Universitatea Tehnică a Moldovei

DETECTAREA VULNERABILITĂŢILOR DE SECURITATE CIBERNETICĂ ÎN CADRUL UNEI ORGANIZAŢII

Masterand:
Ion Strişcă

Conducător:
conf. univ., dr. Victor MORARU

CHIŞINĂU - 2019

ADNOTARE

Studiul de cercetare elaborat constituie o generalizare a procesului de detectare a vulnerabilităților de securitate cibernetică în cadrul sistemelor informaționale ale unei organizații, ca parte componentă a procesului de management al vulnerabilităților prin prisma informațiilor relevante și actuale ale diferitor surse de documentare a acestora, precum și a funcționalităților oferite de diverse instrumente de scanare disponibile.

Obiectivele tezei constituie analiza procesului de detectare a vulnerabilităților de securitate cibernetică, în vederea sprijinului implementării și menținerii sistemului de management al securității informaționale în cadrul organizațiilor; examinarea surselor, tipurilor, clasificarea vulnerabilităților și a impactului acestora asupra activelor informaționale; examinarea instrumentelor disponibile de detectare a vulnerabilităților în vederea identificării funcționalităților acestora.

Noutatea și originalitatea științifică este prezentată prin fundamentarea și aprofundarea investigațiilor teoretice în domeniul detectării vulnerabilităților de securitate cibernetică în vederea sistematizării funcționalităților prezentate de diverși producători de instrumente de scanare disponibile la momentul actual, care pot fi utilizate de organizații în cadrul sistemelor informatice pe care le gestionează.

În teză au fost utilizate următoarele cuvinte-cheie, cum ar fi: vulnerabilitate, securitate cibernetică, securitate informațională, scanare, gestionare, testare, instrument, proces, configurare, sistem, activ, malițios, resurse, penetrare, protecție, încălcare, aplicații, software, politici.

ANNOTATION

The elaborated research study constitutes a generalization of the process of detecting cyber security vulnerabilities within the information systems that belong to organization, as part of the vulnerability management process, from the point of view of relevant and current information from different sources of documentation, as well as the functionality offered by vendors of the various scanning tools available.

The objectives of the thesis are the analysis of the process of detecting cyber security vulnerabilities, in order to support the implementation and maintenance of the information security management system within organizations; examining sources, types, classifying vulnerabilities and their impact on information assets; examining the available tools to detect vulnerabilities in order to identify their functionality.

The novelty and scientific originality is presented by substantiating and deepening the theoretical investigations in the field of cyber security vulnerabilities in order to systematize the functionalities presented by the various manufacturers of scanning tools currently available, which can be used by organizations within the information systems they manage.

The following keywords were used in the thesis, such as: vulnerability, cyber security, information security, scanning, management, testing, instrument, process, configuration, system, active, malicious, resources, penetration, protection, violation, applications, software, policies.

CUPRINS

INTRODUCERE

În prezent, activitățile multor organizații depind de starea sistemelor informatice din posesia acestora. În același timp, infrastructura sistemelor informatice conține adesea noduri și sisteme încălcarea securității cărora poate duce la daune semnificative în desfășurarea activității în cadrul organizație.

Pentru a preveni astfel de cazuri, de regulă, după o analiză efectuată în mod corespunzător, se formează o listă cu amenințările actuale și se elaborează un set de măsuri pentru neutralizarea acestora. În cele din urmă, se implementează un sistem de management al securității informațiilor, care include diverse echipament de protecție care implementează mecanismele de protecție necesare. În cadrul acestui sistem este de obicei inclus și un subsistem de gestionare a vulnerabilităților, care reprezintă un set de măsuri organizaționale și tehnice menite să prevină utilizarea vulnerabilităților cunoscute care pot exista în sistemul sau rețeaua protejată. Gestionarea vulnerabilităților include activități precum monitorizarea periodică a securității sistemelor informatice și eliminarea acestor vulnerabilități detectate.

Pentru o persoană rău-intenționată, vulnerabilitățile din cadrul unei rețele constituie niște resurse ascunse, dar foarte prețioase în același timp. Când sunt expuse, aceste vulnerabilități pot fi direcționate spre exploatare și pot duce la accesul neautorizat într-o rețea, pot expune informații confidențiale, pot furniza oportunități pentru identitățile furate, pot declanșa furtul secretelor de afaceri, încalcă prevederile de confidențialitate din legi și reglementări sau pot paraliza operațiunile comerciale.

Vulnerabilități noi apar în fiecare zi din cauza erorilor în software, configurarea defectuoasă a aplicațiilor și a echipamentelor IT, precum și în urma erorilor umane. Indiferent de sursa lor, vulnerabilitățile nu dispar singure. Detectarea, eliminarea și controlul acestora necesită gestionarea vulnerabilității, adică utilizarea regulată, continuă a instrumentelor de securitate specializate și a fluxului de lucru care ajută activ la eliminarea riscurilor exploatabile.

Provocarea pentru fiecare organizaţie este menținerea unei rețele informatice sigure, deschise și interconectate - ceea ce facilitează schimbul de informații cu clienții, furnizorii și partenerii de afaceri oriunde ar fi localizați aceștia.

În același timp, asigurarea disponibilității și siguranței informației este o muncă grea. Viermii, virușii și alte riscuri de securitate amenință constant sustragerea de informații și perturbarea operațiunilor comerciale. Mai mult, creșterea esențială a noilor vulnerabilități descoperite în fiecare zi - și viteza cu care sunt create noi amenințări - fac ca această provocare să fie și mai accentuată.

Fiecare afacere cu conexiune la Internet este expusă riscului din cauza vulnerabilităților rețelei. Soluția este securizarea rețelei împotriva acestor amenințări de securitate eliminând originea lor: vulnerabilitățile rețelei.

Vulnerabilitățile au afectat sisteme de operare și aplicații software încă din primele zile. Inițial erau în număr limitat, dar acum se înregistrează atacuri de succes prin Internet aproape în fiecare zi. Conectivitatea universală oferită de această cale globală oferă hackerilor și infractorilor acces facil la rețeaua dvs. și la resursele sale de calcul. Atunci când dispozitivele atașate la rețea rulează fără actualizări de securitate curente, aceste dispozitive neactualizate sunt vulnerabile imediat la o varietate de exploatări. Orice afacere este susceptibilă dacă vulnerabilitățile nu sunt identificate și remediate.

O vulnerabilitate este orice greșeală sau slăbiciune în procedurile de securitate a sistemului, de proiectare, implementare sau orice control intern care poate duce la încălcarea politicii de securitate a sistemului. Cu alte cuvinte, posibilitatea intrușilor (hackerilor) de a avea acces neautorizat la resursele informaționale ale organizației.

Erorile de programare provoacă cele mai multe vulnerabilități în software. O greșeală comună constituie ne verificarea dimensiunii bufferului de date - un fel de coș de memorie al calculatorului în care un proces își execută funcțiile. Când memoria se umple până la limită, acesta suprascrie datele în memoria bufer adiacentă. Acest lucru corupe zonele de memorie sau stivă, ceea ce poate permite executarea codului unui atacator pe calculator prin intermediul unui virus, vierme sau alte exploatări neplăcute.

Se estimează că sunt cuprinse aproximativ 5 până la 20 de erori în fiecare mie de linii de cod software, astfel încât nu este surprinzător să se anunțe periodic despre noi vulnerabilități cu corecții și soluții de rezolvare. Riscul de vulnerabilități crește odată cu utilizarea programelor cu Licență Publică Generală, în special deoarece implementatorii conectează module netestate de cod de programare orientate pe obiect. Când calitatea codului este marginală, proastă sau greșită, experții o numesc „non-robustă”. Modulele de cod plasate în domeniul public pot include implementări non-robuste ale standardelor de protocol de Internet, ceea ce le face ținte ușoare pentru atac, atunci când sunt utilizate într-o rețea reală.

Vulnerabilitățile trebuie identificate și eliminate în mod regulat, deoarece noi vulnerabilități sunt descoperite în fiecare zi. De exemplu, Microsoft lansează avertizări și patch-uri în a doua marți a fiecărei luni - denumite în mod obișnuit „Patch Tuesday”.

Programatorii neatenți nu sunt singura sursă de vulnerabilități. De exemplu, configurarea necorespunzătoare a aplicațiilor de securitate, cum ar fi un firewall, poate permite atacatorilor să treacă prin porturile care ar trebui închise. Oamenii care folosesc dispozitive mobile pot accesa un site web neautorizat sau chiar un site infestat cu malware, fără a trece prin rețeaua virtuală privată corporativă

(VPN), poate pentru că VPN-ul oficial este deranjant atunci când oamenii doresc să navigheze pe site-uri ca Facebook, eBay sau în anunțurile personale online.

Exploatarea vulnerabilităților prin Internet este o problemă majoră care necesită control și gestionare proactivă imediată. Acesta este motivul pentru care companiile trebuie să asigure că procesul de detectare și eliminare a vulnerabilităților este în vigoare pentru a reduce riscul general de securitate și pentru a preveni expunerea.

Dezvăluirile publice nesfârșite care apar în știrile privind încălcările de date dezvăluie expunerea neautorizată a milioane de înregistrări confidențiale ale consumatorilor la nivel mondial. Aceasta este o dovadă adecvată de ce organizațiile trebuie să facă mai mult pentru a proteja rețelele împotriva atacurilor. Dar o schimbare dramatică a peisajului amenințării pentru securitate crește bariera pentru organizațiile mari și mici care doresc să minimizeze în mod activ atacurile de succes asupra vulnerabilităților lor.

Datele recente arată că exploatările nu mai sunt limitate la riscurile tradiționale de virusuri generice, viermi, troieni și alte atacuri cu un singur vector. Potrivit cercetărilor globale efectuate de Symantec Corporation, o schimbare fundamentală a amenințărilor relevă „depărtarea de comportări necuviincioase și atacuri distructive către activitatea motivată de câștigul financiar”. Ultimul raport anual al companiei Symantec caracterizează cinci noi tendințe [1], inclusiv:

1. Atacurile de tip formjacking, care au izbucnit, cu o medie de 4.800 de site-uri web compromise în fiecare lună și vizează datele de carduri bancare ale utilizatorilor care sunt extrase inclusiv de pe site-urile companiilor de vânzări legitime.

2. Ransomware-ul și cryptojacking a schimbat țintele de la consumatori la întreprinderi, unde infecțiile au crescut cu 12%.

3. Atacuri țintite prin utilizarea ”lanțurilor de aprovizionare” au rămas o țintă slabă, fiind prezente în aproximativ 78% din atacuri.

4. Atacuri asupra resurselor informaționale amplasate în Cloud;

5. Dispozitivele IoT devin un punct-cheie de intrare pentru atacuri, majoritatea dispozitivelor IoT fiind vulnerabile.

Raportul elaborat de ISACA ”Starea Securității Cibernetice: implicații pentru 2015” [2] denotă ”câștigurile financiare” ca motivația cea mai mare pentru desfășurarea atacurilor cibernetice (32,79 %).

Astfel, atacurile cibernetice reprezintă un risc financiar serios, astfel încât organizația trebuie să oprească programele malware și alte atacuri prin implementarea de straturi de tehnologii de securitate, cum ar fi aplicațiile antivirus / anti-spyware, firewall, detectare / prevenire a intruziunilor, VPN și criptare. Astfel de tehnologii sunt componente esențiale ale securității rețelei, însă, deși sunt eficiente în propriile domenii de scop, nici una nu îndeplinește cea mai fundamentală dintre toate măsurile de securitate: gestionarea vulnerabilității.

De menționat este și faptul că vulnerabilitățile de securitate cibernetică au și alte cauze decât cele intenționat malițioase sau deliberate. Multe dintre incidentele de securitate cibernetică au avut ca cauză de bază vulnerabilități care țin de control slab ala accesului (de exemplu unele notebookuri sau dispozitive externe de memorii USB, HDD pot fi furate sau pierdute), se pot întâmpla dezastre sau catastrofe naturale ambientale sau cauzate de efecte nocive industriale.

Astfel protecția resurselor și activelor informaționale necesită o abordare sistemică și complexă, care să ia în considerare o multitudine de aspecte care pot afecta confidențialitate, integritatea și disponibilitatea informațiilor care prezintă valoare pentru procesul de afaceri ale organizației.

BIBLIOGRAFIE:

1. SYMANTEC, *Raportul amenințărilor de securitate în Internet, sumar executiv*, [accesat 13.12.2019]. Disponibil: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-executive-summary-en.pdf

2. ISACA și RSA Conference, *Starea securității cibernetice: Implicații pentru 2015*, [accesat 11.10.2019]. Disponibil: http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf

3. SM EN ISO/IEC 27001:2017, Tehnologia informaţiei. Tehnici de securitate. Sisteme de management al securităţii informaţiei. Cerinţe – Aprobat: 29.08.2017. – Chișinău: INSM, 2017. – 33 p. – Nepubl. Localizare: INSM (Chișinău);

4. Hotărârea Guvernului Republicii Moldova cu privire la aprobarea Cerințelor minime obligatorii de securitate cibernetică: nr.201 din 28.03.2017. În *Monitorul Oficial al Republicii Moldova*. 2017, nr. 109-118, art. nr.: 277;

5. UNIVERSITATEA CARNEGIE MELLON, *Cyber Resilience Review (CRR), Volum 4 Vulnerability Management*, 2016;

6. PALMAERS Tom, *Implementing a vulnerability management process*, 2013;

7. CURTEA DE CONTURI ROMÂNIA, *Manual audit IT*, 2012 [accesat pe 15.11.2019]. Disponibil: http://www.curteadeconturi.ro/Regulamente/MANUAL_AUDIT_IT.pdf;

8. WILEY John, *Vulnerability management for dummie*s, Qualys ediție limitată, 2008;

9. MITRE, *Enterprise Matrix*, [accesat pe 15.11.2019]. Disponibil: https://attack.mitre.org/;

10. SM ISO 55000:2014, *Managementul activelor. Privire de ansamblu, principii şi terminologie*, - Aprobat 10.09.2014. - Chișinău: INSM, 2014. – 30 p. – Nepubl. Localizare: INSM (Chișinău).

11. https://www.wireshark.org/#download [accesat pe 12.11.2019];

12. https://nmap.org/[accesat pe 12.11.2019];

13. TENABLE, *Configurarea politicilor de scanare*, [accesat pe 21.11.2019] Disponibil: https://docs.tenable.com/nessus/Content/ScanAndPolicyTemplates.htm

14. HACKERTARGET.COM, *Tutorial și sfaturi pentru OpenVAS*, [accesat la 17.11.2019] Disponibil: https://hackertarget.com/openvas-tutorial-tips/

15. QUALYS, [accesat la 06.12.2019] Disponibil: https://www.qualys.com/community-edition/#/freescan

16. SOLARWINDS, [accesat la 07.12.2019] Disponibil: https://www.solarwinds.com/network-configuration-manager

17. RAPID7, *Sistemul de operare Metaspoloitable2*. [accesat la 14.11.2019]. Disponibil: https://sourceforge.net/projects/metasploitable/

18. Malik Mesellem, *Sistem de operare Bee-Box*, [accesat la 14.11.2019]. Disponibil: https://sourceforge.net/projects/bwapp/files/bee-box/

19. NIST, *Baza de date a vulnerabilităților*, [accesat la 11.11.2019]. Disponibil: https://nvd.nist.gov/