TECHNISCHE HOCHSCHULE BRANDENBURG & TECNOCAMPUS MATARO

VULNERABILITY ASSESSMENT
A NATIONAL BENCHMARK

IM RAHMEN DES PROJEKTS UNTERSUCHTEN WIR SICHERHEITSLÜCKEN IN INTERNETZUGÄNGLICHEN SYSTEMEN DEUTSCHER, SPANISCHER UND AUSGEWÄHLTER INTERNATIONALER KRANKENHÄUSER, UM RISIKEN FÜR SENSIBLE PATIENTENDATEN AUFZUDECKEN

TEILNEHMER

Dieses Projekt wurde unter der Aufsicht von Prof. Dr. Pilgermann von Willi Hübner, Paul Leipe, Leander Klan, Björn Eberwein und Aaron Standke mit freundlicher Unterstützung von Benedikt Michaelis durchgeführt.

PARTNERSCHAFT

Die Zusammenarbeit zwischen der Technischen Hochschule Brandenburg und TecnoCampus Mataró vereinte interdisziplinäre Teams aus Deutschland und Spanien, die im Rahmen eines einwöchigen Hackathons die Cybersicherheit in Krankenhäusern untersuchten.

UNTERSTÜTZUNG

ELI-INKUBATOR

DIESES PROJEKT WURDE IM RAHMEN DES ELI-INKUBATORS DER TECHNISCHEN HOCHSCHULE BRANDENBURG (THB) DURCHGEFÜHRT.

DER ELI-INKUBATOR WIRD VOM DEUTSCHEN AKADEMISCHEN AUSTAUSCHDIENST (DAAD) IM PROGRAMM HAW.INTERNATIONAL GEFÖRDERT. ZIEL DES ELI-INKUBATORS IST ES, DIE INTERNATIONALISIERUNG DES CURRICULUMS DURCH ENGLISCHSPRACHIGE LEHRANGEBOTE, INTERNATIONALE KOOPERATIONEN UND DIGITALE PROZESSE NACHHALTIG ZU STÄRKEN. DANK DER UNTERSTÜTZUNG KONNTEN INNOVATIVE LEHRFORMATE, WIE DER EINWÖCHIGE HACKATHON IN MATARÓ, REALISIERT WERDEN.

BETREUUNG DURCH SEBASTIÁN LÓPEZ CASTELLANOS

EIN BESONDERER DANK GILT HERR LÓPEZ, DER UNS IMMER ALS ANSPRECHPARTNER ZUR VERFÜGUNG STAND UND EINEN WESENTLICHEN TEIL ZUR UMSETZUNG BEIGETRAGEN HAT.

ZIEL

Ziel des Projekts war es, Sicherheitslücken in internetzugänglichen Systemen deutscher, sowie spanischer und weiterer Krankenhäuser zu identifizieren.

METHODIK

Das Projekt basierte auf einer Kombination aus OSINT-Analysen (Open Source Intelligence) und der Nutzung spezialisierter Tools zur Sicherheitsbewertung. Mithilfe von Plattformen wie Censys und Shodan wurden systematisch IP-Adressen und Domains analysiert, die das DICOM-Protokoll nutzten. Python-Skripte ermöglichten die automatisierte Extraktion und Verknüpfung von Daten, insbesondere in Verbindung mit Informationen aus dem Bundesklinik-Atlas. Ergänzend dazu fand ein interdisziplinärer Hackathon statt, bei dem in internationalen Teams Ideen und Skripte zur besseren Untersuchung der Zielsysteme entwickelt wurden.
Durch diese Vorgehensweise war es wichtig sich effizient in internationalem Umfeld zu koordinieren.

ERGEBNISSE/ERKENNTNISSE

Das Projekt identifizierte einige ungesicherte DICOM-Server, die sensible Daten wie Patientennamen, Geburtsdaten und Untersuchungsdetails potenziell zugänglich machten. Mithilfe systematischer Analysen und eigens entwickelter Skripte wurden Schwachstellen automatisiert aufgespürt. Die Skripte ermöglichten eine effiziente Erfassung und Kategorisierung der identifizierten Sicherheitslücken, ohne dabei aktiv in die Sicherheitssysteme einzugreifen. Durch die kurze Dauer des Projektes hält sich die Menge der Ergebnisse jedoch in Grenzen.

FAZIT

Das Projekt hat wertvolle Erkenntnisse über potenzielle Schwachstellen in internetzugänglichen Systemen geliefert. Die durchgeführten Analysen und entwickelten Skripte ermöglichen eine effiziente Identifikation solcher Schwachstellen und bieten eine fundierte Grundlage für weitere Untersuchungen. Die Ergebnisse verdeutlichen die Bedeutung einer systematischen Überprüfung und Sensibilisierung im Bereich der Cybersicherheit.
Die internationale Zusammenarbeit mit TecnoCampus Mataró war ein zentraler Bestandteil des Projekts und förderte den Austausch von Perspektiven und Methoden. Durch die interkulturelle Teamarbeit konnten verschiedene Herangehensweisen kombiniert und innovative Ansätze zur Problemlösung entwickelt werden. Die Kooperation bot den Teilnehmenden nicht nur fachlichen Mehrwert, sondern stärkte auch ihre interkulturellen und sprachlichen Kompetenzen.

All Photos by Benedikt Michaelis/ Brandenburg University of Applied Sciences