaßnahmen und Kontrollen, die implementiert werden, um physische IT-Ressourcen, einschließlich Hardware, Netzwerkinfrastruktur und Datenlager, vor physischen Bedrohungen zu sichern.

Durch die Integration physischer Sicherheitsmaßnahmen in das Informationssicherheitskonzept können Arztpraxen sicherstellen, dass ihre Daten und IT-Infrastrukturen umfassend geschützt sind und die Risiken von Datenverlust, unbefugtem Zugriff und möglichen Sicherheitsverletzungen minimiert werden.

Haftungsausschluss:
Dieses Dokument dient ausschließlich der allgemeinen Information und stellt keine individuelle Rechts-, IT- oder sonstige Beratung dar. Die hierin enthaltenen Inhalte wurden nach bestem Wissen erstellt, erheben aber keinen Anspruch auf Vollständigkeit, Richtigkeit oder Aktualität. Die Nutzung der Informationen erfolgt auf eigene Verantwortung. Eine Haftung der CompuGroup Medical für Schäden, die aus der Nutzung dieses Dokuments entstehen, ist – mit Ausnahme von Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit sowie bei Vorsatz oder grober Fahrlässigkeit – ausgeschlossen.

CompuGroup Medical Deutschland AG
Maria Trost 21, 56070 Koblenz
cgm.com/de

CompuGroup Medical