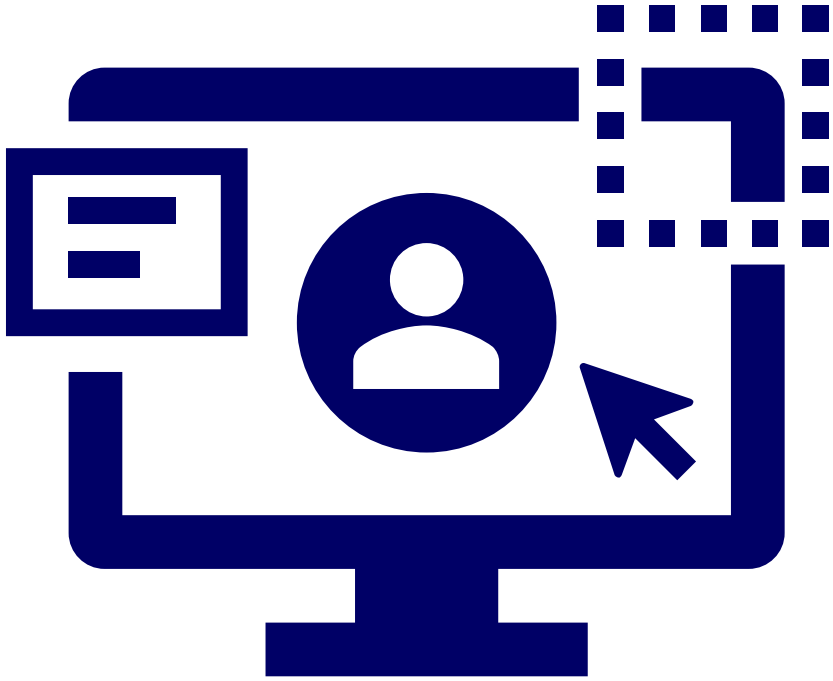
Datensicherheit in Arztpraxen

Referent

Bernd Gemeinder



KVBW
IT in der Praxis

Direktkontakt

IT-Berater

0711 7875-3570

itp@kvbawue.de

Mo – Fr: 8 – 16 Uhr

Alles Gute.
KVBW
Kassenärztliche Vereinigung Baden-Württemberg

Agenda

Gefahren Erläuterungen	dieser Vortrag
Umsetzen	Sie in Ihrer Praxis

Beispiele

- Am 30.09.2021 wurde ein Cyber-Sicherheitsvorfall durch ein städtisches Klinikum in Sachsen-Anhalt gemeldet. Im Netzwerk des Klinikums wurde das unrechtmäßig eingesetzte Penetration-Testing-Tool Cobalt Strike entdeckt. Die Kommunikationssysteme sowie die Nutzung der IT waren nur eingeschränkt möglich. Zudem wurden täterseitig Daten ausgeleitet. Die medizinische Versorgung konnte durchgehend gewährleistet werden.

Malware

- Ein Softwareunternehmen, dessen Softwarelösungen in etwa einem Viertel der deutschen Arztpraxen eingesetzt wird, stellte am 04.11.2021 die Verschlüsselung ihrer Server- und Netzwerkinfrastruktur fest und war ab diesem Zeitpunkt nicht mehr arbeitsfähig. Bei der eingesetzten Ransomware handelte es sich um Conti.

Ransomware

- Am 09.12.2021 wurde eine Zero-Day-Schwachstelle in der weitverbreiteten Protokollierungsbibliothek Log4j bekannt, die Bestandteil zahlreicher Open-Source- sowie kommerzieller Softwareprodukte ist. Die Schwachstelle ermöglicht die Installation von Schadsoftware und führt so zur Verwundbarkeit zahlreicher Unternehmen. Die langfristigen Folgen sind noch nicht absehbar.

Exploit/ Schwachstelle

Abbildung 3: Beispiele für relevante Cyberangriffe in Deutschland 2021

Bundeslagebild | Cybercrime 2021 3

Honeypot-Server der Telekom

TOP10 Gefahren allgemein

Die 10 häufigsten Gefahren	Einteilung
1. Cyberangriffe	Externe Einflüsse - Nicht kontrollierbar!(?)
2. Weitere äußere Einflüsse (Brand, Überschwemmung, …)	
3. Fehler d. User / Mitarbeiter	Interne Einflüsse - Selbst kontrollierbar!
4. Technische Defekte / Fehlfunktionen	
5. Schlechte Organisation	
6. Schlechte Kommunikation	
7. Sparsamkeit	
8. Komplexe Maßnahmen	
9. Fokus auf Technik	
10. Leichtsinnigkeit	

TOP10 Gefahren aus dem Internet

Die 10 häufigsten Gefahren	Gefahrenquelle
1. Drive-by-Downloads von Schadsoftware	Surfen
2. Trojaner/Würmer	E-Mail, Surfen, Apps, Software
3. Attacken auf Datenbanken und Websites	Internet
4. Viren-Baukästen	Als Werkzeug
5. Botnetze	E-Mail, Surfen, Apps, Software
6. Denial-of-Service-Attacken	Internet
7. Social Engineering und Phishing	Social Media, Webseiten
8. Datenklau und Datenverluste	E-Mail, Surfen, Apps, Software
9. Rogueware/Scareware	E-Mail, Surfen, Apps, Software
10. Spam	E-Mail, Surfen, Apps, Software

https://bitkom-akademie.de/news/die-zehn-groessten-gefahren-im-internet

Datensicherheit

Frage	Antwort
Wer	Praxisinhaber, aber auch die MITARBEITER!
Was	Patientendaten und Praxisdaten! Schutzziele: Vertraulichkeit, Integrität und Verfügbarkeit
Wo	In der Praxis und wo auch immer Daten gespeichert werden (Cloud).
Wann	IMMER!
Warum	- Gesetzliche Vorgabe - Eigeninteresse (Praxiserhalt)
Wie	Thema des Vortrags

TOP 8 Maßnahmen

Datensicherung (Backup)
Benutzermanagement

Passwörter (sinnvoll)
Mitarbeiter (Achtsamkeit/Awareness)

Firewall und Virenschutz
regelmäßige Software- und Firmware-Updates

Notfallmanagement
IT-Sicherheitsrichtlinie

Datensicherung!

Backup, Backup, Backup!!!

- Voll- oder Teil-Backups nutzen
- Backup auch funktionstüchtig?
- Cloud-Backup => Empfehlungen beachten!

Benutzermanagement!

- Jeder Benutzer hat eigenen Account auf dem Rechner
- Berechtigungen einschränken (nicht jeder darf alles!)
- Rollenkonzept
- Berechtigungen über Rollen zuweisen
- Administratoren haben eigenen/separaten Account
- Unterschiedliche Benutzer auch in der Praxissoftware
- Eine Aufgabe für den IT-Dienstleister

Passwörter

- Passwörter niemals aus der Hand geben:
  also Passwörter, Zugangsdaten oder Kontoinformationen NIE per Telefon oder E-Mail mitteilen oder an den PC oder unter die Tastatur kleben.

- Sichere Passwörter
  mit Sonderzeichen, Zahlen, sowie Groß- und Kleinschreibung mindestens 12 Zeichen – besser noch 20 Zeichen oder sogar Passwortphrasen nutzen.

- Kein Passwort zweimal verwenden
  schon gar nicht für Shopping-Accounts, ggf. Passwort-Safe verwenden.

- 2-Faktor-Authentifizierungen
  wenn möglich zum zusätzlichen Schutz wichtiger Accounts

Mitarbeiter

- Laut BSI-Statistik lassen sich **6** von **10** erfolgreiche Hacker-Angriffe oder Online-Betrugsfälle auf Fehlverhalten von Menschen und nicht auf Software-Fehler bzw. Sicherheitslücken zurückführen
- Ein perfekt gewartetes IT-System, dass neueste und aktuellste Sicherheitsstandards beinhaltet nicht einmal die Hälfte von potenziellen Angriffen abwehren kann, wenn die Menschen, die diese IT-Systeme nutzen nicht geschult und sensibilisiert sind
- Nicht nur „normale User“ sondern auch administrierende IT-Fachkräfte und Software-Entwickler

Mitarbeiter

- Mitarbeiter mit ins Boot holen:
- Biologische Firewall updaten (**ganzes Praxisteam!**) durch Schulungen, TÜV, KVBW-Seminare etc.
- Regelmäßiger Prozess, IT-Sicherheit muss gelebt werden!
- Umgang mit E-Mails
- Verhalten im Internet
- Auftreten in soziale Medien
- Verhaltensrichtlinien aufstellen und bekannt geben!

Firewall und Virenscanner!

- Software: Virenscanner und Firewall lokal auf PC
- zusätzliche Hardware-Firewall
- TI-Konnektor in Reihenschaltung
  als Hardware-Firewall
  mit SIS (Sicherer Internet Service)

Software- und Firmware-Updates

Software
Anwendungen auf dem Rechner

Firmware
systemnahe Software

Adobe

Office

Immer aktuell halten!
Die automatische Update-Funktion nutzen wenn vorhanden!

Notfallmanagement

VERHALTEN BEI IT-NOTFÄLLEN

Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallrufnummer:

Wer meldet?

Welches IT-System ist betroffen?

Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

Wann ist das Ereignis eingetreten?

Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen | Beobachtungen dokumentieren | Maßnahmen nur nach Anweisung einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

Notfallkarte vom BSI und der dazugehörigen Maßnahmenkatalog

Merkblatt Notfallmanagement der KVBW!

- Ruhe bewahren!
- Praxisteam bzw. verantwortliche Person über die Situation informieren
- Arbeit am IT-System sofort einstellen und relevante Rechner bzw. Server umgehend ausschalten (Netzwerkstecker ziehen)
- Notfallkontakte informieren
- IT-Dienstleister: Tel.
- Datenschutzbeauftragter der Praxis: Tel.
- Cybercrime (ZAC) beim Landeskriminalamt Baden-Württemberg: Tel. 0711 5401-2444
- Cyberwehr – Erstkontakt bei Cyberangriffen: Tel. 0800 292379347
- alle mit dem IT-Notfall im Zusammenhang stehende Sachverhalte dokumentieren

Wichtige Hinweise

- Anweisungen der Notfallkontakte umsetzen
- ggf. Kassenärztliche Vereinigung bezüglich Abrechnung informieren
- Meldepflicht beim Landesdatenschutzbeauftragten (Frist innerhalb 72 Stunden)!

Alles Gute.
KVBW
Kassenärztliche Vereinigung Baden-Württemberg

IT-Sicherheitsrichtlinie

https://hub.kbv.de/site/its

IT-Sicherheitsrichtlinie

ANLAGE 1

Anforderungen für Praxen

	Zielobjekt	Anforderung	Erläuterung	Geltung ab
	Software: Rechner-Programme, mobile Apps und Internet-Anwendungen			
1.	Mobile Anwendungen (Apps)	Sichere Apps nutzen	Nur Apps aus den offiziellen Stores runterladen und nutzen. Wenn nicht mehr benötigt, Apps restlos löschen.	01.04.2021
2.	Mobile Anwendungen (Apps)	Aktuelle App-Versionen	Updates immer zeitnah installieren, um Schwachstellen zu vermeiden.	01.04.2021
3.	Mobile Anwendungen (Apps)	Sichere Speicherung lokaler App-Daten	Nur Apps nutzen, die Dokumente verschlüsselt und lokal abspeichern.	01.01.2022
4.	Mobile Anwendungen (Apps)	Verhinderung von Datenabfluss	Keine vertraulichen Daten über Apps versenden.	01.04.2021
5.	Office-Produkte	Verzicht auf Cloud-Speicherung	Keine Nutzung der in Office-Produkte integrierte Cloud-	01.04.2021

- 5 Anlagen als PDF-Datei in Tabellenform
- Zielobjekten, Anforderungen und Erläuterungen
- Mindestmaß an Anforderungen!
- Zur Einhaltung der Vorgaben der DSGVO (Datenschutzgrundverordnung)

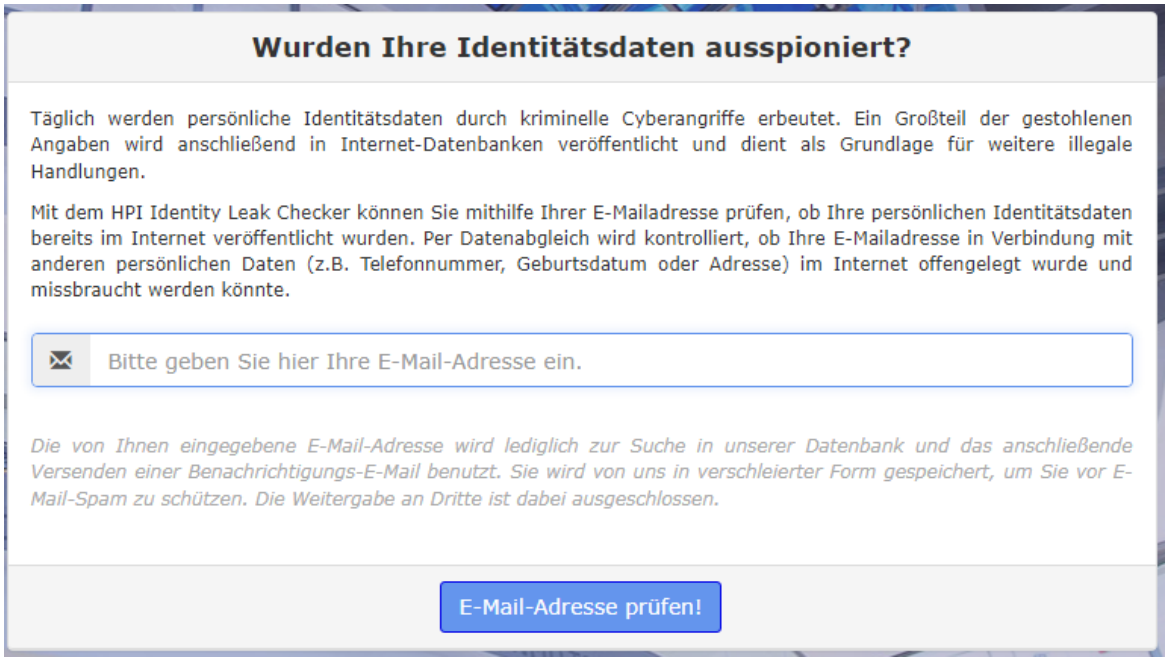
Mehr zum Thema IT-Sicherheit

- Safety first: Die IT-Sicherheitsrichtlinie
  → Nächste Termine: Mi, 26.04.2023 15-19 Uhr
  Mi, 25.10.2023 15-19 Uhr

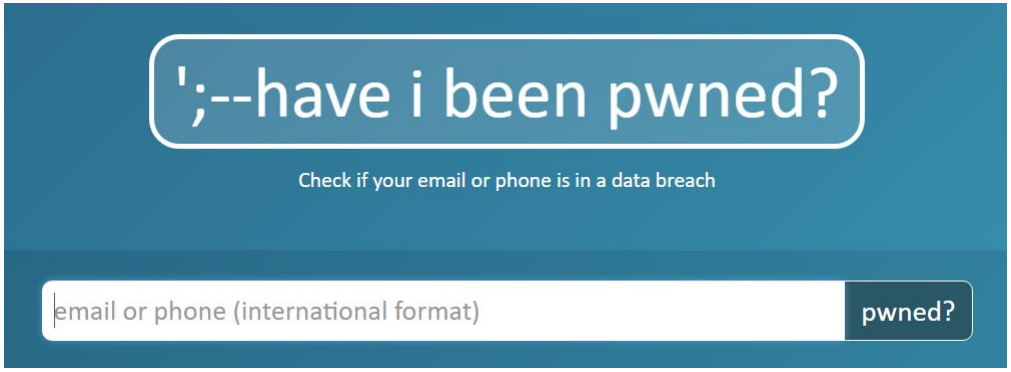
- Die BSI Bürger-CERT-Sicherheitsinfos
  - https://www.bsi.bund.de
  - Das BSI ist die Bundesbehörde für IT-Sicherheit und bietet zahlreiche Angebote ihre IT-Sicherheit zur Verbesserung aufzuklären.

- KBV-Seite zur IT-Sicherheitsrichtlinie
  - https://www.kbv.de/html/it-sicherheit.php
  - Seite der KBV zur IT-Sicherheitsrichtlinie mit Info-Broschüre und Liste von zertifizierten Beratern und Links zum Online-Hub der IT-Sicherheitsrichtlinie

Mehr zum Thema IT-Sicherheit



Quelle: https://sec.hpi.uni-potsdam.de/ilc/



Quelle: https://haveibeenpwned.com

Fragen?

IT in der Praxis
0711 7875 3570
itp@kvbawue.de

Gerne Feedback an uns!

Alles Gute.
KVBW
Kassenärztliche Vereinigung Baden-Württemberg