Academia Navală „Mircea cel Bătrân”

Facultatea de Navigație și Management Naval

LUCRARE DE LICENŢĂ

Coordonator ştiinţific:

Conf.univ.Dr. Băutu Andrei

Absolvent: Antohi Andi-Ionel

Constanţa

-2024-

Academia Navală „Mircea cel Bătrân”

Facultatea de Navigație și Management Naval

Specializarea: Navigație și Transport Maritim și Fluvial

LUCRARE DE LICENŢĂ

Soluție software pentru instruirea angajaților privind securitatea cibernetică pe nave comerciale

Coordonator ştiinţific:

Conf.univ.Dr. Băutu Andrei

Absolvent: Antohi Andi-Ionel

Constanţa

-2024-

Rezumat

Această lucrare propune dezvoltarea unei aplicații informatice folosind limbajul de programare Java, cu ajutorul librăriei Swing. Ea este bogată în resurse, oferind un set extins de componente pentru crearea interfețelor, cu exemple în diverse cărți de programare și platforme de pe internet, precum și în documentația oficială. Aplicația are rolul de a instrui angajații în privința securității cibernetice pe navele comerciale. Scopul principal al proiectului este de a ajuta navigatorii să identifice pericolele la care sunt expuși, atât ei, cât și navele pe care se află, în fața celor mai moderne și complexe metode de atac în domeniul securității cibernetice. Interfața aplicației este complexă din punct de vedere al realizării, dar este proiectată pentru a fi cât mai simplă și accesibilă pentru utilizatorii ei.

Aplicația poate rula pe orice sistem de operare pentru că limbajul Java este cunoscut ca fiind și multiplatformă. Un alt avantaj major al aplicației dezvoltate este că ea e una de tip independentă. Acest lucru înseamnă că nu necesită descărcarea și instalarea altor programe și nu rulează pe platforme web, așa cum se întâmplă în cazul multor programe de pe piață, ci rulează exclusiv în cadrul sistemului de operare. De asemenea, aplicația construită nu necesită o conexiune la internet.

Aplicația abordează punctele esențiale despre atacurile cu viruși și permite utilizatorilor să salveze chiar și anumite noțiuni teoretice în cazul în care consideră că o anumită secțiune reprezintă o informație esențială pentru ei, sub forma unor fișiere cu extensie txt pentru a fi recunoscute de orice sistem de operare sau cu extensia anmb care este recunoscută doar de către programul în cauză. În plus, el are și capacitatea de a afișa texte de mărimi foarte mari.

Pentru realizarea proiectului și a programului, au fost studiate cărți de securitate cibernetică, regulamente, paginile oficiale ale universităților, organizațiilor și firmelor private de pe piață care sunt dispuse să familiarizeze navigatorii cu securitatea cibernetică, precum și forumuri și platforme de angajare, unde specialiștii evidențiază cele mai noi tehnologii, cu scopul de a contribui la formularea unor argumente solide în cadrul aplicației dezvoltate.

Abstract

This thesis proposes the development of a software application using the Java programming language, with the help of the Swing library. It is resource-rich, offering an extensive set of components for creating interfaces, with examples found in various programming books and online platforms, as well as in the official documentation. The application aims to train employees on cybersecurity for commercial ships. The main goal of the project is to help navigators identify the dangers they face, as well as those faced by the ships they are on, against the most modern and complex methods of attack in the field of cybersecurity. The application's interface is complex in terms of its implementation but is designed to be as simple and accessible as possible for its users.

The application can run on any operating system because Java is known for being platform-independent. Another major advantage of the developed application is that it is standalone. This means that it does not require the downloading and installation of additional programs and does not run on web platforms, as is the case with many programs on the market, but runs exclusively within the operating system. Additionally, the built application does not require an internet connection.

The application addresses key points about virus attacks and allows users to save even certain theoretical concepts if they consider a particular section to be essential information for them, in the form of txt files which are recognized by any operating system, or with the extension anmb, which is recognized only by the specific program. Additionally, it has the capability to display very large text sizes.

For the development of the project and the program, cybersecurity books, regulations, official pages of universities, organizations, and private companies on the market that are willing to familiarize navigators with cybersecurity were studied. Additionally, forums and job platforms were reviewed, where experts highlight the latest technologies, with the aim of contributing to the formulation of solid arguments within the developed application.

Cuprins

1.1. Contextul lucrării

Navigația se bazează pe transportul mărfurilor, care pot avea diverse forme, de la solide la lichide sau gazoase și reprezintă una dintre cele mai eficiente modalități de transport al persoanelor, având în vedere capacitatea acestora, în comparație cu alte mijloace de transport, precum cel terestru sau aerian. În acest context, industria maritimă joacă un rol esențial în asigurarea funcționării optime a economiilor moderne.

În prezent, securitatea cibernetică devine tot mai importantă, pe măsură ce atacurile digitale se răspândesc rapid și pirateria capătă forme noi, de natură electronică. Datorită acestor evoluții, securitatea cibernetică a ajuns să fie un domeniu esențial în sectorul maritim. În fața atacurilor tot mai sofisticate, măsurile de protecție cibernetică evoluează constant, în încercarea de a menține buna funcționare a echipamentelor navale și de a sprijini echipajul în îndeplinirea voiajelor.

Pericolul la care sunt expuse navele, echipajele și mărfurile lor este direct proporțional cu progresul tehnologic, în special în contextul dezvoltării accelerate a tehnologiilor informatice. Inovațiile din domeniul tehnologiilor digitale, cum ar fi inteligența artificială, au provocat schimbări radicale în diverse sectoare.

În primul rând, știința datelor se concentrează pe realizarea diverselor rapoarte și statistici, utilizând ca sursă orice tip de informație care poate fi reprezentată. Aceasta include aspecte precum numărul de apăsări ale butoanelor, energia și combustibilul consumate, parametrii echipamentelor de navigație, activitatea echipajului și durata voiajelor.

Învățarea automată realizează predicțiile, controlează și extinde aria de memorare a datelor, formând astfel creierul inteligenței artificiale.

Stocarea datelor se realizează în sisteme cloud, cu ajutorul sectorului specializat denumit partea de server. Acesta se ocupă cu manipularea și stocarea informațiilor primite de la orice dispozitiv electronic capabil să transfere date, cum ar fi parametrii echipamentelor de pe navă.

Aplicația propriu-zisă, cunoscută sub denumirea de parte de client, reprezintă interfața pe care o folosesc echipajele navelor comerciale. Aceasta include instrumente precum radarul, VHF-ul și ECDIS-ul.

Toate acestea se regăsesc chiar la bordul navelor, realizându-se automat prin intermediul unor programe și script-uri în termenii profesioniștilor care activează în domeniul informatic. Așadar, bordul navelor poate fi predispuns atacurilor cibernetice.

În transportul maritim, securitatea cibernetică asigură buna funcționare a sistemelor și echipamentelor întâlnite la bordul navelor, îndeplinirea contractelor și a voiajelor prin asigurarea siguranței digitale în permanență, împiedicarea scurgerilor de informații despre personalul navei sau în cele mai negre scenarii furtul de identitate, datele despre firma de care aparține nava și marfa conținută pe timpul voiajului astfel încât să fie îndeplinite angajamentele contractuale stabilite înainte de începerea voiajului în cauză. În plus, aceasta împiedică libera circulație a unei game variate de viruși care, fie se concentrează pe partea digitală a navei, fie pe partea de componente fizice.

1.2. Scopul aplicației

Obiectivul aplicației este să vină în sprijinul navigatorilor, ajutându-i să înțeleagă terminologia folosită în securitatea cibernetică și să le explice în detaliu gama largă de viruși și atacuri existente în prezent, care pot pune în pericol atât dispozitivele lor, cât și sistemele de la bordul navei. Prin intermediul acestei aplicații, ei vor învăța, de asemenea, despre metodele de apărare împotriva acestor amenințări.

1.3. Problemele întâmpinate pe parcursul realizării proiectului

Realizarea interfeței a fost o adevărată provocare deoarece a fost necesar să se ia în considerare mai multe aspecte. A fost esențial să se asigure că aplicația este accesibilă pentru utilizatorii care nu sunt familiarizați cu aplicații avansate și să se evite problemele legate de compatibilitate, cum ar fi posibilitatea ca aplicația să nu ruleze corect pe laptopurile angajaților din cauza sistemului de operare. Pentru a evita aceste probleme, s-a decis utilizarea limbajului de programare Java, care este multiplatformă, împreună cu vechea sa librărie Swing, pentru a construi o aplicație ușor de înțeles, prin intermediul mai multor componente cu performanță ridicată. În plus, aplicația a fost proiectată pentru a nu necesita componente fizice avansate și pentru a nu depinde de o conexiune la internet, având în vedere că utilizatorii ar putea fi pe mare. De asemenea, ea a fost realizată pentru a fi compatibilă cu diferite sisteme de operare și pentru a suporta redimensionarea ferestrelor.

Un aspect esențial care a necesitat atenție a fost modul de explicare a noțiunilor legate de atacuri și viruși pentru persoanele complet nefamiliarizate cu informatica și cu terminologia securității cibernetice. În acest context, s-a decis dezvoltarea aplicației folosind meniuri interactive și adaptabile, capabile să afișeze texte de dimensiuni mari. Această metoda a permis oferirea unor explicații detaliate referitoare la riscurile asociate cu virușii și atacurile informatice, precum și prezentarea celor mai eficiente metode de apărare împotriva acestora.

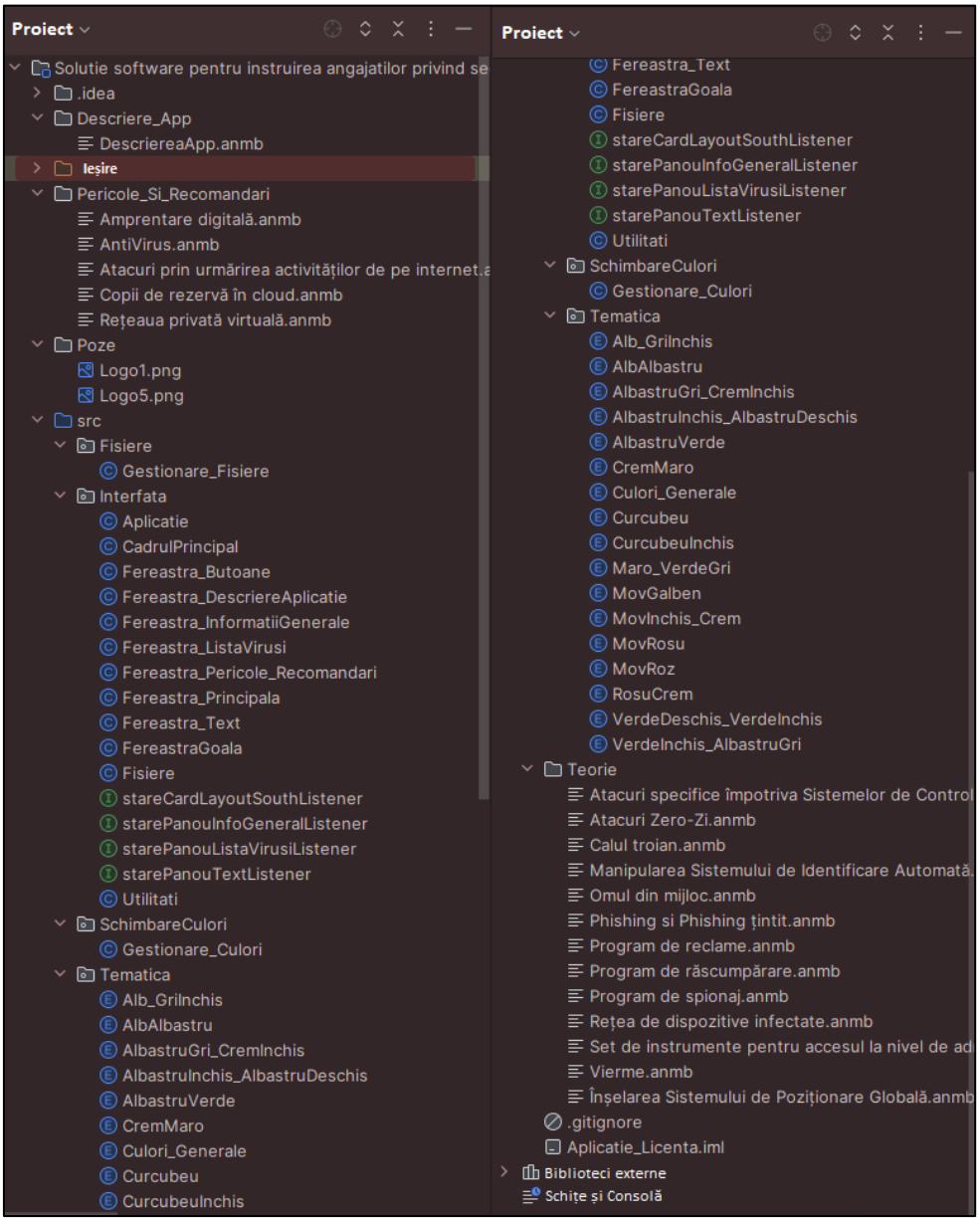

Figura 1.1 În cadrul capturii de ecran, este prezentat directorul proiectului realizat în IntelliJ. Acesta conține mai multe pachete și alte directoare la rândul său, fiecare având un scop precis în cadrul programului. Sursă: [16]

A fost luată în considerare și posibilitatea ca unele persoane să dorească să adauge explicații suplimentare pentru a reține mai ușor anumite noțiuni teoretice. Aceasta a generat, la rândul ei, o altă provocare: crearea unui meniu care să comunice eficient cu dispozitivul pe care rulează aplicația. Astfel, în zona centrală a aplicației a fost construit un meniu dotat cu mai multe butoane și metode de scriere, respectiv de citire implementate la nivelul codului, care permit utilizatorilor să salveze datele din aplicație și să deschidă fișiere cu extensii txt sau anmb din orice locație a memoriei dispozitivului pe care îl utilizează.

Pe partea de programare, a fost utilizat mediul integrat de dezvoltare IntelliJ, recunoscut pentru performanța sa și resursele pe care le pune la dispoziția programatorilor. Codul a fost împărțit în pachete, în funcție de utilitatea acestora. Astfel, un pachet este responsabil pentru citirea și scrierea fișierelor, altul pentru definirea stilurilor, iar altul pentru aplicația în sine, care se deschide atunci când un utilizator dorește să o utilizeze.

2.1. Regulamente

Ca și regulamente active, există actualizarea din 2017 a rezoluției cu numărul 428, publicată de Comitetul pentru Securitate Maritimă, care cere tuturor administrațiilor navale să ia în considerare pericolele cibernetice în cadrul tuturor sistemelor de siguranță ale navelor pe care le dețin, nu mai târziu de 01.2021.

Încă un lucru important este că IMO a mai făcut public un ghid tot în 2017, în care sunt menționate mai multe sfaturi pentru amenințările de la nivelul securității informaționale și operaționale din domeniul maritim. Ele au fost publicate în contextul unor breșe de securitate majore la momentul respectiv.

În acest mod, Codul Internațional de Management al Siguranței (ISM) include atât securitatea informațională și operațională, cât și pericolele generate de ele în cadrul siguranței unei navei. Ea pune accentul pe descoperirea pericolelor, asigurarea funcționării în parametrii normali a sistemelor de navigație, identificarea breșelor de securitate sau pregătirea riguroasă pentru posibilele atacuri și metodele aplicate conform planului stabilit pentru a face față acestora și pentru a combate pierderea datelor, care este cel mai negru scenariu în securitatea cibernetică.

Recomandările și extinderea secțiunilor, cum ar fi cele referitoare la siguranța navelor, au fost luate în serios tocmai în urma unor rapoarte care au stârnit îngrijorare printre experți din cauza vulnerabilității navelor moderne la posibile atacuri cibernetice cu efecte devastatoare. Conform unui studiu realizat în 2020, aproape două treimi dintre companiile de navigație ar fi avut capacitatea de a răspunde adecvat în cazul unui atac cibernetic, însă nu mai puțin de jumătate dintre ele au recunoscut că nu aveau planuri și strategii concrete de apărare, nici măcar măsuri pentru asigurarea copiilor de siguranță ale datelor stocate. În plus, multe dintre aceste companii au recunoscut că angajații lor nu erau suficient de pregătiți pentru asemenea incidente. Mai îngrijorător este faptul că studiul a arătat că mai puțin de jumătate dintre nave nu erau pregătite să facă față provocărilor legate de tehnologia operațională (OT).

2.2. Tehnologia operațională (OT)

Tehnologia operațională se bazează pe Internetul Lucrurilor (IoT), care îmbină partea informatică cu cea fizică a dispozitivelor. Acestea sunt realizate de persoane specializate atât în informatică, cât și în inginerie.

Riscul generat de asemenea neglijențe este uriaș, întrucât tehnologia operațională (OT) se concentrează pe aspectele fizice ale dispozitivelor de navigație. Aceasta este specifică industriei și infrastructurii hardware de la bordul navelor. În contextul securității cibernetice, scopul principal al tehnologiei operaționale este de a proteja corespunzător senzorii, dispozitivele de control și de monitorizare a traficului maritim. De asemenea, protejarea căilor de comunicație (partea de transmitere a semnalelor) este extrem de importantă.

Cel mai frecvent tip de atac împotriva tehnologiei operaționale este programul de răscumpărare, un tip de program malițios care împiedică accesul persoanelor autorizate la sistemele specifice ale unei nave, făcând-o să nu mai poată fi controlată. În astfel de incidente, atacatorii cer recompense pentru a permite echipajului să recâștige controlul asupra navei. Ea reprezintă o formă modernă de piraterie, una digitală, care prezintă și ea riscuri majore pentru echipajul navei. Trebuie luată în calcul și situația în care o persoană neautorizată ar accesa toate meniurile navei fără a avea experiență cu acestea. De exemplu, dacă pompele tancului petrolier sunt blocate, metodele de comunicație sunt întrerupte sau, mai grav, dacă nava ajunge într-o stare critică și nu mai poate fi controlată. Într-un asemenea caz, aceasta poate bloca circulația liberă a navelor într-un canal îngust sau într-o zonă cu trafic maritim aglomerat.

Riscurile sunt extrem de mari atunci când se iau în considerare navele tanc, precum cele pentru Gaz Natural Lichefiat (LNG) și Gaz Petrolier Lichefiat (LPG), unde marfa trebuie monitorizată cu atenție.

2.3. Organizații

2.3.1. Registrul Naval Indian

Registrele navale ajută membrii echipajelor să acumuleze informațiile necesare despre securitatea cibernetică. Printre acestea se numără și Registrul Naval Indian, care oferă un curs de auditor în securitate cibernetică pe o perioadă de o zi. Prin intermediul acestuia, participanții vor avea parte de o introducere în securitatea informațională și în rolul lor de a proteja datele. Ulterior, vor învăța cum să evalueze riscurile și vor fi familiarizați cu reglementările din domeniu. La final, cursanții vor învăța tehnici de audit și cum să realizeze un raport. Acest curs este benefic pentru cei care doresc să se familiarizeze cu codurile ISM dedicate securității cibernetice. Prețul cursului este de aproximativ două sute de dolari și se desfășoară într-o ședință online.

2.3.2. Registrul Coreean (KR)

Un alt registru este cel din Coreea de Sud (KR), unde sunt disponibile nu mai puțin de trei tipuri de instruire pentru același curs dedicat conștientizării securității informaționale. Printre acestea se numără: cursul de dezvoltare a aptitudinilor, cursul personalizat și programul de instruire al academiei din cadrul Registrului Coreean.

Cursul de dezvoltare a aptitudinilor este complet gratuit și disponibil exclusiv personalului firmelor cu care acest registru are anumite acorduri. Ca și obiective principale sunt prezentarea noțiunilor ce țin de practica securității cibernetice și care se referă la înțelegerea acesteia. Practic, cursul se concentrează pe introducerea în securitatea cibernetică, ceea ce implică prezentarea rolurilor, terminologiei și tipurilor de atacuri.

Proiectul de instruire al academiei din cadrul Registrului Coreean implică un anumit preț, dar accesul doritorilor nu este limitat în vreun fel anume. Subiectele abordate includ noțiuni de bază pentru introducere, urmate de metode de protecție specifice, cum ar fi criptarea. După aceea, sunt discutate modalitățile de concepere a planurilor de apărare împotriva atacurilor, cum pot fi acestea detectate și sunt oferite exemple practice pentru a aprofunda cât mai mult partea teoretică predată.

Al treilea tip de instruire reprezintă o combinație între primele două cursuri la nivelul subiectelor abordate. Pentru a se înscrie la oricare dintre aceste cursuri, persoanele interesate trebuie să trimită un e-mail individual către firmă.

2.3.3. Institutul Nautic și HudsonCyber

La ora actuală, există pe piață și un curs de nu mai mult de trei ore sub formă de tutorial, care conține mai multe videoclipuri în cadrul său, exact ca la un playlist de pe YouTube. Persoanele înscrise sunt obligate să parcurgă absolut toate materialele de curs pentru a fi pregătite și pentru a le fi permis să susțină testul pentru obținerea certificatului. Cursul care costă șaptezeci de lire are și ca obiectiv să crească gradul de conștientizare a securității cibernetice pentru toți marinarii și este realizat de către cei de la Institutul Nautic în strânsă colaborare cu HudsonCyber, având acreditare de la Organizația Maritimă Internațională.

Subiectele abordate includ importanța și utilizarea securității cibernetice în contextul cererii mari de pe piață și a pericolelor existente care devin pe zi ce trece din ce în ce mai complexe, mai automate, dar mai ales ale căror efecte devin și mai devastatoare pentru victimele atacurilor. Cursul acoperă și practicile specifice și scenariile din securitatea cibernetică, care se aplică și în zona maritimă, factorii umani care de cele mai multe ori sunt responsabili pentru breșele din sistem, riscurile asociate fiecărui tip de virus și cum trebuie monitorizate dispozitivele și rețelele.

2.4. Universități

La ora actuală, universitățile sunt cele care oferă cel mai mare grad de încredere în formarea cursanților pentru securitate cibernetică. Ele dispun de cursuri de specializare sau de programe de studii, prin care o persoană din domeniul maritim poate dobândi cunoștințele și experiența necesară pentru a satisface cererea de pe piață. Cele mai recunoscute universități în acest moment sunt Solent din Southampton și universitatea Plymouth, academiile maritime din Estonia și Norvegia, dar si registrul Lloyd.

2.4.1. Plymouth, UK

Această universitate din Plymouth, Anglia, deține un laborator dedicat exclusiv securității cibernetice pentru nave. Ideea proiectului a fost anunțată pentru prima dată pe platforma LinkedIn în

anul 2019. Proiectul a fost conceput cu ajutorul centrului de securitate al universității și are ca scop pregătirea cursanților pentru evaluarea riscurilor, politicii și a auditului în domeniul securității cibernetice.

Acest proiect este planificat pe o perioadă de trei ani, iar universitatea din Plymouth este dispusă să ofere burse de până la nouăsprezece mii de lire pe an pentru studenții considerați eligibili. Persoanele interesate care doresc să afle mai multe informații despre taxele de școlarizare internaționale sau despre programa proiectului trebuie să ia legătura cu Dr. Rory Hopcraft, unul dintre inițiatorii acestui laborator de înaltă performanță. Pentru un proiect de asemenea nivel și pentru performanța sa, persoanele care doresc să se înscrie au nevoie de o diplomă de licență cu primele două distincții sau chiar de o diplomă de masterat.

Universitatea din Plymouth oferă, de asemenea, un curs intensiv de conștientizare a securității cibernetice, destinat angajaților navelor comerciale care nu au cunoștințe anterioare în domeniul IT și doresc să se familiarizeze cu acesta. Cursul costă aproximativ două sute cincizeci de lire și se desfășoară într-o clădire a campusului. Pentru informații suplimentare sau nelămuriri, persoanele interesate pot contacta universitatea prin e-mail sau pot vizita magazinul lor online.

2.4.2. Universitatea maritimă din Estonia

Printre universitățile care se oferă să ajute atât navigatorii, cât și informaticienii ca să dobândească noțiunile necesare în acest domeniu se numără și universitatea marină din Estonia, care organizează școli de vară. Scopul acestora este de a le explica participanților riscurile securității cibernetice, precum și comunicațiile și diferite instrumente din domeniul maritim.

Această academie maritimă mai oferă un curs predat în două limbi: engleză și estonă. Obiectivul său este de a asigura fundamentele securității informației și evaluarea riscurilor asociate. Absolvenții vor fi capabili să mențină securitatea sistemelor și să gestioneze procedurile de siguranță digitală astfel încât să fie adecvate. Acest lucru include protejarea datelor sensibile de accesul ilegal, furtul de identitate, accesul neautorizat și divulgarea informațiilor private. Cursul se desfășoară pe o perioadă de un semestru și este susținut pe platforma Moodle, frecvent utilizată în universități.

2.5. Rolurile din securitatea cibernetică

Organizațiile și universitățile oferă cursuri introductive în securitatea cibernetică, în cadrul cărora sunt prezentate și rolurile din domeniu și oportunitățile de carieră disponibile. Printre cele mai cunoscute cariere se numără: auditorul IT care se ocupă cu evaluarea amenințărilor și realizarea rapoartelor și în care absolvenții pot activa după finalizarea cursurilor, specialistul în securitate cloud asigură securizarea rețelelor la nivelul cloud-ului, criptarea datelor și administrarea accesului, specialistul în testele de penetrare a sistemelor care realizează simulări pentru a evalua capacitatea aplicațiilor sau a rețelelor de a rezista în fața unor atacuri reale, analistul în centrul de operațiuni de securitate monitorizează sistemele, detectează atacurile și răspunde la acestea, specialiștii în breșele de securitate caută și remediază vulnerabilitățile și investigatorii în criminalistica digitală care adună probe în cadrul anchetelor legale.

2.6. Instrumentele informatice

În cadrul programelor universitare de cel puțin un semestru, vor fi prezentate pe larg și instrumentele de care cursanții se pot folosi pentru a asigura o protecție corespunzătoare a sistemelor cibernetice și pentru a concepe rapoarte cât mai detaliate, prezentând stadiul actual al acestora. Așadar, ei vor învăța o materie de bază care se numește rețelistică, care include tot ce ține de partea legată de internet, de rețea și de modul în care sunt transmise datele.

Acestea fiind spuse, ei vor avea ocazia să se familiarizeze cu unelte precum: Nmap, Wireshark, Cisco Packet Tracer și sisteme de operare Kali Linux sau Parrot OS.

2.6.1. Kali Linux și sistemul de operare Parrot

În primul rând, Kali Linux și Parrot sunt sisteme de operare des folosite în securitatea cibernetică întrucât au capacitatea de a asigura anonimitatea în mediul online și oferă o gamă largă de programe specifice. Ele sunt recunoscute și pentru faptul că facilitează securitatea cibernetică prin testele de penetrare a sistemelor informatice și scanări de rețea, audit IT, dar și criminalistica digitală pentru a analiza și a strânge probe legate de atacurile cibernetice.

2.6.2. Cisco Packet Tracer

Cisco Packet Tracer este folosit pentru a crea simulări de rețea și pentru a monitoriza funcționarea acesteia. Programul reprezintă un instrument extrem de util pentru conceperea și testarea rețelelor.

2.6.3. Wireshark

Wireshark este o aplicație informatică concepută pentru a monitoriza traficul de date din cadrul unei rețele și constituie un instrument esențial pentru cei care studiază securitatea cibernetică în cadrul universităților. Prin intermediul său, pot fi interceptate pachetele de date, inclusiv IP-urile care transmit cereri sau informații cu scopul de a obține informații în mod ilegal sau de a trimite pachete ce pot conține viruși.

2.6.4. Nmap

Pe baza Nmap-ului se pot efectua scanări de rețea, într-un mod activ pentru a obține informații concrete despre stadiul rețelei, arhitectura sa, porturile sale, dispozitivele conectate și mai ales despre serviciile pe care sistemul respectiv le folosește.

2.7. Firme private

2.7.1. Rina

Pe piața actuală se află o firmă privată care oferă cursuri în materie de securitate cibernetică și dispune de două moduri de predare: la distanță, pe internet și fizic în Grecia. Cursul susținut pe internet costă aproximativ trei sute de euro, iar cel fizic costă trei sute treizeci de euro. Durata fiecărui curs este de o zi. Subiectele abordate includ introducerea în securitatea cibernetică și identificarea amenințărilor, urmate de strategii de apărare împotriva atacurilor ce implică tehnologia informațională și cea operațională. Printre ele se numără metodele de phishing, programele malițioase, atacurile asupra echipamentelor fizice și activitățile suspecte. De altfel, în cadrul său vor fi predate și metodele de răspuns, cum ar fi: zidurile de rețea, antivirusurile care au sisteme de detecție a programelor malițioase, programelor de spionaj, a celor de urmărire, copiile de rezervă și protejarea parolelor.

Cursul este dedicat oricărei persoane din domeniul naval care dorește să învețe despre aceste atacuri și cum să fie capabilă să se protejeze în fața acestor amenințări.

2.8. Concluziile capitolului

În general, registrele navale oferă cursuri de specializare pentru angajații din domeniul maritim pe perioade scurte, de la câteva ore până la câteva zile. Obiectivul principal al acestor cursuri este să ofere o introducere adecvată în securitatea cibernetică. Astfel, participanții vor învăța despre conceptul de securitate cibernetică, ramurile acesteia și diferențele între ele. De asemenea, vor descoperi terminologia specifică, tipurile de atacuri și modul de răspuns la acestea. Spre finalul cursurilor, vor învăța cum să redacteze rapoarte și vor avea ocazia să lucreze cu exemple practice.

În schimb, universitățile oferă de obicei două opțiuni pentru doritori: cursuri intensive de instruire, care se desfășoară pe perioade foarte scurte, sau cursuri care au o durată de cel puțin un semestru. În cadrul acestora, pe lângă noțiunile de bază predate și în cursurile oferite de registrele navale, vor fi abordate în detaliu politicile, instrumentele informatice și strategiile de apărare. De asemenea, cursurile universitare îi vor ajuta pe participanți să elaboreze rapoarte foarte detaliate.

Chiar dacă domeniul maritim dispune de mai multe organizații și universități care oferă pregătiri clasice cu ajutorul unor profesori pe parte de securitate cibernetică, mai sunt și firme care au conceput doar aplicații într-un fel în care să-și poată ajuta cursanții ca să acumuleze noțiunile necesare oricând sunt dispuși să aloce timp aprofundării subiectului în cauză și de la distanță. Au fost folosite noțiuni avansate de inginerie informatică, inteligență artificială și învățare automată pentru a obține asemenea produse informatice de calitate înaltă și care să le ofere persoanelor care au achiziționat acest tip de curs un suport în permanență, chiar dacă sunt la distanță. Ele mai poartă și denumirea de instruire asistată de calculator, fiind cunoscute sub prescurtarea de IAC.

3.1. Virsec

3.1.1. Curs de conștientizare a securității cibernetice

Virsec este firma care oferă un program de conștientizare a securității cibernetice pentru marinari la un nivel avansat. Cu ajutorul dezvoltărilor impresionante în învățarea de pe internet, persoanele au acum șansa de a accesa, prin intermediul platformei firmei, cursuri și subiecte care includ terminologia din domeniul securității informatice. Tot ce este necesar este ca utilizatorul să aibă aplicația achiziționată și o conexiune la internet pentru a intra pe platformă. Această aplicație web vine cu un stil de predare inspirat din zona YouTube-ului și a jocurilor video, sub formă de tutoriale și permite revederea acestora. Ca orice platformă de învățare, aplicația include teste care trebuie susținute de cursanți pentru a obține un certificat. Prețul său este de optzeci și cinci de lire și include și costul transportului pentru certificat.

Printre primele subiecte abordate în cadrul aplicației se numără prezentarea detaliată a tipurilor de atacuri, cu exemple concrete din ziua de azi, precum și noțiuni despre igiena în securitatea cibernetică, metode de apărare pentru a evita atacurile și pentru a reduce riscurile provocate de acestea. Astfel, cursantul va învăța că nu trebuie să-și expună adresa IP reală pe internet și prin urmare, va trebui să folosească o rețea privată virtuală. De asemenea, va învăța că rețeaua trebuie să fie mereu protejată, fiind recomandat să efectueze scanări la nivel de rețea cu un antivirus care dispune de diferite sisteme de detectare incorporate și utilizarea unui zid de rețea pentru a filtra informațiile primite sau trimise de dispozitivele sale. În plus, nu ar trebui niciodată să-și lase expusă adresa de e-mail reală, ci ar trebui să folosească o adresă de e-mail mascată.

Ulterior, accentul se pune pe identificarea precisă a atacurilor în curs și pe măsurile adecvate care trebuie luate în aceste cazuri. Un aspect cheie este modul în care a fost dezvoltat un plan pentru asigurarea securității, precum și evaluarea riscurilor curente și a pagubelor cauzate de atacuri. Așadar, cursantul ar trebui să învețe în cadrul cursurilor că datele trebuie copiate și depozitate fie într-o altă bază de date de pe alt disc de stocare, fie pe alt calculator sau chiar într-un sistem cloud deoarece beneficiază de protecție suplimentară.

Printre ultimele subiecte predate în cadrul aplicației web se numără prezentarea detaliată a rolurilor, responsabilităților și proceselor corecte care facilitează o apărare cibernetică solidă.

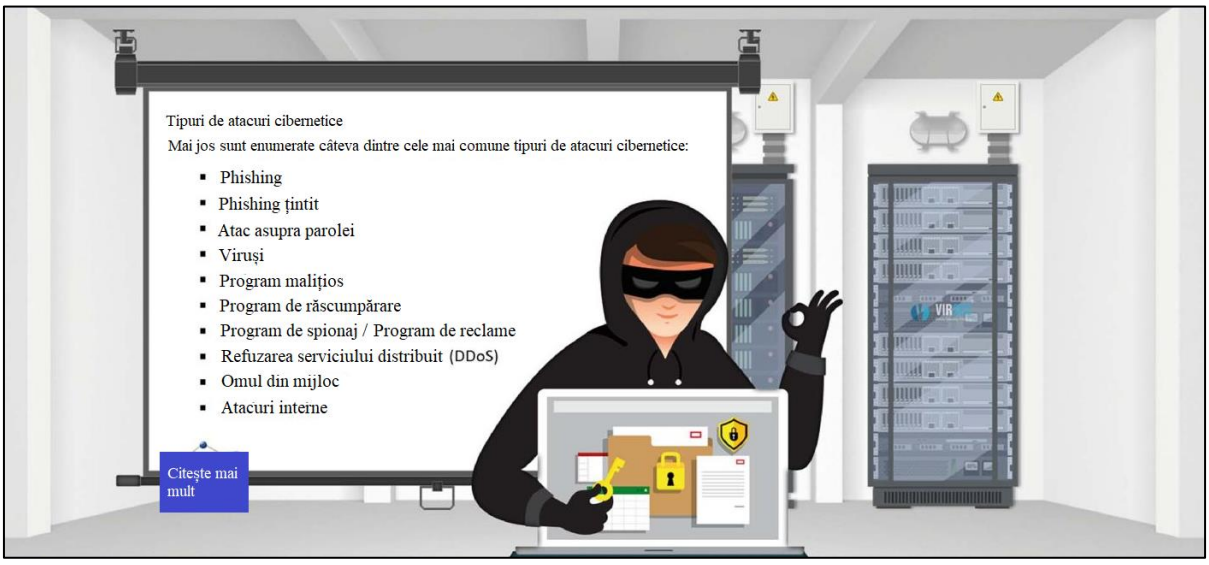

Figura 3.1 În imaginea de mai sus este prezentat cursul firmei Virsec despre tipurile de atacuri din securitatea cibernetică maritimă. Sursă: [46]

3.1.2. Curs de strategie de securitate cibernetică

Virsec oferă, de asemenea, un alt curs dedicat strategiilor în securitatea cibernetică. Acesta poate fi accesat prin intermediul platformei de pe internet a firmei sau printr-un program ce rulează pe sistemul de operare, fără a necesita o conexiune la internet. Durata cursului este de până la cinci ore și utilizează o abordare similară cu cea a YouTube-ului și a jocurilor, pentru a capta atenția cursanților și a le preda prin tehnologia instruirii asistate de calculator. Costul său este de cincizeci și cinci de lire, prețul diplomei fiind inclus în această sumă.

Scopul cursului este de a ajuta participanții să dezvolte strategii pentru protejarea sistemelor expuse atacurilor cibernetice. În acest context, aceștia vor analiza în detaliu pericolele asociate cu atacurile cibernetice și vor învăța despre amenințările specifice domeniului naval, cum ar fi phishing-ul, phishing-ul țintit, programul de răscumpărare, programul de reclame și calul troian. Prin intermediul lecțiilor, cursanții vor învăța să identifice breșele de securitate în sistemele navelor care implementează tehnologiile IT și OT și să înțeleagă metodele prin care persoanele neautorizate se pot folosi de aceste vulnerabilități. După abordarea acestor subiecte, participanții vor învăța măsurile necesare pentru a proteja sistemele și pentru a minimiza pagubele în cazul în care acestea exista.

3.1.3. Curs de conștientizare a securității cibernetice pe superiahturi

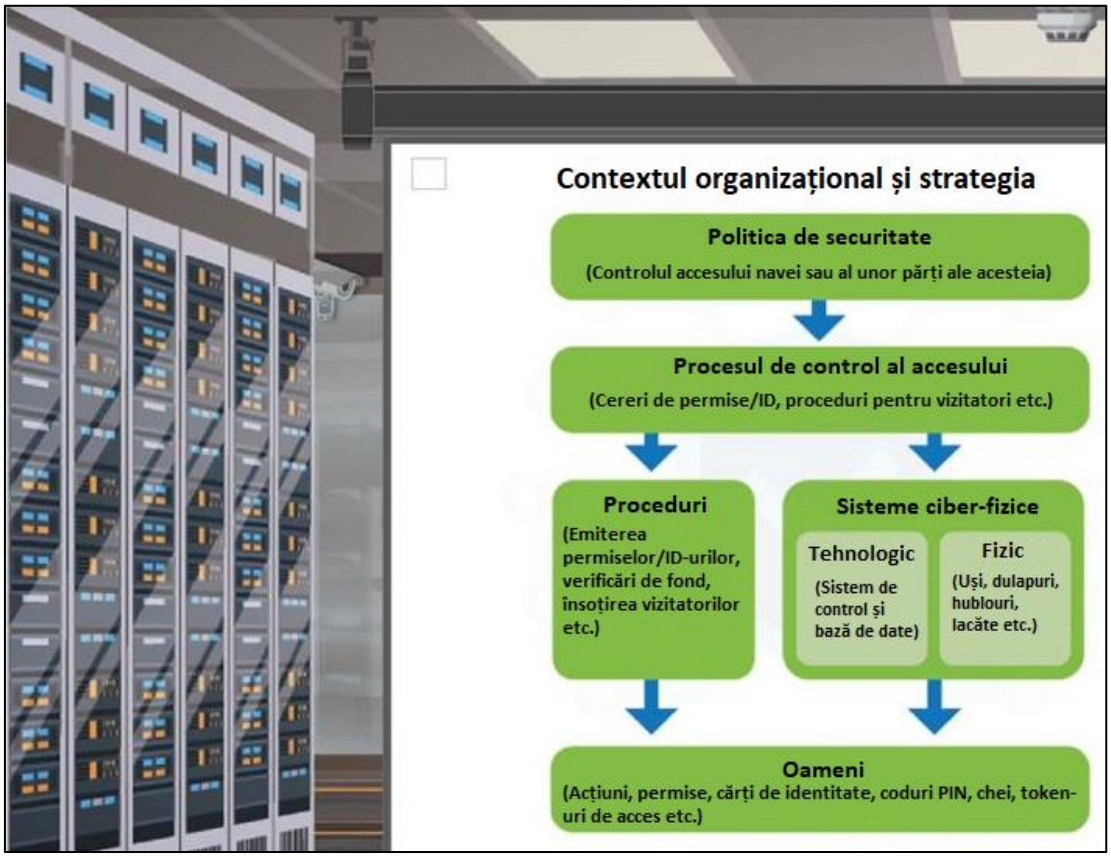

Figura 3.2 În imaginea de mai sus, este prezentată o lecție din aplicația Virsec, care detaliază strategiile organizațiilor din domeniul naval. Sursă: [49]

Virsecul este o firmă privată care oferă o gamă variată de cursuri în domeniul maritim. Pe lângă faptul că deține nu mai puțin de două cursuri bogate în zona de introducere în securitatea digitală, astfel încât orice persoană care este complet nefamiliarizată să poată înțelege noțiunile acesteia, mai

au încă un curs care se axează pe securitatea cibernetică de pe superiahturi. El costă patruzeci și cinci de lire, iar durata sa este de aproximativ două ore. La fel de important este și faptul că acest curs poate fi achiziționat la pachet pentru un întreg echipaj.

Trebuie reținut faptul că acest curs se desfășoară pe două platforme: cea clasică de pe internet și cea din cadrul programului lor, care rulează cu ajutorul sistemului de operare al dispozitivului folosit și prin care un utilizator poate învăța chiar dacă nu are o conexiune la internet. Cursul folosește tehnologia IAC în modul de predare și testare (pentru că, la final, participanții vor obține un certificat în urma promovării unui test) și se concentrează atât pe actualizarea din 2017 a articolului 428 al Comitetului pentru Securitate Maritimă, cât și pe precizările din 2021. Astfel, vor fi discutate pericolele legate de rețelele de socializare folosite de personalul navei, iar ulterior vor fi prezentate amenințările la adresa securității digitale. Aproape de final, cursanții vor învăța cum să ia măsuri pentru a evita situațiile în care pot fi vulnerabili în fața gamei variate și complexe de atacuri.

3.2. Det Norske Veritas (DNV)

În contextul securității cibernetice, se remarcă o companie germană pe piață, care oferă un curs pe internet de conștientizare a securității digitale, folosind instruirea asistată de calculator. Această firmă, cunoscută sub denumirea de Det Norske Veritas, prescurtat DNV, își propune să faciliteze învățarea securității cibernetice de la distanță și susținută de cele mai noi tehnologii informatice. În acest sens, DNV a realizat un curs care implementează IAC în cadrul testelor și a exercițiilor pe care le oferă în cadrul practicii. Ele abordează o gamă variată de atacuri și de metode de apărare împotriva acestora. Cursul lor este structurat în nu mai puțin de patru unități.

Prima unitate introduce cursanții în securitatea cibernetică, le explică rolul lor ca auditor în această industrie și responsabilitățile acestora, cum ar fi evaluarea amenințărilor și întocmirea de rapoarte. În acest mod, ei pot realiza nivelul pericolelor din mediul virtual și vor avea șansa să se familiarizeze și cu primele subiecte despre atacurile cibernetice.

A doua unitate pune un accent mai mare pe tipurile de atacuri. În general, aceasta se axează pe cele care implică metoda phishing, întrucât realizează un număr mare de victime pe internet, dar și pe programele malițioase. Firma oferă cât mai multe exemple teoretice pentru a-i ajuta pe cursanți să înțeleagă metodele prin care pot fi induși în eroare cu ușurință, dar și exemple practice și teste de

antrenament pentru a-i ajuta să conștientizeze cum pot fi atacați de acești profesioniști în infracțiuni cibernetice.

Penultima unitate se axează pe măsurile de securitate operațională, inclusiv protecția împotriva virușilor care pot fi răspândiți prin stick-uri și cabluri USB. Acestea pot instala programe malițioase în dispozitive în doar câteva secunde, atunci când au acces la memoria lor. Unitatea abordează și măsurile de protecție pentru telefoanele personale de la bordul navelor și conexiunile de rețea deoarece acești viruși se pot extinde și prin Wi-Fi, Bluetooth sau fișiere descărcate. Printre măsurile recomandate se numără utilizarea rețelei virtuale private, împărțirea rețelei în mai multe secțiuni, utilizarea zidurilor de rețea și antivirusurilor, dar și blocarea programelor de spionaj prin aplicații specifice de securitate.

Ultimul unitate este destinată managerilor din domeniul informaticii. În cadrul său, vor fi abordate situațiile în care sunt încalcate regulamentele și ce măsuri trebuie luate, pe lângă predarea primelor trei capitole care sunt obligatorii.

3.3. KnowBe4

Metodele practice concepute și utilizate pentru a aprofunda noțiunile teoretice ajută considerabil cursanții din domeniul securității cibernetice să deprindă practicile necesare apărării și să răspundă în mod adecvat și în timp util diverselor atacuri. Din acest motiv, cererile de pregătire din cadrul firmei KnowBe4 au crescut semnificativ datorită ideilor sale inovatoare în materie de învățare la distanță și instruire asistată de calculator.

Aplicația web cu scopuri educaționale, axată în special pe atacurile de tip phishing, este utilizată de firmele private și organizații pentru a-și instrui angajații conform celor mai înalte standarde. Aceasta conține mai multe subiecte despre phishing, oferind cursanților informații teoretice, urmate de teste în care sunt simulate atacurile bazate pe această metodă. În cadrul testelor, participanții sunt nevoiți să aplice noțiunile dobândite în lecțiile postate pe platformă.

Atenția acordată până și celor mai mici detalii și munca depusă de către dezvoltatorii de la KnowBe4 sunt punctele cheie ale aplicației care atrag firmele private. Studiile indică faptul că multe dintre programele concepute pentru educație și disponibile pe internet sunt construite după un model standard, care nu mai captează atenția cursanților. Acestea nu explică în detaliu noțiunile teoretice și

nu oferă exerciții de diferite complexități prin care cursanții să pună în aplicare cât mai mult din ceea ce au învățat în cadrul lecțiilor.

Aplicația web inovativă a celor de la KnowBe4 utilizează videoclipuri integrate în lecții pentru a aborda anumite subiecte, eliminând astfel orice dubii sau lacune în procesul de pregătire al angajaților. În plus, include jocuri și teste pentru a învăța eficient despre phishing, mai ales pentru a dezvolta gândirea critică, astfel încât utilizatorii să poată face față situațiilor dificile. De asemenea, datele platformei sunt actualizate zilnic pentru a oferi cele mai eficiente metode de apărare și cele mai recente informații disponibile din acest domeniu.

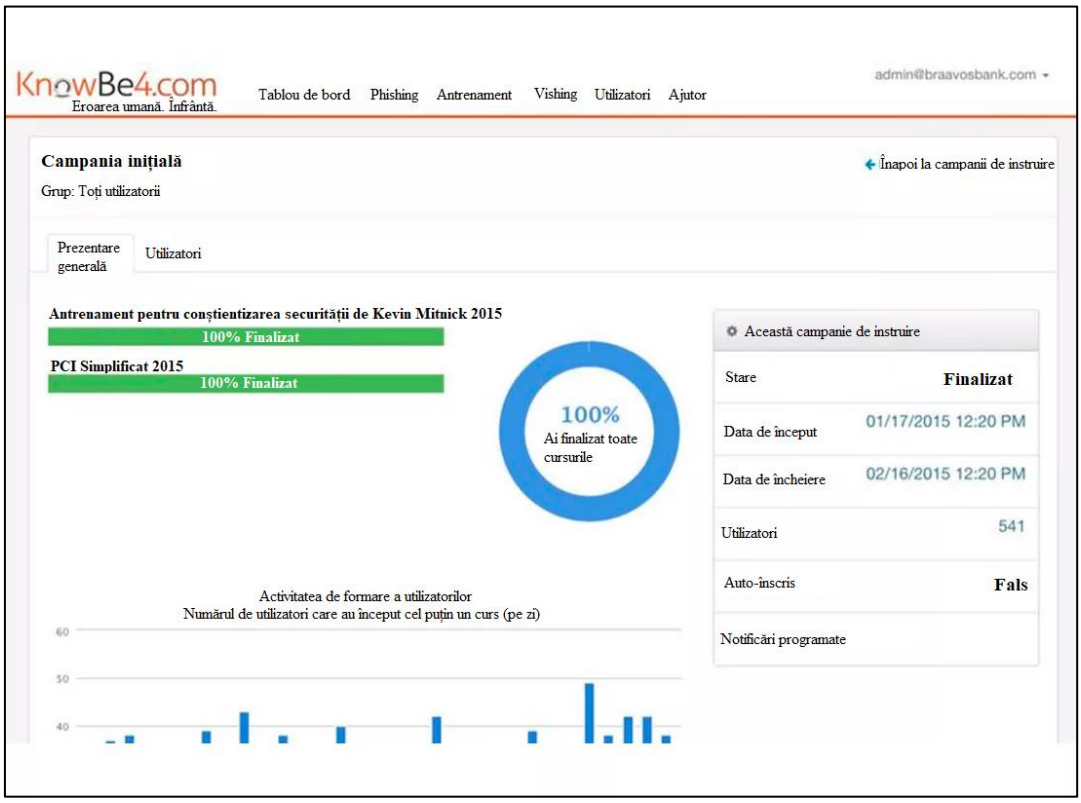

Figura 3.3 Această imagine conține meniul aplicației online KnowBe4, unde este specificat stadiul cursurilor parcurse de către un utilizator. Sursă: [21]

Una dintre persoanele care au contribuit semnificativ la conceperea și verificarea lecțiilor este Kevin Mitnick, un expert în domeniul securității digitale. Productivitatea și aplicarea noțiunilor învățate se realizează prin intermediul jocurilor, unde administratorii lansează atacuri diversificate, precum programe de spionaj, phishing sau diferite programe malițioase, iar utilizatorii trebuie să apere aplicația, exact ca niște adevărați specialiști. La final, sistemul generează rapoarte despre performanța

fiecărui membru al jocului, iar cei care obțin rezultate bune vor fi răsplătiți cu poziții mai mari într-un clasament general.

Acest program se clasează în top datorită capacității sale de a menține publicul într-un ritm care promovează progresul și perseverența. Acest lucru se datorează testelor noi, seturilor bogate de resurse și actualizărilor constante. Astfel, angajații vor învăța sau experimenta mereu ceva nou, fiind puțin probabil să întâlnească teste asemănătoare cu cele din trecut.

Mai mult decât atât, KnowBe4 a făcut progrese semnificative în educație, dezvoltând și o aplicație mobilă. Aceasta aduce o portabilitate suplimentară pentru persoanele interesate de securitatea cibernetică, care sunt deja înscrise pe platforma lor web. Astfel, aplicația are scopul de a ține la curent cursanții cu cele mai recente subiecte, știri, informații și descoperiri din domeniul securității digitale, fără a genera costuri suplimentare pentru cei care au achiziționat aplicația de pe platforma web. Prin această idee inovatoare, KnowBe4 a devenit prima firmă din lume care a lansat o aplicație mobilă dedicată pregătirii personalului în materie de securitate cibernetică.

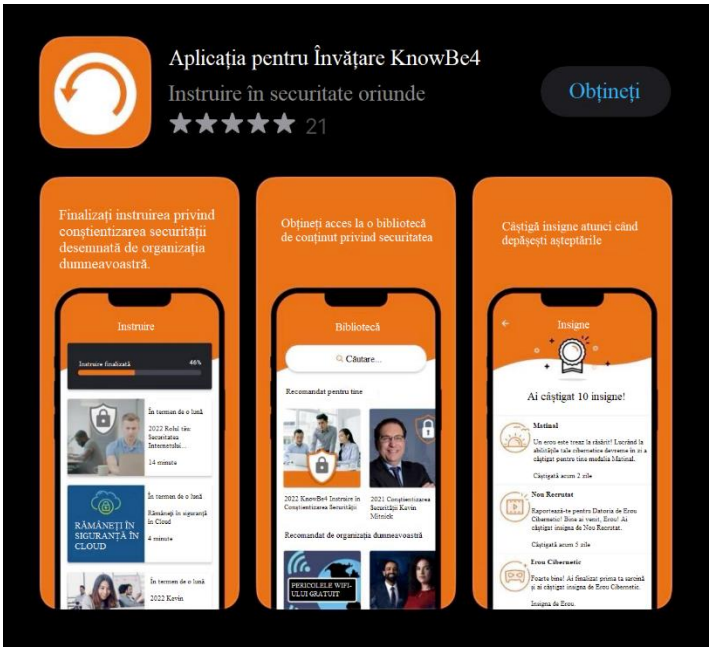

Figura 3.4 În imaginea de mai sus este prezentată aplicația mobilă a firmei KnowBe4, disponibilă în magazinul pentru aplicații al telefoanelor Apple. Sursă: [20]

3.4. Concluziile capitolului

Aceste firme care vin în sprijinul angajaților de pe navele comerciale în domeniul securității cibernetice, prin intermediul instruirii asistate de calculator, se bazează pe concepte avansate de inginerie informatică, inteligență artificială și învățare automată. Se pare că ele mizează foarte mult pe informațiile noi care sunt postate pe platformă sau trimise utilizatorilor prin notificări. În plus, ele își propun să ofere o cantitate mare de informații utilizatorilor, concentrându-se mai mult pe atacurile care implică metodele phishing. De asemenea, încearcă să includă cât mai multe teste și jocuri pentru a oferi utilizatorilor șansa de a aplica ceea ce au învățat.

Printre dezavantajele acestora se numără achiziționarea lor și necesitatea unei conexiuni permanente la o rețea de internet (de la acestea făcând excepție doar firma Virsec). Astfel, o persoană care a achiziționat o aplicație de genul acesta, dar care nu are o conexiune la internet, nu va putea să se folosească de ea. Acest lucru este valabil pentru orice dispozitiv, de la laptopuri până la telefoane.

4.1. Noțiuni introductive despre limbajul de programare

Aplicația dedicată instruirii membrilor echipajelor de pe nave comerciale a fost construită folosind limbajul de programare Java. A fost ales acest limbaj deoarece este unul dintre cele mai orientate din toată gama limbajelor de programare, după C++. Acest lucru presupune că se bazează pe noțiuni din programarea orientată pe obiecte, prescurtată POO și înseamnă că totul este construit sub formă de obiecte. Astfel, clasele constituie schița obiectului, iar obiectul în sine reprezintă o instanță a clasei. La rândul lor, obiectele pot avea atribute și comportamente care sunt definite de metode (funcții în cadrul clasei). Prin urmare, POO reprezintă un stil de programare, iar Java este direct construit folosindu-se de acesta, care urmărește, în final, o implementare a codului cât mai organizată și inspirată din viața reală.

4.2. Avantajele folosirii limbajului Java în cadrul aplicației

Un alt aspect care a determinat alegerea acestui limbaj față de altele este faptul că Java este un limbaj multiplatformă [Figura 4.9, Figura 4.10, Figura 4.11, Figura 4.12, Figura 4.13]. Asta înseamnă că un program realizat cu Java poate rula pe orice sistem de operare, de la Windows, macOS, Linux și până la platforme Android. Totul depinde de modul în care sunt construite aplicațiile, dacă acestea sunt gândite și concepute pentru a se adapta automat în funcție de condițiile mediului în care se regăsesc. Acestea fiind spuse, exact așa a fost gândită și aplicația construită! Ea este una multiplatformă și adaptabilă, adică o aplicație care se adaptează sistemului de operare curent, de la dimensiuni minime și maxime pe care le poate avea și până la nivelul dispozitivului pe care utilizatorul îl folosește, precum calculator sau laptop. A fost luată în calcul portabilitatea aplicației, dovedită și prin modul în care informațiile sunt accesate. În acest sens, aplicația citește fișierele cu extensiile txt și anmb, dar și fișierele Java specifice printr-o cale relativă din folderul proiectului descărcat și nu din locația absolută, pornind de la un anumit disc de stocare. Acest lucru a fost realizat pentru a oferi aplicației capacitatea de portabilitate, pentru a funcționa exact cum a fost gândită și mai ales pentru a nu genera erori sau pentru a crește semnificativ gradul de complexitate al acesteia.

Încă un avantaj major al aplicației dezvoltate este că ea funcționează independent. Acest lucru înseamnă că nu necesită descărcarea și instalarea altor programe și nu rulează pe platforme web, ci

rulează direct în sistemul de operare, la fel ca orice aplicație instalată. De asemenea, un alt aspect important este că programul realizat nu necesită o conexiune la internet.

Aceste aspecte au fost luate în considerare în mod special având în vedere persoanele din domeniul maritim, cum ar fi navigatorii care se pot afla în voiaje și se confruntă cu dificultăți în accesarea unei rețele de internet. Astfel, s-a urmărit reducerea resurselor necesare pentru utilizarea programului și sprijinirea celor care doresc să se familiarizeze cu securitatea cibernetică într-un mod gratuit, fără alți factori care să împiedice dorința de a învăța despre un domeniu atât de important.

4.3. Tehnologia folosită pe parte de interfață

Pe partea de interfață, adică partea vizibilă și interactivă pentru utilizator, a fost folosită una dintre cele mai bogate librării disponibile, și anume Java Swing. Această librărie nu necesită instalarea de noi resurse sau lucrul într-un alt mediu sau platformă; se bazează pe importuri realizate în cadrul codului și utilizarea acestora. Java Swing este cunoscută ca fiind o librărie gratuită, dezvoltată de programatori din întreaga lume care au acces la codul sursă pentru a o îmbunătăți. Deși partea de design nu este la fel de modernă ca în alte tehnologii Java, cum ar fi JavaFX, a fost ales Swing pentru performanța sa.

4.4. Obiectivele aplicației

Se poate afirma că s-a acordat o atenție deosebită productivității utilizatorului, iar atingerea acestui obiectiv a fost realizată prin asigurarea unei aplicații simple, rapide în furnizarea informațiilor, utilizând metode moderne pentru construirea interfețelor și prin punerea accentului asupra detaliilor. În acest sens, au fost implementate mai multe meniuri interconectate. Scopul a fost ca utilizatorii să poată utiliza aplicația fără a fi necesară consultarea descrierii programului sau eforturi considerabile pentru înțelegerea funcționalității acesteia. Utilizatorii au beneficiat de o gama largă de resurse teoretice, printr-o interfață simplă și intuitivă. Au fost luate în considerare toate aspectele necesare pentru prezentarea informațiilor esențiale, permițând utilizatorilor să dobândească cunoștințele necesare, să înțeleagă riscurile cibernetice și potențialele amenințări pentru navele pe care se află sau urmează să se afle. Aplicația include argumente și o terminologie utilizată și de programele companiilor de renume, asigurând astfel o calitate superioară, accesibilitate fără costuri suplimentare

și fără necesitatea unei conexiuni la internet. În plus, aplicația nu impune cerințe la nivelul echipamentelor fizice, fiind compatibilă cu orice laptop echipat cu Java, fără a necesita un procesor avansat, o placă video dedicată sau o cantitate mare de memorie cu access aleatoriu.

4.5. Descrierea aplicației

4.5.1. Fereastra principală

Fereastra care se deschide imediat ce aplicația este lansată reprezintă un cadru în care sunt incorporate mai multe pagini aparținând unor carduri.

În primul rând, fiecare dintre aceste carduri are rolul de a stoca câte două pagini realizate independent și de a permite schimbul între ele în funcție de preferințele utilizatorului. Utilizând această tehnică, a fost realizată o reducere semnificativă a spațiului ocupat de aplicație pe ecran, evitând astfel deschiderea simultană a mai multor pagini.

Asemenea carduri se regăsesc în părțile de vest, sud și centru ale aplicației deoarece cadrul principal este organizat conform punctelor cardinale și include și o poziție centrală.

4.5.2. Meniul aplicației

Aplicația construită conține un meniu clasic în partea de sus, prin care pot fi accesate două submeniuri: fișier și fereastră. În cadrul submeniului fișier sunt disponibile nu mai puțin de trei butoane: import, export și ieșire.

Primul buton, cel de import [Figura 4.2], permite citirea fișierelor cu extensie txt și anmb. Ele pot fi alese de oriunde din memoria dispozitivului deoarece în momentul apăsării acestui buton se va deschide o fereastră specială pentru a naviga în orice director și în orice disc de memorie pentru a alege fișierul dorit. Utilizatorul nu trebuie decât să selecteze fișierul, după care să apese butonul de deschide și textul aflat în cadrul fișierului va fi afișat automat în zona dedicată textului din pagina principală. Dacă va apăsa pe butonul de renunțare, această fereastra se va închide și nu va fi nimic citit și afișat în zona corespunzătoare textului.

Al doilea buton este cel de export și permite salvarea fișierelor cu extensiile txt și anmb pe dispozitivul pe care rulează aplicația. Atunci când acest buton este apăsat, se va deschide o fereastra

similară cu cea pentru citirea fișierelor, dar cu opțiunea de salvare în loc de deschidere. Utilizatorul va trebui să aleagă directorul în care va fi salvat fișierul, să introducă denumirea acestuia împreună cu extensia și după ce apasă pe salvare, fișierul va fi creat conținând textul curent din panoul de text aflat în zona centrală a aplicației.

Al treilea buton, denumit ieșire [Figura 4.3], reprezintă o alternativă pentru a închide aplicația. Așadar, înainte ca angajatul să părăsească programul, va apărea un mesaj de confirmare cu opțiunile da sau nu, pentru a preveni închiderea involuntară a acesteia.

Al doilea submeniu, cel denumit fereastră, conține, la rândul său, încă alte două meniuri: vizibilitate și aspect. Primul dintre ele permite afișarea paginilor aplicației. Ele sunt prezentate sub formă de butoane, fiecare cu o bifă care indică dacă pagina este activă. Acest mecanism automat ajută la prevenirea erorilor și a închiderii neașteptate a aplicației [Figura 4.4].

Mereu, într-un card din orice punct, va fi afișată o pagină astfel încât cadrul principal să nu fie niciodată gol. De asemenea, utilizatorul poate apăsa de câte ori dorește pe un buton sau meniu deoarece acest lucru nu va afecta funcționarea programului în niciun fel.

Există și un meniu special conceput pentru tematică, având rolul de a schimba culorile paginilor în funcție de preferințele fiecărei persoane. Gama de culori disponibilă este extrem de variată, iar denumirile culorilor sunt sugestive: prima denumire reprezintă prima culoare din paleta selectată și este aplicată în zona de vest a programului, în timp ce a doua denumire indică ultima culoare din paletă, aplicată în zona de est. Meniul utilizează butoane grupate astfel încât să permită selectarea unui singur buton pe rând. După alegerea temei, aceasta se aplică întregii aplicații în câteva secunde [Figura 4.5].

4.5.3. Modul de funcționare al zonei de vest

Ca mod implicit, aplicația oferă în partea de vest (stânga paginii) informații despre tema aleasă, coordonatorul și autorul temei de licență. În această secțiune sunt prezente două butoane care fac legătura cu alte două pagini din aplicația curentă: panou text și schimbare panou.

Primul buton trimite un semnal către zona centrală pentru a deschide pagina care conține zona de text și meniul asociat. Astfel, se va face schimbul între cele două pagini independente din cardul dedicat zonei centrale.

Cel de-al doilea buton schimbă pagina care conține informațiile generale cu pagina despre categoriile de atacuri și virușii specifici. Ea conține o gamă variată de butoane, fiecare afișând textul cu informațiile specifice virusului selectat. Dacă înainte de apăsarea butonului pentru virusul sau atacul specific a fost deja accesată pagina dedicată textului, atunci în momentul apăsării butonului, va fi modificat doar textul din zona central [Figura 4.6].

4.5.5.1. Lista cu atacuri și viruși

4.5.3.1.1. Calul troian

Calul troian este un tip de program malițios care se infiltrează în dispozitivul victimei sub o altă formă decât cea pe care o prezintă. De obicei, se deghizează într-un fișier atașat la un e-mail, într-o legatură web dintr-un e-mail, în mesaje text, în conversațiile de pe rețelele sociale, în notificările telefonului prin intermediul abonamentelor la diferite pagini web, în reclamele de pe internet sau, de cele mai multe ori, sub forma unui program aparent normal.

În majoritatea cazurilor, aceste programe se află pe pagini false, recent construite de persoane cu intenții rele, în care sunt promovate pentru a fi descărcate si pentru a infecta, respectiv controla cât mai multe dispozitive. Troianul dă impresia unui program normal, clasic, dar de fapt este un cu totul alt tip de program. În acest sens, punctul forte al acestui virus este mascarea adevăratei sale naturi. De aici reiese și denumirea sa, care își are originile încă din greacă și anume calul troian. El este folosit pentru a accesa ilegal datele sau pentru a permite altor viruși să își facă loc în sistemul de operare al victimei (funcționează pe post de pod; ține anumite porturi din dispozitivul victimei deschise pentru apariția altor viruși). Este de precizat faptul că el nu este folosit pentru injectarea în alte fișiere, ci este responsabil de instalare, monitorizare și acces ilegal.

Ca metode de prevenire, se recomandă evitarea, pe cât de mult posibil, a apăsărilor pe reclame sau pe butoanele care oferă doar două opțiuni, precum: închidere sau da. Într-o astfel de situație, se sugerează închiderea paginii web, a navigatorului web sau utilizarea butonului de înapoi, fie cu

mouse-ul, fie cu butonul specific de pe telefon. Utilizarea aplicanției web Archive.org este de asemenea recomandată. Pe baza legăturii paginii accesate, se poate verifica de cât timp este aceasta disponibilă publicului larg. În general, aceste pagini false au o vechime cuprinsă între câteva zile și până la trei ani.

Se recomandă utilizarea unui antivirus care să blocheze paginile ce facilitează breșele de securitate, incluse în lista neagră din memoria sistemului acestuia. Atunci când se accesează o astfel de pagină, antivirusul poate bloca accesul la ea. Dacă totuși este permisă accesarea ei, înainte de a apăsa pe butonul de descărcare, este indicat să se verifice Archive.org deoarece este gratuit și nu va dura mai mult de cinci minute. În cazul infectării cu viruși, detaliile pot face diferența.

Este extrem de folosit de persoanele cu intenții rele pentru a ataca dispozitivele angajaților navei, fără ca aceștia să conștientizeze pericolul la care sunt expuse informațiile lor și ale navei. Calul troian este precum cu o cutie cu surprize, în sensul că un atac care conține un cal troian poate instala un program de reclame inofensiv sau poate servi drept poartă pentru alte programe malițioase cum ar fi programul de răscumpărare și care pot duce la situația în care nava nu mai poate fi controlată de echipaj din cauza echipamentelor care funcționează defectuos.

4.5.3.1.2. Program de răscumpărare

Programul de răscumpărare este unul tip malițios care se folosește de criptarea informațiilor furate pentru ca ulterior să fie cerută o răscumpărare de către grupările de infractori cibernetici pentru ele. În general, informațiile care sunt criptate pot fi accesate doar de către dispozitivele care au produs criptarea. Este un proces extrem de greu pentru ca o firmă specializată sau un anumit grup de profesioniști să acceseze datele criptate de altcineva. Există o serie de algoritmi și de metode logice și matematice pentru realizarea unei astfel de soluții în materie de securitate cibernetică. În plus, un anumit șir de caractere poate avea o anumită semnificație și aceasta poate fi schimbată la câteva ore cu ajutorul dispozitivelor performante. De aceea, răscumpărarea este cerută pentru a oferi din nou accesul la date.

Programul de răscumpărare este construit în așa fel încât să se răspândească extrem de rapid într-o rețea de internet și să afecteze serverele și bazele de date. El se bazează pe o criptare asimetrică, care utilizează o cheie publică pentru a bloca, cripta fișierele și o cheie privată pentru a le

accesa, decripta. Aceste două chei, unite, formează o pereche unică (una publică și una privată) pentru fiecare victimă în parte. Folosindu-se de cheia privată, atacatorul poate decripta și reda victimei informațiile furate, dar acest lucru se poate întâmpla numai în urma unei răscumpărări. Chiar și așa, nu există garanția obținerii cheii private, care rămâne în mâinile atacatorului. Trebuie reținut faptul că fără accesul la o asemenea cheie, nu se pot recupera datele furate.

După ce a intrat în sistem și a fost instalat complet, acesta rămâne pe dispozitivul victimei până la îndeplinirea misiunii stabilite, și anume: obținerea unui volum mare de date, printre care cele mai importante sunt cele private sau cu caracter personal. După colectarea acestor date, începe procesul de blocare a fișierelor și de deblocare în urma răscumpărării.

Ulterior, programul de răscumpărare rulează cod la nivel binar pentru a începe atacul propriu-zis, moment în care începe căutarea și criptarea informațiilor. Pe lângă efectele devastatoare ale acestuia, el are și capacitatea de a exploata breșele de securitate ale sistemului și rețelei pentru a accesa și alte resurse și sisteme, provocând astfel o răspândire a atacului și producând mai multe daune.

Imediat cum au fost criptate informațiile, programul de răscumpărare îi cere victimei să achite o sumă drept răscumpărare într-un anumit termen pentru a decripta fișierele, altfel va șterge automat informațiile colectate. În cazul în care nu au fost luate măsuri de precauție cu privire la asemenea situații, cum ar fi copiile informațiilor prețioase și stocarea lor în sisteme de cloud sau pe alte dispozitive, atunci acestea pot fi pierdute pentru totdeauna.

Cu ajutorul său se realizează și pirateria modernă, fiind folosit pentru a cripta anumiți parametri sau a bloca diverse metode implementate la nivelul echipamentelor navei, introducând astfel o serie de erori la bordul acestora. De asemenea, pot fi furate planurile de încărcare și rutele de navigație realizate de echipaj sau hărțile din ECDIS, pentru a-i împiedica să stabilească alte rute. Programul de răscumpărare criptează în permanență și datele de la radar, făcând imposibilă detectarea pericolelor din apropierea navei. Din cauza aceasta, nava nu mai poate fi operată, chiar dacă echipamentele sunt uneori înlocuite. În acest caz, se cere o anumită sumă pentru a restabili funcționalitatea echipamentelor.

Pentru asigurarea unui nivel adecvat de securitate, este recomandat să se utilizeze un antivirus de tip premium, care oferă facilități suplimentare, precum rețeaua virtuală privată și funcționalități de

protecție împotriva urmăririi. Este esențial ca utilizatorii să păstreze copii de siguranță ale informațiilor sensibile pe mai multe platforme (preferabil în cloud) sau pe dispozitive separate și să evite conectarea la rețele deschise (fără parolă) sau la rețele cu securitate slabă. De asemenea, este necesar să se efectueze o scanare completă a dispozitivului sau dispozitivelor în fiecare zi.

4.5.3.1.3. Set de instrumente pentru accesul la nivel de administrator

Setul de instrumente pentru accesul la nivel de administrator constituie o colecție de aplicații care accesează dispozitivul victimei sau o anumită parte din sistem în mod ilegal. De cele mai multe ori, prezența acestei colecții în dispozitiv este ascunsă. El poate fi instalat automat sau manual, de obicei după ce atacatorul a obținut controlul de administrator asupra sistemului. Odată ce este instalat, poate modifica și aplicațiile antivirus sau alte programe de securitate, făcând extrem de dificilă detectarea unui astfel de atac.

Atunci când un sistem este infectat cu un astfel de virus, pașii necesari pentru detectarea și eliminarea lui sunt extrem de limitați. Experții în securitatea informatică pot folosi doar un alt sistem de operare (de aceeași versiune) care nu a fost infectat și să efectueze multiple comparații între cele două sisteme de operare, verificând și descărcările în memorie. Este crucial să se determine dacă virusul a reușit să ajungă în memoria sistemului de operare, cunoscută sub numele de nucleu. Dacă virusul nu a ajuns la nucleu, este posibilă reinstalarea sistemului de operare pentru a remedia problema. În schimb, dacă virusul a pătruns în nucleu, este aproape imposibil să se repare sistemul, iar în astfel de cazuri poate fi necesară chiar și înlocuirea componentelor fizice afectate.

Pericolul pe care îl reprezintă acest set de instrumente este dat de faptul că se poate extinde în multiple echipamente de la bordul navei. Extinderea sa este facilitată de modul în care arhitectura echipamentelor este realizată, mai ales că ECDIS-ul comunică imediat cu radarul și sistemul AIS. De cele mai multe ori, specialiștii sunt puși în dificultate când încearcă să elimine virusul acesta dintr-un echipament sau când decid să îl înlocuiască cu altul de rezervă pentru că nu le rămâne altă opțiune. Chiar și în asemenea cazuri, echipamentele noi pot fi infectate la scurt timp, necesitand reluarea intregului proces de verificare a sistemului de operare.

Singurele metode de apărare rămân antivirusurile cu măsuri foarte restrictive, scanările zilnice și utilizarea unui zid virtual cu capacități de detectare a intruziunilor, care să monitorizeze dacă sunt folosite seturi de instrumente pentru accesul la nivel de administrator.

4.5.3.1.4. Vierme

Virusul vierme este un program care se extinde automat într-o rețea și are capacitatea de a se multiplica. Este recunoscut pentru faptul că se folosește de breșele de securitate din sistem și are ca obiectiv să se răspândească cât mai mult în cadrul său. Mai este recunoscut și pentru faptul că poate ține porturile victimei deschise, facilitând astfel infectarea intregului sistem cu programul de răscumpărare.

Viermii sunt responsabili pentru un consum uriaș al traficului de date și pun o presiune enormă pe bazele de date și servere. Acesta este și motivul pentru care ele funcționează defectuos în momentul în care viermii încep să se extindă. Cel mai grav aspect este că pot acționa în mod automat, fără a fi controlați de la distanță de către o persoană.

Extinderea acestora se bazează pe breșele de securitate din sistem sau pe atașamentele din e-mailuri. De cele mai multe ori, simpla apăsare pe o legătură web generează aproape instant descărcarea viermelui, iar utilizatorul nici nu va fi conștient de acest incident.

În domeniul naval, riscul de infectare cu viermi este extrem de mare deoarece aceștia pot duce la suspendarea totală a sistemelor de securitate cibernetică. Acest risc crescut se datorează prezenței unui număr foarte mare de persoane pe navele de croazieră, fiecare având cel puțin un dispozitiv, cum ar fi telefonul mobil. În momentul infectării, viermii se pot multiplica și răspândi rapid datorită numărului mare de aparate apropiate sau conectate la aceeași rețea, fie că este vorba de rețeaua de internet a navei sau cea de televiziune.

Un risc similar se întâlnește și pe navele ro-ro care transportă mașini de ultimă generație ce includ sisteme Android sau iOS, precum și la navele container care transportă diferite produse (calculatoare, laptopuri, telefoane, televizoare inteligente, ceasuri inteligente, console Xbox, routere, comutatoare, sisteme audio, electrocasnice). Numărul dispozitivelor care conțin procesoare și zone de

stocare, având capacitatea de a se conecta la internet sau Bluetooth, este extrem de mare pe aceste nave.

Pentru a fi în siguranță, trebuie luate aceleași măsuri ca pentru protejarea împotriva unui cal troian și poate fi utilizată o metodă suplimentară oferită de antivirusii premium: masca de e-mail. Aceasta reprezintă un alt nume față de adresa clasică de e-mail și are scopul de a păstra anonimitatea în zona online și de a crea o metodă suplimentară de filtrare a mesajelor primite. Masca de e-mail poate fi considerată ca un zid suplimentar în fața atacurilor de acest tip. Un alt indiciu al prezenței unui vierme este viteza redusă cu care rulează dispozitivele.

4.5.3.1.5. Program de spionaj

Acest program este unul dăunator și special conceput pentru a se ascunde în sistemul de operare, astfel încât să-și atingă obiectivul de monitorizare ilegală a traficului de internet, istoricului și informațiilor din navigatorul web, cum ar fi descărcările și datele completate. De cele mai multe ori, se concentrează pe informațiile legate de cardurile bancare. Astfel, informațiile copiate sau furate sunt vândute firmelor de publicitate, diferitor utilizatori și companiilor de date. Acest lucru este extrem de periculos deoarece persoanele neautorizate sunt motivate doar de dorința de a comercializa cât mai multe date, fără a se întreba cui sunt vândute datele și ce vor face cu ele. Pericolul real constă în faptul că datele pot fi folosite în scopuri complet diferite, cum ar fi furtul de identitate, amprentarea digitală sau șantajul. De asemenea, programul poate compromite și sistemele de comunicare, afectând astfel eficiența și securitatea operațiunilor navale.

Orice program instalat fără acordul persoanei care detine dispozitivul poate fi considerat ca fiind unul de spionaj. Nu contează dacă este prezent în sistem din diferite motive, poate unele inofensive. Un lucru este foarte clar: spațiul privat al persoanei este încălcat, iar riscurile de a fi șantajată sunt extrem de mari.

Prin intermediul unei aplicații de monitorizare avansată, se poate urmări locația fizică a unei persoane care folosește un telefon mobil, precum și metodele sale de comunicație, cum ar fi: apelurile telefonice, mesajele, conversațiile web, e-mailurile și galeriile foto.

Programele malițioase de acest tip sunt asociate cu performanța scăzută și consumul ridicat de resurse, cum ar fi descărcarea extrem de rapidă a bateriilor de telefon sau încărcarea dificilă a laptopurilor sau calculatoarelor.

Ar trebui să se utilizeze un antivirus care dispune de sisteme anti-spionaj incluse în scanările complete. În cazul unui antivirus premium pe bază de abonament, acesta poate efectua și scanări la nivelul rețelei. Ele sunt extrem de performante deoarece pot detecta fișierele care sunt utilizate pentru a infecta sistemele sau pentru a identifica programele instalate care ar putea reprezenta o amenințare.

4.5.3.1.6. Program de reclame

Programul de reclame este conceput pentru a afișa reclame publicitare fără acordul utilizatorului și poate provoca disconfort din cauza aparițiilor sale multiple pe paginile web. Este una dintre cele mai utilizate metode în prezent, alături de programul de răscumpărare, pentru a genera venituri semnificative persoanelor care îl folosesc. Prezența sa poate fi observată atât pe calculatoare și laptopuri, cât și pe telefoanele mobile. El reprezintă un pericol la nivel de securitate cibernetică deoarece este folosit pe post de poartă la nivelul rețelei și, de cele mai multe ori, facilitează apariția programului de spionaj, a celui de urmărire sau a calului troian.

Platformele web și sistemele de operare ale dispozitivelor pot fi infectate cu acest program prin intermediul descărcărilor simple de pe internet. Atunci când se descarcă un program, o poză sau un document, există posibilitatea ca acestea să includă, fără nicio notificare, și fișierele programului de reclame. Rezultatul instalării virusului este imediat vizibil deoarece utilizatorii vor fi copleșiți de reclame iritante în navigatorul web.

Încă o metodă prin care se poate intra în contact cu un asemenea program este utilizarea breșelor de securitate ale sistemelor de către grupările infracționale cibernetice. Prin intermediul virușilor deja prezenți în sistem (care au capacitatea de a menține anumite porturi deschise), atacatorii pot descărca și instala programul de reclame.

Pentru navigatori, programul de reclame reprezintă un pericol chiar dacă pare nesemnificativ sau inofensiv. În cele mai negre scenarii, efectele sale pot fi similare cu cele ale unui cal troian, facilitând astfel infiltrarea cu ușurință a altor viruși periculoși care pot provoca daune chiar și

permanente, așa cum se întâmplă în cazul setului de instrumente pentru accesul la nivel de administrator.

Pe partea de recomandări, ar fi bine să se folosească un antivirus care dispune de sisteme anti-urmărire și care realizează rapoarte privind numărul de încercări de atac asupra dispozitivului. Acesta va alerta utilizatorii în legătură cu programele pe care le consideră periculoase și ar putea recomanda chiar și ștergerea lor. În plus, sistemele ar trebui actualizate deoarece acestea vin cu măsuri de securitate sporite.

4.5.3.1.7. Rețea de dispozitive infectate

O rețea de dispozitive infectate este formată dintr-un grup de calculatoare ce conțin programe malițioase și care sunt controlate de un atacator. Aceste dispozitive sunt folosite pentru a desfășura atacuri coordonate.

Cea mai cunoscută metodă de atac folosind rețeaua de dispozitive infectate este refuzarea serviciului distribuit. Aceasta presupune trimiterea unor cereri într-un mod excesiv împotriva unui serviciu pentru a-l copleși în totalitate. În cadrul navei, refuzarea serviciului distribuit are potențialul de a compromite sistemele de navigație și comunicații. Prin infiltrarea în rețelele de pe nave, poate cauza funcționarea defectuoasă a echipamentelor, poate intercepta sau manipula datele esențiale pentru navigație și are capacitatea de a controla sistemele automate.

Printre indiciile care ajută la constatarea unui atac de acest tip se numără: o serie de activități necunoscute, dificultăți în închiderea și pornirea echipamentelor, utilizarea excesivă a memoriei de acces aleatoriu și o conexiune la internet extrem de scăzută.

Printre cele mai eficiente metode de apărare împotriva atacurilor bazate pe rețelele de dispozitive infectate sunt: utilizarea zidurilor de rețea, a rețelelor private virtuale și a aplicațiilor de monitorizare a traficului, care sunt folosite pentru detectarea intruziunilor. De asemenea, se recomandă utilizarea soluțiilor antivirus care efectuează scanări avansate atât la nivelul sistemului de operare, cât și la nivelul rețelei. Pe lângă aceste metode, mai sunt eficiente și folosirea cât mai multor parole (pentru router, telefon, aplicații) și actualizarea antivirusului la zi. În plus, pentru sporirea siguranței în cazul pierderii de informații, este considerată esențială realizarea unor copii de siguranță, în special în cloud, având în vedere riscul ca sistemul de operare atacat să nu mai funcționeze.

4.5.3.1.8. Omul din mijloc

Atacul care implică un om în mijloc se referă la o persoană complet neautorizată care este între utilizatorul unei aplicații și aceasta. El se bazează pe interceptarea mesajelor care sunt trimise în cadrul unei aplicații, modificarea lor astfel încât atacatorul să se dea drept persoana care a trimis mesajul și să înșele destinatarul mesajului respectiv.

Scopul acestui atac este de a obține informațiile personale ale destinatarului, inclusiv datele de conectare, precum și datele de plată, informațiile de pe cardul bancar. Ele pot duce la furtul de identitate, tranzacții și transferuri neautorizate și modificarea datelor conturilor de pe diferite platforme.

De cele mai multe ori, pe lângă scopurile clasice ale acestui atac, în domeniul naval este utilizat ca o metodă pentru a pătrunde și mai adânc în sistemele de la bord. De exemplu, o persoană neautorizată poate accesa stația VHF și se poate da drept ofițer de punte, emițând semnale false către alte nave sau către autoritățile navale. De asemenea, atacatorul poate modifica mesajele, documentele sau testele susținute pe internet de angajații companiei, atacând conturile acestora. Un alt exemplu ar fi atacarea aplicației web a companiei de care aparține echipajul navei prin intermediul conturilor lor. Astfel, scopurile și metodele de atac pot varia.

Pentru apărarea eficientă împotriva atacurilor ce presupun omul din mijloc, se recomandă utilizarea serviciilor de securizare a straturilor de transport și a socket-urilor, care asigură criptarea comunicațiilor și confirmarea identității participanților. În plus, este recomandată folosirea unei rețele private virtuale care creează tuneluri criptate și protejează traficul de rețea. De asemenea, sunt absolut necesare folosirea autentificării cu mai mulți factori, care întărește securitatea accesului la informațiile private, precum și implementarea sistemelor de detecție și prevenire a intruziunilor.

4.5.3.1.9. Înșelarea Sistemului de Poziționare Globală

Ca și o scurtă teorie, semnalul Sistemului de Poziționare Globală este unul slab și transmis prin intermediul sateliților aflați pe orbita. Dacă este folosit un dispozitiv performant, cum ar fi un transmițător radio care să emită semnale cu mult mai puternice față de semnalul clasic al Sistemului de Poziționare Globală, atunci acesta va fi depășit cu ușurință și va conduce la o afișare falsă a

coordonatelor și orei pe echipamentele de navigație, precum și pe celelalte dispozitive care se afla sub raza semnalului mai puternic. De aceea, atacul este asociat cu bruiajul electronic.

Cel mai mare pericol pentru angajații navelor comerciale expuse atacurilor care implică înșelarea Sistemului de Poziționare Globală este ca navele lor să fie ghidate în cu totul alte părți față de rutele stabilite. Aceste atacuri sunt realizate pentru a fura marfa deținută și pentru a cere, uneori, chiar și răscumpărarea echipajului (realizarea pirateriei). Printre practicile utilizate se numără și lacătele cu Sistem de Poziționare Globală, care emit încontinuu semnale puternice pentru a bruia alte semnale și care pot fi deschise numai la ajungerea lor în locația setată.

Pentru prevenirea unor asemenea evenimente, angajații au în ajutor receiverele. Acestea au rolul de a monitoriza direcția de sosire a semnalului, întrucât informațiile care sunt adevărate provin de la mai mulți sateliți în același timp.

4.5.3.1.10. Manipularea Sistemului de Identificare Automată

Atacurile la nivelul Sistemului de Identificare Automată pot fi efectuate în două moduri: asupra emițătoarelor sale sau asupra senzorilor pe care îi folosește. Emițătoarele au nevoie în permanență de informațiile despre poziție, respectiv de cele despre cursul navei, iar ulterior ele sunt transmise și participanților la traficul maritim. În schimb, atacurile asupra senzorilor de poziție presupun transmiterea de informații false, ale căror consecințe se regăsesc la nivelul echipamentului ECDIS sau radar. Printre ele se numără dispariția unor ținte sau oferirea de către ECDIS a unor date de poziție, respectiv de curs ale altor nave complet false, ceea ce ar duce echipajul în eroare. Acest tip de atac este folosit în cazul pirateriei, acolo unde mai întâi se asigură faptul că nava nu va detecta celelalte nave sau ambarcațiuni care se apropie de ea. ECDIS-ul are capacitatea de a efectua verificări pentru a confirma țintele Sistemului de Identificare Automată, prin intermediul radarului și poate depista atacurile folosindu-se de examinarea de tip încrucișată.

Pericolul este generat deoarece Sistemului de Identificare Automată nu trimite informațiile sub o formă criptată întrucât ele nu ar mai putea fi recepționate de alți participanți la trafic și astfel există șanse ca ele să fie interceptate și de pirați.

4.5.3.1.11. Phishing si Phishing țintit

Atacurile ce folosesc metoda phishing se bazează atât pe înșelare, cât și pe inginerie socială pentru a obține informații despre victime, inclusiv detalii despre cardurile lor bancare. Aceste atacuri au loc prin intermediul e-mailurilor, mesajelor și paginilor de pe internet și urmează de obicei același tipar: se prezintă drept o instituție, firmă sau rețea socială care informează victimele despre incidente grave, fie în mediul fizic, fie pe internet.

Phishing-ul țintit este o variantă a phishing-ului clasic, dar cu mult mai complexă, ale căror victime sunt în special organizațiile. Punctul forte al atacurilor cu phishing țintit este că de cele mai multe ori, atacatorii pretind că sunt firme colaboratoare sau clienții lor, întocmai pentru a duce personalul companiilor în eroare și pentru a accesa informațiile acestora.

Documentându-se intens despre victimele lor, folosind ingineria socială (informații de pe internet și platforme de socializare), atacatorii creează mesaje personalizate pentru a le atrage atenția acestora și pentru a le da impresia că discută într-adevăr cu persoana sau compania care i-a contactat.

În zona maritimă, cu ajutorul acestor metode se pot obține datele de conectare de la diferite sisteme și există șanse să fie modificate și actele, rapoartele sau chiar și sistemele de navigație. Dintre toate echipamentele, ECDIS-ul este cel mai sensibil, întrucât atacatorii pot insera informații false în acesta.

Este recomandată utilizarea unui antivirus și a unei măști de e-mail, care implică crearea unui nume suplimentar ce va fi folosit ca adresă de e-mail atunci când aceasta este solicitată. Rolul acesteia este de a crea o zonă de filtrare și de a menține adevărata adresă de e-mail complet necunoscută pentru cei care contactează utilizatorul.

Mai este recomandat să nu se răspundă la mesajele provenite din partea unor adrese necunoscute. Acest lucru este important deoarece o persoană poate deveni victima unei campanii de phishing. În plus, se recomandă evitarea accesării legăturilor web sau a documentelor din e-mailuri. Este esențial să se verifice întotdeauna adresa de e-mail a expeditorului.

4.5.4. Modul de funcționare al zonei centrale

În partea centrală va fi afișată pagina principală a aplicației care conține logo-ul facultății. Ea este prima pagină dintr-un card care include încă o pagină, dedicată textului.

Cea de-a doua pagină a cardului conține zona de text unde sunt prezentate informațiile detaliate despre viruși, atacuri și recomandări. De asemenea, pagina dispune de scroll-uri verticale și orizontale pentru a afișa complet textele, chiar și cele de dimensiuni foarte mari. De altfel, pagina nu este simplă; ea include o altă pagină independentă cu butoane care permit utilizatorului să controleze ce se întâmplă cu pagina dedicată textului și ce informații sunt afișate sau scrise.

Primele două butoane, cele de import și export, reprezintă o alternativă rapidă la butoanele din submeniul fișier al aplicației. Prin intermediul lor, pot fi citite sau scrise diferite fișiere cu extensii txt și anmb.

Cel de-al treilea buton se numește teorie și, atunci când este apăsat, trimite un semnal către cardul care reprezintă zona vestică, pentru a accesa pagina unde sunt informațiile despre viruși și atacuri.

Al patrulea buton este ștergere. De fiecare dată când o persoană dorește să șteargă tot textul din panoul specific, poate apăsa pe acest buton. Înainte de ștergerea propriu-zisă, va primi un mesaj de confirmare, în care trebuie să selecteze dacă renunță sau continuă. Metoda a fost introdusă ca măsură de precauție, în cazul în care un utilizator apasă din greșeală butonul de ștergere.

Ultimul buton din această pagină este cel de închidere și are rolul de a închide pagina care conține zona de text alături de butoanele sale și să le înlocuiască cu pagina principală a aplicației, unde este logo-ul facultății.

4.5.5. Modul de funcționare al zonei de sud

În partea sudică, sunt disponibile două pagini. Una dintre acestea este destinată descrierii detaliate a aplicației, astfel încât utilizatorii să înțeleagă modul în care aceasta funcționează. De asemenea, aceasta reprezintă prima pagină vizualizată atunci când aplicația este lansată în execuție. Pagina utilizează și ea scroll-uri, la fel ca și zona dedicată textului.

A doua pagină utilizată de cardul zonei de sud, atunci când se efectuează schimbarea între pagini, este despre pericole și recomandări. În această pagină, butoanele pot fi selectate pe rând, iar de fiecare dată când este apăsat un alt buton, acesta trimite automat un semnal către cardul zonei centrale pentru a afișa informațiile referitoare la pericolul sau recomandarea selectată [Figura 4.7].

4.5.5.1. Lista cu pericole și recomandări

4.5.5.1.1. Rețea privată virtuală

Rețeaua privată virtuală conectează dispozitivele la un server care aparține unui furnizor privat, în schimbul unui abonament anual. Obiectul stabilirii unei conexiuni de acest gen este de a crea o nouă adresă IP pentru a păstra caracterul anonim al cumpărătorului, mai ales că datele sale sunt criptate și sunt evitate astfel zidurile și restricțiile de rețea.

Este una dintre cele mai folosite metode pentru a păstra datele confidențiale deoarece este la un preț accesibil și nu implică anumite configurări. Este necesar să se achiziționeze un antivirus, care se va ocupa de restul detaliilor. Utilizatorul trebuie doar să se asigure că rețeaua privată virtuală este activată.

Furnizorul de internet poate monitoriza istoricul online prin intermediul adresei IP, care este unică pentru fiecare calculator. Folosind rețeaua privată virtuală, acesta nu mai are acces la cautarile de pe internet ale unei persoane.

4.5.5.1.2. Atacuri prin urmărirea activităților de pe internet

Industria promovărilor utilizează, într-un mod abuziv, aplicații pentru monitorizarea activităților de pe internet prin intermediul unor coduri malițioase stocate în fișiere de mici dimensiuni, care la rândul lor se află în navigatoarele web. Acestea au capacitatea de a afișa utilizatorilor anunțurile ce conțin căutările lor din istoricul de pe internet, iar în momentul în care au fost apăsate, pot obține poziția generală în care se află și IP-ul (țara, respectiv orașul).

Folosindu-se de aceste programe, atacatorii pot afla locația navei și pot urmări activitatea ei, precum și a echipajului. În plus, pot fi urmărite și căutările acestora de pe internet. Astfel, există riscul ca pe baza lor să fie concepute planuri de sabotaj, șantaj sau de piraterie.

Pentru siguranța utilizatorilor de pe internet, este recomandat să se achiziționeze un antivirus, împreună cu încă două funcții de anti-urmărire și rețea virtuală privată. Cu ajutorul acestora, atacurile ce implică programe de urmărire vor fi respinse și monitorizate în permanență.

Figura 4.8 Imaginea (captura de ecran) reprezintă pagina de anti-urmărire pe care antivirusul Norton o pune la dispoziția persoanelor care au achiziționat această funcție. Sursă: [29]

4.5.5.1.3. Amprentare digitală

Amprentarea digitală constituie o etapă importantă din cadrul unui atac de care persoanele cu intenții rele se folosesc. Ea se bazează pe anumite pachete trimise către o țintă (un alt calculator) pentru a descoperi cât mai multe informații despre componentele sale și modul în care a fost construită rețeaua pe care o foloseste, respectiv protocoalele ei. Acestia își pot concepe diverse planuri privind rețeaua în cauză și modul în care să o atace.

Printre variantele de apărare în fața unei astfel de metode, rămân doar achiziționarea unui antivirus care dispune de funcționalități precum rețea privată virtuală, zid de rețea, monitorizarea

traficului în cadrul scanărilor avansate, actualizarea sistemelor la zi și utilizarea de parole pentru diferite aplicații și directoare.

4.5.5.1.4. Antivirus

Antivirusul este folosit pentru a asigura protecția necesară împotriva programelor malițioase care pot avea mai multe forme, precum și împotriva altor pericole de pe internet, cum ar fi phishing-ul, phishing-ul țintit, amprentarea digitală și altele. Antivirusul alertează în timp real dacă sunt descoperite breșe de securitate, vulnerabilități sau viruși, prin intermediul scanărilor automate, în special în cazul soluțiilor premium cu abonament anual.

O persoană care folosește o asemenea aplicație premium poate beneficia de o serie de măsuri de securitate suplimentare, inclusiv o rețea privată virtuală și protecție pentru e-mail. Pe lângă acestea, poate beneficia și de scanări complexe, atât interne, cât și la nivelul rețelei de internet în timp real și de cele mai multe ori dispune de capacitatea de a salva date în cloud de cel puțin 100 GB. În plus, se bucură de protecție împotriva programelor de urmărire și a celor de spionaj, precum și împotriva amprentării digitale. De asemenea, aplicația oferă și pagini dedicate exclusiv reglării vitezei pentru a optimiza performanța calculatorului.

4.6. Concluziile capitolului

A fost creată o aplicație independentă și multiplatformă pentru a sprijini cât mai mult angajații de pe navele comerciale. Spre deosebire de multe programe constuite de firmele renumite de pe piața, aceasta nu necesită o conexiune la internet sau alte unelte informatice (programe) și poate fi utilizată de pe orice calculator sau laptop, indiferent de sistemul de operare, componentele pe care le deține sau dimensiunile acestuia.

S-a acordat o atenție deosebită simplității în dezvoltarea aplicației, care beneficiază de meniuri și butoane convenabile, ce facilitează citirea și afișarea teoriei formatate corect cu o simplă apăsare de buton în cadrul panoului dedicat. Această abordare a permis implementarea unui proces de automatizare eficient. În plus, aplicația, construită pe un cadru principal, include mai multe pagini care se pot schimba conform principiului cardurilor. Prin utilizarea acestei metode, a ferestrelor special dedicate pentru citire și scriere, a mesajelor de prevenire a ștergerilor și a ieșirii accidentale din

aplicație, precum și a mecanismului de afișare a paginilor, a fost posibilă dezvoltarea unei aplicații interactive.

Aplicația dispune, de asemenea, de capacitatea de a afișa texte de dimensiuni mari, ceea ce permite explicarea detaliată a tuturor noțiunilor despre securitatea cibernetică și a riscurilor asociate, precum și metodele de prevenire ale acestora. În plus, aceasta oferă o funcționalitate unică în comparație cu programele de pe piață: permite adăugarea de informații în zona specifică textului (pe lângă teoria afișată) și salvarea acestui text sub formă de fișier txt sau anmb, pentru utilizatorii care doresc să ia notițe.

Lucrarea detaliază dezvoltarea unei aplicații software realizate în limbajul de programare Java, care utilizează concepte avansate de programare orientată pe obiecte și care folosește o interfață grafică construită cu Java Swing. Această aplicație a fost complet realizată în cadrul mediului de dezvoltare IntelliJ și este destinată instruirii angajaților de pe navele comerciale în domeniul securității cibernetice. Ea este concepută pentru a fi compatibilă cu orice sistem de operare și pentru a permite redimensionarea, fiind asigurată în acest mod accesibilitatea sa pe diverse platforme fără cerințe hardware sau software specifice. În plus, programul dezvoltat nu necesită o conexiune la o rețea de internet, astfel încât să fie accesibil chiar și pentru persoanele care se află pe mare. Singurul lucru care este necesar ca acesta să funcționeze este ca dispozitivul pe care rulează aplicația să aibă instalat limbajul de programare Java pentru a recunoaște toate extensiile de fișiere specifice.

Această aplicație funcționează cu ajutorul unei singure fereastre, fără a deschide altele în plus. Utilizatorii ei pot naviga și selecta materialele de învățare dorite prin intermediul unor meniuri interactive. Designul aplicației a fost realizat cu ajutorul unor grupuri de culori definite în cod, care permit personalizarea ferestrei și a tuturor componentelor sale prin intermediul unui meniu, pentru a evita disconfortul vizual.

Soluția software aduce un avantaj considerabil în domeniul instruirii asistate de calculator și la distanță, oferind utilizatorilor posibilitatea de a adăuga informații și a lua notițe în timp real. Utilizatorii au acces constant la informațiile despre viruși și tipurile de atacuri, facilitând astfel procesul de învățare printr-un acces eficient și organizat la informațiile necesare. Această funcționalitate îmbunătățește semnificativ modul de învățare și sprijină utilizatorii în dobândirea cunoștințelor necesare pentru protejarea sistemelor cibernetice.

Securitatea cibernetică a devenit unul dintre cele mai importante domenii în sectorul maritim din cauza avansării sistemelor tehnologice și a numărului copleșitor de atacuri cibernetice, ajungând chiar și la ordinul miilor de atacuri într-o singură zi. De altfel, atât echipajul și pasagerii, cât și marfa de tip electronic de pe aceste nave sunt considerate ca fiind surse potențiale de răspândire a virușilor și de infectare a sistemelor navale.

6. Bibliografie

[1] Allianz für Cybersicherheit, „Sicherheitsanforderungen an Netz- und Systemkomponenten”, Bundesamt für Sicherheit in der Informationstechnik (BSI), (2021), https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005E.pdf?__blob=publicationFile&v=6.

[2] Antohi, A.-I. "Software Solution for Training Employees on Cybersecurity on Commercial Ships." [Prezentare PowerPoint, pptx], The 46th Scientific Conference for Bachelor Degree Students CADET-NAV 2024, ID 146 (24 mai 2024).

[3] Aravind S., „What is Fingerprinting in Cybersecurity?”, LinkedIn, (26 martie 2023), https://www.linkedin.com/pulse/what-fingerprinting-cybersecurity-aravind-s.

[4] Bolton, J., „CEH v10 Actual Exam Dumps & Tests”, (2019): Question 7.

[5] Descoperă. „ChatGPT consumă o cantitate absurdă de apă, arată o nouă cercetare ” Descoperă, (17 aprilie 2023) https://www.descopera.ro/dnews/20353603-chatgpt-consuma-o-cantitate-absurda-de-apa-arata-o-noua-cercetare.

[6] DNV, „Cyber Security eLearning”, DNV, https://www.dnv.com/maritime/maritime-academy/cyber-security-elearning.

[7] Eisenhut, M., „Cybersecurity in Maritime Systems: AIS Attacks”, LinkedIn Pulse, https://www.linkedin.com/pulse/cybersecurity-maritime-systems-ais-attacks-mario-eisenhut-qbxxe.

[8] ENISA, „Phishing and Spear Phishing”, ENISA, https://www.enisa.europa.eu/topics/incident-response/glossary/phishing-spear-phishing.

[9] FindAPhD, „Next Generation of Maritime Skill Development: Future Problems and Technologies”, FindAPhD, https://www.findaphd.com/phds/project/next-generation-of-maritime-skill-development-future-problems-and-technologies/?p168597.

[10] Fitton, Oliver, et al. „The future of maritime cyber security ” (2015).

[11] Fortinet, Worm Virus, Fortinet, https://www.fortinet.com/resources/cyberglossary/worm-virus.

[12] GDS, „What Is KnowBe4 Security Awareness Training? That’s Effective and Entertaining”, GDS, https://www.getgds.com/resources/blog/cybersecurity/what-is-knowbe4-security-awareness-training-that-s-effective-and-entertaining.

[13] Geekflare, „Advantages of Using Antivirus Software for Cybersecurity”, Geekflare, https://geekflare.com/cybersecurity/advantages-using-antivirus/.

[14] Imperva, „Man-in-the-Middle Attack (MITM)”, Imperva, https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/.

[15] Indian Register of Shipping (IRS), „Cyber Security Internal Auditor Course”, Indian Register of Shipping (IRS), https://staging.irclass.net/academy/segment/maritime-management-system/cyber-security-internal-auditor-course/?date=08/08/2022.

[16] IntelliJ IDEA., „Director_App” [Captură de ecran realizată de utilizator, png] (13 august 2024).

[17] Jensen, Lars. „Challenges in maritime cyber-resilience”, Technology Innovation Management Review 5.4 (2015): 35.

[18] Jones, Kevin D., Kimberly Tam, and Maria Papadaki. "Threats and impacts in maritime cyber security." (2016).

[19] Kaspersky, „Adware”, Kaspersky, https://www.kaspersky.com/resource-center/threats/adware.

[20] KnowBe4, „AppStore” [Imagine, png], „Learner Support – KnowBe4 Learner App”, KnowBe4, https://support.knowbe4.com/hc/en-us/articles/7154599334419-Learner-Support-KnowBe4-Learner-App.

[21] KnowBe4, „R” [Imagine, jpeg] „KnowBe4 Automated Training Campaigns Dash”, KnowBe4 (20 iulie 2015). https://th.bing.com/th/id/R.8b5cb0df6abf22842d9af37570eff397?rik=yUDz1izQUSspoQ&riu=http%3a%2f%2fww1.prweb.com%2fprfiles%2f2015%2f07%2f20%2f12857819%2fKnowBe4+Automated+Training+Campaigns+Dash.JPG&ehk=4%2b3wm1y5xiTe03vSI3NFU4b9QRghX8M%2fxEQ70txKfAI%3d&risl=&pid=ImgRaw&r=0.

[22] Korea Register of Shipping, „KRS Cyber Security Guidelines”, Korea Register of Shipping, https://www.krs.co.kr/eng/Content/CF_View.aspx?MRID=431.

[23] Malwarebytes, „What Are Tracking Cookies? ”, Malwarebytes, https://www.malwarebytes.com/cybersecurity/computer/what-are-tracking-cookies.

[24] Malwarebytes, Botnet, Malwarebytes, https://www.malwarebytes.com/botnet?srsltid=AfmBOoqgJfwndhSconoEsbqO7cbsgkj5Rxbyc_gMCuy5ORzvPQhiq4VU.

[25] Microsoft Azure, „What is a VPN? ”, Microsoft Azure, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn.

[26] Mission Secure, „ Complying with the IMO 2021 Cybersecurity Regulations” [pdf], Mission Secure, https://www.missionsecure.com/hubfs/Assets/Collateral/complying-with-imo-cybersecurity-overview-mission-secure.pdf.

[27] Mission Secure, „Maritime Security Perspectives for a Comprehensive Approach”, Mission Secure, https://www.missionsecure.com/maritime-security-perspectives-for-a-comprehensive-approach.

[28] Nettitude, „Zero-Day Impacts on Maritime and Offshore Industry”, Nettitude Blog, (15 august 2019), https://blog.nettitude.com/zero-day-impacts-on-maritime-and-offshore-industry.

[29] Norton Antivirus, „Norton” [Captură de ecran realizată de utilizator, png] (13 august 2024).

[30] Okta, „GPS Spoofing”, Okta, https://www.okta.com/identity-101/gps-spoofing/ .

[31] OpenText, „What Is Cloud Backup?”, OpenText, https://www.opentext.com/what-is/cloud-backup.

[32] Plymouth Business School, University of Plymouth, „Cyber Security Awareness MCA Course”, Plymouth University, https://estore.plymouth.ac.uk/conferences-and-events/faculty-of-arts-humanities-and-business/plymouth-business-school/cyber-securityawareness-mca-course.

[33] Project Plan 365. "Download-1". Project Plan 365, https://www.projectplan365.com/solutions/anmb/.

[34] RINA, „Maritime Cyber Risk Management”, RINA, Cybersecurity in Maritime Industry | Marine training course - RINA.org

[35] SANS Institute, „20 Coolest Cyber Security Careers”, SANS Institute, https://www.sans.org/cybersecurity-careers/20-coolest-cyber-security-careers/.

[36] SDSD, „Phishing: One of the Top 8 Cyberthreats to Marine & Offshore Organizations”, SDSD, (15 februarie 2021), https://www.sdsd.com/phishing-one-of-top-8-cyberthreats-to-marine-offshore-organisation/.

[37] Smith, J., Doe, A., „Advances in Cybersecurity: New Approaches and Solutions”, Journal of Computer Security, vol. 31, nr. 2, (2023): 123-145,

https://doi.org/10.1007/s10207-023-00799-4, https://link.springer.com/article/10.1007/s10207-023-00799-4.

[38] Sprinto. „Best cybersecurity tools". Sprinto. https://sprinto.com/blog/best-cybersecurity-tools/.

[39] Tallinn University of Technology (TalTech), „VLL1480 – Maritime Cyber Security", Tallinn University of Technology (TalTech), https://ois2.taltech.ee/uusois/subject/VLL1480.

[40] Tanasă, Ș., Andrei, Ș., Olaru, C., „Java de la 0 la expert", Iași, POLIROM, (2011): 20, 21, 102-107, 120-201, 251, 286, 346-355, 659-705, 708-713, 720-738, 769-785.

[41] TechTarget, „Spyware", TechTarget, https://www.techtarget.com/searchsecurity/definition/spyware.

[42] The Nautical Institute, „Maritime Cyber Awareness for Seafarers", The Nautical Institute, https://www.nautinst.org/shop/maritime-cyber-awareness-for-seafarers.html .

[43] Trellix, „What Is Ransomware?", Trellix, https://www.trellix.com/security-awareness/ransomware/what-is-ransomware/.

[44] Trend Micro, „Why Do Attackers Target Industrial Control Systems?", Trend Micro, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/why-do-attackers-target-industrial-control-systems.

[45] University of Plymouth, „Cyber Ship Lab", University of Plymouth, https://www.plymouth.ac.uk/research/cyber-ship-lab.

[46] Virsec, „CSSF-9-f0af685b" [Imagine, jpeg], „Online Maritime Cyber Security Course", Virsec, https://virsec.org/courses/online-maritime-cyber-security-course/.

[47] Virsec, „Cyber Security for Superyacht Crew", Virsec, https://virsec.org/courses/cyber-security-superyacht-crew/.

[48] Virsec, „Cyber Security Strategy for Vessels", Virsec, https://virsec.org/courses/cyber-security-strategy-for-vessels/.

[49] Virsec, „CyberSec-Strategy-PNG-8-af881aad" [Imagine, jpeg], "Cyber Security Strategy for Vessels", Virsec, https://virsec.org/courses/cyber-security-strategy-for-vessels/.

[50] Virsec, „Online Maritime Cyber Security Course", Virsec, https://virsec.org/courses/online-maritime-cyber-security-course/.

[51] Webroot, „What Is a Trojan Virus? ", Webroot, https://www.webroot.com/us/en/resources/tips-articles/what-is-trojan-virus.

[52] Wikipedia, „Rootkit", Wikipedia, https://en.wikipedia.org/wiki/Rootkit.

[53] Wikipedia, „Trojan horse (computing)”, Wikipedia, https://en.wikipedia.org/wiki/Trojan_horse_(computing).

7. Anexe

Anexa 1. Imagini din aplicația software

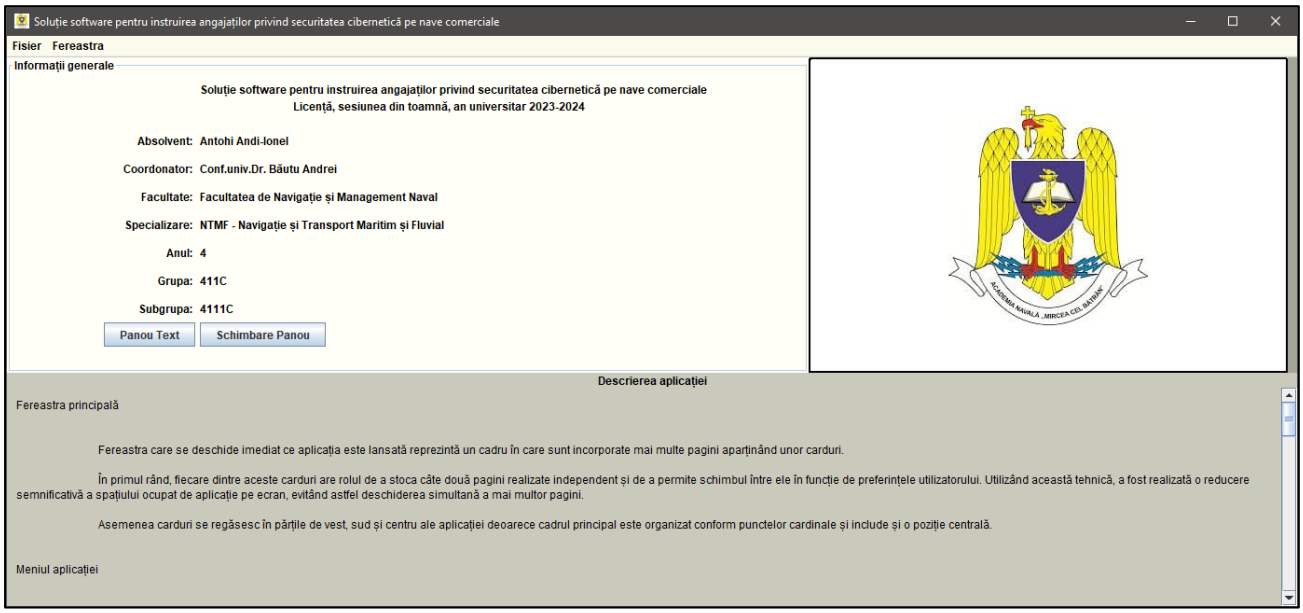

Figura 4.1 În această imagine este prezentată aplicația imediat ce rulează, având meniul principal în partea de sus, informațiile generale afișate inițial în partea vestică, descrierea aplicației realizate în partea sudică și logo-ul facultății în zona centrală.

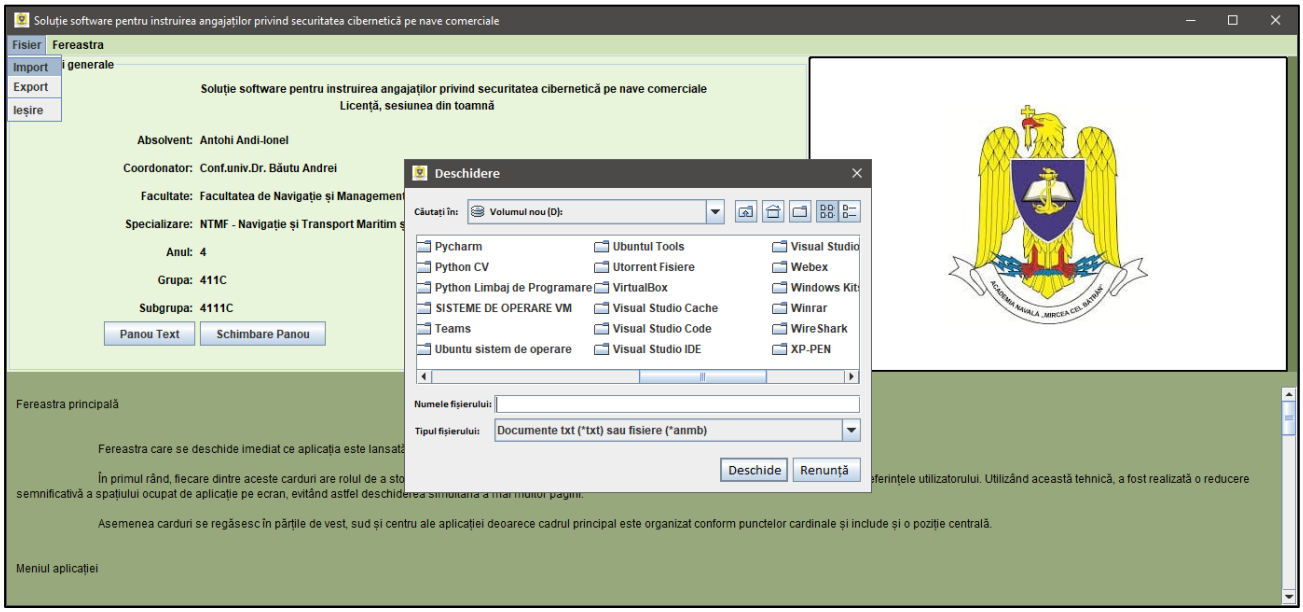

Figura 4.2 În cadrul acestei capturi de ecran este prezentată pagina deschisă special pentru citirea fișierelor din orice director al dispozitivului pe care rulează aplicația.

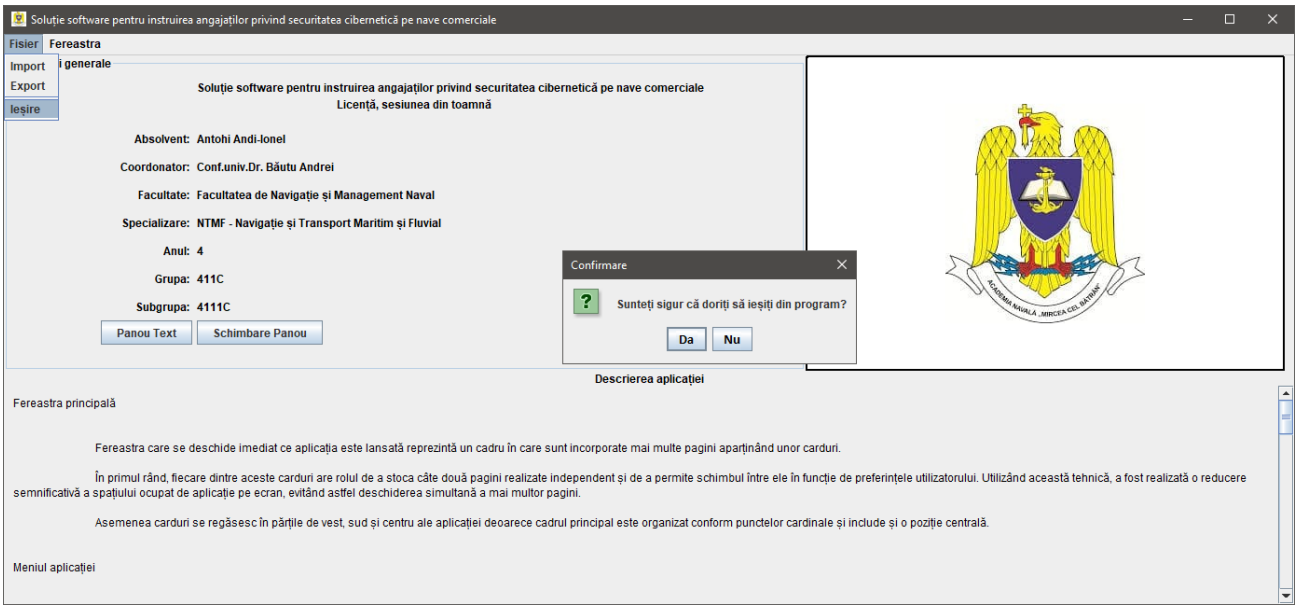

Figura 4.3 În imaginea de mai sus este prezentată pagina deschisă pentru confirmarea ieșirii din aplicație.

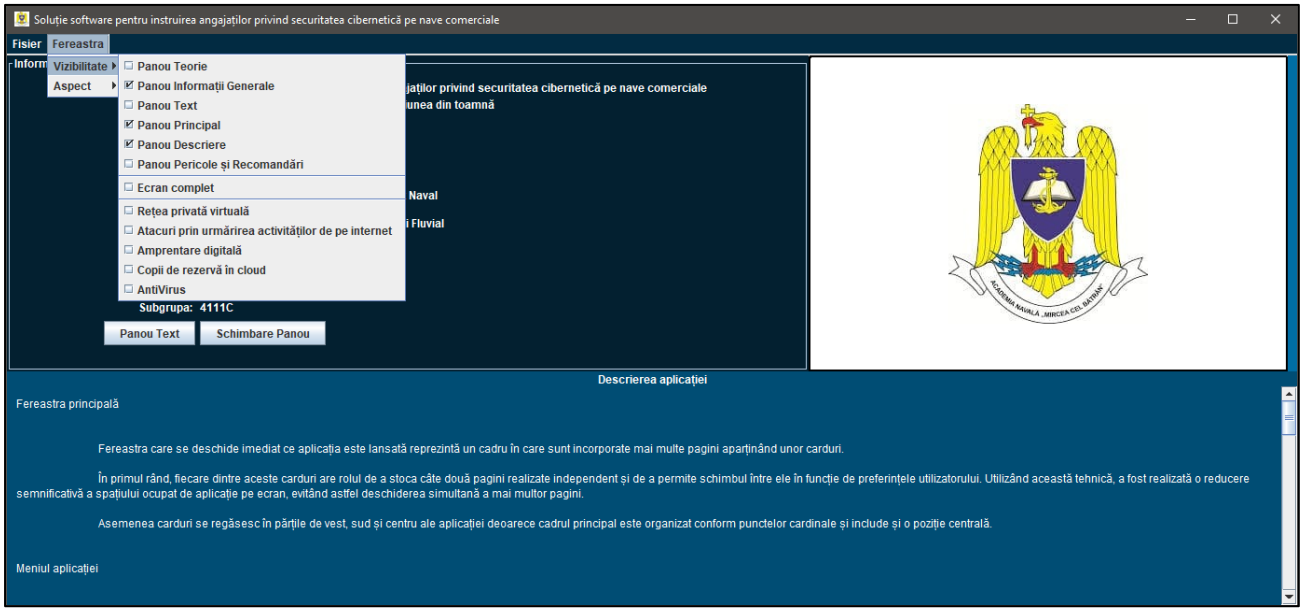

Figura 4.4 Imaginea prezentată este o captură de ecran a aplicației construite, unde este pus în evidență meniul denumit vizibilitate și care are scopul de a afișa paginile, respectiv de a ține evidența celor care sunt active.

Figura 4.5 Imaginea prezentată este este pus în evidență meniul denumit aspect și care are scopul schimba culorile aplicației, în funcție de preferințele utilizatorului.

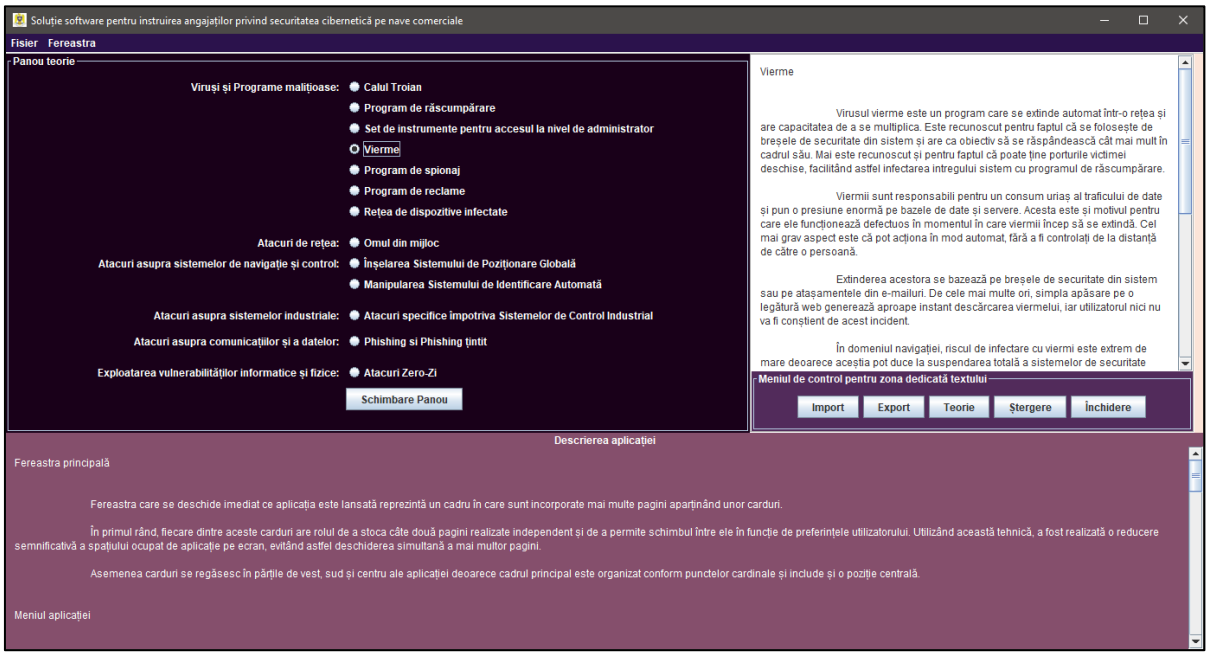

Figura 4.6 În această imagine este prezentată pagina dedicată teoriei, care conține tipurile de viruși și atacuri în partea vestică, precum și pagina dedicată afișării textului, împreună cu meniul său de butoane.

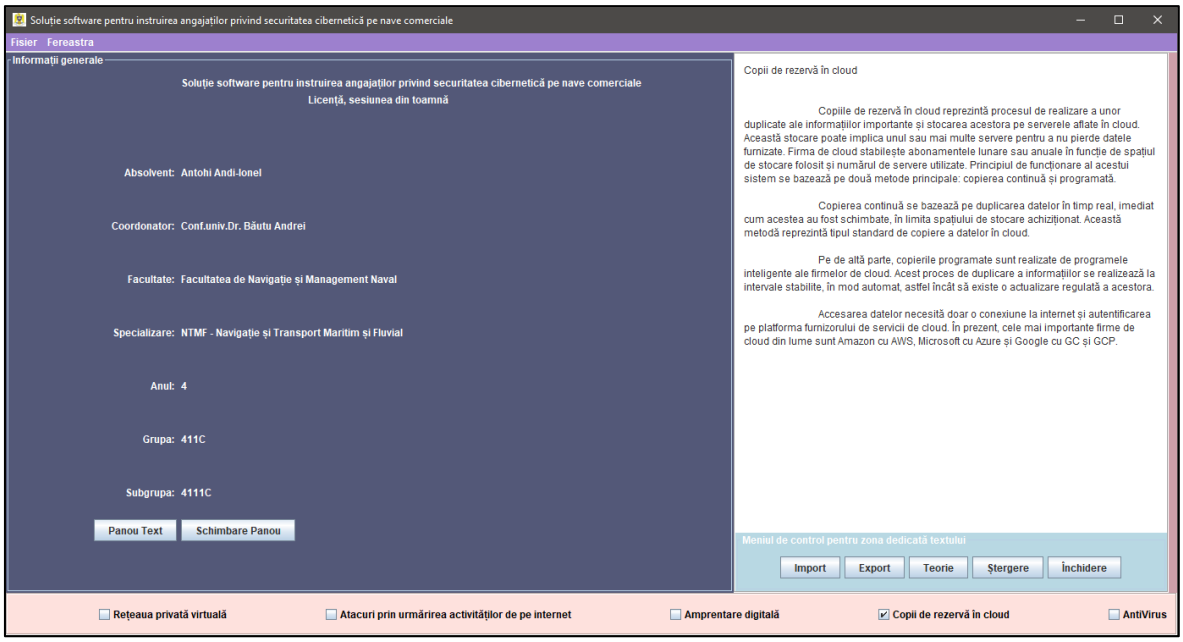

Figura 4.7 Imaginea de mai sus prezintă meniul dedicat pericolelor și recomandărilor în partea sudică și, totodată, teoria specifică a copiilor de rezervă în cloud, din partea centrală a aplicației.

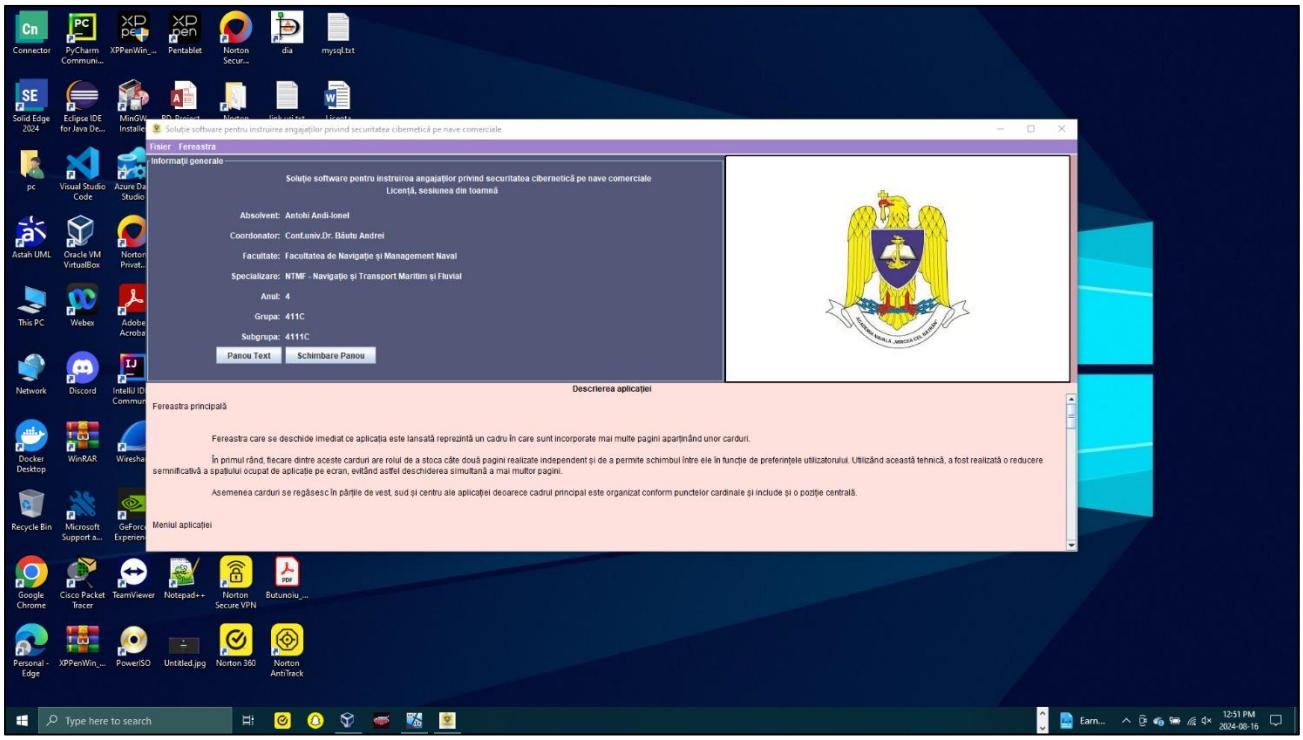

Figura 4.9 În această captură de ecran este prezentată aplicația construită, care rulează în cadrul sistemului de operare Windows 10.

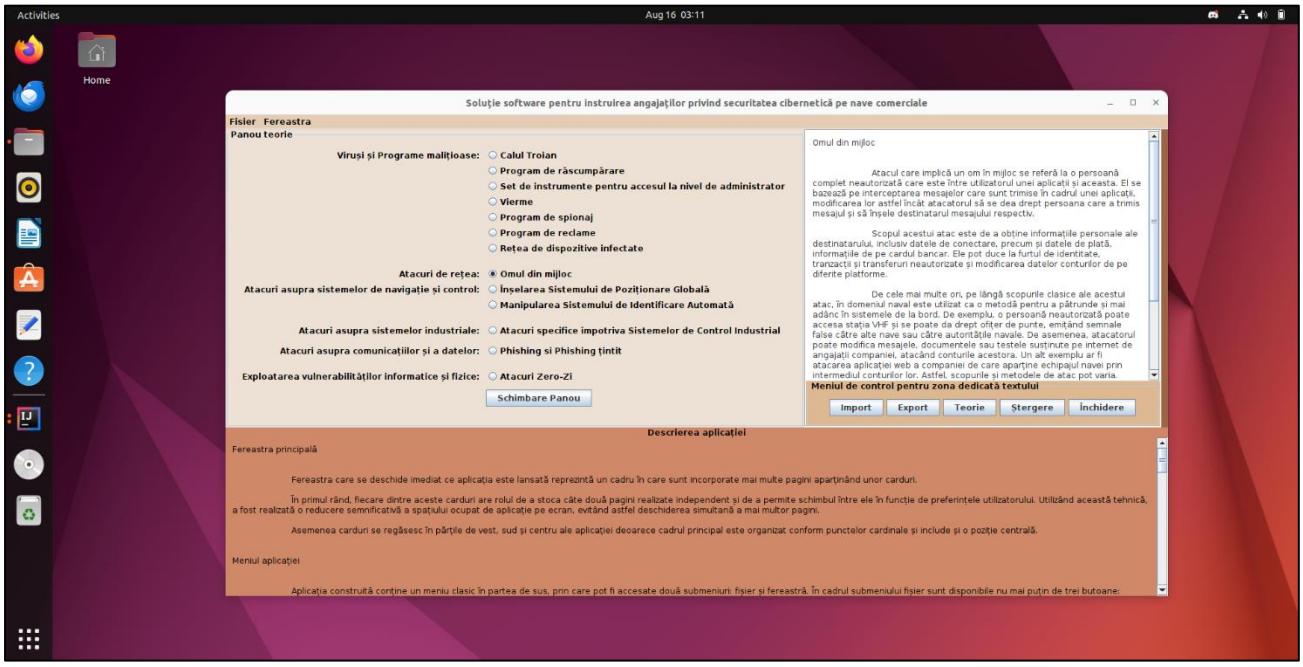

Figura 4.10 În imaginea de mai sus, aplicația este executată în sistemul de operare Linux Ubuntu.

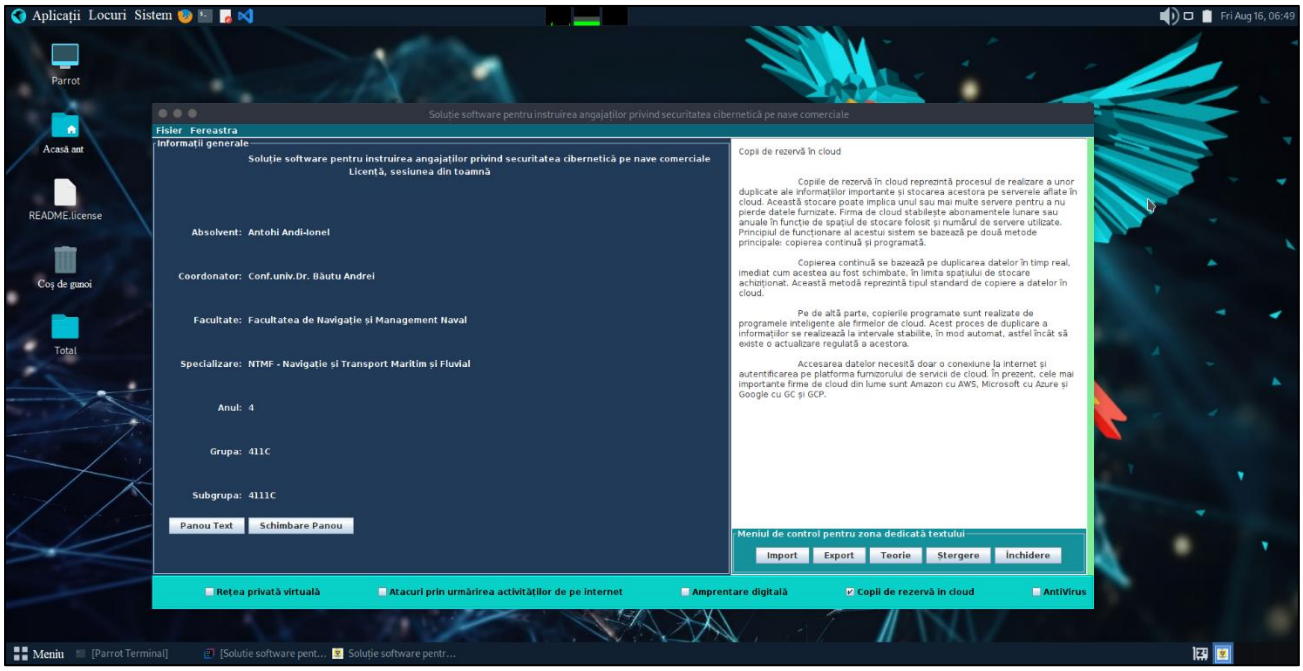

Figura 4.11 În acestă captură de ecran, aplicația este activă pe sistemul de operare Parrot.

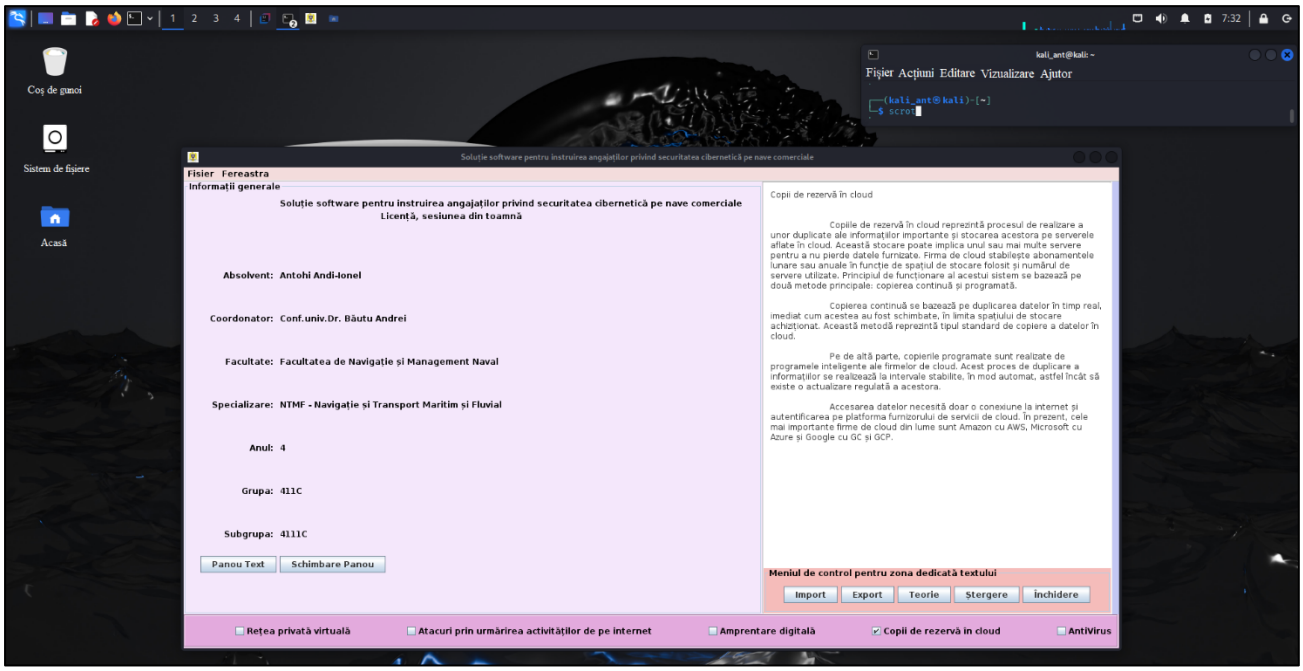

Figura 4.12 În cadrul imaginii este prezentat programul, rulând pe sistemul de operare Kali Linux.

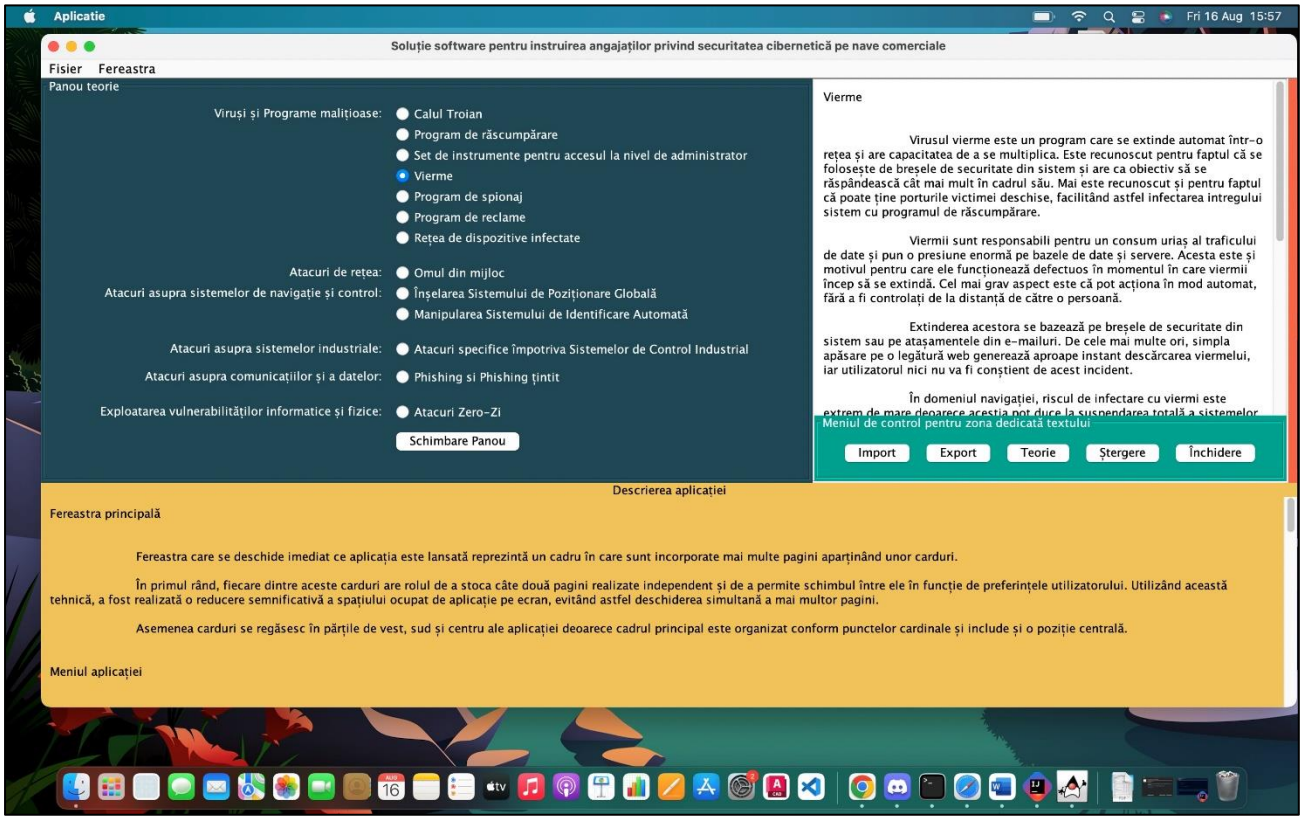

Figura 4.13 Imaginea prezintă soluția informatică, care funcționează în cadrul sistemului de operare macOS Ventura.