Engagiert für Gesundheit.
Kassenärztliche Vereinigung Nordrhein

IT-Sicherheit in der Praxis

29.01.2020 | Düsseldorf

Claudia Pintaric
Franz-Josef Eschweiler

Agenda

- Zugriff und Authentisierung
- Internet, E-Mail und Cyberangriffe
- IT-Sicherheit und Telematik-Infrastruktur
- Backups und Verschlüsselung
- Notfallkonzept und Cyberversicherung

Definition und Bedeutung

Zunehmende Digitalisierung

Cyber-kriminalität

Gesundheits-daten im Fokus

Gewährleistung der Sicherheit digitaler Daten sowie der eingesetzten Informationstechnologien

wird in Praxen immer wichtiger

Datenschutz und Schweigepflicht

Geldbußen/ Freiheitsstrafen möglich

Zugriff und Authentisierung

Zugriff und Authentisierung

Sensible Patientendaten müssen vor unbefugten Zugriff geschützt werden.

Bei digitalen Daten muss dies über Zugriffsschutz erfolgen. Der Zugriff auf Systeme und Anwendungen, die sensible und schützenswerte Daten enthalten, muss mindestens über ein Passwort erfolgen.

Zugriff und Authentisierung

„Passwörter sind wie Unterwäsche. Du darfst sie keinen sehen lassen, musst sie regelmäßig wechseln und solltest sie nicht mit Fremden tauschen.“ (Technik-Blogger Chris Pirillo)

So nicht!

Sicheres Passwort, Empfehlung BSI:
Mindestens 8 Stellen, bestehend aus Buchstaben, Zahlen und Sonderzeichen

Zugriff und Authentisierung

IT-Sicherheitsüberprüfung in 25 Praxen
des Gesamtverbandes der deutschen Versicherungswirtschaft (GDV)
September – Dezember 2018

„Deutschlands Ärzte haben ein Passwort-Problem.
Zugangsdaten häufig im Darknet zu finden.“

Zugriff und Authentisierung

→ 22 von 25 Praxen nutzen sehr einfach zu erratende Passwörter (z. B. Behandlung, Praxis, Name des Arztes) oder gar keine Passwörter

→ In 22 von 25 Praxen teilen sich mehrere Benutzer dieselbe Zugangskennung

→ In 20 von 25 Praxen haben alle Benutzer Administratorenrechte

→ Keine Praxis prüft, ob alte Administratorenrechte noch bestehen.

Quelle: Gesamtverband der Deutschen Versicherungswirtschaft (GDV)

Zugriff und Authentisierung

Awareness-Video vom Bundesamt für Sicherheit in der Informationstechnik zum Surfen mit Administratorenrechten

(1:12 Minuten)

Videos beim BSI
https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Mediathek/Videos/videos_node.html

Zugriff und Authentisierung

Aktivieren Sie <u>immer</u> die Bildschirmsperre, sobald ein Arbeitsplatz unbeaufsichtigt ist!

Manuelle Sperrung über „Windows-Taste“ + L

Entsperrung über Passwort

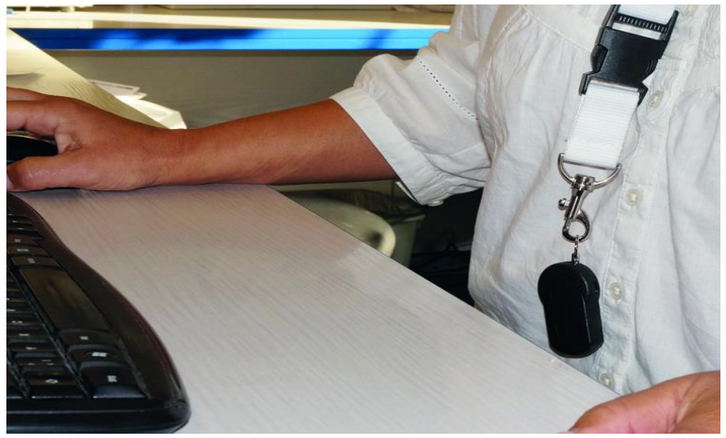
Nachteil:

- Passwörter werden vergessen
- Eingabe umständlich
- Passwörter sollten regelmäßig geändert werden

Zugriff und Authentisierung

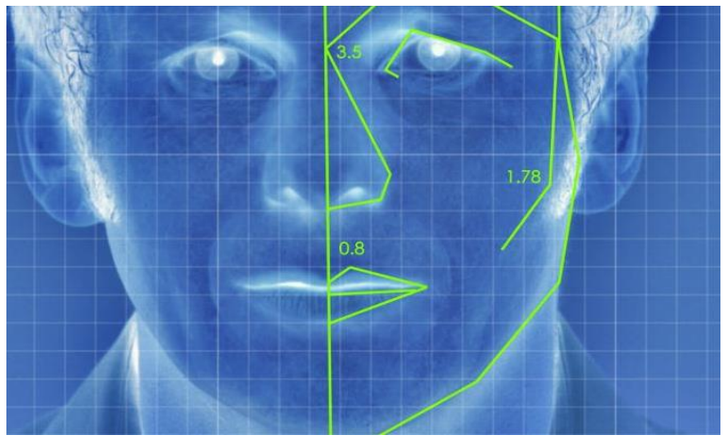
Mögliche Alternativen zur Passworteingabe

Sperrung/Entsperrung über Transceiver



- Sendechip gekoppelt mit Empfängerchip
- Erkennt die Nähe einer befugten Person und entsperrt den PC
- Kosten: ca. 100 – 200 Euro pro Arbeitsplatz

Anmeldung über Gesichtserkennung



- Benötigt Kamera und Software
- Integriert in Windows 10, funktioniert aber nur mit einer RealSense-Kamera

Mögliche Alternativen zur Passworteingabe

Anmeldung über Fingerprint

- Benötigt einen Fingerabdruckscanner
- Integriert in Windows 10
- Scanner bei neueren Notebooks integriert
- Kosten externe Scanner: ca. 100 Euro

Anmeldung über Handvenenerkennung

- Funktioniert über Infrarot-Signal
- Derzeit höchste Sicherheit
- Kosten zwischen 150 und 300 Euro

Zugriff und Authentisierung: Zusammenfassung

- ☑ Nutzen Sie möglichst lange Passwörter ➔ je länger das Passwort, desto schwieriger ist es zu hacken.

- ☑ Jeder Nutzer sollte eigene Zugangsdaten und Passwörter haben.
- ☑ Administratorrechte sollten nur an Administratoren vergeben werden.
- ☑ Halten Sie Ihre Passwörter geheim.
- ☑ Nutzen Sie zur besseren Handhabbarkeit Passwortmanager oder alternative Möglichkeiten zur Zugangserkennung.

Internet, E-Mail und Cyberangriffe

Internet, E-Mail und Cyberangriffe

Bundesamt
für Sicherheit in der
Informationstechnik

Schadprogramme im Umlauf

2017	2019
> 600 Mio.	> 900 Mio.

Neue Schadprogramm-varianten täglich

2017	2019
280.000	320.000

Cyberkriminalität nimmt deutlich zu!

Internet, E-Mail und Cyberangriffe

Februar 2016

Computervirus legt Lukaskrankenhaus lahm

Computervirus legt bayerische Klinik lahm

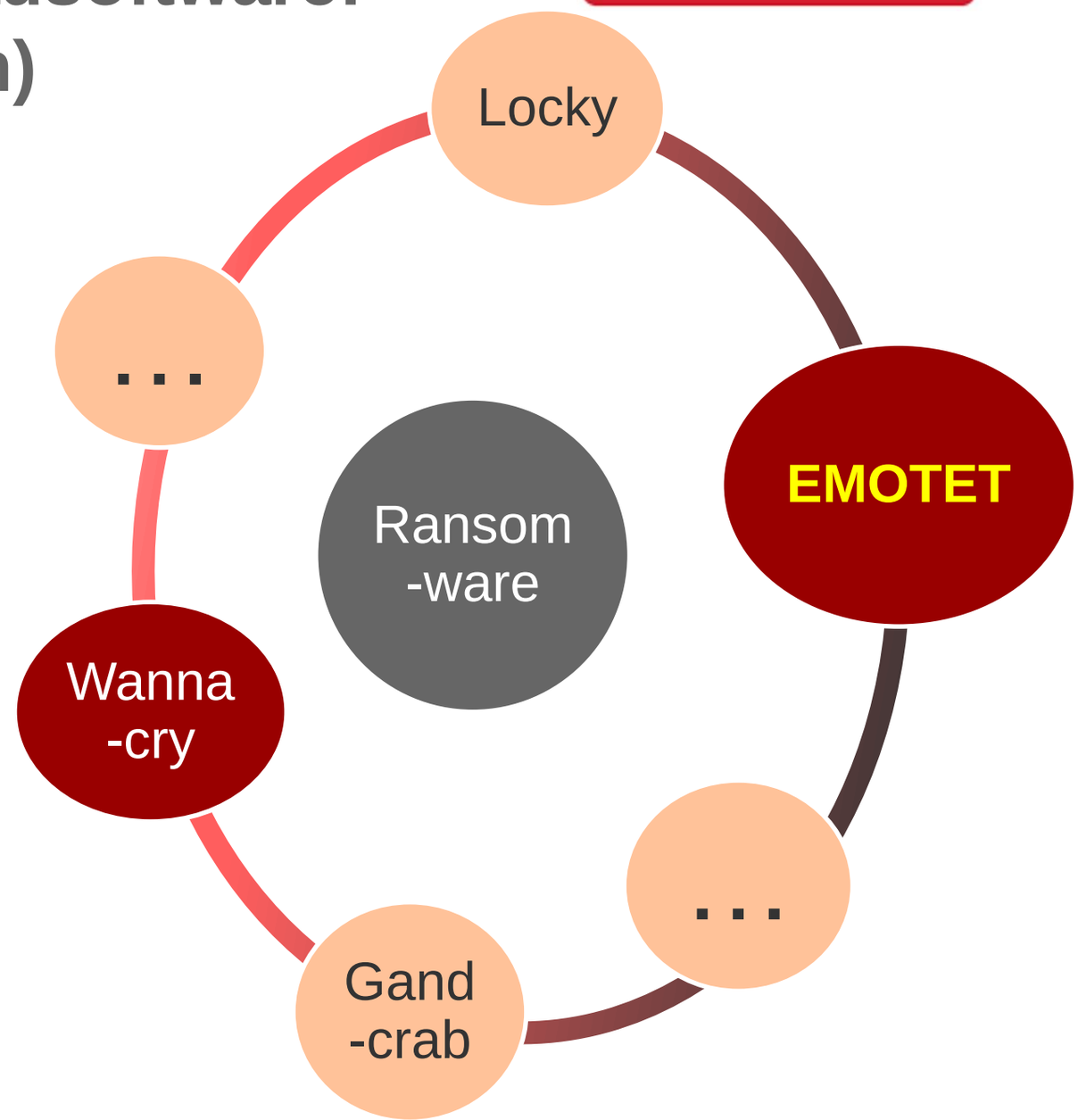
Lösegeld: Hacker verschlüsseln Rechner in Kaiserslauterer Arztpraxis

Protokoll einer Cyberattacke

Eine Bonner Praxis wird Opfer eines Hackerangriffs

Internet, E-Mail und Cyberangriffe

Das größte Einfallstor für Schadsoftware:
➔ E-Mail (75% aller Infektionen)



Internet, E-Mail und Cyberangriffe

Awareness-Video vom Bundesamt für Sicherheit in der Informationstechnik zur E-Mail-Sicherheit

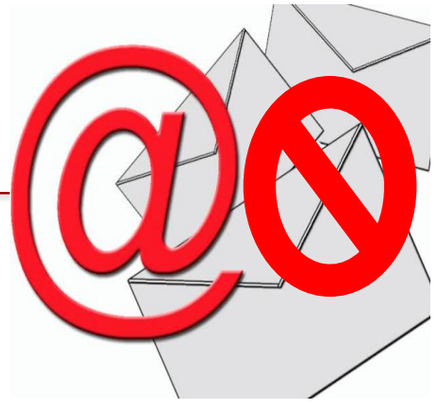
(2:09 Minuten)

Videos beim BSI
https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Mediathek/Videos/videos_node.html

Zusammenfassung: Wie können Sie sich vor Schadsoftware über E-Mail schützen?

- ☑ Löschen Sie E-Mails zweifelhafter Absender sofort!
- ☑ Vorsichtig bei allen E-Mails, die Sie nicht erwartet haben – auch wenn der Absender vermeintlich bekannt ist!
- ☑ Klicken Sie nicht unbedacht auf Anhänge und Links in E-Mails!
- ☑ Achten Sie auf kleine Fehler in der Schreibweise!
- ☑ Öffnen Sie niemals ausführbare Dateianhänge, wie .exe oder .zip!
- ☑ Deaktivieren Sie Makros dauerhaft! Obacht bei Office-Dateien!
- ☑ Sensibilisieren Sie das Praxispersonal!
- ☑ **Am sichersten: Nutzen Sie E-Mail möglichst nicht im Praxisnetzwerk, sondern nur von einem getrennten PC/Notebook/Tablet!**

Internet, E-Mail und Cyberangriffe



By the way…

Unverschlüsselte Patientendaten sollten nicht via E-Mail, WhatsApp & Co. versendet werden.

☹ E-Mail ➔ keine Ende-zu-Ende-Verschlüsselung, vergleichbar mit Postkarte.
WhatsApp ➔ trügerischer Sicherheitsaspekt bei WhatsApp-Verschlüsselung.

☹ Ende-zu-Ende-Verschlüsselung bei E-Mail ist möglich, ABER:
nicht alltagstauglich: Sender + Empfänger müssen Schlüssel erzeugen und austauschen.

😐 E-Mail mit Patient:
➔ nur auf ausdrücklichem Wunsch, schriftliche Einwilligung, Schweigepflichtsentbindung
➔ evtl. weniger problematisch: Terminbestätigung

☺ Sensible Patientendaten nur per Brief (Postgeheimnis) oder persönlich austauschen.

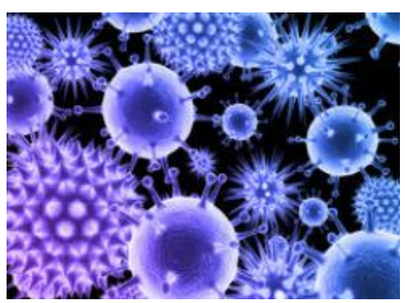
Internetnutzung in der Praxis

- Keine 100-prozentige Sicherheit!
- Adäquate Sicherheitsmaßnahmen ein MUSS!
- Je mehr Sicherheit, umso mehr Komfortverlust (oder Kosten)…

Notwendige technische Maßnahmen bei Internetnutzung

1 **Antivirensoftware**

- ➔ auf allen PCs
- ➔ auch Praxisrechner, die nicht mit dem Internet verbunden sind.



2 **Firewall**

- ➔ stets auf dem neuesten Stand
- ➔ ggfs. individuell anpassen z.B. mit Positivlisten, Port-Sperrung

3 **Sicherheitsupdates**

- ➔ regelmäßig installieren (automatisiert)
- ➔ Betriebssysteme, Virenscanner, Firewall, Browser, ggfs. Anwendungen

Weitere Maßnahmen

- Internetnutzung im Praxisnetz auf notwendige Zugriffe beschränken.
- Netztrennung: z.B. separaten PC / Tablet für Internet über Gast-WLAN nutzen.
- Virtuelle Maschine (VM-Ware), Sandbox
- Plug-Ins im Browser vermeiden, Javascript , ActiveX , Flash deaktivieren, Werbeblocker nutzen.
- Gemanagte IT-Sicherheitslösungen (Kosten!) mit Hardware-Firewall und Dienstleistung
  ➔ fragen Sie Ihren IT-Dienstleister

Weitere Maßnahmen

Praxisteam:

- sensibilisieren, schulen
- Regeln zum Umgang mit dem Internet vereinbaren (Dienstvereinbarung)

BSI
www.bsi-fuer-buerger.de

KBV:
https://www.kbv.de/html/mein_praxischeck.php
https://www.kbv.de/html/datensicherheit.php

IT-Sicherheit und Telematik-Infrastruktur

IT-Sicherheit und Telematik-Infrastruktur

Bin ich mit der Telematik-Infrastruktur noch sicher?

Wer haftet im Falle einer Sicherheitslücke?

Was ist mit Datenschutz und EU-DSGVO?

Sind Installationen im Parallelbetrieb alle unsicher?

IT-Sicherheit und Telematik-Infrastruktur

Jede Praxis ist grundsätzlich für die Sicherheitsmaßnahmen in der Praxis verantwortlich.

- Die korrekte Installation eines Konnektors ändert nichts am bestehenden Sicherheitsniveau der Praxis.
- Mit der Telematikinfrastruktur ist man nicht automatisch im Internet.
- Es kommt immer darauf an, wo und warum sich ein Sicherheitsvorfall ereignet hat ➔ infizierte E-Mails z.B. haben nichts mit der TI zu tun
- Praxen sind verantwortlich für die bestimmungsgemäße Aufstellung und Verwendung des Konnektors.

Die Verantwortung der Praxis endet beim Konnektor, bei einem Datenangriff in der zentralen TI haftet der Betreiber (gematik).

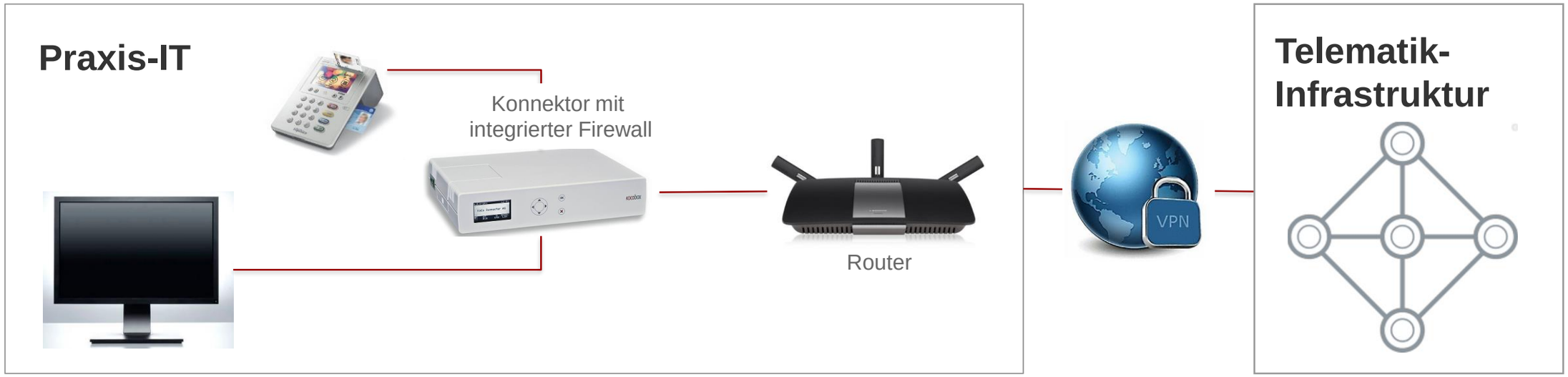
IT-Sicherheit und Telematik-Infrastruktur

Empfehlung für Praxen, die keinen Internetzugang aus dem Praxis-LAN benötigen

Möglichkeiten der Konnektor-Installation

Reihenbetrieb ohne Internetnutzung

- ☑ VPN-Zugangsdienst verbindet nur mit der TI
- ☑ Hohe Sicherheit und durchgängiger Schutz
- ☒ Kein Internetzugriff aus dem Praxis-LAN



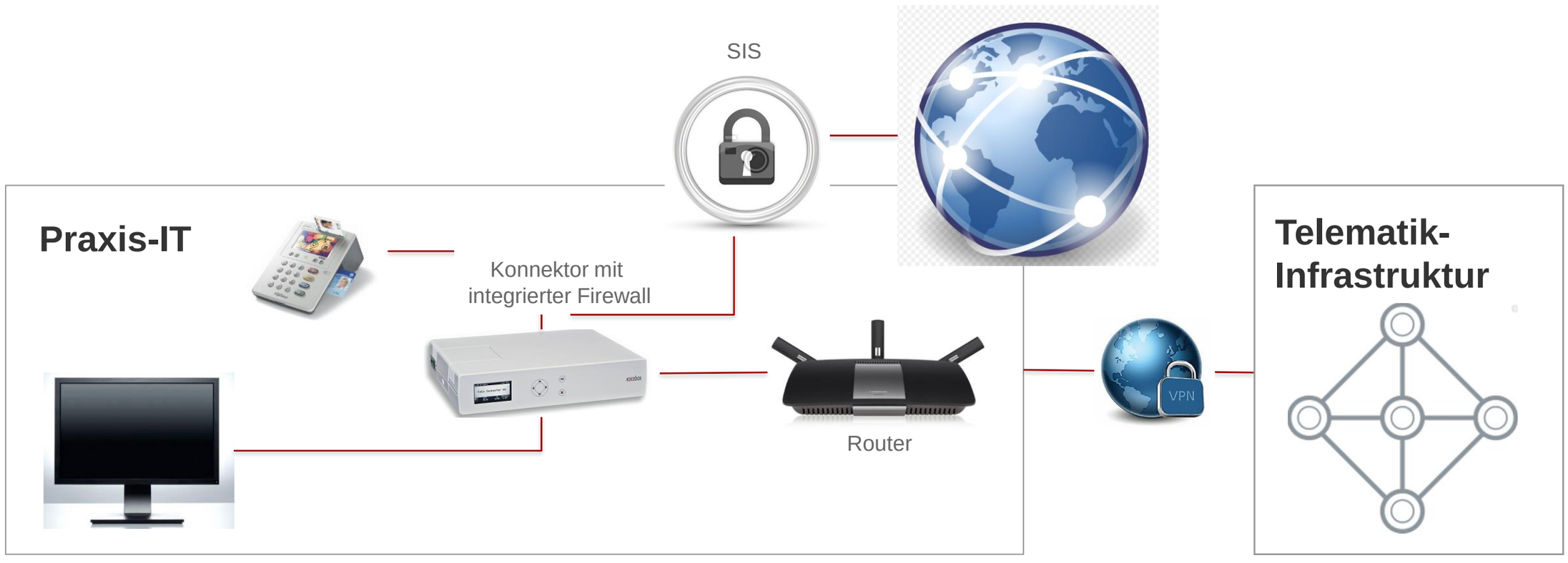
IT-Sicherheit und Telematik-Infrastruktur

Empfehlung für Praxen, die Internet nutzen möchten und keine bestehende Sicherheitsinfrastruktur haben

Möglichkeiten der Konnektor-Installation

Reihenbetrieb mit Internetnutzung

- ☑ Internetzugang über SIS aus dem Praxis-LAN
- ☑ Praxis ist über Firewall des Konnektors geschützt
- ☒ Ggfs. Einschränkungen bei Updates, Fernwartung und WLAN

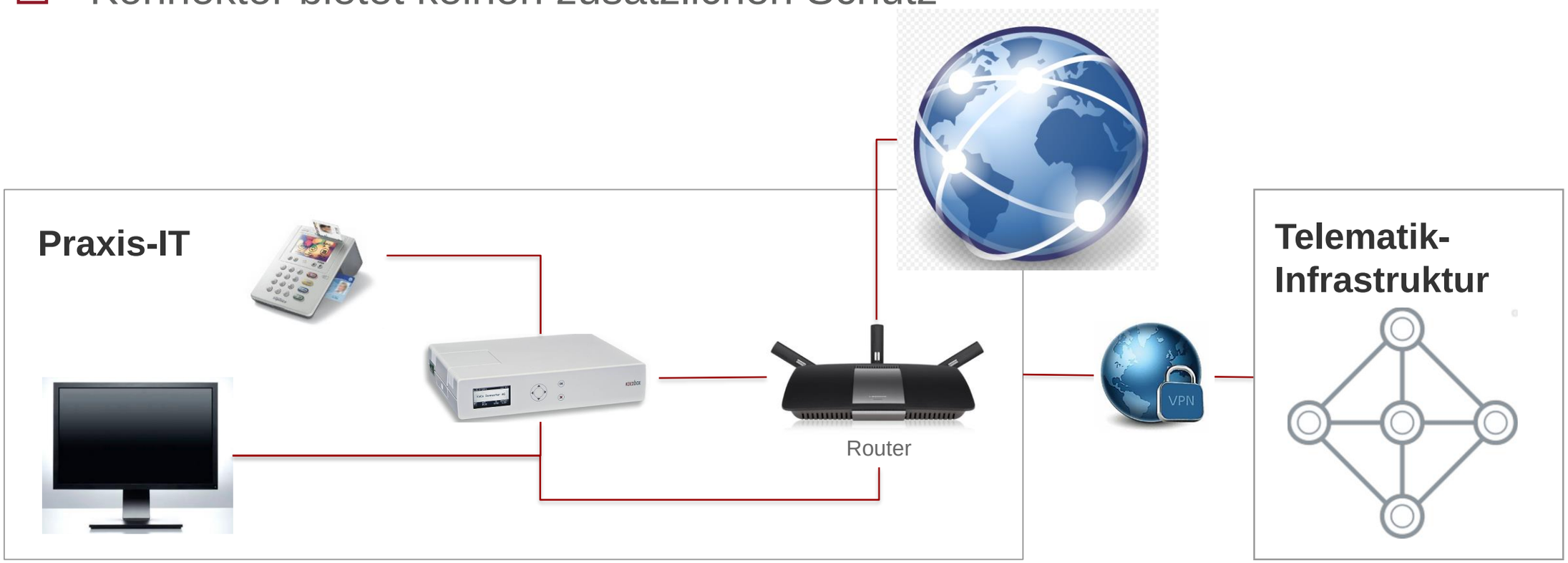


Empfehlung für Praxen mit bestehender Sicherheitsinfrastruktur

Möglichkeiten der Konnektor-Installation

Parallelbetrieb

- ☑ Internetnutzung aus dem gesamten Praxisnetzwerk uneingeschränkt möglich
- ☑ Die Firewall im Router steuert die Kommunikation und schützt die Praxis
- ☒ Konnektor bietet keinen zusätzlichen Schutz



IT-Sicherheit und Telematik-Infrastruktur

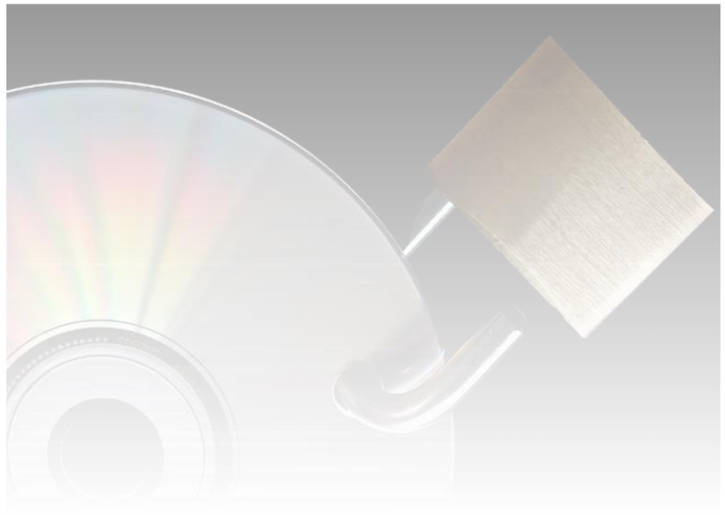
Herausforderung:

Es fehlen einheitliche und eindeutige Sicherheitsvorgaben und eine Datenschutzfolgeabschätzung lt. DSGVO

Lösung:

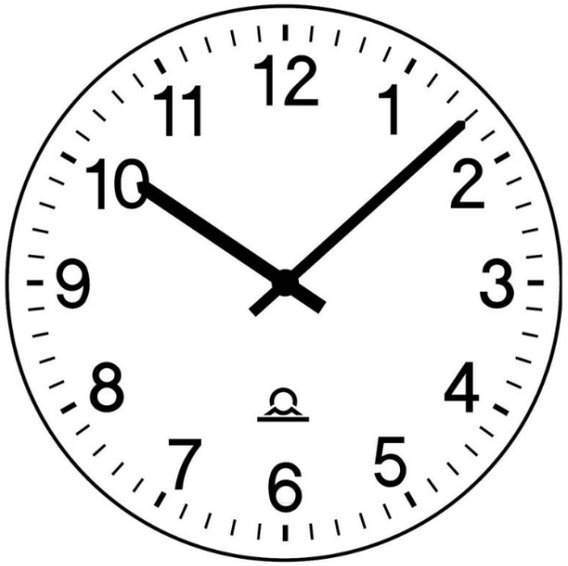
- KBV erarbeitet gemeinsam mit dem BSI eine Sicherheitsrichtlinie
  - Definition von eindeutigen und nachvollziehbaren Angaben für Praxisinhaber
  - Zertifizierung von IT-Dienstleistern für Praxen
- Forderung KBV
  - Für die Kosten des Sicherheitsniveau-Nachweises müssen die Krankenkassen aufkommen
  - Die gematik führt für alle Praxen einheitlich und verbindlich eine Datenschutzfolgeabschätzung durch

Backups und Verschlüsselung



Die „Lebensversicherung“ für Ihre Daten / Praxis

Regelmäßige und zuverlässige Sicherung elektronischer Daten!



Regelmäßig

- So oft wie möglich!
  (abhängig vom Risiko des Datenverlustes)

- Zum Beispiel:
  - mo Vollbackup, di-fr inkrementelles Backup, 1 x monatl. Spiegelung
  - oder tägliches Vollbackup (Speicherbedarf!)
  - oder …

Backups und Verschlüsselung

Zuverlässig

- Neben Sicherungen im Praxisnetz
  ➔ Sicherung **auf externen Medien**!
- Backup an einem anderem sicheren Ort aufbewahren (Diebstahl, Brand).
- Backup vom Praxisnetz trennen / schützen.
- Backups möglichst lange aufbewahren.
- Backup-Erfolg prüfen und ggfs. Wiederherstellungsprozess testen.
- Lebensdauer der Speichermedien beachten.

- Backup als gespiegelte Festplatten im Server nicht ausreichend (RAID).

Backups und Verschlüsselung

Achtung:
Datensicherungen nur verschlüsselt!

Cloud-Backup.
Zugriff durch unberechtigte Dritte MUSS (!) ausgeschlossen sein.

Notfallkonzept und Cyberversicherung

Empfehlenswert: Notfallkonzept

Erstellen Sie sich ein Notfallkonzept für mögliche unterschiedliche Ereignisse (technische Störung, Hackerangriff, Feuer, Einbruch, Stromausfall etc.)

Ziel

- Schnelle und angemessene Reaktion auf Ereignisse
- Schäden können begrenzt oder abgewendet werden

Inhalt

- ☑ Checklisten, die abhängig vom Ereignis abzuarbeiten sind
- ☑ Maßnahmen und Handlungsanweisungen für Beteiligte
- ☑ Mögliche Workarounds
- ☑ Kontaktinformationen und Alarmierungsketten

Zum Abschluss: Was bringt eine Cyberversicherung?

Cyberversicherung: Was wird abgedeckt?

- In der Regel Eigenschäden
  - Betriebsunterbrechungen/Umsatzeinbußen
  - Erstattung der Kosten für Datenwiederherstellung
  - Maßnahmen, um die Ursache für den Schaden aufzuklären
- sowie Fremdschäden
  - Schadenersatzforderung betroffener Patienten

- Darüber hinaus möglich:
  - Prozesskosten
  - Strafzahlungen/Bußgelder
  - Bezahlung von Lösegeldern
  - Öffentlichkeitsarbeit im Falle von Imageschäden
  - Unterstützung beim Managen des Schadenfalles

Cyberversicherung: Darauf sollten Sie achten!

- ☑ Werden Risiken ggfs. schon durch existierende Versicherungen abgedeckt?
- ☑ Wie hoch ist die Eigenbeteiligung?

- Eine Cyberversicherung ist kein Ersatz für präventive Maßnahmen zur IT-Sicherheit, sondern soll Kosten für das Restrisiko minimieren
- Versicherer prüfen vor Abschluss, ob die Praxis umfassend geschützt ist ➔ davon abhängig sind Deckung und Kosten

IT-Beratung der KV Nordrhein

Nicole Elias

0211 5970 8188
It-beratung@kvno.de

Franz-Josef Eschweiler

0211 5970 8197
It-beratung@kvno.de

Britta Lodyga-Gotthardt

0211 5970 8279
It-beratung@kvno.de

Sandra Onckels

0211 5970 8099
It-beratung@kvno.de

Claudia Pintaric

0211 5970 8255
It-beratung@kvno.de