MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Electronică și Telecomunicații

Departamentul Telecomunicații și Sisteme Electronice

Admis la susţinere

Şefă departament:

Tîrșu Valentina, conf. univ., dr

_____

„____”_____ 2024

O arhitectură de referință pentru un Centru Operațional de Securitate emergent, structurat în conformitate cu cadrul de securitate cibernetică NIST

Teză de master

Student: **Malear Ion**
gr. SISRC-221M

Conducător: **Ciobanu Mihai**
conf. univ., dr.

Chișinău, 2024

Rezumatul (Adnotarea)

Scopul lucrării este de a defini o soluție integrată și de a menține mediu virtualizat emergent, cu un înalt grad de reziliență și de încredere, bazat pe cadrul de securitate cibernetică NIST cu o mare varietate de instrumente, care să constituie un important suport pentru securitatea cibernetică și buna guvernare, pentru maximizarea beneficiilor activităților organizației.

Lucrarea reflectă selecția, integrarea și orchestrarea unei varietăți de instrumente eficiente de securitate cibernetică într-o singură infrastructură hiperconvergentă. Soluția „SOC-in-a-Box" concepută pe principiul „plug-and-play" va conține o colecție integrată de instrumente eficiente de securitate pentru majorarea productivității în realizarea activităților operaționale ale echipelor de răspuns la incidente de securitate cibernetică.

În cadrul lucrării se prezintă o cercetare asupra unui model de arhitectură de referință pentru un centru operațional de securitate emergent într-un mediu virtualizat, structurat în conformitate cu cadrul de securitate cibernetică NIST în versiune revizuită și actualizată.

Cuvinte-cheie: *arhitectură, instrumente, SOC, virtualizare, NIST*

Abstract

The purpose of the work is to define an integrated solution and maintain an emerging highly resilient and trusted virtualized environment based on the NIST cybersecurity framework with a wide variety of tools, which is an important support for cybersecurity and good governance to maximize the benefits of the organization's activities.

The paper reflects the selection, integration, and orchestration of a variety of effective cybersecurity tools into a single hyperconverged infrastructure. The "SOC-in-a-Box" solution designed on a plug-and-play principle will contain an integrated collection of effective security tools for increased productivity in performing operational activities of cybersecurity incident response teams.

The paper presents research on a reference architecture model for an emerging security operations center in a virtualized environment, structured in accordance with the NIST Cybersecurity Framework as revised and updated.

Keywords: *architecture, tools, SOC, virtualization, NIST*

CUPRINS

INTRODUCERE

Dezvoltarea accelerată a tehnologiilor informației și a comunicațiilor moderne ridică la un alt nivel abordarea amenințărilor, riscurilor și vulnerabilităților într-o organizație. În prezent, la nivel mondial, atacurile cibernetice capătă o frecvență, o complexitate și o amploare din ce în ce mai mare, aducând pagube enorme în toate sectoarele de activitate, ca urmare a caracterului asimetric.

Atacurile cibernetice prezintă riscuri semnificative pentru toate organizațiile din întreaga lume, iar atunci când apar incidente de securitate cibernetică, organizațiile trebuie să răspundă rapid și eficient. Amenințările și riscurile, atacurile și incidentele cibernetice, precum și alte evenimente survenite în spațiul cibernetic constituie constrângeri la nivel global, materializându-se prin exploatarea vulnerabilităților de natură umană, tehnică și procedurală. Ca urmare a exploatării unor asemenea vulnerabilități provin prejudicii economice semnificative [1].

Deoarece organizațiile nu pot preveni complet incidentele cibernetice, este necesar să atenueze riscurile pe care le prezintă aceste atacuri și să fie pregătite să acționeze atunci când acestea se produc. Este esențial ca o organizație să răspundă rapid și eficient la atacuri prin recunoașterea, analiza și reacția la intruziuni, limitând astfel daunele și reducând costurile de recuperare în urma incidentelor.

Un element primordial pentru aceste eforturi de răspuns la incidente sunt centrele operaționale de securitate cibernetică, care sunt echipe de experți care atenuează amenințările prin identificarea, protejarea, detectarea, răspunsul și recuperarea în urma incidentelor. Aceste centre pot lua forma unor echipe de răspuns la incidente de securitate cibernetică (CSIRT), a unor centre operaționale de securitate (SOC), a unor echipe de răspuns la incidente de securitate a produselor (PSIRT), a unor agenții de tip CERT cu responsabilitate națională sau a altor echipe similare de gestionare a incidentelor. Această consolidare a capacităților internaționale, schimbul de informații și dezvoltarea forței de muncă în domeniul cibernetic la nivel mondial reprezintă eforturi esențiale în urmărirea obiectivelor apărării în spațiul cibernetic.

Dezvoltarea centrelor de securitate cibernetică are ca scop creșterea poziției generale de securitate cibernetică prin dezvoltarea, operaționalizarea și îmbunătățirea capacităților de gestionare a incidentelor ale organizațiilor din sectorul public sau privat, astfel încât acestea să se poată proteja împotriva atacurilor și să limiteze pagubele și amploarea acestora.

În ultimele două decenii, au fost dezvoltate în mod semnificativ capacitățile de răspuns la incidente în întreaga lume. Astfel au fost produse numeroase cadre și metodologii pentru crearea, implementarea și dezvoltarea echipelor de răspuns la incidente.

Specialiștii în domeniul securității cibernetice colaborează cu comunitatea internațională de răspuns la incidente, cu părțile interesate din sectorul guvernamental, cu sectorul privat, cu mediul academic și cu organizațiile regionale și internaționale relevante pentru a promova și a avansa stadiul cooperării în

domeniul securității cibernetice, pentru a dezvolta capacitatea de securitate cibernetică și pentru a promulga cele mai bune practici în aspectele operaționale de securitate și de răspuns la incidente.

Institutul de Inginerie Software (SEI) de la Universitatea Carnegie Mellon este un centru de cercetare și dezvoltare, care desfășoară activități de cercetare și dezvoltare în domeniul ingineriei software, al ingineriei sistemelor, al securității cibernetice și în multe alte domenii ale tehnologiilor informaționale, activând pentru a dezvolta și implementa inovațiile. Experții SEI pregătesc echipele de răspuns la incidente cibernetice pentru a evalua și gestiona eficient incidentele de securitate cibernetică ale organizațiilor. De asemenea oferă sprijin în planificarea și dezvoltarea capacităților și competențelor și lucrează în colaborare cu alte echipe din întreaga lume.

Pe măsură ce domeniul de răspuns la incidente continuă să se adapteze la amenințările emergente, rețeaua CSIRT și-a extins activitatea pentru a continua să sprijine domeniul în dezvoltare al securității cibernetice. Consolidarea capacităților include mentorat continuu, maturizarea serviciilor și îndrumare privind politica și guvernanța în domeniul securității cibernetice. SEI explorează noi metode și mecanisme de schimb de informații și de dezvoltare a răspunsului sectorial la incidente, inclusiv în sectoarele de infrastructură critică.

Pentru a sprijini echipele naționale de răspuns la incidente, membrii SEI au fondat Forumul echipelor de securitate și de răspuns la incidente (FIRST), organizația primară și liderul global recunoscut în domeniul răspunsului la incidente. Potrivit informației actuale cu privire la registrul membrilor înregistrați și acreditați de către FIRST sunt înființate 710 echipe de răspuns la incidente de securitate cibernetică în 106 țări, conform hărții prezentate în figura A.1. Calitatea de membru al FIRST permite organizațiilor de răspuns la incidente să dețină acces la o rețea consolidată de organizații similare și la cele mai bune practici din toate sectoarele de activitate [2].

O altă entitate, Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) desfășoară activități dedicate atingerii unui nivel comun ridicat de securitate cibernetică pe întreg continentul European. ENISA contribuie la politica cibernetică a Uniunii Europene (UE), sporește încrederea în produsele, serviciile și procesele Tehnologiei Informației și a Comunicațiilor (TIC) prin scheme de certificare a securității cibernetice, cooperează cu statele membre și organismele UE și ajuta țările din Europa să se pregătească pentru viitoarele provocările cibernetice.

Potrivit datelor curente cu privire la inventarul ENISA al echipelor de răspuns la incidente de securitate cibernetică (CSIRT-uri) și centrelor operaționale de securitate (SOC-uri) sunt înființate 712 echipe în Europa, conform hărții prezentate în figura A.2. Aceste informații sunt agregate pe baza listelor de membri înregistrați și acreditați de TI-Trusted Introducer sau fie conectate cu ENISA de către un membru relevant al rețelei CSIRT. Informațiile furnizate de ENISA sunt bazate pe materialele de evidență disponibile public, precum este definită de transpunerea Directivei NIS în statele membre ale Uniunii Europene, în beneficiul comunității de răspuns la incidente din Uniunea Europeană [3].

BIBLIOGRAFIE

1. Hotărârea Guvernului Nr. 811 din 29-11-2015 cu privire la Programul național de securitate cibernetice a Republicii Moldova pentru anii 2016-2020. Ministerul Justiției, © 2024 [citat 06.09.2023]. Disponibil: https://www.legis.md/cautare/getResults?doc_id=110324&lang=ro.
2. FIRST Members around the world. Forum of Incident Response and Security Teams, Inc., © 2015-2024 [citat 12.09.2023]. Disponibil: https://www.first.org/members/map.
3. CSIRTs by Country - Interactive Map. European Union Agency for Cybersecurity, © 2005-2024 [citat 12.09.2023]. Disponibil: https://www.enisa.europa.eu/topics/incident-response/csirt-inventory/certs-by-country-interactive-map.
4. National Institute of Standards and Technology (2023) The NIST Cybersecurity Framework 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29 ipd. [citat 18.09.2023]. Disponibil: https://doi.org/10.6028/NIST.CSWP.29.ipd.
5. Barrett, M. (2018), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework, [online], citat 19.09.2023]. Disponibil: https://doi.org/10.6028/NIST.CSWP.04162018, https://www.nist.gov/cyberframework.
6. Security Operations Center (SOC). IBM, © 2023 [citat 02.10.2023]. Disponibil: https://www.ibm.com/topics/security-operations-center.
7. What Is a Security Operations Center? Musarubra US LLC, © 2024 [citat 04.10.2023]. Disponibil: https://www.trellix.com/security-awareness/operations/what-is-soc/.
8. What is a security operations center (SOC)? Microsoft, © 2024 [citat 06.10.2023]. Disponibil: https://www.microsoft.com/en-us/security/business/security-101/what-is-a-security-operations-center-soc.
9. M. Vielberth, F. Böhm, I. Fichtinger and G. Pernul, "Security Operations Center: A Systematic Study and Open Challenges," in IEEE Access, vol. 8, pp. 227756-227779, 2020, doi: 10.1109/ACCESS.2020.3045514. [citat 18.10.2023]. Disponibil: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9296846.
10. How to setup CSIRT and SOC. European Union Agency for Cybersecurity, © 2005-2024 [citat 20.10.2023]. Disponibil: https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc/at_download/fullReport.
11. List of SOC Tools (Security Operation Center) and Technologies. Sprinto, © 2024 [citat 24.10.2023]. Disponibil: https://sprinto.com/blog/soc-tools/.

12. Mughal, A. A. (2022). Building and Securing the Modern Security Operations Center (SOC). International Journal of Business Intelligence and Big Data Analytics, 5(1), 1–15. [citat 25.10.2023]. Disponibil: https://research.tensorgate.org/index.php/IJBIBDA/article/view/21.
13. Greenbone Enterprise Appliance with Greenbone OS 22.04 – Manual. Greenbone AG., © 2015-2023 [citat 07.11.2023]. Disponibil: https://docs.greenbone.net/GSM-Manual/gos-22.04/en/GSM-Manual-GOS-22.04-en.pdf.
14. Suricata User Guide. OISF, © 2016-2024 [citat 08.11.2023]. Disponibil: https://docs.suricata.io/en/latest/index.html.
15. Wazuh – The Open Source Security Platform. Wazuh Inc., © 2024 [citat 10.11.2023]. Disponibil: https://documentation.wazuh.com/current/index.html.
16. TheHive: Installation, operation and user guides. StrangeBee, © 2024 [citat 15.11.2023]. Disponibil: https://docs.thehive-project.org/thehive/.
17. Cortex: Installation, operation and user guides. StrangeBee, © 2024 [citat 17.11.2023]. Disponibil: https://docs.strangebee.com/cortex/.
18. Wolfe, Clifton & Singh, Jai. SOC-in-a-Box [online] . University of Cincinnati, College of Education, Criminal Justice, and Human Services, 20 april 2020 [citat 06.12.2023]. Disponibil: https://scholar.uc.edu/downloads/vx021g487?locale=es.
19. Rolik, O., Telenyk, S., Zharikov, E. (2019). Management of Services of a Hyperconverged Infrastructure Using the Coordinator. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds) Advances in Computer Science for Engineering and Education. ICCSEEA 2018. Advances in Intelligent Systems and Computing, vol 754. Springer, Cham. [citat 12.12.2023]. Disponibil: https://doi.org/10.1007/978-3-319-91008-6_46.
20. Using Wazuh and TheHive for threat protection and incident response. Wazuh Inc., © 2024 [citat 22.12.2023]. Disponibil: https://wazuh.com/blog/using-wazuh-and-thehive-for-threat-protection-and-incident-response/.