IT- / Datensicherheit in der Arztpraxis

Messel, 19.10.2022

be(e)prepared.

- **Der Praxisalltag wird digital**
- Bedrohung durch Cyberkriminalität
- Gefahrenabwehr durch KBV-Sicherheitsrichtlinie
- Ihr Lösungspartner Jupitec

Der Praxisalltag wird digitaler und immer komplexer…

- Standort-vernetzung
- Praxis-verwaltung
- Video-Sprechstunde
- Labordaten-fernübertragung

Quelle: stock.adobe.com

- Telematik-Infrastruktur z.B. eAu / eRezept
- ePA
- KIM

be(e)prepared.

- Der Praxisalltag wird digital
- **Bedrohung durch Cyberkriminalität**
- Gefahrenabwehr durch KBV-Sicherheitsrichtlinie
- Ihr Lösungspartner Jupitec

…dabei sind Praxen aus 3 Gründen für Cyberangriffe sehr attraktiv

- Sensible Daten
- Vermeintlich hohe Liquidität
- Oftmals mangelnde Sicherheit

Komplexität und Attraktivität – eine gefährliche Kombination…

Hackerangriff auf Compugroup Medical

Montag, 20. Dezember 2021

9. November 2021, 12:20 Uhr Hack gegen Software-Firma Medatixx

Warum Tausende Ärzte ihre Passwörter ändern müssen

PRESSEMITTEILUNG · 21.10.2021

BSI-Lagebericht 2021: Bedrohungslage angespannt bis kritisch

…Cyber-Angriffe gefährden zunehmend eine erfolgreiche Digitalisierung…

Schadsoftware

Deutsche Krankenhäuser mit Ransomware infiziert

17. Juli 2019, 18:35 Uhr

Hackerangriff auf die Uniklinik Düsseldorf

Angriff auf die Herzkammer

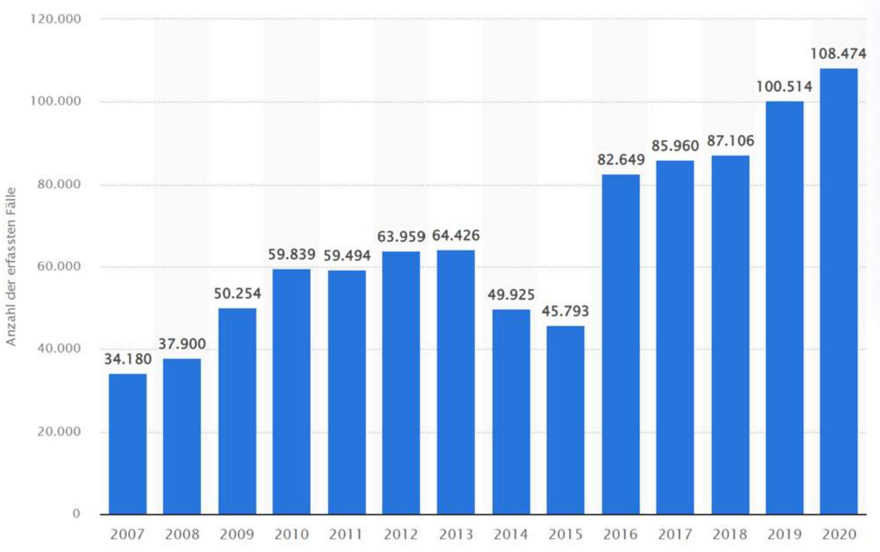
Mitten in der Pandemie legen Hacker die Uniklinik Düsseldorf lahm. Der Vorfall zeigt, wie verwundbar selbst die wichtigsten Einrichtungen unserer Gesellschaft durch Attacken aus dem Netz sind.

Von **Kai Biermann**, **Paul Middelhoff** und **Markus Sehl**

Aktualisiert am 10. Dezember 2020, 19:11 Uhr / 106 Kommentare /

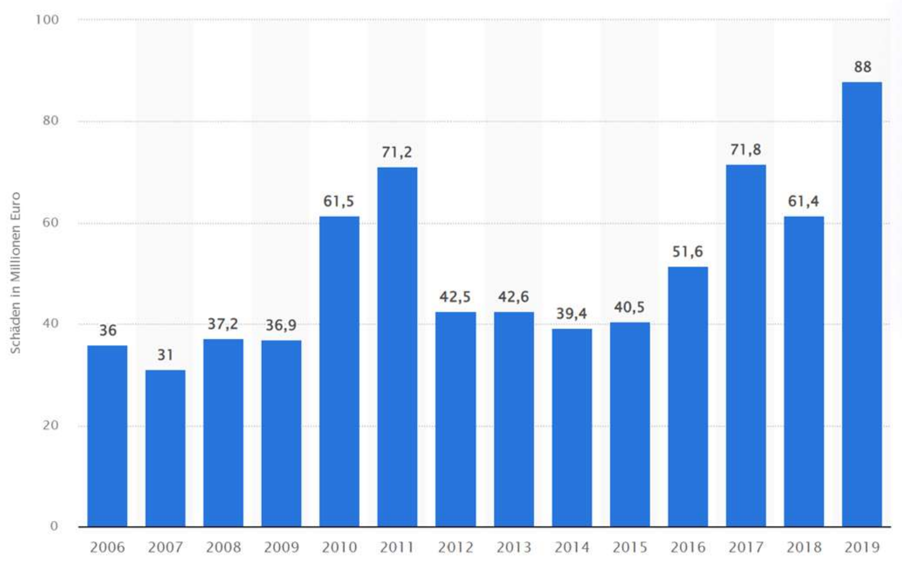
Cyberkriminalität wächst und kostet…

In 2019 wurden in Deutschland **<u>>100.000</u>** Fälle von Cyberkriminalität registriert (Dunkelziffer viel höher)…



Quelle: Statista 2021

… mit einem Schaden von **<u>>88 Mio. EUR</u>** allein im Jahr 2019



Quelle: Statista 2021

be(e)prepared.

Drei relevante Ausprägungen von Cybercrime gefährden Praxen

- Spam
  Phishing
- Malware
  Trojaner
- Ransomware

Drei relevante Ausprägungen von Cybercrime gefährden Praxen

**Spam
Phishing**

Malware
Trojaner

Ransomware

Um an digitale Identitäten zu gelangen, setzen Cyberkriminelle oft auf **Spam- und Phishing-Mails** mit Schadsoftware versehene Anhänge. Die versendeten E-Mails sollen dabei die Opfer zum Herunterladen oder Anklicken der Schadsoftware verleiten.

Drei relevante Ausprägungen von Cybercrime gefährden Praxen

Spam
Phishing

Malware
Trojaner

Ransomware

Mit dem Einsatz von **Malware und Trojanern** werden Daten ausspioniert und abgegriffen, der Datenverkehr manipuliert (beispielsweise beim Onlinebanking) oder Erpressungen begangen (siehe Ransomware)

Drei relevante Ausprägungen von Cybercrime gefährden Praxen

Spam
Phishing

Malware
Trojaner

Ransomware

Bei **Ransomware** werden Opfersysteme verschlüsselt und für die Entschlüsselung Lösegeld verlangt. Häufig werden parallel auch Daten ausgespäht, um zusätzlich mit einer Veröffentlichung der Daten drohen zu können. Dieses Vorgehen wird **Double Extortion** genannt.

be(e)prepared.

Die drei vorgestellten Cybercrime-Methoden greifen ineinander…

Die Vorgehensweise

1. **Schadsoftware** wird programmiert
2. Über **Botnetze** werden Phishingmails verteilt
3. Durch Schadsoftware (Trojaner) werden **Nutzerdaten** gesammelt
4. Verteilte Ransomware verschlüsselt Daten und **erpresst** Anwender
5. Das **Lösegeld** wird genutzt, um Schadsoftware weiterzuentwickeln

Die drei vorgestellten Cybercrime-Methoden greifen ineinander…

Die Vorgehensweise

1. **Schadsoftware** wird programmiert
2. Über **Botnetze** wird Phishingmails verteilt
3. Durch Schadsoftware (Trojaner) werden **Nutzerdaten** gesammelt
4. Verteilte Ransomware verschlüsselt Daten und **erpresst** Anweder
5. Das **Lösegeld** wird genutzt, um Schadsoftware weiterzuentwickeln

Laut BKA ist Cybercrime “ein hochkomplexer, krimineller Wirtschaftszweig mit eigenen Wertschöpfungsketten“

be(e)prepared.

- Der Praxisalltag wird digital
- Bedrohung durch Cyberkriminalität
- **Gefahrenabwehr durch KBV-Sicherheitsrichtlinie**
- Ihr Lösungspartner Jupitec

Die KBV setzt die BSI-Anforderungen in eine IT-Sicherheitsrichtlinie um.

jupitec
Systemlösungen für EDV und Telekommunikation

Sicherer Umgang mit…

Personenbezogenen Daten

Bundesamt
für Sicherheit in der
Informationstechnik

KBV

Die KBV-Anforderungen sind vielfältig…

KBV Sicherheitsrichtlinie § 75b Abs. 5 SGB V

Gefordert werden:

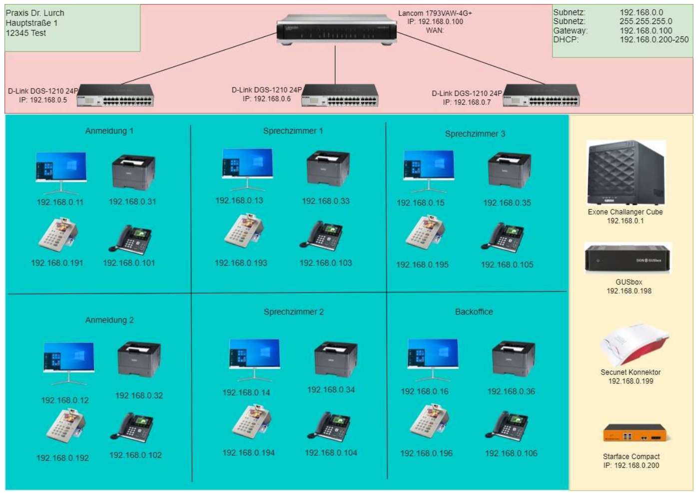
- Verhinderung von Datenabfluss
- Schutz vertraulicher Daten

Maßnahmen:

- Abmelden / Sperren der Geräte
- Virenschutz
- Dokumentation des Netzes
- Nutzung Firewall
- Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen
- Regelmäßige Datensicherung
- Zeitnahe Installation von Aktualisierungen

Exemplarische KBV-Anforderungen:

Dokumentation des Netzes



KBV Sicherheitsrichtlinie § 75b SGB V

Gefordert werden:

- Verhinderung von Datenabfluss
- Schutz vertraulicher Daten

Maßnahmen:

- Abmelden / Sperren der Geräte
- Virenschutz
- **Dokumentation des Netzes**
- Nutzung Firewall
- Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen
- Regelmäßige Datensicherung
- Zeitnahe Installation von Aktualisierungen

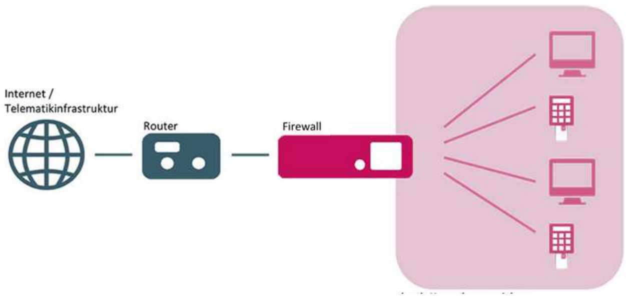
„Das interne Netz ist inklusive eines Netzplanes zu dokumentieren.“

Quelle: KBV-Sicherheitsrichtlinie

be(e)prepared.

Exemplarische KBV-Anforderungen:

Nutzung Firewall



Quelle:
KBV-Sicherheitsrichtlinie

KBV Sicherheitsrichtlinie § 75b SGB V

Gefordert werden:

- Verhinderung von Datenabfluss
- Schutz vertraulicher Daten

Maßnahmen:

- Abmelden / Sperren der Geräte
- Virenschutz
- Dokumentation des Netzes
- **Nutzung Firewall**
- Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen
- Regelmäßige Datensicherung
- Zeitnahe Installation von Aktualisierungen

„…es gibt verschiedene Varianten, die auch miteinander kombiniert werden können:
› Personal Firewall
› geeignete Hardware-Firewall

Quelle: KBV-Sicherheitsrichtlinie

be(e)prepared.

- Der Praxisalltag wird digital
- Bedrohung durch Cyberkriminalität
- Gefahrenabwehr durch KBV-Sicherheitsrichtlinie
- **Ihr Lösungspartner Jupitec**

Jupitec unterstützt Sie mit KBV-zertifizierten Technikern…

Quelle: CanStockPhoto

KBV KASSENÄRZTLICHE BUNDESVEREINIGUNG

ZERTIFIKAT

Hiermit wird im Rahmen der KBV-Zertifizierung im Bereich

ZERTIFIZIERUNG NACH § 75B ABSATZ 5 SGB V

bestätigt, dass

erfolgreich die KBV-Zertifizierung absolviert und seine Kenntnisse und Fähigkeiten im IT-Sicherheitsumfeld nach Vorgaben der „Richtlinie zur Zertifizierung nach § 75b Absatz 5 SGB V" nachgewiesen hat.

Die KBV-Prüfnummer lautet ISAP/20210323/36/00662021 und ist vom 23.03.2021 bis 22.03.2024 gültig.

Kassenärztliche Bundesvereinigung
Körperschaft des öffentl. Rechts
Herbert-Lewin-Platz 2 - 10623 Berlin

Berlin / 23. März 2021

Ort/Datum Unterschrift/Stempel

Kassenärztliche Bundesvereinigung
Informationssicherheit/IT-Security

… bei der Umsetzung der KBV-Richtlinie

Quelle: INDAMED GmbH

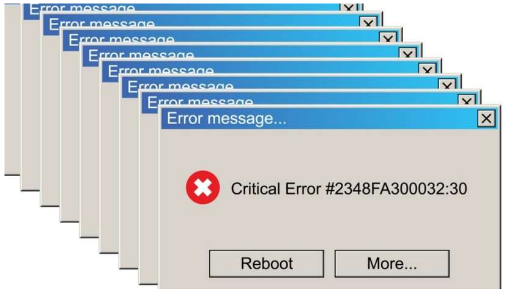
Basis: Vorort IT-Sicherheits-CheckUp

- Technische Maßnahmen
- Awareness-Training
- Maintenance und Monitoring
- Organisatorische Maßnahmen Praxis

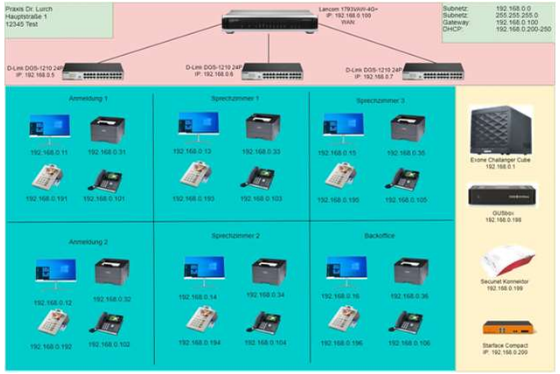
be(e)prepared.

Vorort-IT-Sicherheits-Checkup, der kurz- und langfristig wirkt.

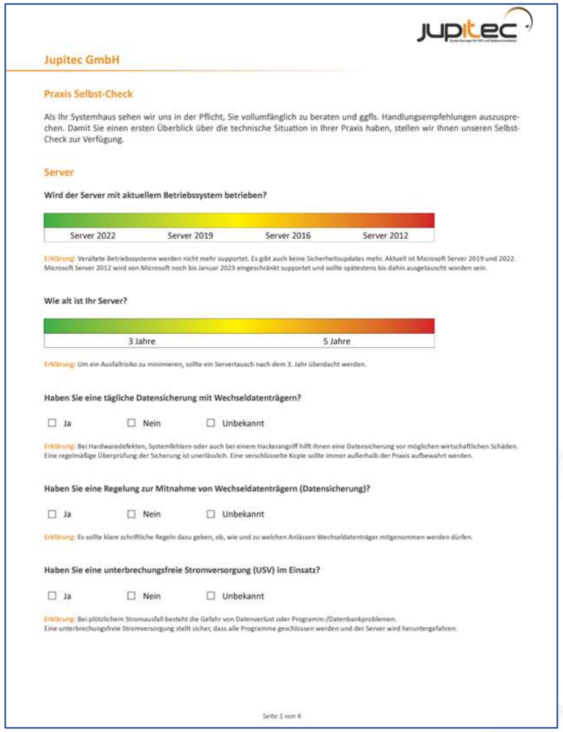
1. Kritische Fehler sofort beheben



2. KBV-Sicherheitsanforderungen umsetzen



3. Auswertung + Umsetzungsempfehlung



Jupitec GmbH

Praxis Selbst-Check

Als Ihr Systemhaus sehen wir uns in der Pflicht, Sie vollumfänglich zu beraten und ggfls. Handlungsempfehlungen auszusprechen. Damit Sie einen ersten Überblick über die technische Situation in Ihrer Praxis haben, stellen wir Ihnen unseren Selbst-Check zur Verfügung.

Server

Wird der Server mit aktuellem Betriebssystem betrieben?

Server 2022 | Server 2019 | Server 2016 | Server 2012

Erklärung: Veraltete Betriebssysteme werden nicht mehr supportet. Es gibt auch keine Sicherheitsupdates mehr. Aktuell ist Microsoft Server 2019 und 2022. Microsoft Server 2012 wird von Microsoft noch bis Januar 2023 eingeschränkt supportet und sollte spätestens bis dahin ausgetauscht worden sein.

Wie alt ist Ihr Server?

3 Jahre | 5 Jahre

Erklärung: Um ein Ausfallrisiko zu minimieren, sollte ein Servertausch nach dem 3. Jahr überdacht werden.

Haben Sie eine tägliche Datensicherung mit Wechseldatenträgern?

☐ Ja ☐ Nein ☐ Unbekannt

Erklärung: Bei Hardwaredefekten, Systemfehlern oder auch bei einem Hackerangriff hilft Ihnen eine Datensicherung vor möglichen wirtschaftlichen Schäden. Eine regelmäßige Überprüfung der Sicherung ist unerlässlich. Eine verschlüsselte Kopie sollte immer außerhalb der Praxis aufbewahrt werden.

Haben Sie eine Regelung zur Mitnahme von Wechseldatenträgern (Datensicherung)?

☐ Ja ☐ Nein ☐ Unbekannt

Erklärung: Es sollte klare schriftliche Regeln dazu geben, ob, wie und zu welchen Anlässen Wechseldatenträger mitgenommen werden dürfen.

Haben Sie eine unterbrechungsfreie Stromversorgung (USV) im Einsatz?

☐ Ja ☐ Nein ☐ Unbekannt

Erklärung: Bei plötzlichem Stromausfall besteht die Gefahr von Datenverlust oder Programm-/Datenbankproblemen.
Eine unterbrechungsfreie Stromversorgung stellt sicher, dass alle Programme geschlossen werden und der Server wird heruntergefahren.

Seite 1 von 4

be(e)prepared.

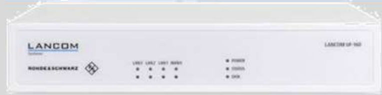
IT-Sicherheits-Checkup: Anforderungen der KBV erfüllen.

- Netzwerkdokumentation inkl. Netzwerkplan
- Datensicherungskonzept
- Dokumentation und Auswertung der KBV-Anforderungen
- Handlungsempfehlung

Mit technischen Maßnahmen wird ein angemessenes Schutzniveau erreicht.

Technische Maßnahmen

Maintenance und Monitoring



Durch eine Kombination aus Virenschutz und Hardware-Firewall sind Sie gegen Angriffe abgesichert. Falls nötig kann auf eine funktionierende Datensicherung zurückgegriffen werden.

Regelmäßige Kontrolle und Wartung erhöht die Funktionalität.

Technische Maßnahmen

Maintenance und Monitoring

Jupitec monitort Ihre Systeme und greift ein **BEVOR** es zu einem Schadensfall kommt, der dann ungleich aufwändiger und kostenintensiver wird.

Treffen Sie Vorsorge!
Werden Sie nicht Teil der Wertschöpfungskette!

- Downloaden Sie unseren kostenlosten CheckUp – **heute noch**!
  Prüfen Sie die Abweichungen in Ihrer Praxis – **ehrlich!**
  https://jupitec.de/images/aktuelles/Jupitec-Selbstcheck-V2.pdf

- Wir beraten Sie kostenfrei bei der Auswertung
  - **Sprechen** Sie mit uns.

- Wir unterstützen Sie bei der technischen Umsetzung
  – **KBV-Zertifiziert**.

Auch Sie kann Cyberkriminalität treffen.
Be(e)prepared!

Ihre Ansprechpartner in Sicherheitsfragen

Auf dem Anwendertreffen: Max Brügel

Für Onlineteilnehmer: Dagmar Zydek-Bührer

security@jupitec.de
Telefon 06159-7155-40

Fragen?

Vielen Dank für Ihre Aufmerksamkeit

be(e)prepared.