REZUMATUL TEZEI DE DOCTORAT

„*Soluții de securitate informațională pentru combaterea ingineriei sociale*”

Autor: *Radu Moinescu*

E-mail: *radu.moinescu@gmail.com*, telefon: *+40.721.507.524*

Conducător de doctorat: *Prof. univ. dr. ing. Ciprian Răcuciu*

Teza de doctorat prezintă o analiză riguroasă a intersecției dintre psihologie, tehnologie și securitatea cibernetică, punând un accent deosebit pe atacurile de inginerie socială. Cercetarea examinează modul în care atacatorii exploatează vulnerabilitățile umane pentru compromiterea sistemelor informatice și analizează strategiile eficiente de apărare împotriva acestor atacuri.

Capitolul introductiv abordează complexitatea securității cibernetice într-un context profund digitalizat, subliniind rolul esențial al factorului uman și evidențiind limitările inerente în atingerea unei securități absolute în spațiul cibernetic.

Capitolul 2 oferă o descriere detaliată a conceptului de inginerie socială, incluzând tehnicile și metodele utilizate pentru manipularea utilizatorilor în vederea obținerii de informații sensibile. De asemenea, este analizat impactul psihologic al acestor tehnici, cum ar fi persuasiunea și eroarea umană, fiind discutate scopurile și circumstanțele care facilitează succesul acestor atacuri.

Capitolul 3 investighează relațiile dintre ingineria socială și factorii psihologici, precum anxietatea, depresia, stresul și trăsăturile de personalitate. Studiul identifică corelații semnificative între stările emoționale negative și vulnerabilitatea utilizatorilor la atacuri, utilizând analize statistice pentru validarea ipotezelor. Concluziile subliniază importanța sprijinului psihologic și a educației pentru diminuarea riscurilor.

Capitolul 4 analizează tehnicile utilizate în atacurile cibernetice, prezentând exemple istorice relevante și explorând relația dintre ingineria socială și exfiltrarea informațiilor. Studiile de caz oferă lecții valoroase despre vulnerabilitățile exploatate, iar analiza comparativă relevă punctele slabe ale sistemelor de apărare.

Capitolul 5 se concentrează pe măsurile tehnologice și strategice de prevenire a atacurilor, accentuând soluții inovatoare, precum Zero Trust Network Access și Content Disarm and Reconstruction. Este realizată o analiză comparativă a tehnologiilor actuale, însoțită de exemple practice de implementare.

Capitolul 6 extinde perspectiva asupra securității informaționale, examinând cultura organizațională și principiile teoretice, cum ar fi modelele clasice de securitate și măsurile de protecție împotriva interceptărilor electromagnetice. Se subliniază importanța educației și adaptabilității organizaționale la amenințările emergente.

Capitolul 7 explorează utilizarea inteligenței artificiale în securitatea cibernetică, discutând atât avantajele, cât și riscurile asociate. Este analizat modul în care inteligența artificială poate amplifica atât apărarea, cât și atacurile de inginerie socială, concluzionând asupra necesității unei implementări etice și echilibrate a acestor tehnologii.

Capitolul 8 examinează utilizarea tehnologiilor automate, cum ar fi software-ul „*Tropes*”, și rolul factorului uman în apărarea împotriva atacurilor. Este evidențiată importanța unui „*firewall uman*” bazat pe conștientizare și instruire, alături de soluții experimentale pentru detectarea phishing-ului.

Capitolul 9 sintetizează rezultatele cercetării, evidențiind contribuțiile originale, inclusiv dezvoltarea unor tehnici noi de prevenire și identificare a atacurilor. Sunt propuse direcții viitoare de cercetare, iar concluziile subliniază impactul interdisciplinar al studiului asupra domeniilor securității cibernetice și psihologiei, demonstrând relevanța teoretică și practică a acesteia.

Aspecte esențiale abordate:

- *Inginerie socială*: Definirea și clasificarea tehnicilor, analiza motivațiilor atacatorilor și identificarea vulnerabilităților umane frecvent exploatate.
- *Psihologia atacurilor*: Explorarea mecanismelor prin care atacatorii manipulează emoțiile, încrederea și utilizarea tehnicilor de persuasiune.
- *Tehnologii de atac*: Analiza unei varietăți de instrumente, incluzând malware, phishing, ransomware și atacuri de tip „*zero-day*”.
- *Apărarea împotriva atacurilor*: Prezentarea unor măsuri tehnologice și umane pentru protejarea împotriva atacurilor de inginerie socială.

- *Inteligența artificială*: Discutarea potențialului inteligenței artificiale în detectarea și prevenirea atacurilor, precum și a riscurilor asociate utilizării acesteia în scopuri malițioase.

Teza aduce o contribuție semnificativă la domeniul securității cibernetice, subliniind necesitatea unei abordări multidisciplinare care să integreze tehnologia, psihologia și factorul uman. Înțelegerea aprofundată a mecanismelor care stau la baza atacurilor de inginerie socială permite dezvoltarea unor strategii eficiente pentru reducerea acestor amenințări.