Киберсигурност в здравеопазването: рискове, регулации и практични решения
16.04.26

Програма:

1. Въведение
DHI Cluster

- Защо киберсигурността вече е критична за болниците

2. Регулаторна рамка и отговорности: Новият Закон за киберсигурност (NIS2)

(ББА)

- Какво променя новият закон за киберсигурност (NIS2) и как се прилага в България
- Отражението на промените върху лечебните заведения
- Основни задължения, докладване на инциденти, срокове
- Отговорност на ръководството
- Последици от неспазване на закона
- Какво предстои?

3. Как да постигнем NIS2 съответствие на практика
Mnemonica

- Модерни кибер рискове с здравеопазването
- Основни изисквания към лечебните заведения
- Практически roadmap към съответствие
- SOC as a Service като модел за изпълнение

3. Уязвимости и реални сценарии за пробив в болнична среда
SoCyber

- Кои системи в една болница могат да бъдат достъпни отвън
- Как медицинска техника, камери и софтуер могат да се окажат уязвими
- Как хакерите намират „входни точки“, без да влизат физически в болницата
- Рискове при отдалечен достъп (външни поддръжки, доставчици)
- Контрол на достъпа и проследимост
- Как се компрометират системите на практика
- Сигурен обмен на данни и дигитална идентичност

4. Криптин обмен на данни и как се случват тези процеси в болниците в Швейцария

Vereign

- Дигитална идентичност - ядрото на доверие
- Следващо поколение имейл комуникация
- Структуриран обмен на данни със семантична сигурност
- Децентрализирана мрежа от доверени точки

5. Q&A и дискусия