



Der Landesbeauftragte für
DATENSCHUTZ und
INFORMATIONSFREIHEIT
Mecklenburg-Vorpommern

Datenschutz und Datensicherheit in der „Praxis“

Thomas Brückmann
Referatsleiter Technik

c/o Der Landesbeauftragte für Datenschutz und
Informationsfreiheit Mecklenburg-Vorpommern



„Praxis“-Beispiel: Cyberangriff



Der Landesbeauftragte für
DATENSCHUTZ und
INFORMATIONSFREIHEIT
Mecklenburg-Vorpommern



„Praxis“-Beispiel: Cyberangriff



Der Landesbeauftragte für
DATENSCHUTZ und
INFORMATIONSFREIHEIT
Mecklenburg-Vorpommern

All your files are locked!

 [Unlock](#)

Time left
95 : 57 : 43

All your important files have been encrypted.
If you want your files back, you need to pay €400 in Bitcoins.
After the payment is received, we will give you access to unlock your files.
Click on the Payment button to get more info.

If you don't pay within 48 hours, the price will be doubled.
After another 24 hours, the price will be doubled again.
If you don't pay within 96 hours your files will be destroyed.

User-ID: 67ZFY613CY Important Payment

„Praxis“-Beispiel: Cyberangriff



Fall einer Gemeinschaftszahnarztpraxis

- Mitarbeiterin öffnet am Montagmorgen eine E-Mail mit dem Titel „Terminvorschläge für die professionelle Zahnreinigung“
- im Anhang befindet sich eine Word-Datei mit den vermeintlichen Empfehlungen
- Öffnen führt zu Installation eines Trojaners
- Lösegeldsumme in Höhe von „nur“ 10 Bitcoins
- 2 Wochen kein Praxisbetrieb möglich
- Reputationsschaden: 40% der Patienten suchten neuen Zahnarzt

Cyberangriff und nun?



- ZIEL: Schadensbegrenzung
- frühzeitig mit einer solchen potenziellen Situation auseinandersetzen und einen **Notfallplan** haben
- IT-Dienstleister, falls vorhanden, kontaktieren
- betroffene Rechner bzw. Server mit der Patientenkartei sofort ausschalten und vom Internet trennen
- (falls noch möglich) Passwörter ändern
- ACHTUNG: **Passwortsicherheit!!!** (Passwörter im Praxisumfeld: „Behandlung“, „Praxis“, Name des Arztes, „Name“ des Computers – oder gar kein Passwort)
- Schaltzentrale E-Mail → wurden hier neue Passwörter für verknüpfte Konten beantragt oder E-Mails versendet (Identitätsdiebstahl)?
- Meldepflichten gem. Art. 33 und 34 DSGVO prüfen
- Strafanzeige erstatten

Cyberangriff und nun?



Meldepflicht gem. Art. 33 DSGVO

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der [...] zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt.

Der Ausdruck „Verletzung des Schutzes personenbezogener Daten“ bezeichnet eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Benachrichtigungspflicht gegenüber den betroffenen Dritten nach Art. 34 DSGVO prüfen – also den Patienten – sofern ein hohes Risiko besteht

Cyberangriff und nun?



Lessons learned

- Ursachenforschung
- Schwachstellen in der IT ausmachen und daraus lernen
- technischen und organisatorischen Maßnahmen der Praxis – wie Passwortmanagement, Backups, Firewall, Virenschutz, Mitarbeitersensibilisierung, Verschlüsselung und vieles mehr – überarbeiten
- Schulung für die Mitarbeiter

Der IT auf den Zahn gefühlt...



Kennen Sie die IT-Sicherheitsrichtlinie nach § 75b SGB V ?



- Die IT-Sicherheitsrichtlinie nach § 75b SGB V (**Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung**) regelt die Anforderungen an das IT-Sicherheitsniveau in den Praxen der Ärztinnen und Ärzte, Zahnärztinnen und Zahnärzte und Psychotherapeutinnen und Psychotherapeuten in der gesetzlichen Versorgung.
- Nach der derzeit gültigen IT-Sicherheitsrichtlinie gelten Praxen mit bis zu fünf Beschäftigten, die ständig mit Aufgaben der Datenverarbeitung betraut sind, als kleine Praxen, sechs bis 20 Beschäftigte als mittlere Größe und über 20 Beschäftigte als große Praxen
- Am 2. Februar 2021 in Kraft getreten.

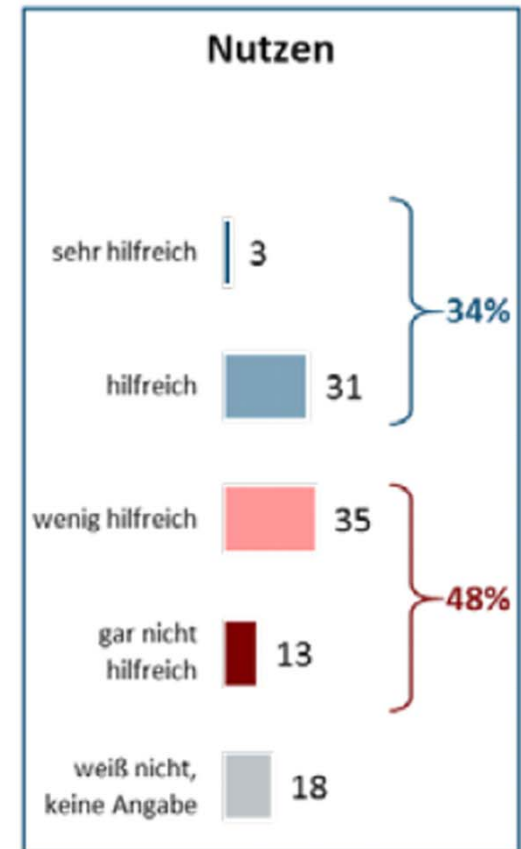
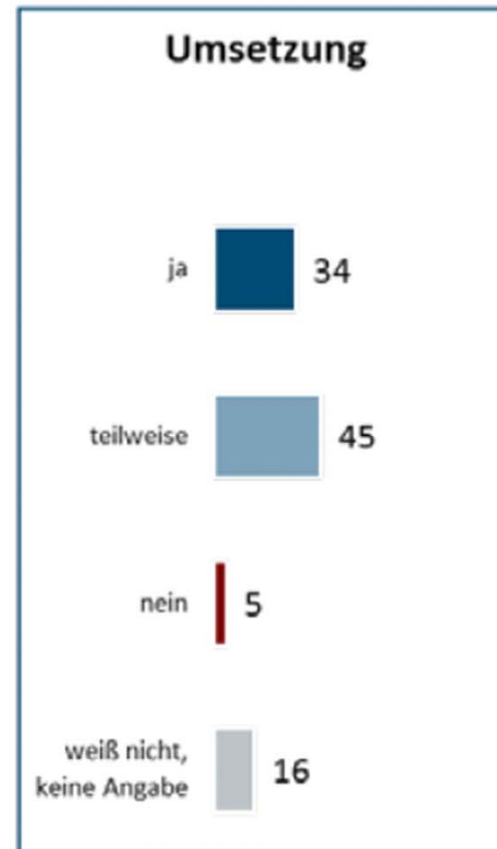
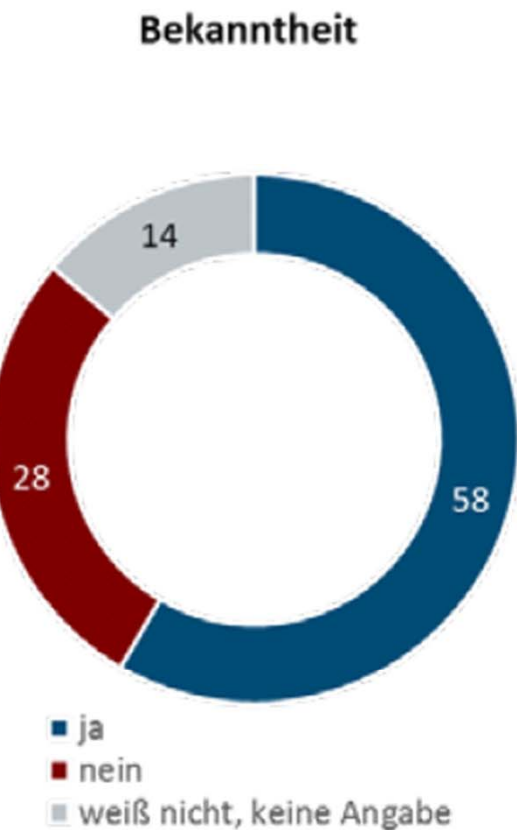


Anforderungen für Praxen

	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-Speicher zur Speicherung personenbezogener Informationen.	01.04.2021
6.	Office-Produkte	Beseitigung von Rest-Informationen vor Weitergabe von Dokumenten	Vertrauliches aus Dokumenten löschen vor einer Weitergabe an Dritte.	01.04.2021

7.	Internet-Anwendungen	Authentisierung bei Webanwendungen	Nutzen Sie nur Internet-Anwendungen, die ihre Zugänge (Login-Seite und -Ablauf, Passwort, Benutzerkonto etc.) strikt absichern.	01.04.2021
8.	Internet-Anwendungen	Schutz vertraulicher Daten	Stellen Sie ihren Internet-Browser gem. Hersteller-Anleitung so ein, dass keine vertraulichen Daten im Browser gespeichert werden.	01.04.2021
9.	Internet-Anwendungen	Firewall benutzen	Verwendung und regelmäßiges Update einer Web App Firewall.	01.01.2022
10.	Internet-Anwendungen	Kryptografische Sicherung vertraulicher Daten	Nur verschlüsselte Internet-Anwendungen nutzen.	01.04.2021
11.	Internet-Anwendungen	Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen	Keine automatisierten Zugriffe bzw. Aufrufe auf Webanwendungen einrichten oder zulassen.	01.01.2022

Evaluation in 2024 durch das BSI





Die IT-Sicherheitsrichtlinie

nach § 75b SGB V

Hinweise des BSI für Anwenderinnen und Anwender



Lfd

Datenschutz & IT-Sicherheit in der Zahnarztpraxis

Leitfaden

+ Empfehlungen zur Umsetzung der IT-Sicherheitsrichtlinie

06/2021



KZBV

» Kassenzahnärztliche
Bundesvereinigung



BUNDEZAHNÄRZTEKAMMER

Vorsorge ist besser als Nachsorge



Quick-Wins:

- Updates, Updates, Updates...
- Schulung für die Mitarbeiter, insbesondere im Umgang mit Mails (z.B. „Bewertung Ihrer Praxis auf DocCheck mit einer Note von 4-“ oder fingierte Bewerbungsmails, Paketdienste,...)
- aktuellen Virenschutz/Firewalls
- sichere einmalige Passworte für **jeden** Nutzer und 2-Faktor Authentifizierung wo möglich
- Rechte- und Rollenkonzept -> Wer darf was?

Vorsorge ist besser als Nachsorge



Lfd

Beispiel für den Einstieg in ein Rechte- und Rollenkonzept:

Zur Dokumentation der Rollen und Rechte der Mitarbeitenden dient eine Tabelle, wie im Folgenden beispielhaft skizziert:

Funktion/Personengruppe	Alle Mitarbeitenden	Spezialisierte Mitarbeitende (bspw. Empfang oder Sekretariat)	Administrator
Patientinnen und Patienten empfangen	×	×	
Rezepte & Überweisungen ausstellen	×	×	
Digitale Kommunikation mit anderen medizinischen Fachkräften		×	
Verwaltung der IT			×

Vorsorge ist besser als Nachsorge



LfD

Beispiel für das Fortschreiben des Rechte- und Rollenkonzeptes:

Funktion/Personengruppe	Alle Mitarbeitenden	Spezialisierte Mitarbeitende (bspw. Empfang oder Sekretariat)	Administrator
Einrichten/Konfigurieren (neuer) IT-Komponenten (z.B. Rechner, Router, Telefone)			×
Installation von Updates			×
Anlegen und Vergabe (neuer) Nutzeraccounts			×
Vergabe von Zugangsdaten			×
Sperrung von Zugängen			×
Zugriff auf E-Mailpostfächer		×	×
Zugriff auf Kalendereinträge	×	×	
	(lesend)	(ohne Einschränkungen)	

Vorsicht ist besser als...



Quick-Wins:

- Updates, Updates, Updates...
- Schulung für die Mitarbeiter, insbesondere im Umgang mit Mails (z.B. „Bewertung Ihrer Praxis auf DocCheck mit einer Note von 4-“ oder fingierte Bewerbungsmails)
- aktuellen Virenschutz/Firewalls
- sichere einmalige Passworte für **jeden** Nutzer und 2-Faktor Authentifizierung wo möglich
- Rechte- und Rollenkonzept -> Wer darf was?
- keine Administrationsaccounts im Alltag nutzen
- Makros deaktivieren
- „analoges“ Notfallkonzept (Notfallnummern, Administrations-Passwörter und Zugangsdaten [sicher aufbewahrt], Verträge und Ansprechpartner)
- Übersicht über die vorhandenen IT-Geräte und den Anwendungen (Netzplan)
- sichere Entsorgung (Papier, [defekte] Festplatten [auch Drucker], USB-Sticks)

UND:

***Kein Backup?
Kein Mitleid!***



Warum ist ein Backup wichtig?

- Verschlüsselungs-Trojaner/Cyberangriff
- Hardwaredefekt (Konfiguration gespeichert?)
- Daten können *versehentlich* gelöscht werden
- Virenbefall (es muss nicht immer der gezielte Angriff sein)
- Konto (z.B. E-Mail/Cloudanwendung) wurde deaktiviert
- ...

Frage 3-2-1: Haben Sie eine Backupstrategie?


Haben Sie Ihr(e) Backup(s) getestet?

Was gilt es zu beachten?


- komplexen Gerätesperrcode verwenden
- nach der Nutzung muss sich die Person abmelden bzw. das Gerät sperren
- bei Verlust muss das Gerät und die darin verwendete SIM-Karte zeitnah gesperrt werden
- Apps nur aus den offiziellen App-Stores beziehen und restlos löschen, wenn sie nicht mehr benötigt werden
- App-Berechtigungen prüfen

one.de 16:37

brightest flashlight

 **Brightest Taschenlampe**
GOLDENSHORES TECHNOLOGIES, LLC

INSTALLIEREN



★ 1.004.207 08.09.2013
1.000+ Downloads 1,21 MB

66 Tsd. Personen geben hierfür +1

Beschreibung

Brightest Taschenlampe - kostenlos
Aktiviert alle verfügbaren Lichter auf dem Gerät
Blitz auf Maximum * Screen LED am Maximum
Turbeleuchtung auf Maximum

Vodafone.de 16:38

App-Berechtigungen

Brightest Taschenlampe benötigt folgende Berechtigungen:

System-Tools
Verknüpfungen deinstallieren, Verknüpfungen installieren

Kamera
Bilder und Videos aufnehmen

Speicher
USB-Speicherinhalte ändern oder löschen

Netzkommunikation
Voller Netzwerkzugriff

Anrufe
Telefonstatus und Identität abrufen

Ihren Standort
Genauer Standort (GPS- und netzwerkbasiert),
Ungefäher Standort (netzwerkbasiert)

Alle anzeigen

AKZEPTIEREN

Lizenz

DEUTSCH

**GOLDENSHORES TECHNOLOGIES, LLC
BRIGHTEST TASCHENLAMPE
SOFTWARELIZENZVERTRAG**

BITTE LESEN SIE DIESEN SOFTWARELIZENZVERTRAG („LIZENZ“) SORGFÄLTIG DURCH, BEVOR SIE DIE GOLDENSHORES TECHNOLOGIES SOFTWARE IN BETRIEB NEHMEN. INDEM SIE DIE GOLDENSHORES TECHNOLOGIES SOFTWARE VERWENDEN, ERKLÄREN SIE IHR EINVERSTÄNDNIS MIT DEN BESTIMMUNGEN DES NACHSTEHENDEN LIZENZVERTRAGS. **INSTALLIEREN UND FORTVERWENDEN**

Akzeptieren **Verweigern**

Smartphones und Tablets



Was gilt es zu beachten?

- komplexen Gerätesperrcode verwenden
- nach der Nutzung meldet sich die Person ab
- bei Verlust muss das Gerät und die darin verwendete SIM-Karte zeitnah gesperrt werden
- Apps nur aus den offiziellen App-Stores beziehen und restlos löschen, wenn sie nicht mehr benötigt werden
- App-Berechtigungen prüfen
- keine vertraulichen Daten über Apps versenden

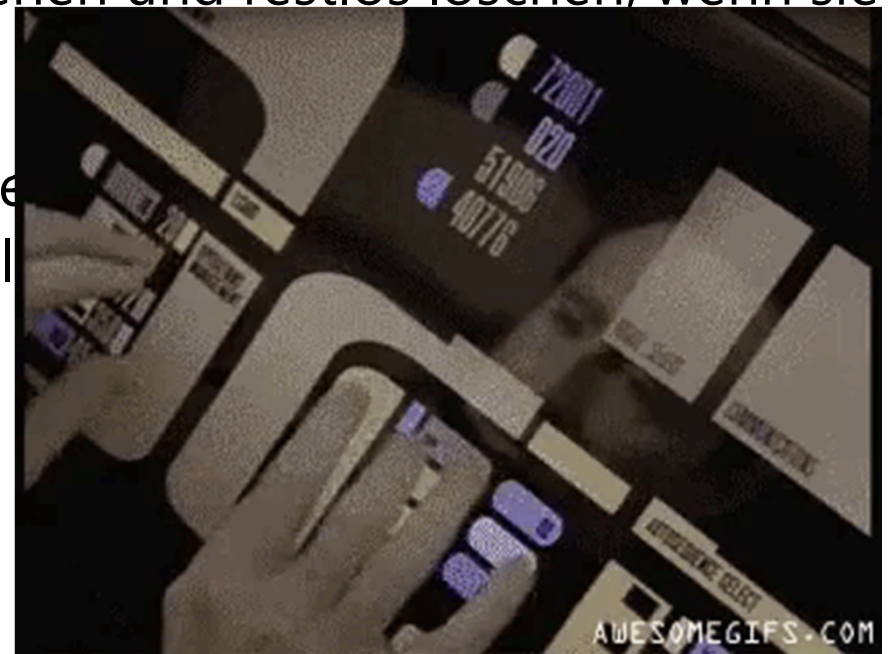


Smartphones und Tablets

Was gilt es zu beachten?

- komplexen Gerätesperrcode verwenden
- nach der Nutzung meldet sich die Person ab
- bei Verlust muss das Gerät und die darin verwendete SIM-Karte zeitnah gesperrt werden
- Apps nur aus den offiziellen App-Stores beziehen und restlos löschen, wenn sie nicht mehr benötigt werden
- App-Berechtigungen prüfen
- keine vertraulichen Daten über Apps versenden
- nur Apps nutzen, die Dokumente verschlüsseln
- Updates, Updates, Updates...

Frage: Haben Sie ein Backup? ;-)





Der Landesbeauftragte für Datenschutz und Informationsfreiheit

Telefon: 0385 59494-0

E-Mail: info@datenschutz-mv.de

Internetseite: www.datenschutz-mv.de
