IT-SICHERHEIT IN DER ARZTPRAXIS

Die IT-Sicherheitsrichtlinie der Kassen(zahn)ärztlichen Bundesvereinigung im Blick

Sandra Zunabovic

KRANKENHÄUSER

§ 8a Abs. 1 BSI-G für KRITIS
§ 75c SGB V für Nicht-KRITIS

19,4 MIO.

Behandlungsfälle pro Jahr

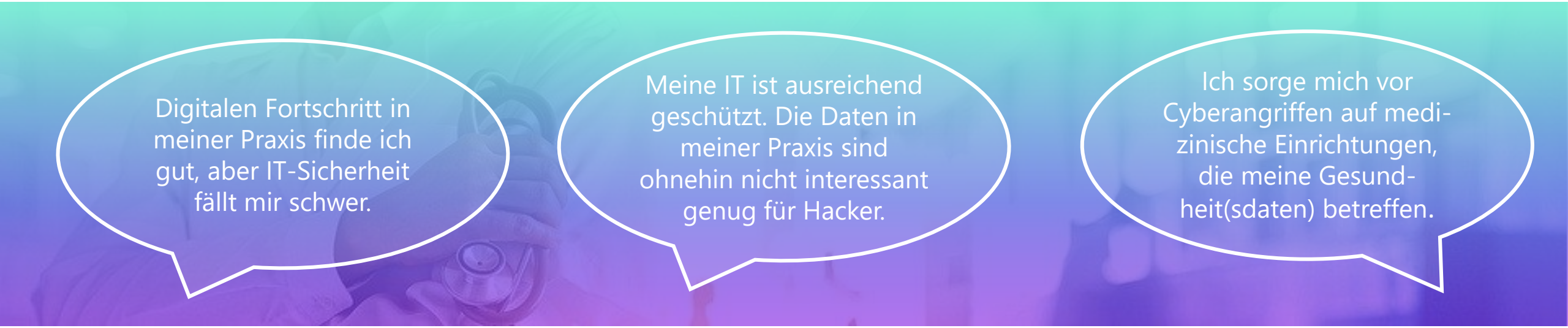
= 10 Mio. Behandlungs-fälle pro Jahr

NIEDERGELASSENE ÄRZT:INNEN

570 MIO.

Behandlungsfälle pro Jahr

STIMMEN AUS DER PRAXIS



PraxisBarometer Digitalisierung

KBV (2019 & 2020)

Cyberrisiken bei Ärzten und Apothekern

Gesamtverband der deutschen Versicherungswirtschaft e.V. (2018)

Datensicherheit in Kliniken und Arztpraxen

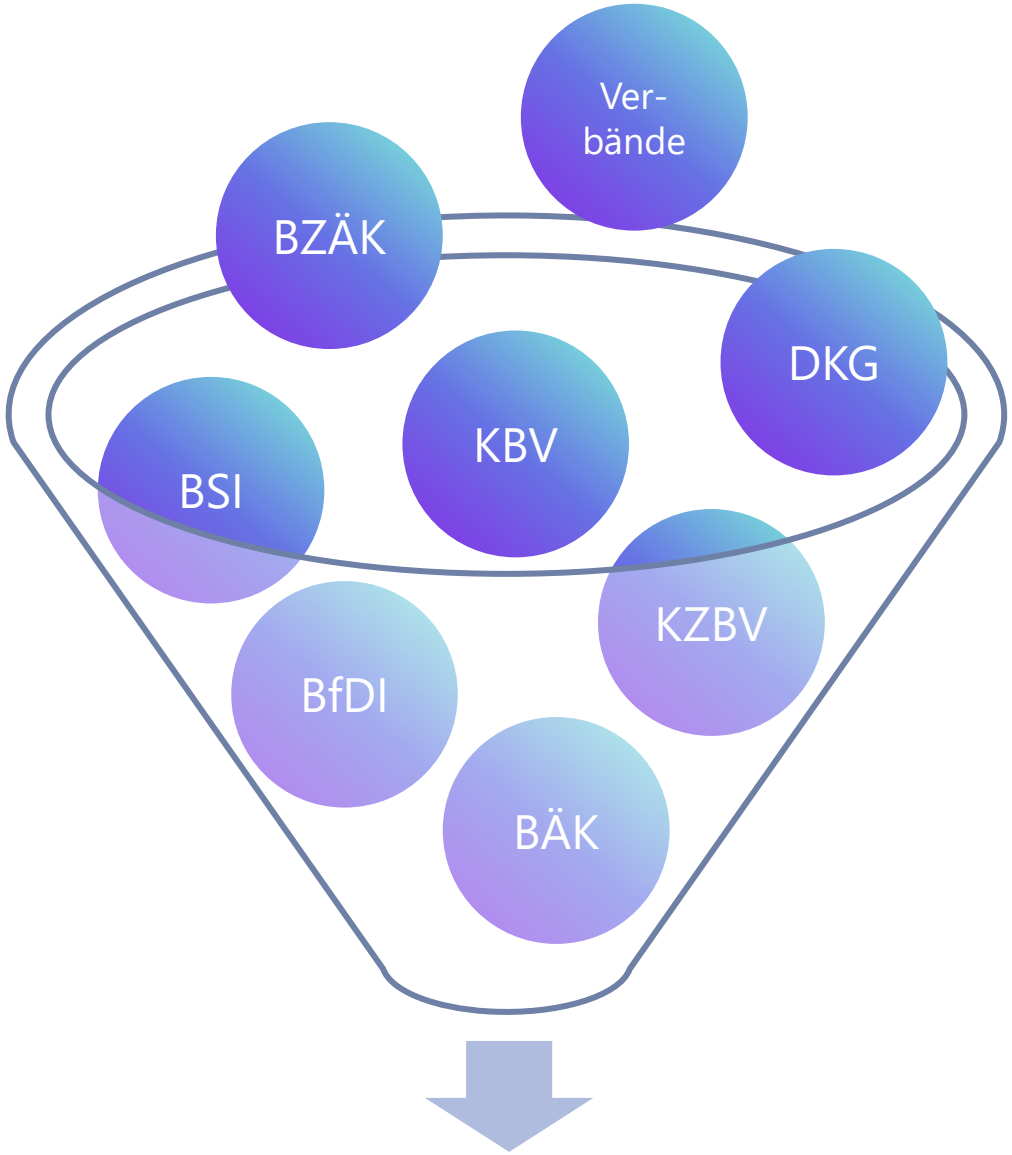
PwC Deutschland (2019)

§ 75b SGB V

„Die Kassenärztlichen Bundesvereinigungen legen […] in einer Richtlinie **die Anforderungen zur Gewährleistung der IT-Sicherheit** in der vertragsärztlichen und vertragszahnärztlichen Versorgung fest.

[Diese] müssen geeignet sein, abgestuft im **Verhältnis zum Gefährdungspotential** und dem **Schutzbedarf** der verarbeiteten Informationen, Störungen […] in Bezug auf **Verfügbarkeit, Integrität und Vertraulichkeit** […] zu vermeiden.

[Die] Anforderungen müssen dem **Stand der Technik** entsprechen und sind **jährlich** […] **anzupassen.**“



IT-SICHERHEITSRICHTLINIE

§ 75b SGB V

AUFBAU DER RICHTLINIE

	Zielobjekt	Klein (Anlage 1)	Mittel (Anlage 2)	Groß (Anlage 3)	Großgeräte (Anlage 4)	Telematik (Anlage 5)
Software	Mobile Anwendungen (Apps)	4	1			
Software	Office-Produkte	2				
Software	Internet-Anwendungen	5	1			
Hardware	Endgeräte	4	1			
Hardware	Endgeräte Windows	3	1			
Hardware	Smartphone und Tablet	6	2	3		
Hardware	Mobiltelefon	3	2			
Hardware	Mobile Device Management (MDM)			6		
Hardware	Wechseldatenträger / Speichermedien	4	1	2		
Hardware	Netzwerksicherheit	3	1	1		
GG	Großgeräte				6	
TI	Telematik					7
	Praxisgröße	**<= 5 Personen**	**6 – 20 Personen**	**>= 21 Personen „Mehr als normale Datenübermittlung“**	**Praxen mit Großgeräten (z.B. MRT)**	**Praxen mit Telematik-Infrastruktur (= alle)**
	Anforderungen (kumuliert)	**34**	**45**	**57**	**6**	**7**

ANLAGE 2

Zusätzliche Anforderungen für mittlere Praxen

	Zielobjekt	Anforderung	Erläuterung	Geltung ab
2.	Internet-Anwendungen	Zugriffskontrolle bei Webanwendungen	Sicherstellung von Berechtigungen.	01.01.2022
	Hardware: Endgeräte und IT-Systeme			
3.	Endgeräte	Nutzung von TLS	Benutzer sollten darauf achten, dass zur Verschlüsselung von Webseiten TLS verwendet wird.	01.01.2022
4.	Endgeräte	Restriktive Rechtevergabe	Restriktive Rechtevergabe.	01.01.2022
5.	Endgeräte mit dem Betriebssystem Windows	Sichere zentrale Authentisierung in Windows-Netzen	In reinen Windows-Netzen SOLLTE zur zentralen Authentisierung für Single Sign On (SSO) ausschließlich Kerberos eingesetzt werden.	01.07.2022
6.	Smartphone und Tablet	Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten	Es sollte eine verbindliche Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten erstellt werden.	01.07.2022
8.	Mobiltelefon	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung	Werden Mobiltelefone für dienstliche Zwecke verwendet, muss eine Nutzungs- und Sicherheitsrichtlinie erstellt werden.	01.07.2022

SCHWÄCHEN DER RICHTLINIE

Wording

Kontext Datenschutz & Informations-sicherheit

Fokus auf technischen Maßnahmen

Diskrepanz Praxisgröße und Benennung DSB

- „Daten“
- „Vertraulichem“
- „vertraulichen Daten“
- „persönlichen Daten“
- „personenbezogenen Informationen“
- „Informationen“
- „Rest-Informationen“
- „schützenswerten Informationen“

- Internet-Anwendungen

- Mobile Geräte
  (Smartphones vs. Mobiltelefone vs. MDM)

Zugriffskontrolle bei Webanwendungen	Sicherstellung von Berechtigungen.
Firewall benutzen	Verwendung und regelmäßiges Update einer Web App Firewall.
Kryptografische Sicherung vertraulicher Daten	Nur verschlüsselte Internet-Anwendungen nutzen.

6.	Smartphone und Tablet	Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten	Es sollte eine verbindliche Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten erstellt werden.	01.07.2022
8.	Mobiltelefon	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung	Werden Mobiltelefone für dienstliche Zwecke verwendet, muss eine Nutzungs- und Sicherheitsrichtlinie erstellt werden.	01.07.2022
1.	Smartphone und Tablet	Festlegung einer Richtlinie für den Einsatz von Smartphones und Tablets	Bevor eine Praxis Smartphones oder Tablets bereitstellt, betreibt oder einsetzt, muss eine generelle Richtlinie im Hinblick auf die Nutzung und Kontrolle der Geräte festgelegt werden.	01.01.2022

SCHWÄCHEN DER RICHTLINIE

Wording

Kontext Datenschutz & Informations-sicherheit

Fokus auf technischen Maßnahmen

Diskrepanz Praxisgröße und Benennung DSB

SCHWÄCHEN DER RICHTLINIE

Wording

Kontext Datenschutz & Informations-sicherheit

Fokus auf technischen Maßnahmen

Diskrepanz Praxisgröße und Benennung DSB

SCHWÄCHEN DER RICHTLINIE

Wording

Kontext Datenschutz & Informations-sicherheit

Fokus auf technischen Maßnahmen

Diskrepanz Praxisgröße und Benennung DSB

LÖSUNGSENTWICKLUNG

Kategorie	Pflicht (KBV)	Empfehlung	Gesamt
1. Management und Organisation	1	3	4
2. Physische Sicherheit	0	3	3
3. Server-Sicherheit	0	7	7
4. Sensibilisierung der Mitarbeitenden	1	3	4
5. Identitäts- und Berechtigungsmanagement	3	4	7
7. Clients (Computer)	5	2	7
7. Smartphones und Tablets	19	0	19
8. Wechseldatenträger	5	2	7
9. Entsorgung	0	5	5
10. Webseiten und Webservices	3	2	5
11. Netzwerk	5	2	7
12. Notfallmanagement	1	3	4
Summe	**43**	**36**	**79**

CONCLUSIO

- Einführung der Richtlinie richtig und wichtiges Signal
- Aber: Potenzial nicht vollumfänglich ausgeschöpft
- Aktualisierung ausstehend: Welche Änderungen kommen (wenn überhaupt)?

VIELEN DANK!

Sandra Zunabovic
Studentin „IT-Sicherheit“ (M.Sc.) @ Hochschule München
Information Security Consultant @ secjur GmbH

linkedin.com/in/szunabovic/
sandra.zunabovic@hm.edu