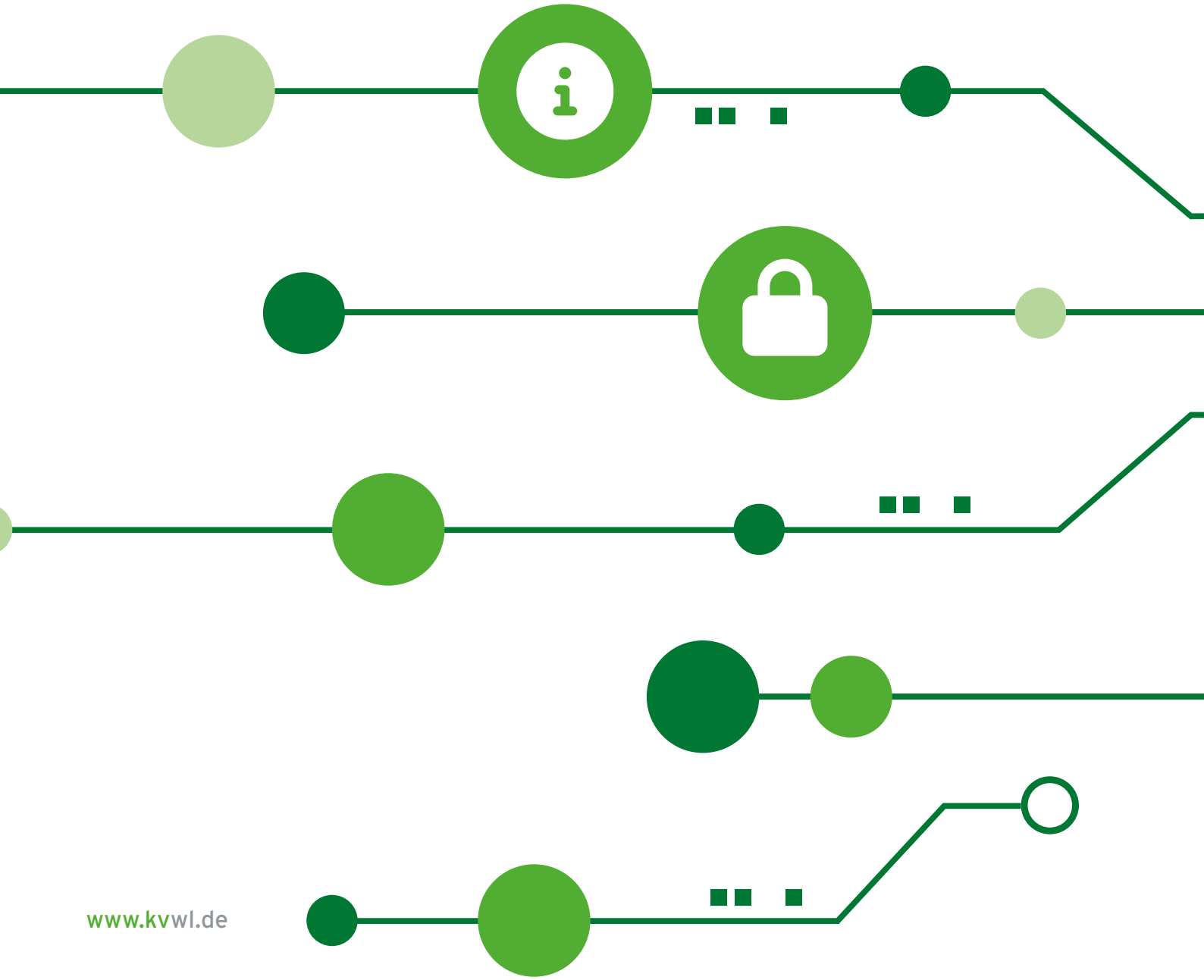
KVWL
Kassenärztliche Vereinigung
Westfalen-Lippe

Leitfaden zum Umgang mit IT-Sicherheitsvorfällen



www.kvwl.de

Kassenärztliche Vereinigung
Westfalen-Lippe

Inhalt

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 bzw. 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. Jede(r) sollte in der Lage sein, im Falle eines Falles schnell und richtig zu reagieren - auch wenn der/die Praxisinhaber(in) vielleicht gerade nicht anwesend ist!

Kapitel 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 (z.B. die Patienten) 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

Kapitel 2

Erkennen von IT-Sicherheitsvorfällen

Wichtige Hinweise können sein:

- Berichte in den Medien (z.B. Presseberichte, Newsletter KVWL, Radio, Fernsehen)[1]
- Informationen von Herstellern (z.B. TI-Komponenten, Praxisverwaltungssystem)[1]
- Beobachtungen durch Mitarbeiter, Patienten oder aus anderen Praxen[1]
- Warnmeldungen[1] oder Protokolle[2] von Firewalls
- Warnmeldungen[1] oder Protokolle[2] des Virenscanners
- Protokolle der Server und Anwendungen[2]
- Warnmeldungen oder Protokolle von Sicherheitsfiltern für Internet und E-Mailverkehr[2]
- Protokolle der Benutzer- und Berechtigungsverwaltung[2]

[1] Dies sind üblicherweise die für den Nutzer relevantesten Quellen.
[2] Diese wertet in der Regel ein IT-Dienstleister im Wartungs- oder Störungsfall aus.

Kapitel 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 ggf. die verfügbaren Sicherheitsupdates oder Softwareaktualisierungen.

Gibt es aktuell keine entsprechenden Updates, existiert ggf. 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 des Herstellers

Informiert Sie der Hersteller des Produktes, 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 auf Grund seltsamer bzw. verdächtiger, angeblich von Ihnen versendeter E-Mails, beauftragen Sie Ihren IT-Dienstleister mit der Suche nach Schadsoftware.

Dokumentieren Sie Fehlermeldungen sowie alle Schritte, die Sie bereits durchgeführt haben – idealerweise mit Bildern (z.B. mit dem Handy).

Trennen Sie auch hier das System vom Internet bzw. Netzwerk.

(siehe 3.5.3: Bild 1, 2 und 3)

3.4 Warnmeldungen oder Protokolle Firewall/Virenscanner

Prüfen Sie, was direkt vor dem Erscheinen der Warnmeldung am Gerät gemacht wurde. Dokumentieren Sie die Warnmeldung möglichst mit allen Details (z.B. 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 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 bereits eine entsprechende Meldung sehen, gilt es schnell und überlegt zu handeln.

3.5.1 Sofortmaßnahmen

- Ruhe bewahren, alle Mitarbeiter informieren, Dokumentation beginnen.
- Keine Anmeldung an betroffenen oder verdächtigen Geräten mit Administratorrechten!
- 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 4.5.3: 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 ca. 5 Sekunden gedrückt halten, bis das Gerät ausschaltet) *(siehe 4.5.3: 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 auch hier das Risiko, Hardware zu beschädigen und Daten zu verlieren. Kann der Verschlüsselungstrojaner allerdings seine Arbeit „ungestört" erledigen, sind Ihre Daten mit großer Wahrscheinlichkeit unwiederbringlich verloren!
- 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 z.B. FritzBox/Speedport). Beachten Sie, dass dadurch ggf. das Festnetztelefon ebenfalls nicht mehr funktioniert!
- Stimmen Sie mit dem IT-Dienstleister ab, 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

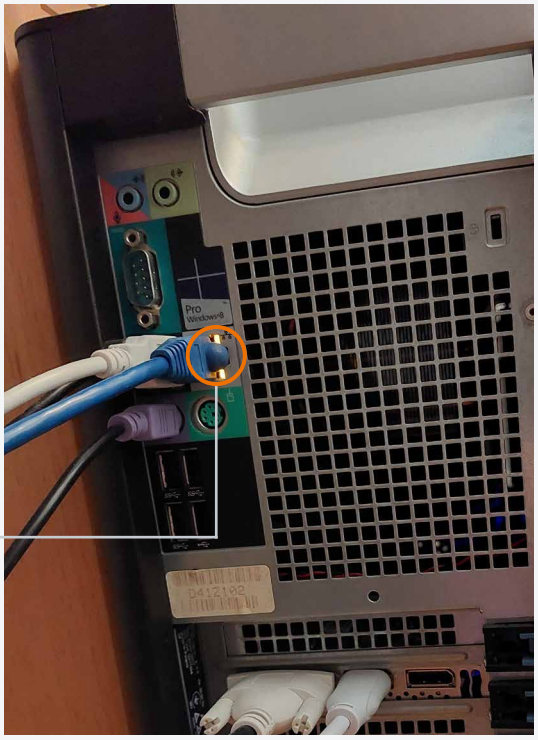
- Die verschlüsselten Datenträger ausbauen und an sicherem Ort verwahren. Sie benötigen diese ggf. für Strafanzeige, Gerichtsverfahren, Versicherung, Ursachenanalyse oder einen späteren Wiederherstellungsversuch.
- Wenn das Gerät bereits komplett verschlüsselt ist (wenn Sie den Bildschirm oben sehen, ist dies in der Regel der Fall), lassen Sie es eingeschaltet, sofern Sie eine forensische Analyse wünschen (es ist ja bereits vom Netzwerk/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 vorhanden Backups, ob diese aktuell und nicht verseucht oder ebenfalls verschlüsselt sind.
- Prüfen Sie, ob es an anderer Stelle womöglich noch Daten oder Backups gibt (z.B. Rechner, 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. Ggf. 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 Geräte, 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 Geräte werden dennoch vollständig geprüft, bevor diese wieder in das Netzwerk eingebunden werden.
- Prüfen Sie alle Ihre 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 bei der Gelegenheit 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, empfehlen wir dringend die komplette Neueinrichtung dieser Serverlandschaft! Zumindest muss das Passwort des eingebauten Key Distribution Service Accounts (KRBTGT) zweimal zurückgesetzt werden. Dies invalidiert alle „Golden Tickets“, welche 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 z.B. Monitor, Tastatur, Maus und Drucker etc.

Bild 2: Der Datenanschluss ist meist mit zwei LEDs versehen. Eine leuchtet dauerhaft und zeigt eine Verbindung an. Die andere blinkt meist bei Datenübertragung.



LEDs am Datenanschluss zeigen Verbindung und Aktivität an. Die meisten Datenkabel haben eine „Sicherungsnase“. Diese muss man drücken, um das Kabel entfernen zu können.

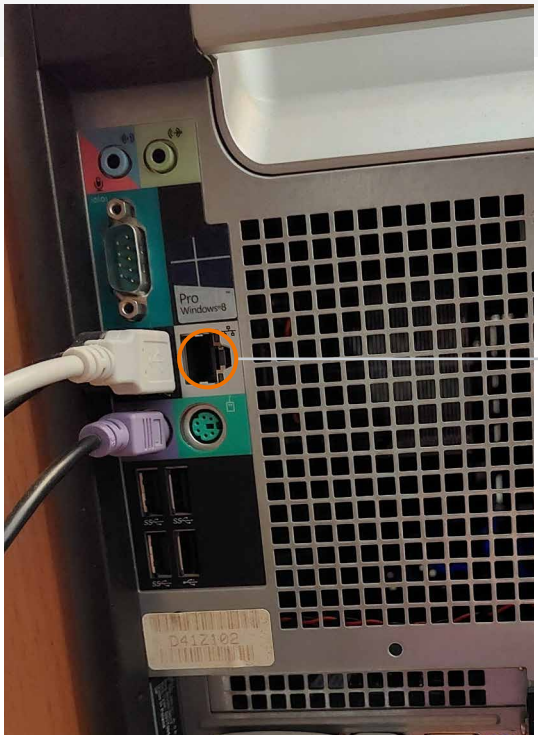
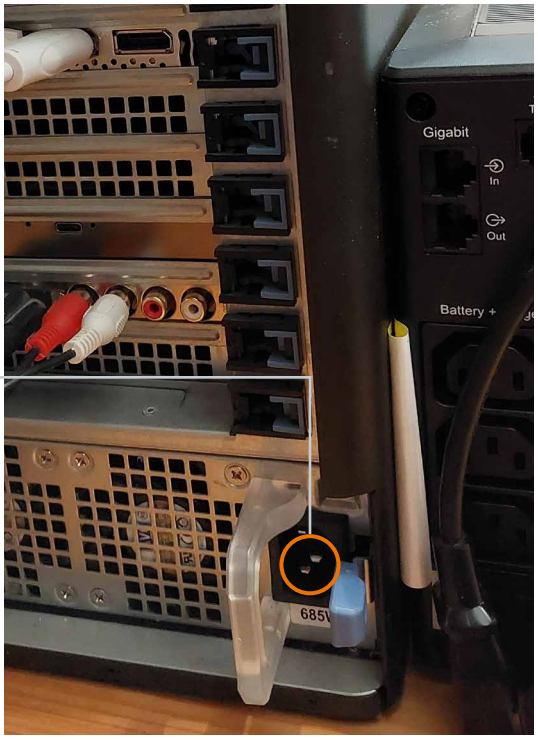


Bild 3: Gerät von Internet und Netzwerk getrennt und die LEDs an diesem Anschluss sind komplett aus.

So sieht der Anschluss ohne Kabel aus.

Bild 4: Netzstecker am Gerät entfernt, keine Aktivität mehr.



3.5.4 Anzeige erstatten

Melden Sie Sich bei der lokalen Polizeibehörde (https://polizei.nrw/wachenfinder) und erstatten Sie eine Anzeige. Größere Dienststellen haben häufig bereits eine Cyberabteilung. Von kleineren Dienststellen werden Sie ggf. auch an eine solche in einer anderen Stadt/Dienststelle verwiesen. Melden Sie Sich ggf. auch beim Landeskriminalamt (https://lka.polizei.nrw/artikel/das-cybercrime-kompetenzzentrum-beim-lka-nrw).

Zahlen Sie kein Lösegeld! Die Wahrscheinlichkeit, dass Sie alle Daten vollständig zurückerhalten ist gering. Das Risiko, dass die Daten trotz Zahlung (zumindest teilweise) verlorengehen oder sogar veröffentlicht werden, ist deutlich größer. Zahlungen halten das „Geschäftsmodell“ weiterhin attraktiv und wer einmal gezahlt hat, zahlt ggf. auch ein zweites Mal. Es gibt keine Garantie gegen einen Wiederholungsfall (auch wenn dies behauptet wird).

3.5.5 Meldepflichten

Sobald personenbezogene Daten, insb. Gesundheitsdaten, verändert oder vernichtet wurden, müssen Sie dies **innerhalb 72 Stunden nach Kenntnisnahme** der Behörde „Landesbeauftragte für Datenschutz und Informationsfreiheit“ melden. Bei Verstößen gegen diese Pflicht drohen Bußgelder.

Das Formular finden Sie aktuell hier:
https://ldi-fms.nrw.de/lip/action/invoke.do?id=Datenschutzverletzung

Erklärungen und Informationen dazu finden Sie unter:
https://www.ldi.nrw.de/kontakt/meldeformular-fuer-datenpannen

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 von der Verletzung benachrichtigen.

Die Benachrichtigung der Patienten muss folgende Informationen in klarer und einfacher Sprache erhalten und sollte zu Beweiszwecken in Textform (z.B. per E-Mail) erfolgen.

a) eine Beschreibung der Art der Verletzung (z.B. 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 (z.B. 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 (z.B. 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 (z.B. Selbstverletzung, Suizidgefahr) oder 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.

Glossar / 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.
- **Administrator-Rechte** – 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 Zugriffsrechten gegenüber einem Computer.
- **Domänencontroller** – Ist ein Server zur zentralen Authentifizierung von Computern und Benutzern in einem Rechnernetz.
- **Endgeräte** – Alle Produkte die der Anwender für Eingaben und Anzeigen nutzt, z.B. Computer, Mobiltelefone und Tablets.
- **Server** – Spezielle Computer, die Daten und Dienste für die Endgeräte zur Verfügung stellen.
- **Firewall** – Hard- oder Software zur Kontrolle von Verbindungen und Datenaustausch in einem Netzwerk.
- **Integrität von Informationen** – Nachweis bzw. 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, welches 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.
- **Logs** – Textdatei in der Geräte und Software Informationen, Fehler oder Hilfstexte für die Fehlersuche abspeichern.
- **Multifaktorauthentifizierung** – Der Nachweis einer Identität oder 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 für z.B. Überweisungen.
- **Router** – Ist ein Gerät welches Datenpakete zwischen unterschiedlichen Rechnernetzen oder Netzwerksegmenten weiterleitet.
- **Single Sign On** – Ein Verfahren, um sich in einem Netzwerk nur einmal zu authentifizieren und anschließend automatisch an allen Diensten und Ressourcen sicher angemeldet zu werden.
- **Switch** – Ist ein Gerät, welches Datenpakete zwischen Endgeräten und Servern im gleichen Netzwerksegment transportiert.

- **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.
- **LAN** – Local Area Network: Ein auf Leitungen basierendes Netzwerk zum Datenaustausch von Geräten in einem räumlich begrenzten Bereich.
- **WLAN** – Wireless Local Area Network: Wie LAN jedoch basierend auf Funkstandards.
- **WAN** – Wide Area Network: Ein Netzwerk über einen räumlich begrenzten Bereich hinaus (über Ländergrenzen und Kontinente).
- **Verfügbarkeit von Informationen** – Zu dem Zeitpunkt an dem ich die Informationen benötige, kann ich diese auch abrufen.
- **Vertraulichkeit von Informationen** – Nur Personen oder Computer die berechtigt, sind können diese Informationen abrufen.

Kassenärztliche Vereinigung
Westfalen-Lippe

Impressum

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

Geschäftsbereich IT & eHealth
E-Mail: mitgliederberatung@kvwl.de
Tel.: 0231 / 94 32 39 90

www.kvwl.de

Stand: Juni 2022