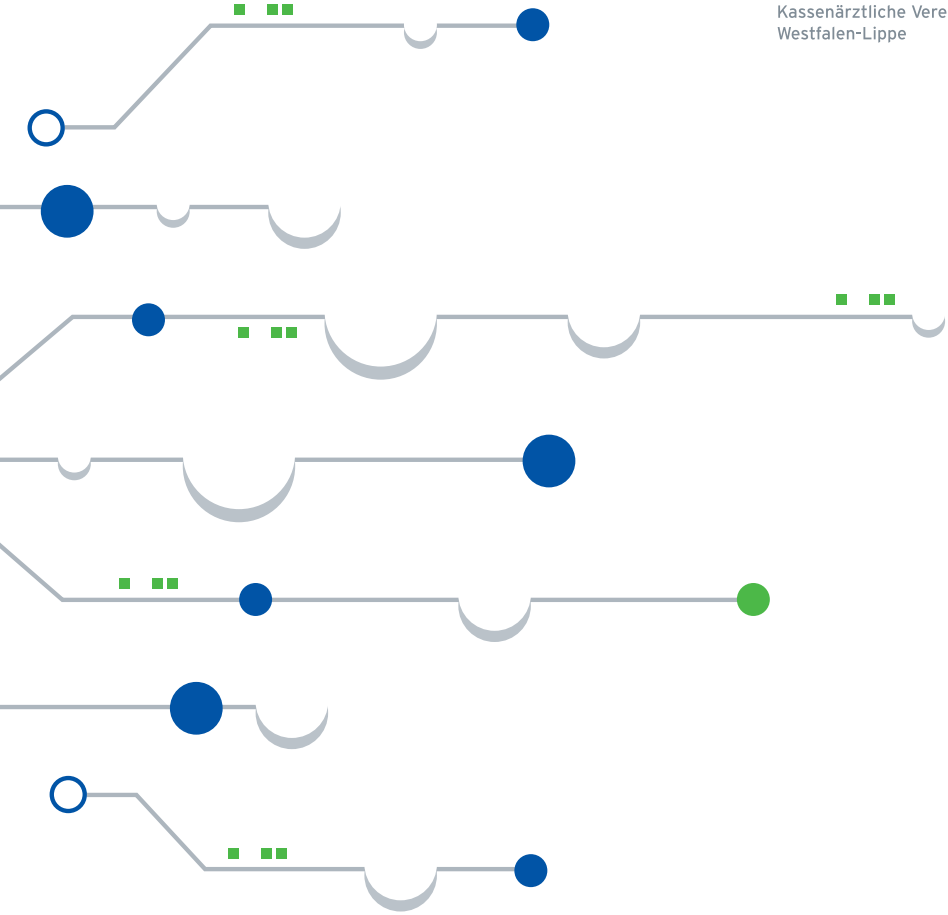
KVWL
Kassenärztliche Vereinigung
Westfalen-Lippe



Empfehlungen zur

IT-Sicherheit in Praxen

Inhalt

Sicherheit geht vor!

Die Digitalisierung gewinnt zunehmend an Bedeutung. Sie spüren dies nahezu täglich auch in Ihren Praxen. Aktuell geht es darum, die TI zu nutzen und einzelne Anwendungen mit Leben zu füllen. Dabei legen Sie, die niedergelassenen Ärztinnen und Ärzte sowie Psychotherapeutinnen und Psychotherapeuten, großen Wert auf den Schutz und die Sicherheit der Patientendaten. Ein Anspruch, den die KVWL selbstverständlich teilt, denn Gesundheitsdaten sind ein hohes Gut!
Auch der Gesetzgeber hat hierzu konkrete Anforderungen formuliert. Voraussichtlich im Sommer dieses Jahres wird die Kassenärztliche Bundesvereinigung (KBV) eine umfassende Richtlinie zur IT-Sicherheit herausgeben.
Die vorliegende Broschüre verfolgt einen etwas anderen Ansatz. Sie ist als konkrete Arbeitshilfe für den Praxisalltag gedacht und listet verschiedene Anforderungen und Maßnahmen auf, die Sie selbst bzw. Ihr Praxisteam – gegebenenfalls in Kooperation mit Ihrem Systembetreuer – ohne großen Aufwand umsetzen können.
Ein Service Ihrer KVWL zum Schutz sensibler Daten – denn Sicherheit geht vor!

Thomas Müller, KVWL-Vorstandsmitglied

Eine Gefährdung der IT-Systeme und Patientendaten in Arzt- und Psychotherapiepraxen durch Schadsoftware ist eine ernstzunehmende Bedrohung. Es gilt also beim Umgang mit den Systemen und insbesondere bei der Nutzung von Internet-Diensten ausreichend technische Sicherheitsmaßnahmen umzusetzen. Damit Sie besser bewerten können, ob Sie und Ihr IT-Dienstleister alle notwendigen und wichtigen Sicherheitsmaßnahmen umgesetzt haben, geben wir Ihnen im Folgenden die KVWL-Empfehlungen zur IT-Sicherheit in Praxen als Checkliste an die Hand.

Hinweis: Diese Empfehlungen stellen keine abschließende Darstellung von Maßnahmen für den Einzelfall dar. Es handelt sich um grundsätzliche und wesentliche Erkenntnisse, die regelmäßig zu beachten sind. Dies ersetzt nicht die individuelle eigene Analyse sowie Risikobewertung, die sinnvollerweise auch einen externen Systembetreuer mit einschließen sollte.

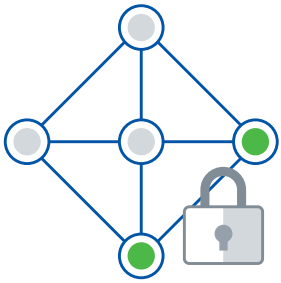
Organisation

- Informieren Sie sich und Ihr Praxispersonal regelmäßig zu aktuellen Sicherheitsproblemen und -techniken **(z. B. auf www.bsi-fuer-buerger.de).**
- Sprechen Sie die Themen Sicherheit und Datenschutz regelmäßig in Ihrer Praxis an, damit Ihnen grundlegende Gefahren wie Verschlüsselungstrojaner / Ransomware sowie Gegenmaßnahmen dazu bekannt sind (z. B. dass nicht unbedacht jeder Mailanhang geöffnet wird). Sinnvollerweise kann Ihr Datenschutzbeauftragter oder Systembetreuer hierbei unterstützen.
- Regeln Sie die Nutzung von privaten Geräten (Smartphones, Tablets) des Personals zu dienstlichen Zwecken. Wenn Sie es nicht verbieten, stellen Sie Regeln zur Nutzung auf und sensibilisieren Sie das Personal für einen sicheren Umgang damit.
- Verwenden Sie Passwort-Tresor-Programme, die Ihre Passwörter verschlüsselt speichern, statt Ihre Passwörter aufzuschreiben.
- Lassen Sie Fernwartungen von externen Technikern nur nach vorheriger Absprache zu. Halten Sie die nötigen Passwörter oder Codes unter Verschluss.
- Beachten Sie schon bei der Beschaffung von neuen IT-Geräten deren Sicherheitsfunktionen.
- Lassen Sie niemals Dienstleister (z. B. IT-Support) Tests mit echten Patientendaten durchführen. Entweder werden diese vorher anonymisiert oder der Dienstleister muss selber generierte Daten ohne Patientenbezug verwenden.

Telematikinfrastruktur

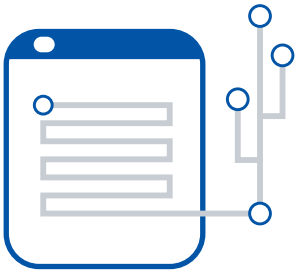
- Sollten Sie noch nicht an die Telematikinfrastruktur (TI) angeschlossen sein, achten Sie darauf, dass der IT-Dienstleister bei der Installation ein Installationsprotokoll ausfüllt. Idealerweise nutzt er das Muster-Installationsprotokoll „Sichere TI-Installation" der gematik. Das Protokoll soll neben technischen Details auch einen Vermerk über die Beratung zu sicherheitsrelevanten Aspekten enthalten.
- Sind Sie bereits an die TI angeschlossen, prüfen Sie, ob Ihr Installationsprotokoll die Punkte des Muster-Installationsprotokolls enthält. Sprechen Sie Ihren IT-Dienstleister an, wenn Sie gravierende Abweichungen feststellen.
- Sie können Ihre Praxis im sogenannten Reihen- oder Parallelbetrieb an die TI anschließen lassen. Beide Installationsvarianten sind von der gematik als Standard-Szenarien für den sicheren Anschluss an die TI vorgesehen. Welche Variante für eine Praxis am besten ist, hängt von der IT-Infrastruktur der Praxis und den schon vorhandenen Sicherungsmaßnahmen ab.
- Wenn Sie keine Internetdienste nutzen wollen und nur wenige Endgeräte in Ihrem Netzwerk verwenden, empfehlen wir Ihnen, den Konnektor in Reihe zu schalten. Im Reihenbetrieb befinden sich alle Komponenten im selben Praxisnetzwerk und erhalten Zugang über den Konnektor zur TI. Durch die integrierte Firewall des Konnektors wird das Praxisnetz vor unautorisierten Zugriffen von außen geschützt. Im Reihenbetrieb kann optional der Sichere Internet Service (SIS) aktiviert werden, um im Praxisnetzwerk einen Internetzugang zu ermöglichen, um beispielsweise Updates des Betriebssystems oder des PVS herunterzuladen. In diesem Fall baut der Konnektor einen zweiten sicheren Kanal zum SIS des Zugangsdienstbetreibers auf. Detaillierte Informationen zum Leistungsangebot des SIS erhalten Sie von Ihrem Zugangsdienstbetreiber.

- Der Reihenbetrieb ermöglicht auch durch eine Netztrennung einen uneingeschränkten Internetzugang für Geräte, die direkt an den Internetrouter angeschlossen sind. Der Konnektor setzt dabei eine Netztrennung zwischen dem Praxisnetz und den Netz mit direktem Internetzugang durch. Für das Praxisnetz kann der optionale SIS aktiviert werden.
- In größeren Praxen mit mehreren Endgeräten im Netzwerk kann die Parallelschaltung sinnvoll sein. Im Parallelbetrieb sind alle Komponenten über einen Router miteinander verbunden. Der Konnektor kann hierbei nicht als Firewall nach außen genutzt werden. Daher müssen eigene Sicherheitsmaßnahmen wie eine eigene Firewall die Praxis-IT absichern. Achten Sie hierbei auf eine möglichst genaue Einstellung der Firewall-Regeln unter den Maßgaben: „Alles ist verboten, außer es wird erlaubt“ und „So wenig wie möglich erlauben“.
- Stellen Sie – aus Haftungsgründen – sicher, dass die TI-Geräte (Konnektor, Chipkartenleser etc.) ordnungsgemäß aufgestellt und betrieben werden. Hierzu gehört, dass der Konnektor an einem zugriffsgeschützten Ort installiert wird, angebotene Sicherheitsupdates für den Konnektor und das Kartenterminal stets umgehend eingespielt werden sowie eine regelmäßige Kontrolle, dass die Geräte unverändert sind (Gehäuse, Siegel), und keine unerlaubten Geräte angeschlossen wurden. Informieren Sie bei Beschädigungen sofort den Support.



E-Mail

- Versenden Sie personenbezogene / medizinische Daten verschlüsselt. Nutzen Sie hierzu die vom BSI (Bundesamt für Sicherheit in der Informationstechnik) empfohlenen Programme bzw. Standards wie S/MIME oder GnuPG. Für einzelne Dateien im Mailanhang kann auch die Verschlüsselung von Archivprogrammen wie WinZIP oder 7zip verwendet werden.
- Trennen Sie private und dienstliche Mailkonten, da sonst die Angriffsfläche vergrößert wird.
- Nutzen Sie bestenfalls einen gesonderten Rechner für den Zugriff auf Mailkonten und nicht den PVS-PC.
- Seien Sie kritisch bei E-Mails mit merkwürdigen Absender- oder Empfängeradressen. Löschen Sie solche E-Mails besser direkt. Weitere Verdachtsmomente sind Inhalte, mit denen man offensichtlich nichts zu tun hat (z. B. Rechnungen von eBay, wenn man dort gar nicht angemeldet ist) oder auch Webadressen und Anhänge, die man unbedingt anklicken oder öffnen soll. Lassen Sie sich auch nicht von E-Mails, die angeblich von Banken, Polizei oder Behörden kommen, einschüchtern. Solche Behörden würden wirklich relevante Schreiben nicht per E-Mail zustellen.



Internet

- Nutzen Sie eine 2-Faktor-Authentisierung wenn Ihre Online-Dienste (z. B. Banking) diese anbieten. Hierbei erfolgt die Anmeldung mit einem Passwort und einem zusätzlichen Faktor wie eine am Handy generierte PIN.
- Trennen Sie private und dienstliche Tätigkeiten im Internet (Surfen, Social Media, Chatten etc.), da sonst die Angriffsfläche vergrößert wird.
- Nutzen Sie einen gesonderten Rechner für Internetrecherchen und nicht den PVS-PC.
- Setzen Sie Skript- und Werbeblocker ein, die im Browser als Erweiterung installiert werden können. Hierdurch werden viele unnötige – und teilweise auch schadhafte – Inhalte rausgefiltert.

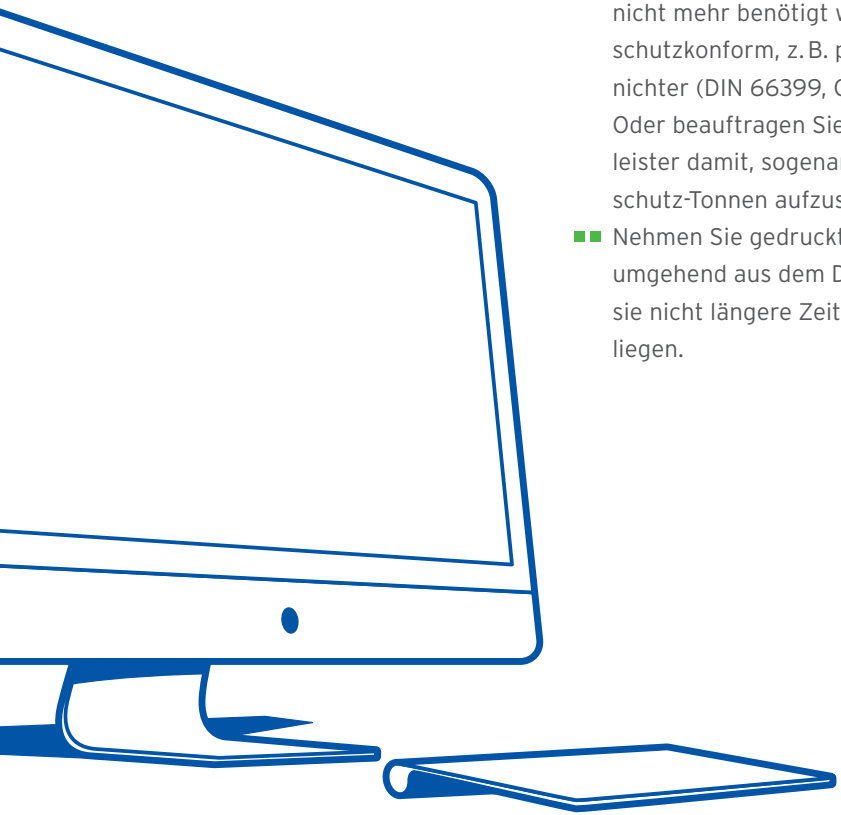
Praxis-PCs & Server

- Führen Sie regelmäßig Updates vom Betriebssystem und Programmen wie Browser und Virenschutz durch. Nutzen Sie überall, wo es möglich ist, die automatische Update-Funktion.
- Schalten Sie bei Windows die Virenschutzfunktion an und halten Sie die Erkennungsdateien aktuell. Alternativ installieren Sie ein gängiges Virenschutzprogramm namhafter Hersteller. Eine Übersicht finden Sie unter www.av-test.org
- Schalten Sie die in Windows enthaltene Firewallfunktion ein. Oft bringen heute die Sicherheitsprogramme namhafter Hersteller neben dem Virenschutzprogramm auch eine Firewallfunktion mit, die verwendet werden kann.
- Arbeiten Sie nicht dauerhaft mit Administratorrechten (erweiterte Systemrechte, die nur für die Administration nötig sind). Legen Sie für die tägliche Arbeit ein Standard-Benutzerkonto an.
- Kontrollieren Sie die angelegten Kennungen regelmäßig und löschen Sie nicht mehr benötigte Kennungen für z. B. ausgeschiedene Praxis-Mitarbeiter.
- Nutzen Sie komplexe Passwörter mit Groß- und Kleinschreibung, Sonderzeichen und Ziffern mit einer Mindestlänge von 8 Zeichen. Vermeiden Sie Wörter, die man im Wörterbuch findet.
- Vergeben Sie unterschiedliche Passwörter für die Anmeldung am Betriebssystem und an Ihrem Praxisverwaltungssystem (PVS).
- Richten Sie zum Schutz vor Daten-Diebstahl eine Festplattenverschlüsselung ein. Wenn hierbei – abhängig vom Betriebssystem und verwendeter Software – Passwörter nötig sind, verwenden Sie hierfür komplexe Passwörter und hinterlegen diese an sicheren Stellen (z. B. Passwort-Tresor-Programme).
- Schalten Sie auf den PCs den Bildschirmschoner bzw. die Bildschirmsperre ein, so dass der Rechner bei Abwesenheit (z. B. 5 oder 10 Minuten) automatisch gesperrt wird.

- Installieren Sie keine dienstlich unnötigen Programme (Spiele, Chats, Video etc.) auf den Praxisrechnern.
- Verwenden Sie niemals fremde USB-Sticks (z. B. geschenkte oder gefundene), deren Herkunft Sie nicht genau kennen. Verzichten Sie möglichst auch auf die Verwendung privater Sticks, beschaffen Sie für dienstliche Zwecke lieber gesonderte.
- Erstellen Sie regelmäßig Datensicherungen der Daten auf dem Server. Sollten Sie wesentliche praxisrelevante Daten auch auf den PCs speichern, sollten auch hier Datensicherungen erfolgen. Stellen Sie ein Konzept mit täglichen, wöchentlichen und monatlichen Teil- und Voll-Sicherungen auf.
- Nutzen Sie für die Datensicherung externe Festplatten, die bestenfalls auch nach der Sicherung vom Rechner getrennt werden, so dass die gesicherten Daten nicht für Schadsoftware erreichbar sind. Lagern Sie die Datensicherung an einem geschützten Ort gegen Diebstahl und Brand etc. Erstellen Sie wenn möglich verschlüsselte Datensicherungen. Testen Sie die Wiederherstellung von Daten mit den Sicherungen regelmäßig.
- Vernichten Sie alte Festplatten mit Patientendaten physisch oder überschreiben Sie diese mehrfach mit Zufallsdaten; hierzu verwenden Sie vom BSI (Bundesamt für Sicherheit in der Informationstechnik) empfohlene Programme bzw. bei neueren Festplatten des SSD-Typs die Programme des jeweiligen Herstellers. Alternativ beauftragen Sie einen Dienstleister mit der Entsorgung/Zerstörung der Platten.
- Schalten Sie Dateifreigaben – insbesondere auf den Servern – soweit wie möglich ab.
- Stellen Sie den Server zutrittsgeschützt auf (z. B. abgeschlossener Raum oder abgeschlossener Schrank).
- Löschen Sie regelmäßig den „Papierkorb“ im System (meist über einen Rechtsklick auswählbar), damit sensible Dokumente wirklich gelöscht werden. Denn in den meisten Systemen werden Dokumente beim Löschen erst nur in einen „Papierkorb“ verschoben, sind dort aber weiterhin zugreifbar.

Drucker

- Stellen Sie Drucker so auf, dass keine Praxisfremden, z. B. Patienten, Zugang dazu bekommen können.
- Vernichten Sie Ausdrucke mit personenbezogenen Daten, die nicht mehr benötigt werden, datenschutzkonform, z. B. per Aktenvernichter (DIN 66399, Cross-Cut). Oder beauftragen Sie einen Dienstleister damit, sogenannte Datenschutz-Tonnen aufzustellen.
- Nehmen Sie gedruckte Dokumente umgehend aus dem Drucker, damit sie nicht längere Zeit offen herumliegen.



Telefax

- Stellen Sie Faxgeräte so auf, dass keine Praxisfremden, z. B. Patienten, Zugang dazu bekommen können.
- Verwenden Sie gespeicherte Empfängernummern, um Tippfehler beim Eingeben der Nummern zu vermeiden.
- Schalten Sie die Faxgeräte außerhalb der Dienstzeiten aus, damit niemand Zugriff auf zwischenzeitlich eingegangene Faxe im Gerät hat.
- Vereinbaren Sie bei sensiblen Daten einen Sendezeitpunkt mit dem Empfänger, da Sie als Absender keine Kontrolle über das Faxgerät auf Empfangsseite haben.
- Nutzen Sie alle von den Faxgeräten angebotenen Sicherheitsmaßnahmen (Anzeige der störungsfreien Übertragung, gesicherte Zwischenspeicherung, Abruf nach Passwort, Sperrung der Fernwartungsmöglichkeit etc.).
- Löschen Sie vor Verkauf, Weitergabe oder Aussortierung alle im Gerät gespeicherten Daten wie z. B. Textinhalte, Verbindungsdaten und Kurzwahlziele.
- Verzichten Sie auf das Versenden von sehr sensiblen Daten per Telefax, da dieses bekannte Schwächen aufweist (insbesondere die fehlende Verschlüsselung). Versuchen Sie, zukünftig sicherere Kommunikationsformen wie den eArztbrief hierfür zu verwenden.

Medizingeräte

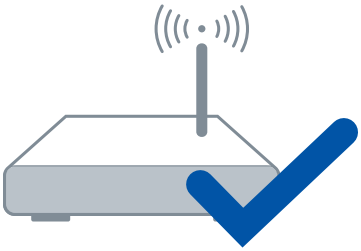
- Stellen Sie sicher, dass Medizingeräte, die an das IT-Netzwerk angeschlossen werden, immer eine Authentisierung (z. B. mit Passwort) vorsehen, damit niemand im Netzwerk an medizinische Daten gelangen kann.
- Hängen Sie Medizingeräte niemals in öffentliche Netzwerkbereiche, da diese dann ggf. vom Internet zugänglich sein könnten.
- Schalten Sie wenn möglich die Verschlüsselung der gespeicherten medizinischen Daten ein, damit niemand durch den Diebstahl des Gerätes oder seiner Speicher an Patientendaten gelangen kann.

Mobile Geräte

- Schalten Sie den Passwortschutz des Gerätes ein, ggf. kombiniert mit Fingerabdruck oder Gesichtserkennung.
- Führen Sie regelmäßig Updates vom Betriebssystem und von den installierten Apps durch, um Schwachstellen zu schließen.
- Speichern Sie keine unverschlüsselten Patientendaten auf Smartphones oder Tablets.
- Schalten Sie zum Schutz der eigenen Daten, Bilder, Kontakte oder Kalender insbesondere bei Android-Geräten auch die Verschlüsselung des Speichers ein.

Netzwerk

- Trennen Sie bei größeren Praxis-Netzwerken die sensiblen Bereiche (PVS-Server mit Patientendaten) von unkritischen bzw. öffentlichen Bereichen (Webserver) durch eine Firewall.
- Schalten Sie die WLAN-Funktion aus, wenn sie nicht zwingend benötigt wird.
- Schalten Sie die Verschlüsselung (mindestens WPA2) an, falls WLAN für interne Zwecke der Praxis nötig ist. Nutzen Sie lange und sichere Passwörter zur Einwahl. Schalten Sie den Netzwerknamen (SSID) auf unsichtbar. Legen Sie die zugelassenen Geräte im Router fest (MAC-Filter).
- Nutzen Sie die Gast-WLAN-Funktionen des Routers, falls Sie Ihren Patienten ein WLAN im Wartezimmer bereitstellen möchten. Hierdurch wird Ihr internes WLAN vom Gast-WLAN getrennt.
- Schalten Sie die im DSL-Router enthaltene Firewallfunktion ein. Sperren Sie dabei alle Netzverbindungen von außen



Notfallplan

- Erstellen Sie einen Notfallplan, um die Abläufe und Zuständigkeiten während der Bewältigung des Notfalles zu regeln und die Beteiligten in die Lage zu versetzen, wieder den Normalbetrieb herzustellen. Bereiten Sie sich auf mögliche Szenarien wie einen Rechner-Ausfall oder Schadsoftware vor.
- Stellen Sie Möglichkeiten eines Notbetriebs auf, z. B. für den Ausfall von PCs, den Ausfall des PVS, den Ausfall des Internets oder einen Stromausfall. Halten Sie z. B. einen Ersatzrechner bereit.
- Überlegen Sie, wen Sie im jeweiligen Notfall informieren müssen. Das können je nach Art des Notfalls die Polizei, die Datenschutzbehörden, die Versicherungen oder Patienten sein.

Cyberversicherung

- Eine Cyberversicherung kann im Schadenfall (IT-Ausfall, Schadsoftware, Bedienungsfehler, vorsätzliche Manipulation etc.) die Kosten für Sachverständige, externe Berater, Krisenmanager, Juristen, Presse-/Medienexperten, Call-Center erstatten, Schadenersatz leisten oder auch den Ertragsausfall nach einer Betriebsunterbrechung kompensieren.
- Meist stellt die Versicherung Ansprechpartner zur Verfügung, die im Notfall schnell Hilfe leisten können. Hierzu zählen Service-Hotlines, Sicherheits-Experten und IT-Forensiker.
- Die einzelnen genauen Pflichten und Leistungen sind vor Vertragsabschluss mit der Versicherung zu klären. Da es bei den Verträgen und Rahmenbedingungen durchaus Unterschiede geben kann, sollten Sie mehrere Angebote einholen und vergleichen.

Weitere Informationsquellen

https://www.kbv.de/html/datensicherheit.php
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/empfehlungen_node.html
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/bausteine_node.html
https://fachportal.gematik.de/erste-schritte/anschluss-medizinischer-einrichtungen/
https://www.datenschutzkonferenz-online.de/kurzpapiere.html
https://www.bundesaerztekammer.de/aerzte/telematiktelemedizin/sicherheit-von-gesundheitsdaten/

Ihr Ansprechpartner zum Thema IT-Sicherheit in Praxen ist das Service-Center der KVWL: Tel. 0231/94 32 10 00

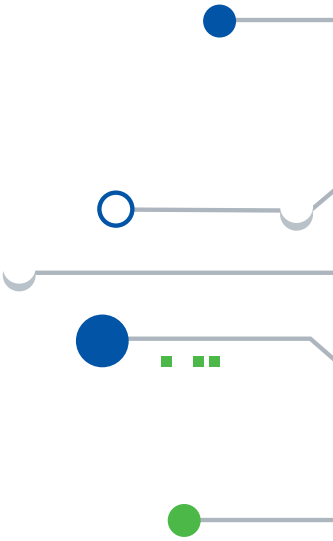
Impressum

Kassenärztliche Vereinigung
Westfalen-Lippe
Robert-Schimrigk-Straße 4–6
44141 Dortmund

Geschäftsbereich Kommunikation
E-Mail: redaktion@kvwl.de
Tel. 0231/94 32 0

www.kvwl.de

Stand: januar 2020/ **Bildnachweis:** Seite 14 © nikizdiez_AdobeStock; Seite 19 © 380632883310_AdobeStock



www.kvwl.de