Infrastrutture critiche e sicurezza per la salute

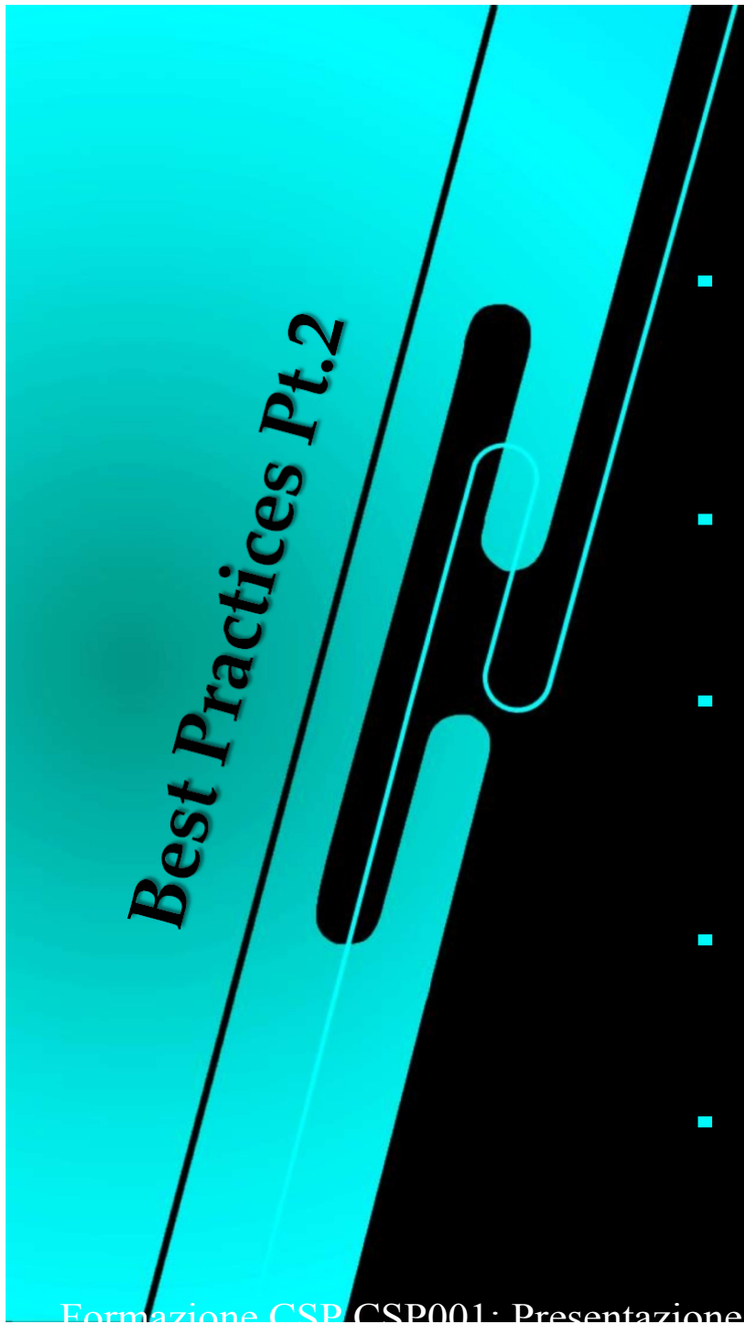
CSP008

PRESENTAZIONE DA PARTE DI: STYLIANOS KARAGIANNIS (PDMFC, PORTOGALLO)

Settore sanitario

Migliori pratiche Pt.1

- Crittografia dei dati: Crittografare i dati sensibili sia in transito che a riposo per impedire l'accesso non autorizzato, in particolare le cartelle cliniche dei pazienti e i dati di imaging medico.
- Controllo degli accessi: Implementare il controllo degli accessi basato sui ruoli (RBAC) per limitare l'accesso ai dati dei pazienti e ai sistemi sanitari in base ai ruoli e alle responsabilità degli utenti.
- Gestione delle patch: Mantenere i sistemi e i software aggiornati con le ultime patch di sicurezza per risolvere le vulnerabilità e proteggersi dalle minacce note.
- Segmentazione della rete: Segmentare le reti per isolare i sistemi e i dati sanitari sensibili da altre parti della rete, riducendo il rischio di movimento laterale da parte degli aggressori.
- Autenticazione forte: Implementare l'autenticazione a più fattori (MFA) per l'accesso ai sistemi e ai dati sensibili, per aggiungere un ulteriore livello di sicurezza oltre alle password.



Settore sanitario

Migliori pratiche Pt.2

- Piano di risposta agli incidenti: Sviluppare e testare regolarmente un piano di risposta agli incidenti per garantire una risposta tempestiva ed efficace agli incidenti di sicurezza, comprese le violazioni dei dati e gli attacchi ransomware.
- Audit e valutazioni regolari: Condurre regolarmente audit di sicurezza e valutazioni del rischio per identificare le vulnerabilità e le lacune nei controlli di sicurezza e adottare di conseguenza azioni correttive.
- Backup dei dati e disaster recovery: Mantenere backup regolari dei dati critici e stabilire solide procedure di disaster recovery per garantire la disponibilità dei dati e ridurre al minimo i tempi di inattività in caso di incidenti di sicurezza.
- Gestione del rischio dei fornitori: Valutare e monitorare la posizione di sicurezza dei fornitori terzi e dei fornitori di servizi che hanno accesso ai dati o ai sistemi sanitari.
- Sicurezza fisica: Implementare misure di sicurezza fisica per proteggere strutture sanitarie, server e altre infrastrutture da accessi non autorizzati o manomissioni.

Grazie

Presentatore: Stylianos Karagiannis (PDMFC, Portogallo)

Si prega di inviare tutte le domande a:
stylianos.karagiannis@pdmfc.com