Sviluppo di software sanitario sicuro

CSP009

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

Software Security and Health

Introduzione alla sicurezza del software per la sanità

Sicurezza e salute del software

In questo corso esploreremo gli aspetti critici della sicurezza del software sanitario, tra cui le vulnerabilità, i cyberattacchi e le strategie di mitigazione.

Asset critici nel settore sanitario

- Cartelle cliniche: Informazioni di identificazione personale (PII) e informazioni sanitarie protette (PHI) memorizzate nei sistemi di cartelle cliniche elettroniche (EHR).
- Dispositivi medici: Dispositivi connessi come pompe di infusione, pacemaker e macchine per la risonanza magnetica che sono vulnerabili ai cyberattacchi.
- Sistemi informativi ospedalieri (HIS): Sistemi centralizzati per che gestisce i dati dei pazienti, gli appuntamenti e la fatturazione, come Epic c Cerner.
- Sistema di archiviazione e comunicazione delle immagini (PACS): Archivia e recupera immagini mediche come radiografie e risonanze magnetiche, come il Centricity PACS di GE Healthcare.

Main Cyberattacks in Healthcare

Principali attacchi informatici nel settore sanitario

Ransomware, DoS, violazioni di dati, minacce interne

- Attacchi ransomware: Tra gli incidenti degni di nota vi è l'attacco WannaCry del 2017, che ha colpito gli ospedali dell'NHS, criptando i dati critici e chiedendo un riscatto per le chiavi di decrittazione.
- Violazioni dei dati: Nel 2015, Anthem Inc. ha subito una violazione che ha compromesso i dati di 78,8 milioni di persone, evidenziando la vulnerabilità dei dati dei pazienti.
- Attacchi DDoS: Ospedali come il Boston Children's Hospital hanno subito attacchi DDoS che hanno causato interruzioni del servizio e ritardi nell'assistenza ai pazienti.
- Minacce interne: Sono stati segnalati casi di dipendenti che hanno avuto accesso ai dati dei pazienti e li hanno venduti, sottolineando la necessità di controlli di accesso e di monitoraggio rigorosi.

Vulnerabilità dei sistemi operativi

Vulnerabilità ed esposizioni comuni (CVE)

- CVE-2020-0601: Una vulnerabilità critica che interessa il sistema operativo Windows e che consente agli aggressori di falsificare i certificati digitali e di aggirare i meccanismi di autenticazione.
- CVE-2019-17026: una vulnerabilità nel kernel Linux, che potenzialmente consente l'escalation dei privilegi o attacchi denial-of-service.
- CVE-2020-9832: Una vulnerabilità nel kernel di macOS, che consente l'accesso ad arbitrari
  esecuzione di codice con privilegi di sistema.
- Iniezione SQL: Nei sistemi sanitari sono state scoperte vulnerabilità come CVE-2017-8890, che consentono agli aggressori di eseguire query SQL arbitrarie e di ottenere accesso non autorizzato ai dati dei pazienti.
- Cross-Site Scripting (XSS): CVE-2020-12694 esponeva vulnerabilità nelle applicazioni sanitarie basate sul Web, consentendo agli aggressori di iniettare script dannosi e rubare informazioni sensibili.
- Esecuzione di codice remoto (RCE): CVE-2019-19781 riguardava Citrix ADC e Gateway, consentendo agli aggressori remoti di eseguire codice arbitrario e compromettere le reti sanitarie.

Grazie

Presentatore: Stylianos Karagiannis (PDMFC, Portogallo)

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