Ασφαλής ανάπτυξη λογισμικού για την υγειονομική περίθαλψη

CSP009

ΠΑΡΟΥΣΊΑΣΗ ΑΠΌ: ΣΤΥΛΙΑΝΟ ΚΑΡΑΓΙΑΝΝΗ (PDMFC, ΠΟΡΤΟΓΑΛΙΑ)

Software Security and Health

Εισαγωγή στην ασφάλεια λογισμικού για την υγεία

Ασφάλεια λογισμικού και Υγεία

Σε αυτό το μάθημα, θα εξερευνήσουμε κρίσιμες πτυχές της ασφάλειας του λογισμικού υγειονομικής περίθαλψης, συμπεριλαμβανομένων των ευπαθειών, των κυβερνοεπιθέσεων και των στρατηγικών μετριασμού.

Κρίσιμοι Πόροι στον τομέα της υγειονομικής περίθαλψης

- Αρχεία ασθενών: Προσωπικά αναγνωρίσιμες πληροφορίες (PII) και προστατευόμενες πληροφορίες υγείας (PHI) που είναι αποθηκευμένες σε συστήματα ηλεκτρονικών καταγραφών υγείας (EHR).
- Ιατρικές συσκευές: Συνδεδεμένες συσκευές όπως αντλίες έγχυσης, βηματοδότες και μηχανήματα μαγνητικής τομογραφίας που είναι ευάλωτες σε κυβερνοεπιθέσεις.
- Νοσοκομειακά συστήματα πληροφοριών (HIS): Κεντρικά συστήματα για διαχείριση δεδομένων ασθενών, ραντεβού και τιμολόγηση, όπως το Epic ή το Cerner.
- Σύστημα αρχειοθέτησης και επικοινωνίας εικόνων (PACS): Αποθηκεύει και ανακτά ιατρικές εικόνες, όπως ακτινογραφίες και μαγνητικές τομογραφίες, όπως το GE Healthcare Centricity PACS .

Main Cyberattacks in Healthcare

Κύριες επιθέσεις στον κυβερνοχώρο στην υγειονομική περίθαλψη

Ransomware, DoS, παραβιάσεις δεδομένων,εσωτερικές απειλές

- **Επιθέσεις Ransomware:** Η επίθεση WannaCry του 2017, η οποία έπληξε νοσοκομεία του NHS, κρυπτογράφησε κρίσιμα δεδομένα και απαίτησε λύτρα για τα κλειδιά αποκρυπτογράφησης.
- **Παραβιάσεις δεδομένων:** Το 2015, η εταιρεία Anthem Inc. , βίωσε μια διαρροή δεδομένων που εξέθεσε τις καταγραφές 78,8 εκατομμυρίων ατόμων, επισημαίνοντας την ευπάθεια των δεδομένων των ασθενών.
- **Επιθέσεις DDoS:** Νοσοκομεία όπως το Νοσοκομείο Παίδων της Βοστώνης έχουν αντιμετωπίσει επιθέσεις DDoS που οδήγησαν σε ανατρεπτικές διακοπές υπηρεσιών και καθυστερήσεις στη φροντίδα των ασθενών.
- **Απειλές εκ των έσω:**Υπάρχουν αναφορές για υπαλλήλους του προσωπικού που έχουν πρόσβαση και πωλούν δεδομένα ασθενών , υπογραμμίζοντας την ανάγκη για ισχυρούς ελέγχους πρόσβασης και παρακολούθηση.

Vulnerabilities

Ευπάθειες λειτουργικών συστημάτων

Κοινά σημεία ευπάθειας και εκθέσεις(CVE)

- CVE-2020-0601: Ευπάθεια που επηρεάζει το Windows OS (Operating System - λειτουργικό σύστημα) και επιτρέπει στους επιτιθέμενους να παραποιήσουν ψηφιακά πιστοποιητικά και να παρακάμψουν μηχανισμούς ταυτοποίησης χρήστη.
- CVE-2019-17026: Ευπάθεια στον πυρήνα του Linux (λειτουργικό σύστημα ανοιχτού κώδικα βασισμένο στο Unix), η οποία δυνητικά επιτρέπει την κλιμάκωση προνομίων ή επιθέσεις άρνησης παροχής υπηρεσιών.
- CVE-2020-9832: Ευπάθεια στον πυρήνα του macOS, που ενεργοποιεί την αυθαίρετη εκτελέσιμος κώδικας προγραμματισμού με προνόμια συστήματος.
- Έγχυση SQL: Ευπάθειες όπως η CVE-2017-8890 έχουν ανακαλυφθεί σε συστήματα υγειονομικής περίθαλψης, επιτρέποντας στους επιτιθέμενους να εκτελούν αυθαίρετα ερωτήματα SQL και να αποκτούν ανεξουσιοδότητη πρόσβαση σε δεδομένα ασθενών.
- Cross-Site Scripting (XSS): CVE-2020-12694 εξέθεσε ευπάθειες σε διαδικτυακές εφαρμογές υγειονομικής περίθαλψης, επιτρέποντας στους επιτιθέμενους να εισάγουν κακόβουλα κομμάτια κώδικα και να κλέβουν ευαίσθητες πληροφορίες.
- Απομακρυσμένη εκτέλεση κώδικα προγραμματισμού (RCE): Το CVE-2019-19781 επηρέαζε τα Citrix ADC και Gateway, επιτρέποντας σε απομακρυσμένους επιτιθέμενους να εκτελέσουν αυθαίρετο κώδικα προγραμματισμού και να θέσουν σε κίνδυνο δίκτυα υγειονομικής περίθαλψης.

Σας ευχαριστώ

Παρουσιαστής: Στυλιανός Καραγιάννης PDMFC, Πορτογαλία

Παρακαλούμε στείλτε όλες τις ερωτήσεις στη διεύθυνση:
stylianos.karagiannis@pdmfc.com