Informationsblatt

Verschlüsselungstrojaner (Ransomware) in Arztpraxen

1. *Führen Sie regelmäßige automatisierte Backups Ihrer Patientendaten durch?*
   Regelmäßige Backups sind wichtig, um die Verfügbarkeit der Patientendaten sicherzustellen. Im Falle einer Verschlüsselung der Daten durch Schadsoftware, können die Daten aus aktuellen Backups schnell wiederhergestellt werden und somit kann auch die Beeinträchtigung der Betroffenen minimiert werden.

2. *Mit welcher Software führen Sie die automatisierten Backups durch?*
   Eine geeignete Software in einer aktuellen Version kann die Erstellung automatisierter Backups erleichtern. Solch eine Software hilft aber auch bei der Wiederherstellung der Daten im Falle eines Datenverlustes.

3. *Auf welchen Speichermedien werden die Backups gespeichert?*
   Wichtig bei der Auswahl des Speichermediums ist, dass die erstellten Backups getrennt von den entsprechenden Rechnern liegen. Nur so ist im Falle eines Verschlüsselungstrojaners sichergestellt, dass nicht auch die Backups verschlüsselt und somit unbrauchbar werden.

4. *Welchen Virenscanner setzen Sie ein?*
   Bei der Auswahl eines Virenscanners ist es entscheidend, eine für den jeweiligen Zweck geeignete Software in einer aktuellen Version einzusetzen. Nur wenn die Schadcode-Datenbank des Virenscanners aktuell gehalten wird, besteht ein höchstmöglicher Schutz vor bekannter Schadsoftware.

5. *Testen Sie regelmäßig (z. B. 1x/Jahr) das Zurückspielen von Backupdaten?*
   Nur ein regelmäßiges Testen der Backups kann sicherstellen, dass im Falle eines Datenverlustes auch alle Daten wiederhergestellt werden können. So werden Fehler bei der Erstellung der Backups schnell erkannt und können gegebenenfalls auch schnell behoben werden.

6. *Ist das Praxisverwaltungssystem (PVS) an das Internet angeschlossen?*
   Wenn das Praxisverwaltungssystem an das Internet angeschlossen ist, wird es anfällig für Angriffe durch Schadsoftware. Aus diesem Grund sollten Sie das Praxisverwaltungssystem so isoliert wie möglich in Ihrem Netzwerk einbinden, um damit eine höhere Sicherheit der Daten zu gewährleisten. Trennen Sie auf jeden Fall das Praxisverwaltungssystem immer von Ihren Recherche-Rechnern und den Rechnern für die E-Mail-Kommunikation.

7. *Befinden sich an das Internet angeschlossene (Recherche-)Rechner in anderen Netzsegmenten als das Praxisverwaltungssystem?*
   Wenn sich (Recherche-)Rechner, die an das Internet angeschlossen sind, und das Praxisverwaltungssystem im gleichen Netzsegment befinden, besteht die Gefahr, dass auch das Praxisverwaltungssystem bei einer Verschlüsselung durch Schadsoftware betroffen ist. Eine Trennung auf Netzwerkebene von (Recherche-)Rechnern und Praxisverwaltungssystem verringert deshalb das Risiko, dass auch die Daten aus dem Praxisverwaltungssystem verschlüsselt werden.

8. *Sind Netzlaufwerke mit relevanten Patientendaten mit Rechnern verbunden, die an das Internet angeschlossen sind?*
   Wenn die Netzlaufwerke mit Rechnern verbunden sind, die an das Internet angeschlossen sind, erhöht sich die Gefahr, dass auch die Daten auf diesen Netzlaufwerken verschlüsselt werden. Eine strikte Trennung der unterschiedlichen Systeme ist deshalb wichtig.

9. *Wurden Awareness-Schulungen durchgeführt, die Internetbedrohungen (z. B. Schadcode, Phishing, …) zum Inhalt hatten?*
   Awareness-Schulungen der Mitarbeiter sind wichtig, da der Nutzer häufig die größte Schwachstelle bei etwaigen Angriffen ist. Wenn sich der Nutzer der bestehenden Gefahr bewusst ist, können viele Angriffe mittels Schadsoftware verhindert werden. Ein großes Risiko besteht beispielsweise durch Klicken auf Links in einer dubiosen E-Mail oder beim Öffnen von Dateianhängen ebenfalls aus einer dubiosen E-Mail heraus. Hier hilft es, wenn der Nutzer die Gefahr erkennt, und beispielsweise Links und Anhänge in E-Mails auf ihre Plausibilität prüft. Dabei helfen u. a. Fragen wie: Kenne ich diesen Absender? Handelt es sich tatsächlich um den entsprechenden Absender? Erwarte ich eine Nachricht von diesem Absender?

10. *Ist bekannt, dass bei einem erfolgreichen Angriff durch einen Verschlüsselungstrojaner eine Meldung beim Bayerischen Landesamt für Datenschutzaufsicht durchgeführt werden muss?*
    Die DS-GVO legt in Art. 33 fest, wann eine Datenschutzverletzung an die Aufsichtsbehörde gemeldet werden muss. Nur wenn für die Betroffenen kein Risiko besteht, muss keine Meldung der Datenschutzverletzung an die Aufsichtsbehörde erfolgen. Eine Verschlüsselung von Daten durch einen Trojaner gehört in der Regel zu den meldepflichtigen Vorfällen – vor allem dann, wenn eine der beiden folgenden Bedingungen erfüllt ist:
    - Die Daten können nicht wiederhergestellt werden oder
    - Der Zeitraum bis zur Wiederherstellung der Daten ist so lang, dass dies zu einer nicht unerheblichen Beeinträchtigung der Patienten führt.