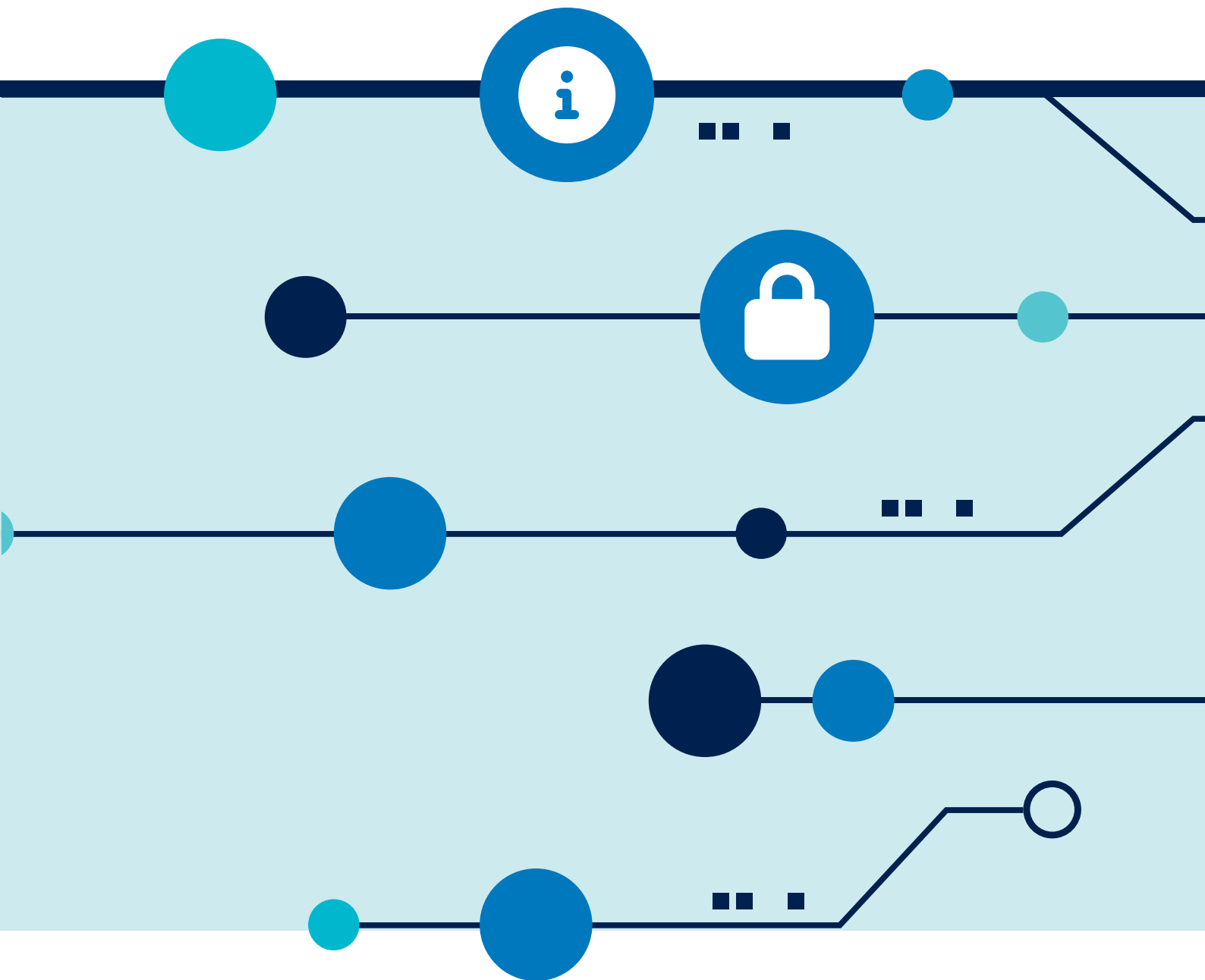


Leitfaden zum Umgang mit IT-Sicherheitsvorfällen



Einleitung	3
1. Definition IT-Sicherheitsvorfälle	4
2. Erkennen von IT-Sicherheitsvorfällen	4
3. Handeln bei IT-Sicherheitsvorfällen	5
3.1 Berichte in den Medien.....	5
3.2 Informationen vom Hersteller.....	5
3.3 Beobachtungen durch Mitarbeiter, Patienten oder andere Praxen	5
3.4 Warnmeldungen oder Protokolle Firewall/Virens Scanner	5
3.5 Rechner starten nicht oder Anzeige „Rechner wurde verschlüsselt“	5
3.5.1 Sofortmaßnahmen.....	6
3.5.2 Wiederherstellungsmaßnahmen: Arbeitshinweise für den IT-Dienstleister.....	6
3.5.3 Hilfreiche Bilder	8
3.5.4 Anzeige erstatten.....	10
3.5.5 Meldepflichten	10
3.5.6 Nachbereitung	10
4. Glossar und Abkürzungen	11
Impressum	12

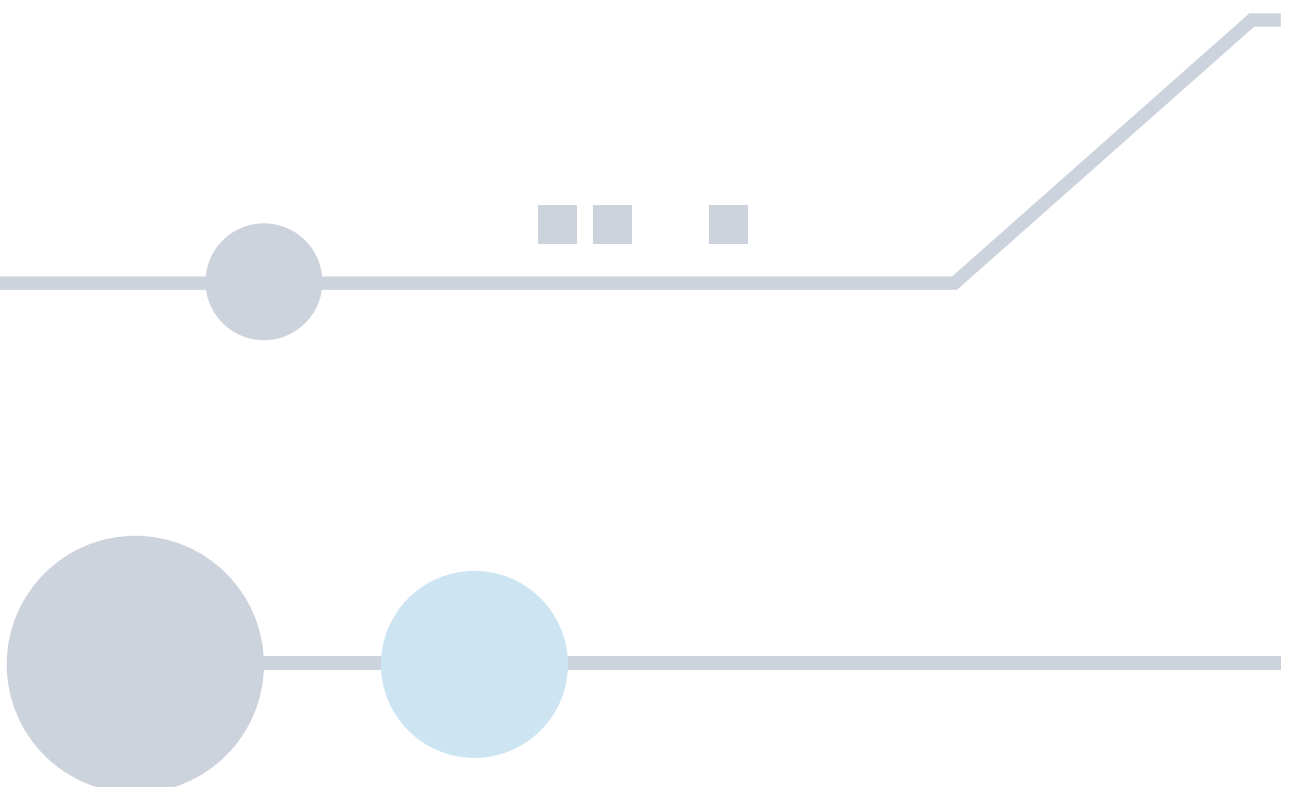
Hinweis

Aus Gründen der besseren Lesbarkeit werden die Sprachformen (wie beispielsweise „Ärztinnen und Ärzte“) nicht in jedem Einzelfall gleichzeitig verwendet. Sämtliche Personenbezeichnungen gelten für alle Geschlechter gleichermaßen.

Einleitung

Dieser Leitfaden soll Sie unterstützen, IT-Vorkommnisse in der Praxis richtig einzuordnen und angemessen zu reagieren. Vieles können Sie auch ohne tieferes Fachwissen selbst erledigen, um mögliche Datenverluste beziehungsweise Schäden gering zu halten. Anderes gehört in die Hände von IT-Spezialisten, so zum Beispiel Maßnahmen zur Wiederherstellung verschlüsselter Daten. Wichtig ist in jedem Fall, schnell und zielgerichtet zu handeln!

Wir empfehlen Ihnen, mögliche Bedrohungsszenarien einmal frühzeitig mit dem gesamten Praxisteam durchzuspielen, um alle mit der Verarbeitung von Daten betrauten Personen für die Gefahren zu sensibilisieren. Dazu gehören nicht nur externe Angriffe auf digitalem Weg, sondern zum Beispiel auch Wasserschäden, Stromausfälle oder der physische Diebstahl von Datenträgern. Alle sollten in der Lage sein, im Falle eines Falles schnell und richtig zu reagieren - auch wenn die Praxisleitung vielleicht gerade nicht anwesend ist.



1. Definition IT-Sicherheitsvorfälle

IT-Sicherheitsvorfälle sind Ereignisse, welche die Sicherheit des Geschäftsbetriebs und der Informationen – im Sinne von Vertraulichkeit, Integrität oder Verfügbarkeit – mit hoher Wahrscheinlichkeit beeinträchtigen und damit Schäden für die Praxis oder Dritte herbeiführen können.

■ Beispiele:

- Ausfall von Endgeräten und Servern aufgrund eines Software-/Hardwarefehlers oder Hacker-Angriffs
- Verschlüsselung von Daten auf Endgeräten und Servern
- unberechtigter Zugriff auf personenbezogene Daten (Patientendaten, Gesundheitsdaten, Arbeitsverträge, Mitarbeiterakten)
- unerlaubtes Kopieren von Betriebsgeheimnissen (Behandlungsverfahren, Abrechnungsdaten, Wirtschaftspläne)
- Fernwartungszugriff durch unberechtigte Personen



2. Erkennen von IT-Sicherheitsvorfällen

■ Quellen für die Erkennung sind:

- Berichte in den Medien (zum Beispiel Presseberichte, KBV-PraxisNachrichten, Radio, Fernsehen)¹
- Informationen von Herstellern (zum Beispiel TI-Komponenten, Praxisverwaltungssystem)¹
- Beobachtungen durch Mitarbeiter, Patienten oder aus anderen Praxen¹
- Warnmeldungen¹ oder Protokolle² von Firewalls
- Warnmeldungen¹ oder Protokolle² vom Virens Scanner
- Protokolle der Server und Anwendungen²
- Warnmeldungen oder Protokolle von Sicherheitsfiltern für Internet und E-Mailverkehr²
- Protokolle der Benutzer- und Berechtigungsverwaltung²

1) Dies sind üblicherweise die für den einzelnen Arzt relevantesten Quellen.

2) Diese wertet in der Regel ein IT-Dienstleister im Wartungs- oder Störfall aus.



3. Handeln bei IT-Sicherheitsvorfällen

3.1 Berichte in den Medien

Werden Sie durch externe Quellen auf mögliche IT-Sicherheitsvorfälle aufmerksam, prüfen Sie, ob in Ihrer Praxis die entsprechenden Produkte eingesetzt werden (Hard- und Software). Installieren Sie gegebenenfalls die verfügbaren Sicherheitsupdates oder Softwareaktualisierungen.

Gibt es aktuell keine entsprechenden Updates, existiert gegebenenfalls eine Handlungsempfehlung, um die Risiken zu minimieren. Wenn Sie oder Ihr IT-Dienstleister diese nicht kurzfristig umsetzen können, oder keine Updates verfügbar sind, trennen Sie das Gerät vom Internet/Netzwerk (siehe 3.5.3: Bild 1, 2 und 3).

3.2 Informationen vom Hersteller

Informiert Sie der Hersteller des Produkts, prüfen Sie die Verfügbarkeit von Updates oder Handlungsempfehlungen. Auch hier gilt: Trennen Sie das Gerät im Zweifel vom Internet/Netzwerk (siehe 3.5.3: Bild 1, 2 und 3).

3.3 Beobachtungen durch Mitarbeiter, Patienten oder andere Praxen

Verhalten sich die Systeme auffällig (Programme starten nicht, stürzen öfter als üblich ab, langsame Reaktion auf Klicks, Fehlermeldungen), melden sich Patienten oder andere Praxen aufgrund seltsamer beziehungsweise verdächtiger, angeblich von Ihnen versendeter E-Mails, beauftragen Sie Ihren IT-Dienstleister mit der Suche nach Schadsoftware.

Dokumentieren Sie Fehlermeldungen und was gemacht wurde, idealerweise mit Bildern (zum Beispiel mit dem Handy).

Trennen Sie auch hier das System vom Internet und Netzwerk (siehe 3.5.3: Bild 1, 2 und 3).

3.4 Warnmeldungen oder Protokolle Firewall/Virens Scanner

Prüfen Sie, was direkt vor dem Erscheinen der Warnmeldung am Gerät gemacht wurde. Dokumentieren Sie die Warnmeldung möglichst mit allen Details (zum Beispiel Foto mit dem Handy).

Klicken Sie im Zweifel bei Warnmeldungen auf „Verbindung verweigern“/„Nicht zulassen“ oder sinngemäß.

Informieren Sie den IT-Dienstleister und prüfen Sie andere Arbeitsstationen auf ähnliche Fehlermeldungen. Achten Sie auf ungewöhnliches Verhalten (siehe 3.3).

3.5 Rechner starten nicht oder Anzeige „Rechner wurde verschlüsselt“

Sollten Sie Ihre(n) Rechner nicht starten oder sich nicht anmelden können, informieren Sie Ihren IT-Dienstleister. Häufig handelt es sich um größere technische Störungen, eventuell um Schadsoftware.

Sollte der IT-Dienstleister einen Verschlüsselungstrojaner als Ursache ausmachen oder Sie sehen eine entsprechende Meldung, gilt es schnell und überlegt zu handeln.

3.5.1 Sofortmaßnahmen

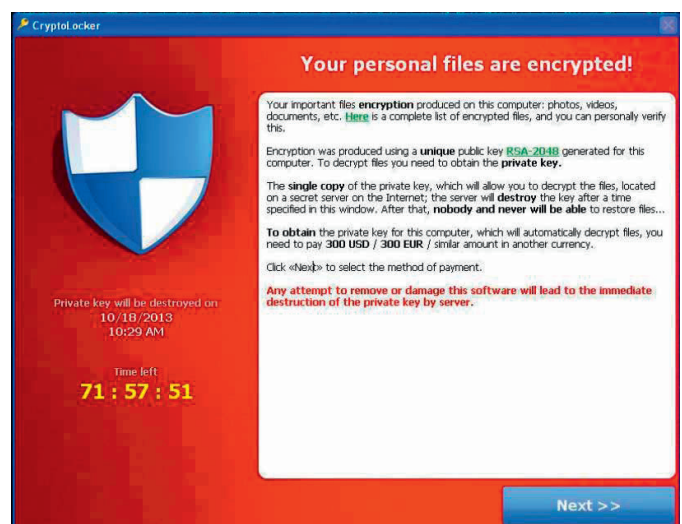
- Ruhe bewahren, Mitarbeiter informieren, Dokumentation beginnen.
- **Keine Anmeldung an betroffenen oder verdächtigen Geräten mit Administratorrechten durchführen!**
- Alle betroffenen oder verdächtigen Geräte vom Netzwerk trennen (Datenkabel am jeweiligen Gerät entfernen, WLAN abschalten). Erst dann ist eine Anmeldung als Administrator wieder erlaubt (siehe 3.5.3: Bild 1, 2 und 3).
- Wenn noch nicht alle Daten verschlüsselt sind, Gerät „hart“ ausschalten (Netzstecker am Gerät ziehen, bei Laptops Akku entfernen oder Ausschaltknopf zirka fünf Sekunden gedrückt halten, bis das Gerät ausschaltet) (siehe 3.5.3: Bild 1 und 4).
- Achtung bei Servern, die eine unterbrechungsfreie Stromversorgung (USV) haben, die Stromversorgung von USV zum Server trennen, nicht vom Stromnetz zur USV.
- Es besteht zwar das Risiko, Hardware zu beschädigen und Datenverlust zu erleiden. Wenn der Verschlüsselungstrojaner aber nicht gestoppt wird, verlieren Sie mit Sicherheit Ihre Daten.
- Im Zweifel komplette Praxis vom Internet trennen, um Risiko von Datendiebstahl, Nachladen oder Versenden weiterer Schadsoftware zu verhindern (ziehen Sie das Datenkabel für WAN aus dem Router oder schalten Sie diesen aus zum Beispiel FritzBox/Speedport). Beachten Sie, dass dadurch gegebenenfalls das Festnetztelefon ebenfalls nicht mehr funktioniert!
- Abstimmung mit dem IT-Dienstleister, ob dieser oder ein spezieller IT-Forensiker die weitere Arbeit übernimmt.

Eine aktuelle Liste spezialisierter Dienstleister finden Sie unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.pdf.

3.5.2 Wiederherstellungsmaßnahmen:

Arbeitshinweise für den IT-Dienstleister

- Die verschlüsselten Datenträger ausbauen und an sicherem Ort verwahren. Sie benötigen diese gegebenenfalls für Strafanzeige, Gerichtsverfahren, Versicherung, Ursachenanalyse oder eine mögliche spätere Wiederherstellung.
- Wenn das Gerät bereits komplett verschlüsselt ist (wenn Sie den unten abgebildeten Bildschirm sehen, ist dies in der Regel der Fall), lassen Sie es an, wenn Sie eine forensische Analyse wünschen (es ist ja bereits vom Netzwerk und Internet getrennt).
- Prüfung aller verfügbaren Logs (Router, Firewall, Switches, Server und Endgeräte), ob erkennbar ist, dass Daten in größerem Umfang aus der Praxis kopiert wurden.
- Prüfung der vorhandenen Datensicherungen, ob diese aktuell und nicht verseucht oder ebenfalls verschlüsselt sind.
- Prüfen Sie, ob es an anderer Stelle womöglich noch Daten oder Datensicherungen gibt (Endgeräte die vor kurzem außer Betrieb genommen wurden, alte Server, alte Datensicherungsmedien, Kopien zu Hause etc.).
- Prüfen Sie, ob unter <https://www.nomoreransom.org/> oder <https://id-ransomware.malwarehunterteam.com/> ein Schlüssel für Ihren Verschlüsselungstrojaner bekannt ist. Gegebenenfalls lassen sich so die Daten mit geringeren Kosten wiederherstellen. Eine erneute quartalsweise



Prüfung ist hier sinnvoll. Manchmal werden Generalschlüssel gefunden und veröffentlicht und Sie kommen damit wieder an Ihre Daten. Nutzen Sie für den notwendigen Test keine patientenbezogenen Dokumente oder Daten!

- Alle Endgeräte, die infiziert waren, müssen komplett neu installiert werden (verwenden Sie neue Datenträger, wenn Sie die alten – wie zu Beginn dieser Liste empfohlen – aufbewahren wollen).
- Alle – nicht offensichtlich betroffenen – Endgeräte werden dennoch vollständig geprüft, bevor diese wieder in das Netzwerk eingebunden werden.
- Prüfen Sie alle Accounts und Zugänge, ob es notwendig ist, Zugangsdaten zu ändern (sowohl für die Praxissysteme und Mitarbeiter als auch Internetanwendungen wie Online-Banking etc.).
- Dies gilt auch für Infrastruktur (Router, Firewall, Switches, TI-Komponenten...).
- Wenn möglich, richten Sie gleich eine Multifaktorauthentifizierung ein. Dies gilt insbesondere für E-Mail-Konten, die Sie für die Anmeldung an Internetdiensten verwendet haben. Wurden diese gehackt, können die Verursacher auch bei anderen Internetdiensten neue Kennwörter erstellen und Sie so aussperren sowie weiteren Schaden verursachen.

- Falls Sie ein größeres Netzwerk mit Domänencontroller und Active Directory nutzen, wird eine komplette Neu-einrichtung dieser Serverlandschaft dringend empfohlen! Zumindest muss das Passwort des eingebauten Key Distribution Service Accounts (KRBTGT) zweimal zurückgesetzt werden. Dies invalidiert alle „Golden Tickets“, die mit dem zuvor gestohlenen KRBTGT-Hash und allen anderen Kerberos-Tickets erzeugt wurden.



3.5.3 Hilfreiche Bilder

Bild 1:

Übersicht Computer von hinten mit USV. Anschlüsse für Energieversorgung und Datenanschluss sind verbunden. LEDs zeigen den Betrieb und die Aktivität des Computers an. Diverse Kabel verbinden den Computer mit zum Beispiel Monitor, Tastatur, Maus und Drucker etc.

Datenanschluss
(in der Regel Internet und Netzwerk)

Energieversorgung
(Netzstecker) Computer

USV

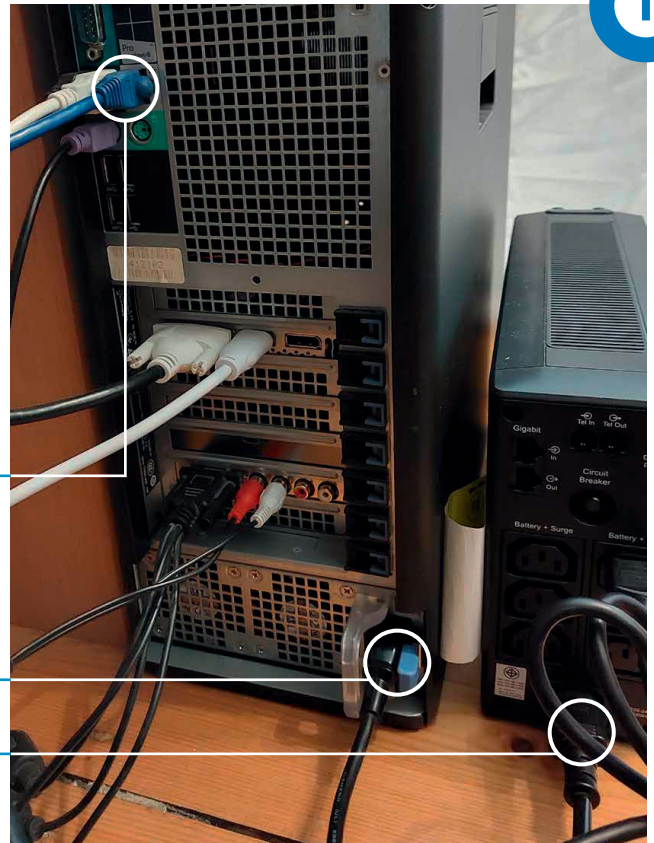
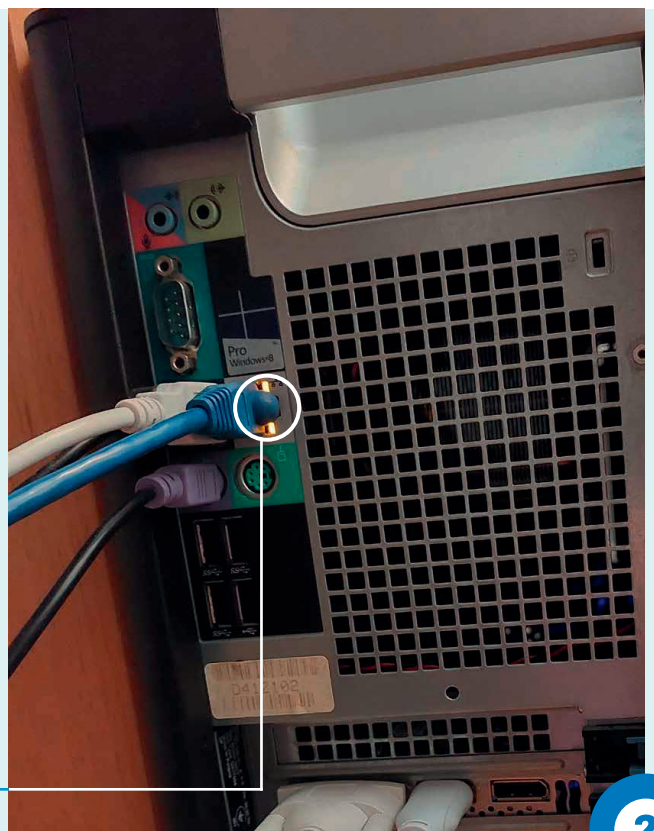


Bild 2:

Der Datenanschluss ist meist mit zwei LEDs versehen. Eine leuchtet dauerhaft und zeigt eine Verbindung an. Die andere blinkt meist bei Datenübertragung.

Achten Sie auf die „Sicherheitsnase“ des Steckers. Diese müssen Sie gedrückt halten, während Sie das Kabel herausziehen.



3

Bild 3:

Gerät von Internet und Netzwerk getrennt.
Die LEDs an diesem Anschluss sind komplett aus.

So sieht der Anschluss ohne Kabel aus.

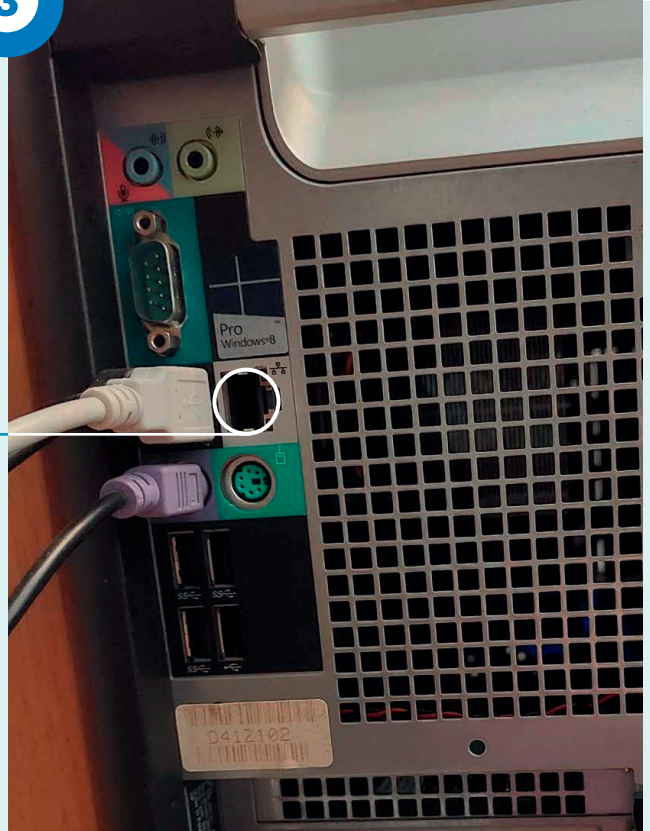
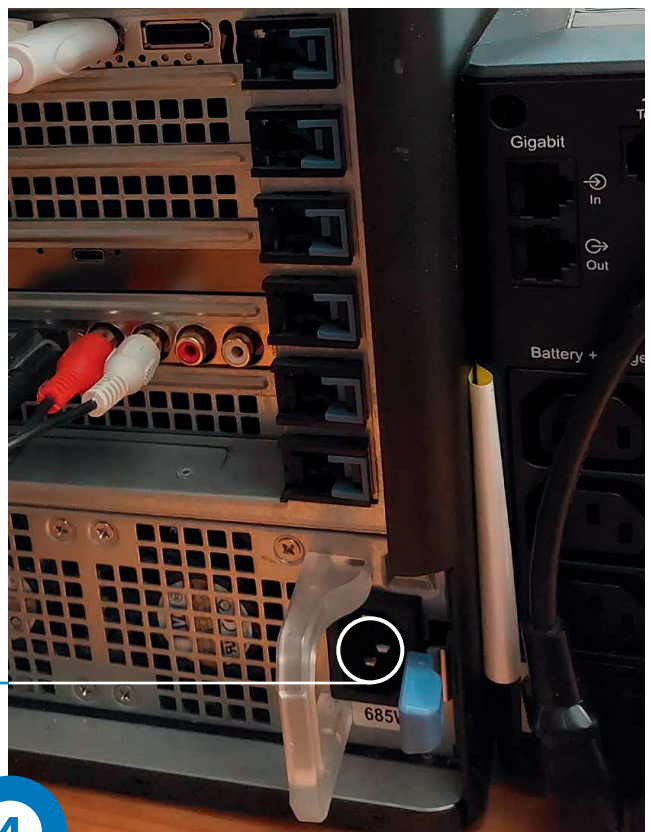


Bild 4:

Netzstecker am Gerät entfernt, keine Aktivität mehr.

Netzstecker entfernt.

4



3.5.4 Anzeige erstatten

Melden Sie sich bei der lokalen Polizeibehörde (**Die Bayerische Polizei - Dienststellensuche**) und erstatten Sie eine Anzeige. Größere Dienststellen haben häufig bereits eine Cyberabteilung. Von kleineren Dienststellen werden Sie gegebenenfalls an die Zentrale Ansprechstelle Cybercrime für die Wirtschaft in Bayern verwiesen (**Die Bayerische Polizei - Zentrale Ansprechstelle Cybercrime für die Wirtschaft in Bayern**).

Zahlen Sie kein Lösegeld! Die Wahrscheinlichkeit, dass Sie alle Daten vollständig zurückerhalten ist eher gering. Das Risiko, dass die Daten trotz Zahlung (zumindest teilweise) verloren gehen oder sogar veröffentlicht werden, ist deutlich größer.

Zahlungen halten das „Geschäftsmodell“ weiterhin attraktiv und wer einmal gezahlt hat, zahlt gegebenenfalls auch ein zweites Mal. Es gibt keine Garantie gegen einen Wiederholungsfall (auch wenn dies behauptet wird).

3.5.5 Meldepflichten

Sobald eine Verletzung des Schutzes personenbezogener Daten erfolgt ist, also personenbezogene Daten, insbesondere Gesundheitsdaten, verändert oder vernichtet wurden, müssen Sie innerhalb von **72 Stunden nach Kenntnisnahme** eine Meldung an das Bayerische Landesamt für Datenschutzaufsicht oder an den „Bayerischen Landesbeauftragten für den Datenschutz“ machen. Bei Verstößen gegen diese Pflicht drohen Bußgelder.

Die Online-Meldung finden Sie hier:

<https://www.lida.bayern.de/de/datenpanne.html>

Erläuterungen zu den Meldepflichten finden Sie hier:

https://www.datenschutz-bayern.de/datenschutzreform2018/OH_Meldepflichten.pdf

Sofern die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten Ihrer Patienten zu Folge hat, müssen Sie die betroffene(n) Person(en) unverzüglich benachrichtigen.

Die Benachrichtigung der Patienten muss folgende Informationen in klarer und einfacher Sprache enthalten und sollte zu Beweis-zwecken in Textform (zum Beispiel per E-Mail) erfolgen:

- a) eine Beschreibung der Art der Verletzung (zum Beispiel unerlaubte Einsichtnahme, Kopie, Löschung, Veröffentlichung) des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien (wessen Daten sind betroffen? Mitarbeiter, Patienten, andere Praxen?) und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien (zum Beispiel Name, Adresse, Telefonnummer, Geburtsdatum oder Behandlungsdaten, Befunde, Laborwerte) und der ungefähren Zahl der betroffenen personenbezogenen Datensätze,
- b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen (im Zweifel immer der Praxisinhaber),
- c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten (zum Beispiel Erpressungsversuch, Veröffentlichung, Diskriminierung),
- d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Je nach Risiko, das sich aus den Daten ergibt (zum Beispiel Selbstverletzung, Suizidgefahr), oder nach persönlichem Ermessen kann eine **zusätzliche** telefonische Kontaktaufnahme und Information sinnvoll sein.

3.5.6 Nachbereitung

Überwachen Sie Ihre Systeme nach einem Vorfall weiter und häufiger als üblich, um sicherzustellen, dass keine kompromittierten Systeme übersehen wurden oder ein erneuter Angriff stattfindet.

Besprechen Sie mit Ihrem IT-Dienstleister Maßnahmen, um die Wahrscheinlichkeit eines erneuten Angriffs sowie dessen Auswirkungen zu reduzieren, seien es technische oder organisatorische Maßnahmen.

4. Glossar und Abkürzungen

Active Directory: Zentrale Benutzerverwaltung in einem Computernetzwerk, um sich an jedem Endgerät mit den gleichen Daten anmelden zu können.

Administrator: Verwaltet die Einstellungen von Endgeräten, Servern und der Software.

Administratorrechte: Ein Benutzer mit diesen Berechtigungen kann vielfältige Einstellungen an Endgeräten, Servern und Software vornehmen. Schadsoftware versucht diese Berechtigungen zu erlangen, um andere Endgeräte und Server im Netzwerk ebenfalls zu infizieren.

Authentifizierung: Der Nachweis einer Identität oder von Zugriffsrechten gegenüber einem Computer.

Domänencontroller: Ein Server zur zentralen Authentifizierung von Computern und Benutzern in einem Rechnernetz.

Endgeräte: Alle Produkte, die der Anwender für Eingaben und Anzeigen nutzt, wie Computer, Mobiltelefone und Tablets.

Firewall: Hard- oder Software zur Kontrolle von Verbindungen und Datenaustausch in einem Netzwerk.

Integrität von Informationen: Nachweis beziehungsweise Überprüfbarkeit, dass die Information unverändert ist.

IT-Forensiker: IT-Spezialist für die Analyse von Angriffen mit Schadsoftware und für die Wiederherstellung von Systemen nach solchen Angriffen.

Kerberos: Protokoll zur Authentifizierung auch in unsicheren Netzen, das auch Single Sign On (SSO) ermöglicht.

Key Distribution Service Accounts: Spezieller Dienst auf einem Domänencontroller für die zentrale Verwaltung von Benutzern und Endgeräten. Steuert, wer auf welche Ressourcen zugreifen darf und wie die Daten im Netzwerk verschlüsselt werden.

LAN: Local Area Network: Ein auf Leitungen basierendes Netzwerk zum Datenaustausch von Geräten in einem räumlich begrenzten Bereich.

Logs: Textdatei, in der Geräte und Software Informationen, Fehler oder Hilfstexte für die Fehlersuche abgespeichert.

Multifaktorauthentifizierung: Der Nachweis einer Identität oder von Zugriffsrechten auf ein System nicht nur mit Benutzernamen und Passwort, sondern einem zusätzlichen Faktor wie Fingerabdruck, Gesichtsscan, PIN per SMS oder spezieller APP. Kennen Sie vermutlich vom Onlinebanking, wo Sie eine TAN mit Bankkarte und Generator erzeugen müssen, zum Beispiel für Überweisungen.

Router: Ist ein Gerät, das Datenpakete zwischen unterschiedlichen Rechnernetzen oder Netzwerksegmenten weiterleitet.

Server: Spezielle Computer, die Daten und Dienste für die Endgeräte zur Verfügung stellen.

Sicherheitsfilter (Security Gateway): Ein Gerät oder eine Software, welche die Nutzung von speziellen Anwendungen wie E-Mail und Internet sicherer macht, indem der Datenverkehr überprüft und schädliche Inhalte herausgefiltert werden.

Single Sign On: Ein Verfahren, um sich in einem Netzwerk nur einmal zu authentifizieren und anschließend automatisch an allen Diensten und Ressourcen sicher anzumelden.

Switch: Ein Gerät, das Datenpakete zwischen Endgeräten und Servern im gleichen Netzwerksegment transportiert.

WAN (Wide Area Network): Ein Netzwerk über einen räumlich begrenzten Bereich hinaus (über Ländergrenzen und Kontinente).

WLAN (Wireless Local Area Network): Wie LAN, jedoch basierend auf Funkstandards.



Impressum

Herausgeber

Kassenärztliche Vereinigung Bayerns
Elsenheimerstraße 39
80687 München

www.kvb.de

Redaktion

Gesamtteam Digitalisierung
mit freundlicher Unterstützung der
KV Westfalen-Lippe

Layout

Stabsstelle Kommunikation

Bilder und Grafik

KV Westfalen-Lippe

Stand

Mai 2026