KBV KASSENÄRZTLICHE BUNDESVEREINIGUNG

IT-SICHERHEIT: PRAXEN IM VISIER VON HACKERN UND TROJANERN

BEISPIELE UND TIPPS ZUR PRÄVENTION

Die Bedrohung durch Erpressungssoftware (auch Ransomware oder Verschlüsselungstrojaner) hat weltweit massiv zugenommen – auch im Gesundheitswesen. Die Vorgehensweise der Hacker ähnelt sich und häufig findet ungewollt eine aktive „Mitarbeit“ der Betroffenen selbst statt – etwa durch Anklicken eines Links. In der Folge eines Angriffs werden beispielsweise Zugänge gesperrt, Daten geklaut, verschlüsselt und anschließend ein „Lösegeld“ gefordert.

Bedrohung durch Cyber-Kriminalität nimmt zu

Die folgenden Beispiele aus der Praxis sollen für das Thema sensibilisieren und Handlungsoptionen für den Ernstfall aufzeigen.

PRAXISBEISPIELE

BEISPIEL 1: UNBERECHTIGTER ZUGRIFF AUF DSL-ROUTER

Beschreibung

Eine Praxis hat ihren DSL-Router im Flur stehen. Durch Zufall wird festgestellt, dass sich fremde Smartphones in das Netzwerk eingewählt haben (im Systemprotokoll aufgelistet). Offenbar wurden die aufgedruckten Zugangsdaten des Routers dafür benutzt, sich Zugang zum Router und/oder dem WLAN zu verschaffen.

Beispiel 1

Risiko

Ein direkter Einfluss auf die Prozesse, Geräte und Patientendaten der Praxis kann nicht festgestellt werden. Dennoch ist eine Manipulation von Praxis-Endgeräten im WLAN und eine Offenlegung von Patientendaten nicht auszuschließen. Im günstigsten Falle wurde der Zugang nur für das Surfen im Internet missbraucht.

Reaktion

Im Anschluss an den Vorfall werden folgende Schritte unternommen:

- Der IT-Dienstleister wird beauftragt, den DSL-Router auf Werkseinstellungen zurückzusetzen.
- Es werden sichere, individuelle Kennwörter und ein neuer Netzwerkschlüssel für den Zugriff auf den Router vergeben.
- Für Patientinnen und Patienten sowie andere externe Personen wird ein Gast-WLAN eingerichtet.

- Der Router wird in einem abschließbaren Raum aufgestellt und alle dezentralen technischen Komponenten der Telematikinfrastruktur, zum Beispiel der Konnektor, in demselben Raum untergebracht.
- Der Vorfall wird protokolliert (interne Dokumentationspflicht nach Art. 33 Abs. 5 Datenschutzgrundverordnung).

Tipps zur Prävention

- Router nie bei den Standard-Einstellungen belassen.
- Geräte wie DSL-Router restriktiv konfigurieren, zum Beispiel WPS-Tastenfunktion deaktivieren, mit der ansonsten mittels Knopfdruck am Router eine unkomplizierte Verbindung eines Gerätes mit dem WLAN möglich ist.
- Wichtige Geräte räumlich vor dem Zugriff durch Dritte schützen.

BEISPIEL 2: SUPPORT-BETRUG DURCH ANRUF

Beschreibung

Eine Praxis erhält einen Anruf – angeblich von der Firma Microsoft. Der Mitarbeiter behauptet, dass der Praxis-PC von einem Virus befallen sei und daher das Windows-System per Fernwartung geprüft werden müsse („Support Scam“). Die Praxisinhaberin stimmt aufgrund der professionellen und vertrauenserweckenden Gesprächsführung zu. Es findet eine Scheinprüfung statt, bei der sich der kriminelle Anrufer auf den Computer schaltet. Anschließend wird ein kostenpflichtiges Schutzprogramm angeboten. Die Praxisinhaberin schöpft Verdacht und beendet das Telefonat und die Fernwartung.

Beispiel 2

Risiko

Es ist nicht auszuschließen, dass der Praxis-PC und andere Endgerät sowie das Netzwerk ausgespäht wurden. Datendiebstahl oder Datenmanipulation sind wahrscheinlich.

Reaktion

Die Praxisinhaberin ruft ihren IT-Dienstleister an und die Netzwerkverbindung des betroffenen Computers wird sofort gekappt, um Schlimmeres zu verhindern.

Im Anschluss an den Vorfall werden folgende Schritte unternommen:

- Der IT-Dienstleister nimmt eine komplette Neuinstallation des Computers vor und spielt die Datensicherung des Vortags auf.
- Es erfolgt eine Meldung an die Polizei und eine Meldung innerhalb von 72 Stunden an die Landesdatenschutzbehörde (nach Art. 33 Datenschutzgrundverordnung).
- Der Vorfall wird protokolliert (interne Dokumentationspflicht nach Art. 33 Abs. 5 Datenschutzgrundverordnung).

Tipps zur Prävention

- Polizei, Microsoft, Apple und sonstige Firmen und Behörden würden niemals einen Fernzugriff auf ein IT-Endgerät verlangen – bei einem solchen Anruf einfach auflegen.

Social Engineering: Cyber-Kriminelle nutzen persönliche Kontakte zu Menschen, um sie dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu

umgehen oder selbstständig Schadprogramme auf ihren Systemen zu installieren. Diese Methode der Manipulation heißt Social Engineering.

BEISPIEL 3: SUPPORT-BETRUG DURCH WARNMELDUNG IM BROWSER

Beschreibung

Während mit dem Internet-Browser gearbeitet wird, erscheint folgender Hinweis: „Der Server meldet: Windows wurde aufgrund verdächtiger Aktivitäten blockiert. Bitte rufen Sie uns an: 032-221-850-307!“ In der Warnmeldung wird der Praxismitarbeiter dazu aufgefordert, seinen Windows-Benutzernamen und das Kennwort einzugeben. Das Fenster lässt sich nicht schließen und es ertönt ein anhaltender Warnton. Der Mitarbeiter ruft bei der Hotline an und wird zu einer Fernwartung überredet: Die Betrüger greifen dabei auf den Computer zu und geben vor, dass System zu prüfen. Irgendwann schöpft der Praxismitarbeiter Verdacht und legt auf.

Beispiel 3

Risiko

Es kann nicht ausgeschlossen werden, dass der Praxis-PC und das Netzwerk ausgespäht wurden. Ein Datendiebstahl oder eine Datenmanipulation sind wahrscheinlich.

Reaktion

Der Praxismitarbeiter schaltet den Computer über den Ein-/Ausschalter ohne Herunterfahren aus („Hartes Ausschalten“) und ruft den IT-Dienstleister an.

Im Anschluss an den Vorfall werden folgende Schritte unternommen:

- Der IT-Dienstleister nimmt eine komplette Neuinstallation des Computers vor und spielt die Datensicherung des Vortags auf.
- Es erfolgt eine Meldung an die Polizei und eine Meldung innerhalb von 72 Stunden an die Landesdatenschutzbehörde (nach Art. 33 Datenschutzgrundverordnung).
- Der Vorfall wird protokolliert (interne Dokumentationspflicht nach Art. 33 Abs. 5 Datenschutzgrundverordnung).

Tipps zur Prävention

- Das Risiko-Bewusstsein beim Praxisteam kann durch Aufklärung und Schulungen geschärft werden. Dabei werden Bedrohungen und Sicherheitsvorkehrungen kennengelernt, um im Ernstfall eine gefährliche Mischung aus Panik und Unwissen zu minimieren.

BEISPIEL 4: DIGITALER EINBRUCH ÜBER FERNZUGANG DER PRAXIS

Beschreibung

In einer Praxis läuft dauerhaft ein Computer, auf den von Zuhause aus zugegriffen werden kann – über das Internet und den von Microsoft bereitgestellten Dienst Remote Desktop Protocol (RDP). An einem Morgen lässt sich in der gesamten Praxis nicht mehr auf den Server zugreifen und das Praxisverwaltungssystem nicht starten. Auch auf dem Fernzugriff-Computer können lokal abgelegte Dokumente nicht geöffnet werden. Höchstwahrscheinlich ist über den RDP-Zugang ein digitaler Einbruchsversuch gelungen und die Cyber-Kriminellen haben mit Ransomware

Beispiel 4

zugeschlagen. Es ist kein normaler Praxisbetrieb möglich (kein Zugriff auf Patientenakten, Terminkalender, Adressen, Formulare, etc.) und Patientinnen und Patienten müssen nach Hause geschickt werden.

Risiko

Auch wenn es keine Erpressung gibt, ist die Vertraulichkeit von Patientendaten möglicherweise gefährdet. Nicht alle patientenbezogenen Dokumente lagen innerhalb einer verschlüsselten Datenbank und sind damit nur unzureichend gegen Einsichtnahme und Diebstahl geschützt.

Reaktion

Die Praxis ruft ihren IT-Dienstleister an, es werden keine weiteren Computer im Netzwerk gestartet, der Fernzugriff-PC wird vom Netz getrennt und der RDP-Zugriff deaktiviert.

Im Anschluss an den Vorfall werden folgende Schritte unternommen:

- Der IT-Dienstleister nimmt eine komplette Neuinstallation des Servers und des Fernzugriff-Computers vor und spielt die Datensicherung des Vortags auf.
- Es erfolgt ein Virenscan und eine Sicherheitsprüfung weiterer, auch scheinbar nicht betroffener Arbeitsstationen sowie von Druckern, Geräten der Telematikinfrastruktur, etc.
- Es erfolgt eine Meldung an die Polizei und eine Meldung innerhalb von 72 Stunden an die Landesdatenschutzbehörde (nach Art. 33 Datenschutzgrundverordnung).
- Der Vorfall wird protokolliert (interne Dokumentationspflicht nach Art. 33 Abs. 5 Datenschutzgrundverordnung).

Tipps zur Prävention

- Von Fernzugriffsmöglichkeiten auf die Praxis-IT mittels RDP über das ungesicherte Internet ist dringend abzuraten. Falls ein Fernzugriff erforderlich ist, sollte dieser mittels Zugang über ein professionelles Virtuelles Privates Netzwerk (VPN) gesichert sein.
- Die Praxis sollte gemeinsam mit einem IT-Dienstleister prüfen, welche Daten wo liegen und wie sie abgesichert werden. Gegebenenfalls sollten sie zusammengelegt und verschlüsselt werden.

BEISPIEL 5: VERLUST EINER UNVERSCHLÜSSELTEN DATENSICHERUNG

Beschreibung

Beispiel 5

Eine Praxis speichert täglich die eigenen Dateien und ein Back-up des Praxisverwaltungssystems auf USB-Sticks (Standard-Geräte ohne zusätzliche Sicherheitsfeatures). Ein Stick wird am Ende des Tages mit nach Hause genommen, ein zweiter Stick bleibt als Tagessicherung in der Praxis. Die Daten werden ohne weitere Maßnahmen zum Schutz der Vertraulichkeit abgespeichert. An einem Tag geht der eine USB-Stick auf dem Heimweg verloren.

Risiko

Durch den Verlust des USB-Sticks wurden die Daten offengelegt, eine Korrektur ist nicht mehr möglich. Es besteht ein hohes Risiko für die Patientendaten, persönliche Rechte und Freiheiten sind unmittelbar betroffen.

Reaktion

Im Anschluss an den Vorfall werden folgende Schritte unternommen:

- Der Verlust wird der Polizei und der Versicherung gemeldet.
- Nach Anraten der Polizei wurde der IT-Dienstleister zwecks Datenschutz/Datensicherheitsmaßnahmen eingeschaltet. Es werden zwei sichere externe Festplatten mit USB-Anschluss angeschafft und weitere Konfigurationen des Praxis-Computers vorgenommen.
- Die betroffenen Patientinnen und Patienten werden unverzüglich benachrichtigt (nach Art. 34 Datenschutzgrundverordnung).
- Es erfolgte eine Meldung innerhalb von 72 Stunden an die Landesdatenschutzbehörde (nach Art. 33 Datenschutzgrundverordnung).
- Der Vorfall wird protokolliert (interne Dokumentationspflicht nach Art. 33 Abs. 5 Datenschutzgrundverordnung).

Tipps zur Prävention

- Zusätzliche externe Datensicherungen sind absolut notwendig, müssen aber hinreichend gesichert werden (z.B. Speichermedien, die eigene Verschlüsselung mitbringen).

EMPFEHLUNGEN ZUR PRÄVENTION

Praxen sollten die Gefahren durch Cyber-Angriffe ernstnehmen, sich mit dem Thema auseinandersetzen und sich präventiv schützen. Hilfestellung dabei bietet die IT-Sicherheitsrichtlinie der KBV, die jeweils an die aktuelle Bedrohungslage angepasst wird (s. Infokasten unten).

Am besten wird ein professioneller IT-Dienstleister beauftragt, eine entsprechende IT-Sicherheitsarchitektur in der Praxis aufzubauen. Die Expertinnen und Experten können gewährleisten, dass alle relevanten gesetzlichen Vorgaben aus der Datenschutzgrundverordnung der EU sowie der IT-Sicherheitsrichtlinie beachtet werden. Auch treffen sie Vorsorge, damit Schadsoftware gar nicht erst auf den Praxis-Computer gelangt.

IT-Dienstleister beauftragen

SO KÖNNEN SIE IHRE PRAXIS SCHÜTZEN

- Wichtig sind regelmäßiges Update des Betriebssystems, des Browsers und sämtlicher genutzter Software – in Kombination mit einer aktuellen Antiviren-Software und einer richtig konfigurierten Firewall als virtuelle Schutzmauer bei der Internetnutzung.

Updates, Antiviren-Software und Firewall

- Betrüger versuchen oft, ihre Schadsoftware per E-Mail mit Dateianhang oder über Verlinkungen zu verteilen. Daher gilt es, beim Öffnen von E-Mails und insbesondere den Dateianhängen und mitgeschickten Links größte Vorsicht walten zu lassen:
  - Prüfen Sie die Identität des Absenders – E-Mail-Adressen lassen sich leicht fälschen. Handelt es sich wirklich um die bekannte E-Mail-Adresse oder wird beispielsweise nur der Name des Absenders angezeigt und es ist eine unbekannte Adresse hinterlegt? Im Zweifelsfall sollten Dateianhänge beziehungsweise Links nicht geöffnet werden.

Vorsicht bei E-Mails

- Beliebt sind auch E-Mails, die den Nutzer auffordern, sich auf einer ihm bekannten Website mit seinen Anmeldedaten einzuloggen, um beispielsweise bestimmte Angaben zu überprüfen. Meldet er sich über den mitgeschickten Link an, können die Betrüger Nutzernamen und Passwort ganz einfach aufzeichnen und klauen.

› Als Back-up für den Ernstfall sollten alle Daten routinemäßig gesichert werden – hierbei bauen die IT-Dienstleister ein geeignetes Back-up-Konzept auf und überprüfen regelmäßig in sogenannten Recovery-Tests, ob die gesicherten Daten fehlerfrei zurückgespielt werden können.

Back-up-System zur Datensicherung

› Eine wichtige Maßnahme, die Praxen eigenständig durchführen können, ist die Etablierung einer transparenten und vertrauensvollen Fehlerkultur im Team. Hierdurch lässt sich wichtige Präventionsarbeit leisten und potenzieller Schaden begrenzen.

Positive Fehlerkultur etablieren

› Praxisinhaberinnen und -inhaber können für sich und ihr Praxisteam Schulungen zum Thema IT-Sicherheit organisieren und regelmäßig darüber aufklären. Für den Notfall helfen praktische Checklisten wie die IT-Notfallkarte des Bundesamts für Informationssicherheit – sie enthält die wichtigsten Schritte bei einem IT-Notfall und kann um Telefonnummern zum jeweiligen IT-Dienstleister ergänzt und in der Praxis aufgehängt werden: https://bit.ly/BSI-Notfallkarte

Schulungen

IT-Notfallkarte aufhängen

Auch die KBV hat ein breites Informationsangebot rund um die IT-Sicherheitsrichtlinie aufgebaut – bestehend aus einer Website, einem Serviceheft, einem Erklär-Video und einer Online-Schulung im Fortbildungsportal im Sicheren Netz (2 CME-Punkte): www.kbv.de/html/it-sicherheit.php

Informationsangebot der KBV

IT-SICHERHEITSRICHTLINIE

IT-Sicherheitsrichtlinie

Die KBV hat im Auftrag des Gesetzgebers eine IT-Sicherheitsrichtlinie entwickelt. Darin wird das Mindestmaß der zu ergreifenden Maßnahmen beschrieben, um die IT-Sicherheit in Praxen zu gewährleisten. Die Vorgaben sollen dabei helfen, IT-Systeme und sensible Daten in den Praxen noch besser zu schützen.

Sie wollen sich detailliert zu den einzelnen Sicherheitsanforderungen informieren oder suchen Musterdokumente? Dann nutzen Sie den Hub der KBV: https://hub.kbv.de/display/itsrl

Online-Plattform mit Details

Einen Überblick zur IT-Sicherheitsrichtlinie finden Sie zudem in einem Serviceheft aus der Reihe PraxisWissen. Darin werden wichtige Schritte, Fristen und Anforderungen vorgestellt. Außerdem bietet es eine Checkliste, Beispiele und Praxis-Tipps sowie weiterführende Informationen: www.kbv.de/media/sp/PraxisWissen_IT-Sicherheit.pdf

Serviceheft für Praxen

Weiterführende Informationen: www.kbv.de/html/it-sicherheit.php

Weitere Infos

MEHR FÜR IHRE PRAXIS

www.kbv.de

↗ **PraxisWissen**
↗ **PraxisWissenSpezial**
Themenhefte für Ihren Praxisalltag

Abrufbar unter:
www.kbv.de/838223
Kostenfrei bestellen:
versand@kbv.de

↗ **PraxisInfo**
↗ **PraxisInfoSpezial**
Themenpapiere mit Informationen für Ihre Praxis

Abrufbar unter:
www.kbv.de/605808

↗ **PraxisNachrichten**
Der wöchentliche Newsletter per E-Mail oder App

Abonnieren unter:
www.kbv.de/PraxisNachrichten
www.kbv.de/kbv2go

IMPRESSUM

Herausgeber:
Kassenärztliche Bundesvereinigung
Herbert-Lewin-Platz 2, 10623 Berlin
Tel.: 030 4005-0, Fax: 030 4005-1590
info@kbv.de, www.kbv.de

Redaktion:
Stabsbereich Strategie, Politik und Kommunikation
Dezernat Digitalisierung und IT

Stand:
November 2021

Hinweise:
Aus Gründen der Lesbarkeit wurde meist nur eine Form der Personenbezeichnung verwendet. Hiermit sind auch alle anderen Formen gemeint.