KBV

KASSENÄRZTLICHE
BUNDESVEREINIGUNG

BASIS-SCHULUNG: IT-SICHERHEIT

SCHULUNGSMATERIAL FÜR PRAXEN

KBV

- TEIL 1: IT-SICHERHEIT
- TEIL 2: PASSWÖRTER
- TEIL 3: SICHERER ARBEITSPLATZ
- TEIL 4: SCHUTZ VOR ANGRIFFEN
- TEIL 5: MELDEN VON INFORMATIONSSICHERHEITSVORFÄLLEN
- TEIL 6: VERANTWORTUNG IN DER VERTRAGSÄRZTLICHEN PRAXIS
- WEITERE INFORMATIONEN

- TEIL 1: IT-SICHERHEIT
- TEIL 2: PASSWÖRTER
- TEIL 3: SICHERER ARBEITSPLATZ
- TEIL 4: SCHUTZ VOR ANGRIFFEN
  - SOCIAL ENGINEERING
  - PHISHING
  - RANSOMWARE
- TEIL 5: MELDEN VON INFORMATIONSSICHERHEITSVORFÄLLEN
- TEIL 6: VERANTWORTUNG IN DER VERTRAGSÄRZTLICHEN PRAXIS
- WEITERE INFORMATIONEN

Motivation für IT-Sicherheit in der Praxis

Patienten vertrauen Praxen besonders schutzbedürftige Informationen an.

Bereits vor der IT-Sicherheitsrichtlinie existierten empfindliche Strafen bei Datenschutzverstößen oder Verletzung der Schweigepflicht (z. B. § 9 (Muster-) Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte, § 203 Strafgesetzbuch (StGB)).

Zur Konkretisierung der abstrakten Anforderungen der Datenschutz-Grundverordnung (DSGVO) hat der Gesetzgeber einheitliche und verbindliche Vorgaben für Praxen in einer zu erstellenden Richtlinie gefordert:

→Richtlinie nach § 390 SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit

Ärztliche Schweigepflicht (§ 9 MBO-Ä)

- Geregelt in § 9 Abs. 1 (Muster-) Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBO-Ä) beziehungsweise den entsprechenden Bestimmungen der Berufsordnungen der Landesärztekammern

- Ärztinnen und Ärzte haben über das, was ihnen in ihrer Eigenschaft als Arzt anvertraut oder bekannt geworden ist, auch nach dem Tod des Patienten, zu schweigen.

- Ärztinnen und Ärzte haben ihre Mitarbeiterinnen und Mitarbeiter und die Personen, die zur Vorbereitung auf den Beruf an der ärztlichen Tätigkeit teilnehmen, über die gesetzliche Pflicht zur Verschwiegenheit zu belehren und dies schriftlich festzuhalten.

- Nebenpflicht aus dem zwischen Arzt und Patient geschlossenen Behandlungsvertrag
- Seit Inkrafttreten des Patientenrechtegesetzes in den §§ 630a ff. Bürgerliches Gesetzbuch (BGB) geregelt (26. Februar 2013)

Europäische Datenschutz-Grundverordnung (DSGVO)

- Seit 25. Mai 2018 angewendet

- Ziele:
  - Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten
  - Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten
  - weitgehende Vereinheitlichung europäischen Datenschutzrechts

- Betrifft alle gesellschaftlichen Bereiche mit Umgang von personenbezogenen Daten – so auch Praxen, die in der Regel Gesundheitsdaten als „besondere Kategorie personenbezogener Daten“ gemäß Art. 9 Abs. 1 DSGVO verarbeiten und dies auch im Rahmen der ärztlichen Behandlung dürfen

- TEIL 1: IT-SICHERHEIT
- TEIL 2: PASSWÖRTER
- TEIL 3: SICHERER ARBEITSPLATZ
- TEIL 4: SCHUTZ VOR ANGRIFFEN
  - SOCIAL ENGINEERING
  - PHISHING
  - RANSOMWARE
- TEIL 5: MELDEN VON INFORMATIONSSICHERHEITSVORFÄLLEN
- TEIL 6: VERANTWORTUNG IN DER VERTRAGSÄRZTLICHEN PRAXIS
- WEITERE INFORMATIONEN

Mein Passwort

Passwörter sind persönliche und geheime digitale Schlüssel. Mit ihnen sichern wir verschiedenste Bereiche unseres digitalen Lebens. Passwörter sichern z. B.

- Datenbanken,
- soziale Netzwerke,
- Online-Banking,
- Benutzerkonten unterschiedlicher Dienste (E-Mail, Fortbildungsportal, PVS etc.),
- Computer, Laptop, Mobiltelefon.

Daher sind **gute Passwörter** und deren **sichere Verwahrung** besonders wichtig.

Wie erstellen Sie ein sicheres Passwort? (I)

Als **sicher** werden Passwörter angesehen, wenn sie nicht (in annehmbarer Zeit) von einem Angreifer erraten oder von einem böswilligen Programm errechnet werden können.

Bei der Sicherheit eines Passwortes kommt es vor allem auf die Länge und den Grad der Zufälligkeit an. Computerprogramme können zufällige Zeichenkombinationen nur sehr schwer knacken, da sie um schnell ein Passwort erraten zu können, nach einem bestimmten Schema vorgehen. Dabei kommen zum Beispiel folgende Schema zum Einsatz:

- Probieren aller möglichen Buchstaben- und Zeichenkombinationen
- Probieren von Buchstaben- oder Ziffernketten wie „abc“ oder „987“
- Probieren von Tastenfolgen wie „qwert“ oder „.,mn“
- Nutzung des Inhalts von Wörterbüchern in Kombination mit Ziffern und Sonderzeichen

Wie erstellen Sie ein sicheres Passwort? (II)

Ab einer bestimmten Länge des Passwortes muss ein Programm sehr viele Kombinationen errechnen; das macht das Passwort sicher. Hierbei gilt sogar die Faustregel:
„Länge schlägt Komplexität“

Grundsätzlich gelten folgende Regeln für die sichere Zusammensetzung eines Passwortes:

- mindestens 12 Zeichen Länge
- mindestens 1 Großbuchstabe
- mindestens 1 Kleinbuchstabe
- mindestens 1 Ziffer
- mindestens 1 Sonderzeichen

Im Folgenden stellen wir Ihnen zwei Methoden vor, mit denen Sie sichere Passwörter bilden können, die einfacher zu merken sind als eine rein zufällige Kombination.

Methode A: (scheinbar) zufällige Buchstaben

Bei dieser Methode bilden Sie das Passwort aus den ersten Buchstaben der Wörter eines Satzes. Wir nehmen diesen Satz aus einem Kinderlied: „Kommt ein Vogel geflogen setzt sich nieder auf mein‘ Fuß.“ und reichern ihn um Ziffern und Sonderzeichen an:

Kommt **e**in **V**ogel **g**eflogen **s**etzt **s**ich **n**ieder **a**uf **m**ein‘ **F**uß
→ KeVgssnamF
→ !K€Vg5?5namF.

Methode B: zufällige Wörter

Wählen Sie mindestens drei zufällige Wörter, im besten Fall sind diese nicht direkt in einem Wörterbuch zu finden, und reichern ihn um Ziffern und Sonderzeichen an:

außerordentlich Glöckchen Tach → außer0rdentlicherGlöck+chenTach

Vermeiden Sie bei dieser Methode Wörter, die sich aus dem Kontext des Zugangs oder aus Ihrem persönlichen Umfeld ergeben wie zum Beispiel „Google“ für Ihr Passwort zu Ihrem Google-Mail-Konto.

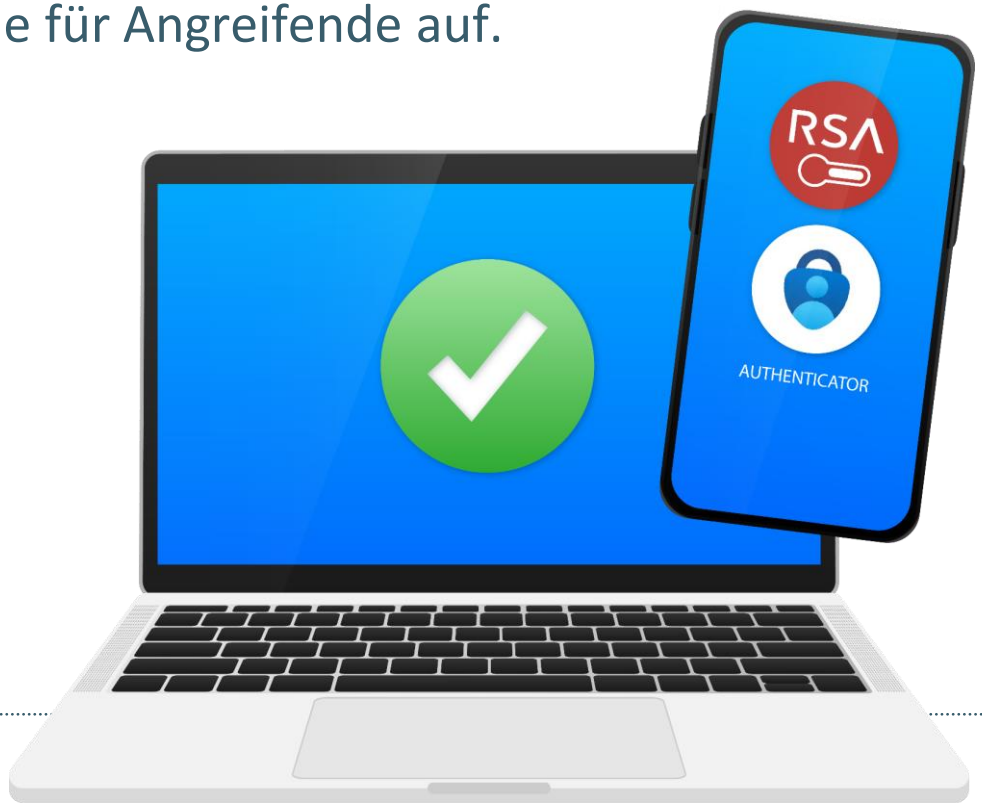
Mehrfaktor-Authentifizierung

Wer von unterwegs auf seine E-Mails und Dokumente der Praxis zugreift, sollte zusätzlich zu seinem Passwort eine **zweite Information** angeben: eine nur kurz gültige Zahlenkombination. In diesem Falle spricht man von einer Mehrfaktor- oder Zweifaktor-Authentifizierung (kurz: **MFA** oder **2FA**). Der zusätzliche Faktor baut eine weitere große Hürde für Angreifende auf.

Selbst wenn Ihr Passwort geklaut wird:

man kann sich nicht ohne diesen **zweiten Faktor**

in Ihrem Namen von extern anmelden.



- TEIL 1: IT-SICHERHEIT
- TEIL 2: PASSWÖRTER
- TEIL 3: SICHERER ARBEITSPLATZ
- TEIL 4: SCHUTZ VOR ANGRIFFEN
  - SOCIAL ENGINEERING
  - PHISHING
  - RANSOMWARE
- TEIL 5: MELDEN VON INFORMATIONSSICHERHEITSVORFÄLLEN
- TEIL 6: VERANTWORTUNG IN DER VERTRAGSÄRZTLICHEN PRAXIS
- WEITERE INFORMATIONEN

Szenario: Sicherer Arbeitsplatz (I)

Heute Morgen kam ich gut gelaunt zur Arbeit.

Szenario: Sicherer Arbeitsplatz (II)

Als Erstes habe ich die hübsche Zeichnung, die mir meine Nichte geschenkt hat, aufgehängt.

Szenario: Sicherer Arbeitsplatz (III)

Dann erschien meine Chefin und hat mir die neue Patientenbefragung hingelegt.

Szenario: Sicherer Arbeitsplatz (IV)

Außerdem sollte ich mir ganz schnell einen aussichtsreichen Bewerber für unsere Praxis ansehen.

Szenario: Sicherer Arbeitsplatz (V)

Aber ich glaube nicht, dass er der Richtige für uns ist.

Szenario: Sicherer Arbeitsplatz (VI)

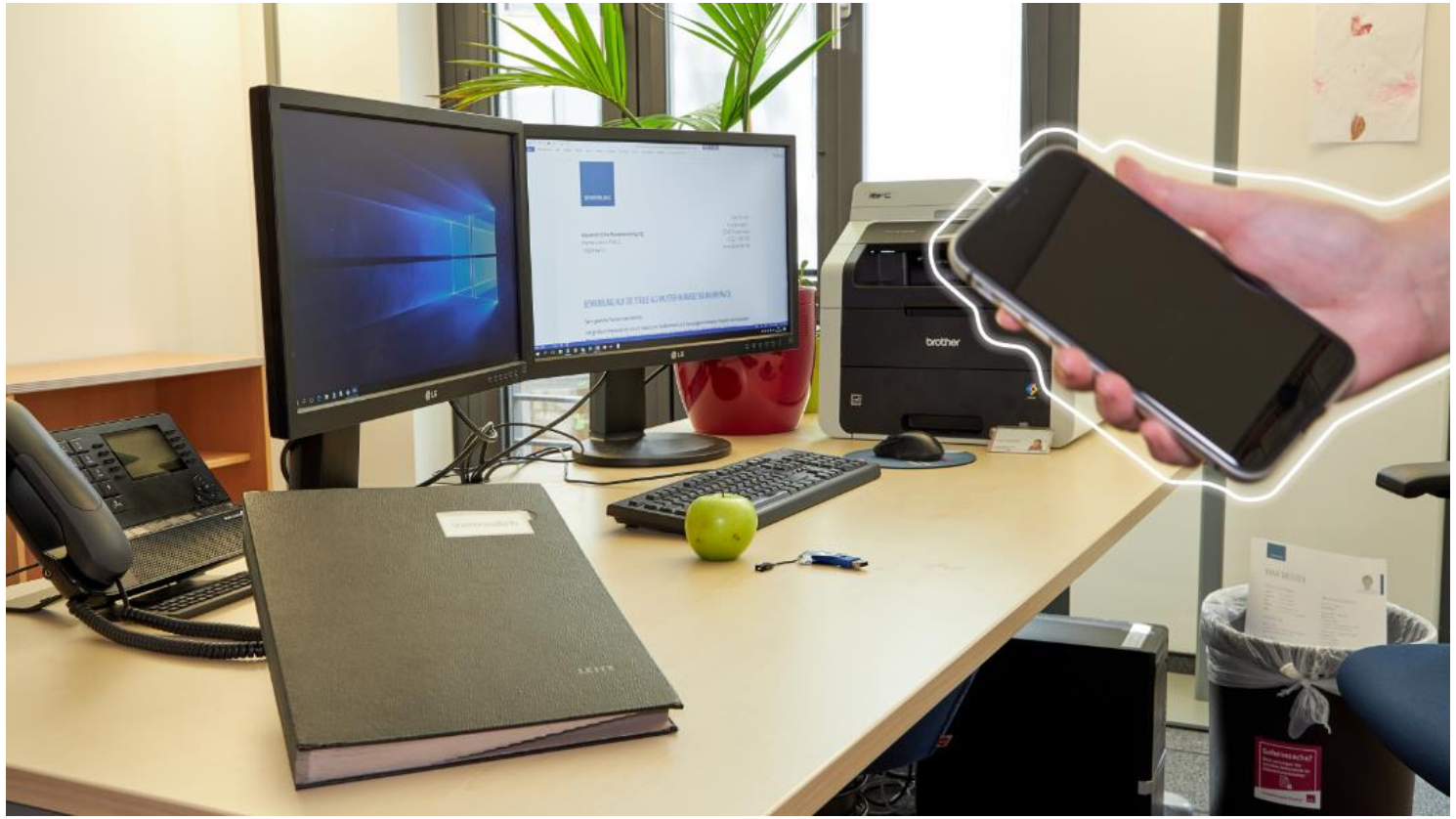
Und ich muss unbedingt ein gutes Programm zur Projektorganisation installieren, das mir ein Kollege empfohlen hat.

Szenario: Sicherer Arbeitsplatz (VII)

Aber vorher noch einen Apfel zur Stärkung.

Szenario: Sicherer Arbeitsplatz (VIII)

„Eine Pause? Sehr gute Idee, ich komme. Aber höchstens zehn Minuten!“



Szenario: Sicherer Arbeitsplatz (IX)

In der Zeit kann ich auch frische Luft reinlassen.

Szenario: Sicherer Arbeitsplatz (X)

In diesem Szenario treten einige Probleme auf, die sich mit Hilfe von hauseigenen Regeln zum aufgeräumten Schreibtisch vermeiden lassen. Diese zeigen wir Ihnen im nächsten Schritt.

Halten Sie sich immer an die „Clean-Desk“-Regeln

- Sperren Sie Ihren Bildschirm, auch wenn Sie den Arbeitsplatz nur kurz verlassen mit dieser Tastenkombination: Windows-Taste ⊞ + L.
- Lassen Sie vertrauliche Dokumente niemals unbeaufsichtigt liegen.
- Schließen Sie Fenster und Türen, wenn das Büro nicht besetzt ist.
- Tragen Sie mobile Geräte und persönliche Wertgegenstände bei sich oder schließen Sie sie weg.
- Entsorgen Sie Dokumente und Datenträger sicher.

Sicher entsorgen

Fehldrucke und Fehlkopien müssen entsprechend ihrer Vertraulichkeit sicher entsorgt werden. Das heißt, dass vertrauliche Dokumente **nicht in den normalen Praxis-Mülleimer** gehören. Unterlagen, Daten und Datenspeicher müssen entsprechend der Vertraulichkeit entsorgt werden, um sicherzustellen, dass die Informationen nicht in falsche Hände gelangen.

Vertrauliche Unterlagen gehören beispielsweise in eine Datenschutztonne oder in einen Papier-Schredder.

Besucherregeln

Externe sowie Vertragspartner und Vertragspartnerinnen müssen in jedem Fall eine **Verschwiegenheitsvereinbarung** unterzeichnen, mit der sie sich verpflichten, Informationen und Daten der Praxis vertraulich zu behandeln und nicht an Dritte weiterzugeben.

- TEIL 1: IT-SICHERHEIT
- TEIL 2: PASSWÖRTER
- TEIL 3: SICHERER ARBEITSPLATZ
- **TEIL 4: SCHUTZ VOR ANGRIFFEN**
  - SOCIAL ENGINEERING
  - PHISHING
  - RANSOMWARE
- TEIL 5: MELDEN VON INFORMATIONSSICHERHEITSVORFÄLLEN
- TEIL 6: VERANTWORTUNG IN DER VERTRAGSÄRZTLICHEN PRAXIS
- WEITERE INFORMATIONEN

Definition Social Engineering

› Social Engineering [ˈsəʊʃl ˌɛndʒɪˈnɪəɹɪŋ] (engl. eigentlich „angewandte Sozialwissenschaft“, auch „soziale Manipulation“) nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen.

› Social Engineers sind **schauspielernde Diebe** mit dem Ziel, wertvolle Insiderinformationen oder Geld zu erhalten, zum Beispiel:
- Preisgabe von vertraulichen Informationen
- Kauf eines bestimmten Produktes
- Freigabe von Finanzmitteln

Menschen hacken

- Angreifende schlüpfen in unterschiedliche Rollen, um auszunutzen, dass die meisten Menschen gerne helfen, empfänglich für Lob sind oder sich einschüchtern lassen. Darauf aufbauend werden Opfer manipuliert.

- Für einen größeren Erfolg spionieren Social Engineers das persönliche oder berufliche Umfeld ihres Opfers aus, täuschen Identitäten vor (**Identitätsfälschung**) oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus.

- Lassen Sie sich nicht beirren, sollte Ihr Gegenüber etwa den großen Boss markieren oder unschuldig um Hilfe bitten.

Social Engineering

Vor Ort (abhängig von der Praxisgröße)

- Trotz Sicherheitsmaßnahmen gelingt es Social Engineers immer wieder in Bereiche einzudringen, die für Besucher nicht öffentlichen zugänglich sind.
- Begegnen Sie deswegen fremden Personen, die sich nicht zuordnen lassen, mit einer gesunden Portion Misstrauen und sprechen Sie sie an.

Aus der Ferne

- Social Engineering Angriffe können auch über E-Mail oder Telefon erfolgen.
- Auch hier gilt: Begegnen Sie Personen, zu denen Sie noch keinen Kontakt hatten, mit einer gesunden Portion Misstrauen.
- Wenn Sie keinen internationalen Anruf erwarten, gehen Sie auch nicht ans Telefon.

Social Engineering – Beispiel Per Telefon (I)

› Sie haben einen Herrn am Telefon, der sich als Mitarbeiter des Microsoft Support Teams ausgibt.

Ich rufe an, weil Ihr Computer von Viren befallen ist und unbedingt mit der richtigen Software bereinigt werden muss, bevor all Ihre Daten an Hacker gelangen und verschlüsselt werden. Ich zeige Ihnen, woran Sie erkennen, dass Sie betroffen sind: Öffnen Sie mit der Kombination Windows-Taste ⊞+R ein Fenster und tippen Sie „eventvwr“ ein.

› In dem nun geöffneten Fenster werden Ihnen ganz viele Warnungen und Fehler angezeigt.

Social Engineering – Beispiel Per Telefon (II)

Diese ganzen Fehler zeigen, dass ein Hacker in den Computer eingedrungen ist. Sie können aber mit meiner Software die Säuberung des Geräts schnell und unkompliziert durchführen.

Auch wenn wir aus Höflichkeit ungerne zu solch drastischen Maßnahmen greifen: Legen Sie in solchen Fällen einfach auf. Microsoft wird nie unaufgefordert Kunden anrufen.

Social Engineering – Beispiel Identitätsfälschung (I)

- Ihr Telefon klingelt und auf dem Display erscheint eine unbekannte Mobilfunknummer.
- Es meldet sich die Leitung einer Krankenkasse, die aufgeregt berichtet, eigentlich im Feierabend zu sein, aber dringend Daten zur äußerst eiligen Bearbeitung für die Bewilligung einer Behandlung zu benötigen.
- Die Krankenkasse bittet Sie, die Daten per E-Mail an eine private E-Mail Adresse zu schicken.
- Sie zögern, da Sie die Regeln zum Umgang mit internen Informationen kennen, und weigern sich.
- Die Krankenkasse fährt Sie an, Sie würden absichtlich die dringende Bewilligung für die Behandlung eines Patienten, der namentlich genannt wird, verhindern und droht Ihnen, Ihrer Praxisleitung, die ebenfalls namentlich benannt wird, umgehend über Ihre Arbeitsverweigerung in Kenntnis zu setzen.
- Nach einem kurzen Moment des Überlegens drücken Sie schließlich doch auf das „Senden“-Feld.

Social Engineering – Beispiel Identitätsfälschung (II)

- So oder so ähnlich erging es in den vergangenen Jahren vielen Mitarbeitenden, deren Organisationen Opfer des sogenannten, neudeutschen CEO-Fraud geworden sind.

- Oft wurden dann jedoch nicht nur vertrauliche Informationen übermittelt, sondern hohe Geldbeträge auf ein Konto im Ausland transferiert.

- Beim CEO-Fraud nehmen Angreifende die Identität eines Geschäftsführers (**C**hief **E**xecutive **O**fficer) oder leitende Angestellte an, um Mitarbeitende zu bestimmten Verhaltensweisen zu bewegen.

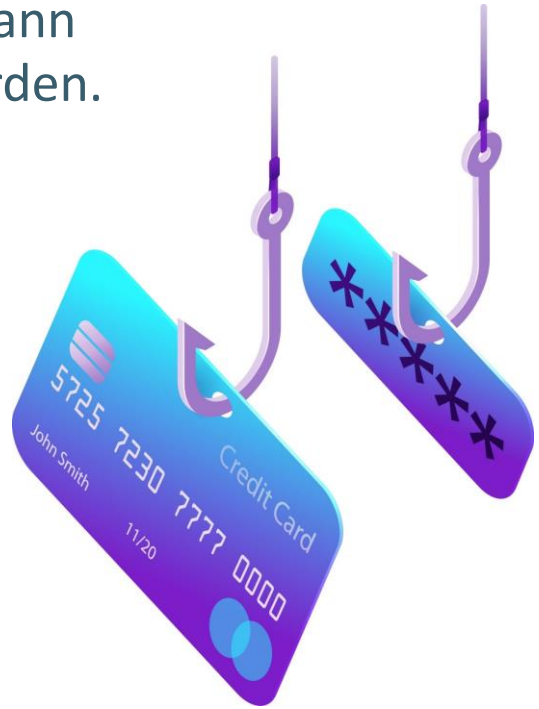
- TEIL 1: IT-SICHERHEIT
- TEIL 2: PASSWÖRTER
- TEIL 3: SICHERER ARBEITSPLATZ
- **TEIL 4: SCHUTZ VOR ANGRIFFEN**
  - SOCIAL ENGINEERING
  - PHISHING
  - RANSOMWARE
- TEIL 5: MELDEN VON INFORMATIONSSICHERHEITSVORFÄLLEN
- TEIL 6: VERANTWORTUNG IN DER VERTRAGSÄRZTLICHEN PRAXIS
- WEITERE INFORMATIONEN

Definition Phishing (I)

› Der Begriff Phishing ist ein englisches Kunstwort, das sich aus password harvesting (Passwörter ernten) und fishing (Angeln, Fischen) zusammensetzt und bildlich das **Angeln nach Passwörtern** mit Ködern verdeutlicht.

Definition Phishing (II)

- Unter dem Begriff Phishing versteht man Versuche, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner auszugeben, um vertrauliche Daten zu stehlen.
- Ziel sind in der Regel persönliche und vor allem Zugangsdaten, mit denen dann beispielsweise Kontoplünderungen oder Identitätsdiebstähle begangen werden.
- Vorgehen:
  - Es wird eine Nachricht (z. B. E-Mail oder SMS) mit einer gefälschten Absenderadresse gesendet. Diese enthält eine Aufforderung zu einem Klick auf einen Link, welcher zu einer nachgebauten bzw. gefälschten Webseite führt.
  - Auf der Webseite werden die Opfer aufgefordert, vertrauliche Daten (z. B. Zugangsdaten oder Kontodaten) einzugeben.



Phishing Beispiel (I)

Di 05.07.2022 16:09

Personalabteilung <personal@kbv.de>

<<Extern>> Überraschung

An [redacted] (KBV)

Liebe Kolleginnen und Kollegen,

dafür, dass Sie stets Ihr Bestes geben, haben wir uns eine kleine Überraschung für Sie überlegt.

Unser Partner hat hier für Sie eine Auswahl an Belohnungen bereitgestellt. Nach dem Login können Sie sich eine Belohnung aussuchen, die Ihnen am besten gefällt. Wir hoffen es ist für jeden etwas dabei.

Viele Grüße
Ihre Personalabteilung

***** Bitte beachten Sie, dass es sich um eine E-Mail von einem externen Absender handelt. Prüfen Sie daher den Absender, bevor Sie Links oder Anhänge öffnen. *****

› Der/die Angreifende gibt sich als die Personalabteilung aus und lockt mit einer Überraschung als Belohnung.

Phishing Beispiel (II)

› Nach dem Aufrufen des Links wird eine nachgebaute Webseite mit der folgenden Eingabemaske geöffnet:

› Sobald Mitarbeitende ihre Zugangsdaten eingegeben haben, werden diese an den Angreifenden gesendet.

- TEIL 1: IT-SICHERHEIT
- TEIL 2: PASSWÖRTER
- TEIL 3: SICHERER ARBEITSPLATZ
- **TEIL 4: SCHUTZ VOR ANGRIFFEN**
  - SOCIAL ENGINEERING
  - PHISHING
  - RANSOMWARE
- TEIL 5: MELDEN VON INFORMATIONSSICHERHEITSVORFÄLLEN
- TEIL 6: VERANTWORTUNG IN DER VERTRAGSÄRZTLICHEN PRAXIS
- WEITERE INFORMATIONEN

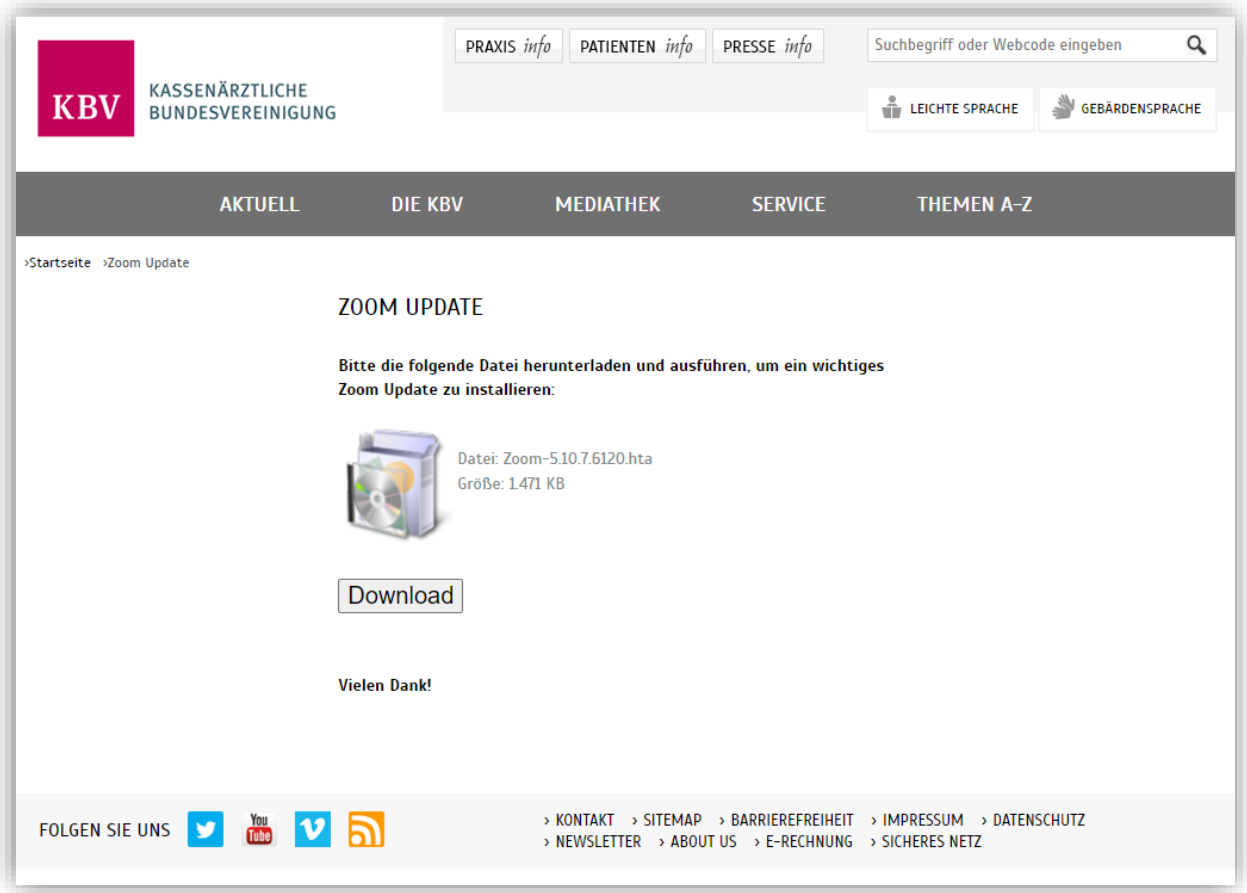
Definition Ransomware

- Ransomware (auch Erpressungstrojaner, Erpressungssoftware, Kryptotrojaner oder Verschlüsselungstrojaner genannt) sind Schadprogramme, die den Zugriff auf Daten oder ganze Computersysteme durch Verschlüsselung verhindern.
- Die Bezeichnung setzt sich zusammen aus „ransom“ (englisch für Lösegeld) und „ware“ (vgl. Software, Malware etc.).
- Vorgehen:
  - Es wird eine E-Mail mit einer gefälschten Absenderadresse gesendet, die einen präparierten Anhang oder Link enthält.
  - Durch Öffnen bzw. Ausführen der geschickten Datei startet die Verschlüsselung des PCs und weiterer Systeme im ganzen Netz.
  - Auf befallenen Geräten wird ein Hinweis platziert, der eine Frist zur Zahlung von Lösegeld (in der Regel in Form von Kryptowährungen) enthält.

Ransomware Beispiel (II)

- Nach dem Aufrufen des Links wird eine nachgebaute Webseite mit einem Download geöffnet:

- Sobald Mitarbeitende die Datei herunterladen und ausführen, bekommen die Angreifenden Zugriff auf das System und können Daten verschlüsseln.



- TEIL 1: IT-SICHERHEIT
- TEIL 2: PASSWÖRTER
- TEIL 3: SICHERER ARBEITSPLATZ
- **TEIL 4: SCHUTZ VOR ANGRIFFEN**
  - SOCIAL ENGINEERING
  - PHISHING
  - RANSOMWARE
- TEIL 5: MELDEN VON INFORMATIONSSICHERHEITSVORFÄLLEN
- TEIL 6: VERANTWORTUNG IN DER VERTRAGSÄRZTLICHEN PRAXIS
- WEITERE INFORMATIONEN

Schutz vor Social Engineering

- Ein schmeichelnder Tonfall, die Aufforderung zur Geheimhaltung und der Ausschluss anderer Kommunikationswege sollten Sie skeptisch machen. Lassen Sie sich nicht einschüchtern oder unter Druck setzen.
- Kontaktieren Sie die Person über bereits bekannte Kontaktinformationen (z. B. Telefonnummer einer Visitenkarte oder eine interne Durchwahl).
- Lassen Sie sich Anweisungen intern bestätigen und nehmen Sie eine kritische Grundhaltung gegenüber Abweichungen vom Soll-Prozess ein.

Tipps bei E-Mails (I)

- Nehmen Sie sich bei E-Mails am besten immer Zeit für den **3-Sekunden-Check** (vorher **auf keinen Fall** auf einen Link oder Anhang klicken):
  - Ist der Absender bekannt?
  - Ist der Betreff sinnvoll?
  - Wird ein Anhang von diesem Absender erwartet?
- Seien Sie bei externen E-Mails besonders wachsam.

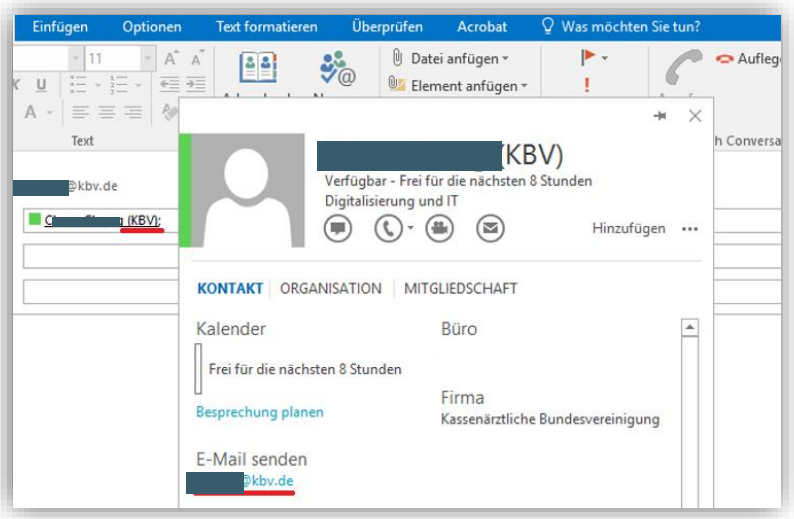
Tipps bei E-Mails (II)

PRAXIS TIPPS!

- Angreifer haben bei E-Mail-Nachrichten viele Möglichkeiten ihre wahre Identität zu verschleiern:
  - Sie nehmen zum Beispiel ähnlich aussehende Adressen: mmustermann@kbu.de oder sie entscheiden sich für plausible Adressen: mmustermann@kbv-online.de
  - Manchmal verstecken sie die wahre Adresse auch hinter dem in Outlook angezeigten Namen

- Überprüfen Sie die E-Mail Adresse des Gegenübers
  - Wird mit Doppelklick auf den angezeigten Namen in Outlook die richtige/plausible Adresse mit @-Zeichen angegeben?

- Überprüfen Sie auch Inhalt und Betreff der E-Mail auf Plausibilität.



Tipps bei der Nutzung von USB-Sticks

PRAXIS TIPPS!

- Verwenden Sie keine fremden USB-Sticks. Angreifende können Schadprogramme auf den USB-Sticks hinterlegen, welche beim Einstecken automatisch installiert werden.

- Denken Sie bei der Benutzung eigener USB-Sticks daran, diese mit Hilfe von Anti-Virenprogrammen auf Schadsoftware zu prüfen. Denn auch eigene USB-Sticks können unbewusst Schadprogramme enthalten.

Schutz vor Angriffen

- Wenn Ihnen eine Person oder eine Nachricht seltsam vorkommen, halten Sie Rücksprache mit Kolleginnen oder Kollegen oder sprechen Sie mit Ihren Vorgesetzten.

- Melden Sie seltsame Vorfälle, um sich und ihre Praxis vor weiteren Schaden zu schützen.

Übrigens

Automatische Abwesenheiten an externe Personen sind in E-Mail-Programmen bedenklich. Nicht nur kriegen Spam-Versender eine Bestätigung, dass eine E-Mail Adresse existiert und genutzt wird, sondern daraus können auch wertvolle Informationen für Angriffe abgeleitet werden.

- TEIL 1: IT-SICHERHEIT
- TEIL 2: PASSWÖRTER
- TEIL 3: SICHERER ARBEITSPLATZ
- TEIL 4: SCHUTZ VOR ANGRIFFEN
  - SOCIAL ENGINEERING
  - PHISHING
  - RANSOMWARE
- TEIL 5: MELDEN VON INFORMATIONSSICHERHEITSVORFÄLLEN
- TEIL 6: VERANTWORTUNG IN DER VERTRAGSÄRZTLICHEN PRAXIS
- WEITERE INFORMATIONEN

Informationssicherheitsvorfälle - Wenn es doch passiert

- Die Erfahrung zeigt, dass sich auch bei ausreichend umgesetzten Maßnahmen immer wieder (Informationssicherheits-)Vorfälle ereignen.
- Natürlich ist niemand unfehlbar und manchmal bemerkt man einen Fehler erst im Nachhinein.
- In einem kurzen Augenblick der Unaufmerksamkeit ist es mit einem Klick auf den falschen Link oder Anhang geschehen, aber es ist nicht gleich alles verloren.

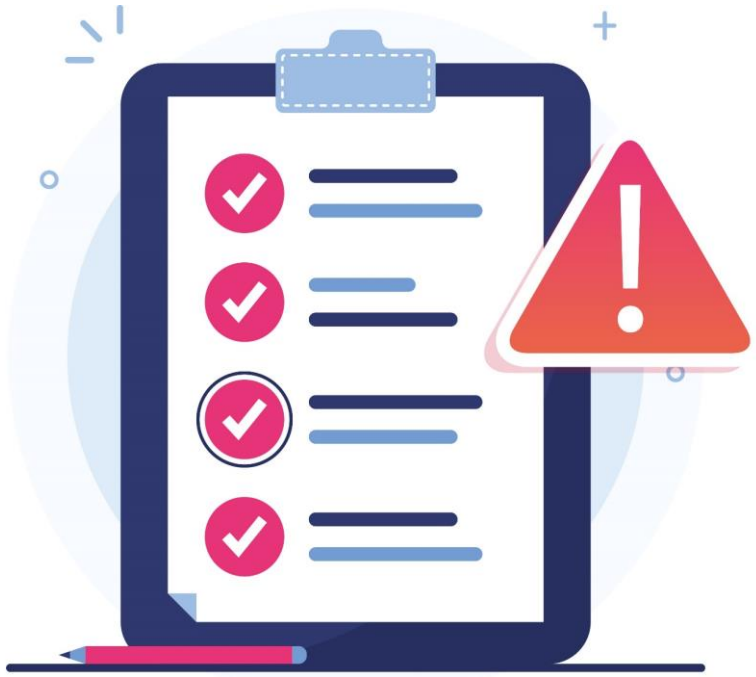
Melden von Informationssicherheitsvorfällen – Beispiel

- Nach einer schlaflosen Nacht beginnt Max morgens um 9 Uhr seinen Arbeitstag und geht routinemäßig seine ungelesenen Mails durch.
- Unter anderem eine Mail von seinem Vorgesetzten: Er solle doch bitte die sehr wichtige Bewerbung bis 10 Uhr durchsehen und eine Einschätzung zurücksenden.
- In Hektik verfallen, lädt er schnell die Datei im Anhang herunter und öffnet diese.
- Statt der Bewerbung erscheint jedoch ein Fenster mit einer Warnmeldung.
- Nach einem kurzen Moment bemerkt Max, dass die geöffnete Datei gar keine Bewerbung ist.
- Jetzt ahnt er, was passiert ist.

Informationssicherheitsvorfälle – Gekonnt handhaben

› Mit den folgenden Schritten lassen sich etwaige Schäden gekonnt eindämmen:

1. Tief durchatmen und **Ruhe bewahren**!
2. Es sollten zunächst eventuell aufgetretene Warn- oder Hinweismeldungen mittels Screenshots gesichert werden.
3. Auch das Speichern und Schließen aktiver Anwendungen sollte erfolgen.
4. Vorfälle sind an eine vorher festzulegende Stelle zu melden.
5. Die genannten Stellen begleiten Sie beim weiteren Vorgehen.



- TEIL 1: IT-SICHERHEIT
- TEIL 2: PASSWÖRTER
- TEIL 3: SICHERER ARBEITSPLATZ
- TEIL 4: SCHUTZ VOR ANGRIFFEN
  - SOCIAL ENGINEERING
  - PHISHING
  - RANSOMWARE
- TEIL 5: MELDEN VON INFORMATIONSSICHERHEITSVORFÄLLEN
- TEIL 6: VERANTWORTUNG IN DER VERTRAGSÄRZTLICHEN PRAXIS
- WEITERE INFORMATIONEN

Verantwortung der vertragsärztlichen Praxis

Für die vertragsärztlichen Praxis ist es wichtig, dass die Grundsätze der IT-Sicherheit eingehalten werden, um die eigenen Praxiswerte und die Patientendaten zu schützen.

Um dies zu erreichen, muss die Praxisleitung dafür Sorge tragen, dass **alle Mitarbeitenden** ausreichend informiert sind, einen Kontakt für Fragen haben und eine geeignete technische und personelle Infrastruktur zur Verfügung steht.

Verantwortung der Mitarbeiterinnen und Mitarbeiter

- Wenn es darum geht, die vorgeschriebenen IT-Sicherheits-Regelungen einzuhalten, liegt die Verantwortung in erster Linie **bei Ihnen selbst**. Sie tragen einen maßgeblichen Teil zum Schutz der vertragsärztlichen Praxis bei.
- Wenn Sie unsicher sind, wie Sie sich in einer bestimmten Situation verhalten sollen oder wie ein Sachverhalt zu beurteilen ist, aber auch wenn Sie eine grundsätzliche IT-Sicherheit haben, scheuen Sie sich bitte nicht, Ihre Führungskraft zu kontaktieren.

↗ TEIL 1: IT-SICHERHEIT
↗ TEIL 2: PASSWÖRTER
↗ TEIL 3: SICHERER ARBEITSPLATZ
↗ TEIL 4: SCHUTZ VOR ANGRIFFEN
↗ TEIL 5: MELDEN VON INFORMATIONSSICHERHEITSVORFÄLLEN
↗ TEIL 6: VERANTWORTUNG IM UNTERNEHMEN
↗ WEITERE INFORMATIONEN

Weitere | Informationen

- KBV Webseite zur IT-Sicherheitsrichtlinie
  - https://www.kbv.de/html/it-sicherheit.php
- KBV Informationshub für weitere Informationen
  - https://hub.kbv.de/display/itsrl
- BSI für Bürger
  - https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html
- BSI für Unternehmen und Organisationen
  - https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/unternehmen-und-organisationen_node.html

Vielen Dank!

Wir sind für Sie nah.

rettet-die-praxen.de