Sicherheit in medizinischen Institutionen

E-Mail

- MAHN, Jan. 2022.Mailsicherheit in Arztpraxen: : Verschlüsselung mit Schwächen, heise online, 11.10.2022 (abgerufen am 11.10.2022)

- Bei der Übermittlung von (besonders schützenswerten) personenbezogenen Gesundheitsdaten via E-Mail muss die Vertraulichkeit der Daten über technische oder organisatorische Maßnahmen geschützt werden.
- Der höchste Schutz wäre eine E2E-Verschlüsselung. Die zugehörigen Verfahren wie bspw. PGP sind jedoch in den meisten Arztpraxen nicht vorhanden bzw. Ärzt*innen nicht damit vertraut.
- Mindestens muss daher eine Transportverschlüsselung - üblicherweise durch TLS - gewährleistet werden, insbesondere die Verbindung zwischen dem Mailserver des Absenders und dem Mailserver des Empfängers.
- TLS ist jedoch bis heute zwischen Mailservern nicht verpflichtend. Überwiegend wird die sogenannte opportunistische Verschlüsselung genutzt. Die Mailserver versuchen dabei untereinander mittels STARTTLS einen sicheren Kanal zu etablieren. Gelingt dies nicht, erfolgt unverschlüsselte Übertragung.



- Medizinische Einrichtungen sollten in ihren Mailservern die obligatorische Transportverschlüsselung konfigurieren.
- Zudem sollte sichergestellt sein, dass nur die als sicher eingestufte TLS-Versionen 1.2 und 1.3 zum Einsatz kommen
- Im Optimalfall kommt zudem die auf DNSSEC basierende Authentifizierung DANE zum Einsatz, bei der ein Fingerabdruck des verwendeten Zertifikats in einem DNS-Eintrag vom Typ TLSA hinterlegt wird.

- ODER: Verwendung von KIM 

From:
https://www.gesunde-vernetzung.de/ - **DigHealthWiki**

Permanent link:
https://www.gesunde-vernetzung.de/doku.php?id=dighealth:div:sichereumgebung&rev=1665477439

Last update: **2022/10/11 08:37**