Universitatea Tehnică a Moldovei

SOLUȚII DE MINIMIZARE A RISCURILOR DE INGINERIE SOCIALA

RISK MINIMIZATION FOR SOCIAL ENGINEERING ATTACKS

Masterand:

Stupina Daria

Conducător:

lector universitar Bulai Rodica

Chişinău 2020

Ministerul Educaţiei, Culturii şi Cercetării
Universitatea Tehnică a Moldovei
Facultatea Calculatoare Informatică şi Microelectronică
Departamentul Ingineria Software şi Automatică

Admis la susţinere
Şef departament:
dr.conf.univ. Ion Fiodorov.
„18" decembrie 2019

SOLUȚII DE MINIMIZARE A RISCURILOR DE INGINERIE SOCIALA

Teză de master în Securitate Informațională

Masterand: (D.Stupina)
Conducător: (R. Bulai)

Chişinău 2020

Rezumat

Proiectul de master *Soluții de minimizare a riscurilor de inginerie sociala* are trei capitole, și anume:

Capitolul 1, *Analiza domeniului de studiu*, descrie domeniul, obiectivele și importanța temei.

Capitolul 2, *Analiza metodologiilor de conștientizare a securității informaționale*, descrie analiza și punctele cheie standardelor NIST 800-50 și NIST 800-16.

Capitolul 3, *Programul de conștientizare securității informatice*, descrie metodele de protecție împotriva atacurilor de inginerie socială, definirea rolurilor și întrebărilor cheie, dezvoltarea programului de conștientizare și post-implementare.

Teza actuală este axată pe conceptul de inginerie socială și metodele de minimizare a riscurilor pentru acest tip de atac. În special, a fost proiectat un program de sensibilizare în domeniul securității cibernetice bazat pe NIST 800-50 și NIST 800-16. Programul de conștientizare în materie de securitate proiectat este destinat unui model al unei noi companii care oferă servicii de dezvoltare software și suport IT și care nu are încă programul de sensibilizare în materie de securitate. Ca parte a programului de sensibilizare în domeniul securității cibernetice, au fost definite rolurile în funcție de care este structurată conștientizarea securității informațiilor, precum și cunoștințele de securitate a informațiilor de care are nevoie fiecare dintre aceste roluri. În plus, au fost definite: recomandările privind metodele de creare a materialelor de conștientizare, metodele de înregistrare a participării la instruire, metodele de identificare dacă angajații recunosc că au citit / înțeles politica de securitate a informațiilor. Programul de conștientizare în domeniul securității IT al unei organizații poate fi repede depășit dacă nu se acordă o atenție suficientă progreselor tehnologice, infrastructurii IT și schimbărilor organizaționale și schimbării misiunii și priorităților organizaționale. Acesta este motivul pentru care partea de post-implementare este menționată în teză. Sunt descrise soluțiile și instrumentele necesare, care într-un fel sau altul pot proteja împotriva atacurilor de inginerie socială: antivirus, autentificare multifactor, actualizarea programelor antivirus și anti-malware, o soluție de prevenire a pierderilor de date, controlul accesului, antispam.

Abstract

The master project *Risk minimization for social engineering attacks* has three chapters, namely:

Chapter 1, *Analysis of the field of study*, describes the field, the objectives and the importance of the theme.

Chapter 2, *Analysis of information security awareness methodologies*, describes the analysis and key points of NIST 800-50 and NIST 800-16 standards.

Chapter 3, *Information Security Awareness Program*, describes the methods of protection against social engineering attacks, the definition of key roles and questions, the development of the awareness and post-implementation program.

Present thesis is focused on the concept of social engineering and the methods of the risk minimization for this type of attack. In particular, a cyber security awareness program based on NIST 800-50 and NIST 800-16 was designed. The designed security awareness program is destinated for a model of a new company that provides software development services and IT support and which does not yet have the security awareness program. As part of cyber security awareness program roles depending on which information security awareness is structured have been defined, as well as information security knowledge that each of these roles needs. In addition, there were defined: the recommendations regarding the methods of creating awareness materials, the methods of recording attendance at training, the methods of identification if the employees acknowledge that they have read / understood the information security policy. An organization's IT security awareness program can quickly become outdated if insufficient attention is paid to technological advances, IT infrastructure and organizational changes and to changing organizational mission and priorities. This is why the post-implementation part is mentioned in the thesis. Necessary solutions and tools are described, which in one way or another can protect against social engineering attacks: antivirus, multifactor authentication, updating of anti-virus and anti-malware programs, a data loss prevention solution, access control, antispam.

Cuprins

Introducere

Încă de la început, World Wide Web devenind o resursă principală, infractorii au folosit-o în avantajul lor. Unul dintre primele exemple ale acestui tip particular de crimă a avut loc la începutul anilor '80. Un grup cunoscut sub numele de 414s (numit după codul lor de zonă Milwaukee) a fost arestat pentru că au fost afectate aproximativ 60 de calculatoare diferite. Acestea au inclus dispozitive în Centrul Memorial Sloan-Kettering Cancer până la cele situate în laboratorul național Los Alamos.

Guvernul a răspuns rapid la această nouă amenințare. Legi precum „Legea privind fraudele și abuzurile informatice" au fost adoptate pentru a preveni și pedepsi încercările acestor părți rău intenționate. Echipe de intervenție în caz de urgență privind incidentele de securitate, de asemenea, au fost formate printr-un efort de a investiga numărul tot mai mare de hacks și metodele potențiale de protecție.

Deceniul s-ar încheia cu prima versiune recunoscută a unui vierme. Robert Morris a fost hackerul din spatele atacului și, chiar la început, acești viruși autopropagabili au fost capabili de cantități masive de distrugere. De fapt, a închis aproape întregul World Wide Web la acea vreme. Virusul Morris a fost și prima versiune a unui atac răspândit DoS (Denial of Service). Cu acest atac, companiile au început să-și dea seama cât de vulnerabile erau cu adevărat.

Acest lucru și atacurile ulterioare au fost impulsul pentru marea parte din ceea ce considerăm azi ca Securitate cibernetică. Ca urmare, au fost create CERT-urile (echipele de reacție). Un mesaj pe care îl auzim acum tot timpul în comunitatea de securitate cibernetică, „Prevenirea este mai bună decât un remediu", a fost creată în acest timp.

În mare parte a anilor '90, hackerii și-au continuat atacurile, deși majoritatea victimelor erau agenții guvernamentale și corporații uriașe multinaționale. Până la urmă, Internetul nu a fost un instrument răspândit în acest moment.

Unul dintre primele exemple de hacking care a afectat publicul principal a avut loc în 1997. Motorul de căutare, Yahoo!, a fost ținta. Hackerii au susținut că o „bombă logică" va fi detonată pe orice calculator folosind Yahoo! în ziua de Crăciun, dacă celebrul hacker Kevin Mitnick nu va fi eliberat din închisoare.

Un alt exemplu a apărut în 1998. Biroul Statisticilor Muncii a devenit victima uneia dintre primele versiuni de spaming atunci când a primit sute de mii de solicitări de informații.

Ca urmare a acestor și altor atacuri cibernetice, Departamentul de Justiție al SUA a introdus Centrul Național de Protecție a Infrastructurii. Misiunea sa a fost să protejeze sistemele de telecomunicații, transport și tehnologie din țară de hackeri.

Într-adevăr, de la începutul și până la sfârșitul anilor 2000, hackingul a evoluat către problema răspândită pe care o știm astăzi. Din nou, o mare parte din aceasta se întoarce la creșterea proporțională a țintelor (de exemplu, tot mai multe persoane care utilizează internetul).

În același timp, hackingul devenea mult mai simplu. Au dispărut zilele în care singurele persoane care au putut să execute aceste atacuri aveau abilități tehnice egale sau mai bune decât cei mai importanți programatori din lume.

În 2005, un hacker pe nume Albert Gonzalez și-a folosit abilitățile pentru a crea un inel criminal de hackeri - crimă organizată digital, dacă veți dori - pentru a fura informațiile de la peste 45 de milioane de carduri de plată emise de TJX, un retailer american care deține TJ Maxx și versiunea din Marea Britanie, TK Maxx.

Înainte de a fi prins și condamnat la 20 de ani de închisoare, echipa lui Gonzalez ar fi responsabilă pentru daune în valoare de 265 de milioane de dolari.

În afară de scopul evident al infracțiunii, acest incident este remarcabil datorită efectului pe care l-a avut asupra întreprinderilor. Natura datelor furate a fost reglementată, astfel încât fiecare incident a cerut ca autoritățile să fie notificate. În plus, aceste companii trebuiau să aloce bani pentru a compensa victimele.

Acesta a fost un exemplu de reper, deoarece a devenit imediat clar pentru lumea afacerilor că hacking-ul a fost mult mai mult decât o simplă problemă.

Concluzii

În teza dată este descrisă noțiunea de inginerie socială, sunt descrise cele mai comune tehnici de inginerie socială și după ce domeniul de studii este analizat, programul de conștientizare a securității cibernetice este proiectat și dezvoltat pe baza standardurilor NIST 800-50, NIST 800-16 și mai multe surse bibliografice. A fost acoperit un program de conștientizare a securității pentru o companie nouă care prestează serviciile de dezvoltare software și asistența IT și care încă nu are programul de conștientizare a securității: tipuri de roluri în dependență de care să fie structurată conștientizarea securității informației, au fost identificate și au fost definite cunoștințe în securitatea informațională de care fiecare dintre aceste roluri are nevoie. Adăugator a fost formulate recomandările referitor la metodele de creare a materialelor de conștientizare, metodele de înregistrare a prezenței la antrenament, metodele de asigurare a tuturor angajaților la formare, metodele de identificare dacă angajații recunosc că au citit / înțeles politica de securitate a informațiilor. Este important de menționat că rolurile manageriale sunt ținta cea mai frecventă atacatorilor, deci managerii trebuie să aibă formare și înstruire mai înaltă decât totul personalul companiei. În plus, manageri trebuie să arate exemplu de atitudine serioasă către securitatea informațiilor și să încurajeze tot personalul companiei să păstreze principiile conștientizării securității. Developer-ii și administratori de sistem trebuie să înțelege bazele securității informationale și să îmbunătățească întotdeauna cunoștințele lor tehnologice în ceea ce privește aspectele securității cibernetice. Programul de conștientizare în domeniul securității IT al unei organizații poate deveni rapid învechit dacă nu se acordă o atenție suficientă avansurilor tehnologice, infrastructurii IT și schimbărilor organizaționale și modificării misiunii și priorităților organizaționale. Din cauza aceasta în teză este menționată partea de post-implementare și metode pentru a solicita feedback. Îmbunătățirea continuă ar trebui să fie întotdeauna importantă pentru conștientizarea securității și inițiativele de formare, deoarece acesta este un domeniu în care „nu poți face niciodată suficient”. Sunt descrise soluții și instrumente necesare, care într-un fel sau altul poate să protejeze împotriva atacuri de inginerie socială: antivirus, autentificare multifactor, actualizarea programelor antivirus și anti-malware, o soluție data loss prevention, acces control.

Ca punct slab al tezei, trebuie de menționat că lucrarea nu acoperă momentul pregătirii unei echipei de securitate pentru răspunsul la incidente (incident response) legat de atacurile de inginerie socială, nu acoperă plsanificare răspunsului la incident legat de atacurile de inginerie socială.

Bibliografie

1. Radu Boncea, Securitatea Informațională [Resursa electronică]. – Regim de acces: http://raduboncea.ro/2009/01/21/securitatea-informa%C8%9Bionala/ (15.09.19)
2. ISO, IEC, ISO 27001
3. Ani, U.D., He, H. and Tiwari, A. (2018) Human factor security: evaluating the cybersecurity capacity of the industrial workforce. Journal of Systems and Information Technology. ISSN 1328-7265 [Resursa electronică]. – Regim de acces: https://doi.org/10.1108/JSIT-02-2018-0028 (25.09.2019)
4. Cyber Health Check Prepared for Evelyn Murphy, Chief Information Officer, Baratheon PLC
5. Microsoft Security Intelligence Report VOLUME 23
6. Hussain Aldawood, and Geoffrey Skinner, Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues
7. Fungai Bhunu Shava and Attlee M. Gamundani, A User Awareness Model for averting Computer Threats
8. Lector universitar Rodica Bulai - Lectia 9. Amenintarile din spatiul online
9. NIST special publication 800-50
10. NIST special publication 800-16
11. Phishing E-mail Analysis - Shamal Firake, Pravin Soni, Dr. B.B.Meshram
12. Analyzing malicious Emails, Kyle Bubp, [Resursa electronică]. – Regim de acces: https://medium.com/@kylebubp/analyzing-malicious-emails-fb4ddcf0663e (22.10.19)
13. What is Social Engineering, Forcepoint, [Resursa electronică]. – Regim de acces: https://www.forcepoint.com/cyber-edu/social-engineering (22.10.19)
14. Avoiding Social Engineering and Phishing Attacks, CISA, [Resursa electronică]. – Regim de acces: https://www.us-cert.gov/ncas/tips/ST04-014 (25.10.19)
15. SANS Institute, A Multi-Level Defense Against Social Engineering, David Gragg, [Resursa electronică]. – Regim de acces: https://www.sans.org/reading-room/whitepapers/engineering/multi-level-defense-social-engineering-920 (25.10.19)
16. Defense Methods Against Social Engineering Attacks, Jibran Saleem, Dr. Mohammad Hammoudeh, Manchester Metropolitan University
17. PCI DSS V1.0 Best_Practices for Implementing Security Awareness Program
18. Computer security training & awareness course compendium, Kathie Everhart Editor U.S. DEPARTMENT OF COMMERCE Technology Administration National Institute of Standards and Technology, [Resursa electronică]. – Regim de acces: https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir4846.pdf (30.10.19)

19. Education in Cybersecurity, Rodica Bulai, Dinu Țurcanu, Dumitru Ciorbă
20. IT Governance Cyber Health Check Sample report, Prepared for Evelyn Murphy, Chief Information Officer, Baratheon PLC
21. Cyber Risk Aware, The Ultimate Guide To Security Awareness Training
22. Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues Hussain Aldawood and Geoffrey Skinner, School of Electrical Engineering and Computing, University of Newcastle, Newcastle 2308, Australia
23. A User Awareness Model for averting Computer Threats, Fungai Bhunu Shava and Attlee M. Gamundani
24. NIST Special Publication 800-16 Revision 1 (3rd Draft), A Role-Based Model for Federal Information Technology/Cybersecurity Training, Patricia Toth, Penny Klein
25. Rochester Institute of Technology, Thesis/Dissertation Collections 2011, Mitigating the risk of social engineering attacks Matthew Spinapolice
26. Measuring the Effectiveness of an Information Security Training and Awareness Program, Roshan Dhakal Doctor of IT, Charles Sturt University
27. SANS Institute, Information Security Reading Room, A Multi-Level Defense Against Social Engineering, David Gragg
28. Defense Methods Against Social Engineering Attacks, Jibran Saleem, Mohammad Hammoudeh
29. Information security training and awareness program: An Investigation, Roshan Dhakal, Rafiqul Islam, Champake Mendis